“VASIL LEVSKI” NATIONAL MILITARY UNIVERSITY

“ARTILLERY, AIRCRAFT DEFENSE AND CIS” FACULTY

INTERNATIONAL SCIENTIFIC CONFERENCE 2019

C O L L E C T I O N O F P A P E R S

DEFENSE AND SECURITY

ARMS, TECHNOLOGIES, LOGISTICS

COMMUNICATION AND COMPUTING TECHNOLOGIES

CYBERSECURITY

SOCIAL SCIENCE

Shumen, Bulgaria
2019

TO THE READERS

This collection is divided in three parts and includes science papers presented on the International Scientific Conference "Defense Technology Forum 2019" 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

Col. Prof. Eng. K. KALEV Ph.D., "Vasil Levski " National Military University
Col. Assoc. Prof. A. St. ATANASOV Ph.D., "G.S. Rakovski" National Defence College
Col. Eng. Assoc. Prof. A. L. ATANASOV Ph.D, NMU
Col. Eng. Assoc. Prof. S. STANCHEV Ph.D., NMU
Colonel Eng. Assoc. Prof. V. GANEV Ph.D., NMU
LTC Eng. Assoc. Prof. M. LAMBEVA Ph.D., "Vasil Levski NMU
LTC Eng. Assoc. Prof. C. CONEV Ph.D.,"Vasil Levski" NMU
Maj. Eng. S. ANTONOV Ph.D., "Vasil Levski " NMU
Prof. PhD. Zh. SAVOVA,"Vasil Levski" NMU
Prof. PhD. V. PETROV - "Vasil Levski " NMU
Assoc. Prof. PhD. R. BOGDANOV - "Vasil Levski" NMU
Colonel Eng. Prof. T. ROTARIU Ph.D., Military Technical Academy "Ferdinand I", Bucharest, Romania
Col. Assoc.Prof. Eng. M. LUPOAE Ph.D., MTA "Ferdinand I"
Prof. PhD. L. LAZOV, D.h.c, Leading researcher Laser technology, Rezekne Academy of Technologies, Latvia
Col. Assoc.Prof. V. SANDRU, Ph.D., "Henry Coanda" AFA
Col. Assoc. Prof. L. GHERMAN Ph.D., "Henry Coanda" AFA
LTC D. STEFANESCU, Ph.D, "Henri Coanda" AFA
Assoc. Prof., Ph.D. C. CARSTEA, "Henry Coanda" AFA
Assoc.Prof., Ph.D. C. STRIMBU, "Henry Coanda" AFA
Assoc.Prof., Ph.D. G. CONSTANTINESCU, "Henry Coanda" AFA
LTC Assoc. Prof. Eng. B. BIERNACIK, Ph.D., War Studies University, Warsaw, Poland
LTC. K. FRĄCIK, PhD Eng., War Studies University
Maj. W. MATERAK, PhD, War Studies University
Col. Assoc. Prof. K. KALCHEV, Ph.D., "G.S. Rakovski" NDC
Prof. D.Sc.Tech. H. I. HRISTOV, Defence Institute, MoD
Ts. KARADZHOV, Ph.D, Technical University Gabrovo, Bulgaria
Assoc. Prof. Dr. D. DUMITRU, „Spiru Haret" University
Associate Professor Dr. R. IOAN, „Spiru Haret" University
Lt. Assoc. Prof. Marchin GORNIKIEWICZ, Ph.D,WAT, Poland
Prof. assoc. Piotr MALINOWSKI, Polish Air Force University
Ph.D. Paweł BERNAT, Polish Air Force University
Ph. D. Daniel MICHALSKI, Polish Air Force University

© "Vasil Levski" National Military University -
Artillery, Air Defense and CIS Faculty, Shumen, Bulgaria, 2019.
c/o Jusautor, Shumen
ISSN 2367-7902

СЪДЪРЖАНИЕ

Table of Contents

PLENARY SESSION **6**

Paweł Rafał Ostolski, A CULTURE OF SECURITY IN A SMALL HOMELAND 7

Benedictos Iorga, PETROVTHE IMPACT OF 5G TECHNOLOGY ON CYBERSECURITY ENVIRONMENT 15

Adam Radomyski, Paweł Bernat, ASSESSMENT OF IRAQ’S AIR DEFENSE SYSTEM IN THE IRAQI FREEDOM OPERATION 27

DEFENSE AND SECURITY **40**

Zhivko St. Yordanov, EMPIRICAL RESEARCH OF INTERACTION BETWEEN BLGARIAN ARMED FORCES AND OTHER INSTITUTIONS IN THE PROTECTION OF INTERNAL SECURITY 41

Atanas St. Atanasov, TYPES OF EFFECTS IN JOINT OPERATIONS 51

Atanas St. Atanasov, NEW ARTILLERY SYSTEMS AND CONCEPTS FOR USE OF ARTILLERY 56

Atanas St. Atanasov, Atanas Vl. Atanasov, AERIAL SURVEYLLANCE EFFICIENCY DURING ARTILLERY FIRING SERVICE 61

Kalin V. Gradev, CHALLENGES TO LAND FORCES EMERGING FROM NEW TECHNOLOGIES 69

Lyubomir K. Duchev, GOVERNANCE, COMMAND AND MANAGEMENT OF THE ARMED FORCES IN PARTICIPING IN DISASTER PROTECTION OPERATIONS IN THE COUNTRY 76

Radoslav B. Chalakov, PLANNING OF THE FIRE SUPPORT IN THE PROCESS OF PLANNING ON OPERATIONS 85

Radoslav B. Chalakov, HISTORY AND CURRENT POTENTIALS NEEDED TO IMPROVE THEM 93

Radoslav B. Chalakov, Dimitar Shomov, EFFECTIVENESS OF REACTIVE ARTILLERY IN DESTROYING DIFFERENT OBJECTIVES OF THE FIELD 98

Yordan Petkov, BASIC GUIDELINES FOR INCREASING THE SKILLS OF RECONNAISSANCE FORMATION PERSONNEL 106

Hristo A. Hristov, Veliko P. Petrov, MILITARY COUNTERINTELLIGENCE IN THE INTELLIGENCE COMMUNITY OF RUMANIA 112

Hristo Al. Georgiev, PARTICIPATION AND SPECIFIC TASKS OF THE SOF IN PEACETIME CRISIS MANAGEMENT OPERATIONS 118

Dimo V. Ginev, MISSION, FUNCTIONS, AND TASKS OF THE NON-MILITARY COMPONENT IN THE COLLECTIVE DEFENSE 125

Milen N. Kisyov, CROSS-BORDER MIGRATION AND THE RECEIVING COMMUNITY: MECHANISMS AND PRACTICES FOR MUTUAL ADAPTATION 131

Nikolay Y. Dosev, Vladislav S. Savov, CHALLENGES FOR DEFENSE POLICY IN THE NATIONAL SECURITY STRATEGY 144

Zhaneta St. Georgieva-Panayotova, SECURITY SYSTEMS IN THE COMMERCIAL BANKS 150

Svetlin E. Stefanov, JUDICIAL REVIEW OF THE SECURITY SECTOR - A GUARANTEE FOR HUMAN RIGHTS PROTECTION 153

Stoyan N. Chanev, THE ARMED FORCES COMMAND AND CONTROL SYSTEM IN HYBRID WARS 162

Atanas L. Atanasov, AEROSPACE FORCES AS A MEANS OF STRATEGIC DETERRENCE 168

Anatoly I. Andreev, ENERGY SECURITY AS AN ELEMENT OF NATIONAL SECURITY 172

Dilyan K. Markov, INFLUENCE OF THE INTERVALS BETWEEN THE ARTILLERY SYSTEMS PLACEMENT ON FIRE POSITION 177

Hristo A. Desev, ENERGY CRITICAL INFRASTRUCTURE RISK ASSESSMENT TECHNOLOGY 184

Veliko P. Petrov, Stancho G. Stanchev, HYBRID WAR, THE MOST MODERN CONCEPT OF MILITARY CONFLICTS 188

Stancho G. Stanchev, Veliko P. Petrov, FORMATION OF CREATIVE PERSONALITIES IN THE SYSTEM OF PROFESSIONAL QUALIFICATION OF ARTILLERY SPECIALISTS 195

Kaloyan A. Iliev, AUTHORITIES FOR PLANNING AND MANAGING JOINT EFFECTS IN NATIONAL JOINT FORCE OPERATIONS 201

Kaloyan A. Iliev, PROCEDURE FOR THE OPERATION OF JOINT EFFECTS PLANNING AND MANAGEMENT BODIES IN THE OPERATIONS OF NATIONAL JOINT FORCES 209

Kaloyan A. Iliev, "INFORMATION WAR" FACTOR IN MODERN MILITARY CONFLICTS 216

Ivelin G. Katsev, METHOD FOR EVALUATION OF THE ARTILLERY FIRE EFFECTIVENESS AGAISNT AREA TARGET 224

Ivelin G. Katsev, REGRESSION AND CORRELATION ANALYSIS OF FACTORS INFLUENCING ARTILLERY FIRE 230

Ivelin G. Katsev, METHOD FOR CLASSIFICATION AND PRIORITIZATION OF THE TARGETS ENGAGED BY ARTILLERY 235

ARMS, TECHNOLOGIES, LOGISTICS **242**

Florin-Marian Dîrloman, Traian Rotariu, Tudor-Viorel Ţigănescu, Mihai Ionuţ Ungureanu, ECO–FRIENDLY OXIDIZERS: MINIREVIEW 243

Cristian-Emil Moldoveanu, Alin-Constantin Sava, Pamfil Somoiag, THE INTERNATIONALIZATION PROCESS IN THE TECHNICAL MILITARY HIGHER EDUCATION INSTITUTIONS 250

Cristian Ene, Cristian-George Constantinescu, INCREASING THE AIR DEFENSE CAPACITY BASED ON THE IMPLEMENTATION OF THE MODERN AIR DEFENSE MISSILES 253
Marius Alexandru Rizescu,George Bucăţa, ORGANIZATIONAL CHANGE STRATEGIES AND METHODS OF EVALUATION .259
Svetozar B. Botev, SHAPED CHARGE WITH DIFFERENT LINER MATERIALS....267
Svetozar B. Botev, Valya M. Simeonova, DEVELOPMENT BULGARIAN ARMY FULL INTEGRATED LOGISTIC SYSTEM....271
Maxim M. Alashki, DOCUMENT REGULATING THE LIFE CYCLE MANAGEMENT OF DEFENSE PRODUCTS IN THE MINISTRY OF DEFENCE....275
Ivaylo I. Ralev, IMPROVING THE SUPPLY OF THE AIR FORCE UNITS DURING OPERATIONS 285
Miroslav St. Dimitrov, THEORETICAL ASPEcTS OF THE SUPPLY OF AMMUNITION 290
Andrey I Bogdanov, A NEW APPROACH TO STORAGE CAPACITY INCREASE....297
Conuy G. Conev, Hristo A. Hristov, EXPERIMENTAL RESEARCH ON THE VARIATIONS IN HIT DISTANCE AND DEVIATION ELLIPSE DURING THE USE OF DIFFERENT GUNPOWDER TYPES WHEN OPERATING THE 82MM MORTAR AND 82MM REUSABLE TRAINING MORTAR ROUND FOR SHORT DISTANCE ENGAGEMENT....301
Subi S. Minev, PREPARATION OF GROSS PROPERTIES AFTER LONG STORAGE THROUGH INTERNAL BALLISTICS....306

COMMUNICATION AND COMPUTING TECHNOLOGIES 315

Anastas N. Madzharov, Technical implementation of a reporting system and its workflows....316
Kolyo P. Kolev, Radoslav K.Velikov, CALCULATION OF COMBUSTION CHAMBER DINAMIC CHARACTERISTICS OF AVIATION BOMB FOR FIRE EXTINGUISHING BY COMPUTER-ASSISTED MODELING....323
Kolyo P. Kolev, Radoslav K.Velikov, CALCULATION OF DINAMIC CHARACTERISTICS OF AVIATION BOMBS FOR PENETRATION INTO MULTILAYER STRUCTURE BYCOMPUTER-ASSISTED MODELING....328
Kolyo P. Kolev, Radoslav K.Velikov, CALCULATION OF COMBUSTION CHAMBER DINAMIC CHARACTERISTICS OF ROCKET MOTOR SOLID-PROPELLANT ENGINE BY COMPUTER-ASSISTED MODELING 333
Plamen A. Ananiev, COMPARISION OF DISCRETE SINE TRANSFORM BASED OFDM WITH DFT....338
Borislav A. Minchev, IMPLEMENTATION AND CONTRASTING COMPARISION OF TRANSFORM TECHNIQUES OF OFDM344
Rosen A. Bogdanov, Nikolay Zh. Kulev, Miroslav G. Nedelchev, ESTIMATION OF DIRECTIONS OF ARRIVAL, APPLIED TO FIFTH GENERATION NETWORKS....348
Todor G. Peshev, RADAR SYSTEM WITH SYNTHESIZED ANTENNA APERTURE 354
Georgi N. Mazadzhiev, Sasho S. Evlogiev, Valentin T. Atanasov, CONCEPTUAL MODEL OF SMART HOME MOBILE TECHNOLOGICAL SYSTEM....360
Dimitar G. Chobanov, ASK DISCRETE SINE TRANSFORM BASED ORTHOGONAL FREQUENCY – DIVISION MULTIPLEXING....367
Angela R. Borisova, CONTEMPORARY LANGUAGES FOR PROGRAMMING ARTIFICAL INTELLIGENCE....372
Dimitar I. Sumulyov, FORMATION OF TARGET RADAR IMAGE, BY COMPARING OF TWO CORES FOR ANALIZE THE RADIOLOCATION INFORMATION....379
Dyanko K. Hubenov, Nikolay Zh. Kulev, Rosen A. Bogdanov, ADALM-PLUTO BUILD SDR SYSTEM PROGRAMMING 386
Dyanko K. Hubenov, Nikolay Zh. Kulev, Rosen A. Bogdanov, ADALM-PLUTO BUILD SDR SYSTEM TESTING....392
Dyanko K. Hubenov, Nikolay Zh. Kulev, Rosen A. Bogdanov, ADALM-PLUTO BUILD SDR SYSTEM FREQUENCY BAND SWITCH TESTS 396

CYBERSECURITY 403

Георги Т. Герасимов, СЪВРЕМЕННИ РЕШЕНИЯ ЗА ЗАЩИТА НА СТАЦИОНАРНИ СТРАТЕГИЧЕСКИ ОБЕКТИ 404
Павел Г. Герасимов, ХИБРИДНИ ОБЛАЧНИ ТЕХНОЛОГИИ ОТ НОВО ПОКОЛЕНИЕ....414
Yana E. Kolegova-Delcheva, CRYPTOGRAPHY - A PART OF CYBER SECURITY IN THE ARMED FORCES....422
Petar Kr. Boyanov, Zhaneta N. Savova, IMPLEMENTATION OF CREDENTIAL HARVESTER ATTACK METHOD IN THE COMPUTER NETWORK AND SYSTEMS 427

SOCIAL SCIENCE....435

Krasimir M. Markov, FOR BASIC CONCEPTS IN EXTREME PSYCHOLOGY 436
Veliko P. Petrov, Hristo A. Hristov, INTERNATIONAL ORGANIZATIONS AND INSTITUTIONS WORKING ON ENVIRONMENTAL PROBLEMS....441
Mariyana St. Todorova, ECOLOGICAL MIGRATION 452
Valya M. Simeonova, COMMUNICATION STYLES IN THE MILITARY ORGANIZATION 457

STUDENTS AND KADETS....462

Lyuboslav M. Bochev, APPLICATION OF MODERN INFORMATION TECHNOLOGIES IN THE COMMUNICATION AND INFORMATION SYSTEMS FOR DEFENSE....463
Plamena Tsv. Tsvetanova, Veselka T. Stoyanova, RESEARCH OF SYSTEMS FOR INTERACTION BETWEEN PEOPLE AND MACHINES IN THE MANAGEMENT OF PHYSICAL OBJECTS....468
Dancho D. Talev, STUDYING PRODUCTS AND SERVICES FOR HIDING DATA IN IMAGES....475

Stefani S. Georgieva, ARTIFICIAL INTELLIGENCE: IMPLICATIONS FORARMED FORCES 481
Aleksandar D. Kumanov, Gancho H. Hristev, RFID MODULE INTERFACING WITH ARDUINO UNO.....487
Gancho H. Hristev, Aleksandar D. Kumanov, CONTROLLING 12 LEDS WITH ARDUINO UNO 495
Mihaela A. Karadocheva, Ekaterina M. Konstantinova, Albena B. Aleksandrova, SOCIAL NETWORKS AND DIGITAL SECURITY 500
Nikolay A. Arhangelov, Viktor V. Lilov, ANALYSIS OF MAGNETIC PARTICLE INSPECTION AS A TYPE OF NON-DESTRUCTIVE TESTING METHOD.....505
Ekaterina M. Konstantinova, Viktor V. Lilov, INFLUENCE OF DIGITAL TECHNOLOGY ON E-LEARNING 512
Ekaterina M. Konstantinova, Mihaela A. Karadocheva, Tsvetoslav S. Tsankov, THE INVISIBLE INTERNET AND CYBER SECURITY 519
Ekaterina M. Konstantinova, Aleksandyr S. Bradvarov, POWER OF BLOCKCHAIN TECHNOLOGY: REDEFINING AND DEMOLISHING TRUST IN DIGITAL ECONOMY 525
Miroslav P. Dimitrov, Stamen I. Antonov, APPLICATION OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING IN CAD/CAM SYSTEMS.....531
Miroslav P. Dimitrov, Stamen I. Antonov, PLOTTING DHT11 SENSOR READINGS ON MATLAB 538
Miroslav S. Karov, INOVATIONS IN SMALL ARMS SYSTEMS 546
Marina R. Monova, IMPROVISED SMALL ARMS DURING CRISES OF NON-MILITARY CHARACTER 552
Rositsa K. Pencheva, ELECTROMAGNETIC BOMBS.....559
Petya R. Petkova, LASER WEAPON 563
Ivan S. Savov, APPLICATION OF FIELD-PROGRAMMABLE GATE ARRAYS IN DEFENSE.....572
Miroslav E. Stoimenov, CAPABILITIES AND NEW APPLICATIONS FOR NON-LETHAL WEAPON SYSTEMS IN THE FIELD OF SECURITY ANDDEFENCE 577
Aleks R. Aleksiev, PENETRATION OF ELECTRONICS INTO FIRE SYSTEM AND GUNS 584

PLENARY SESSION

Paweł Rafał Ostolski,

A CULTURE OF SECURITY IN A SMALL HOMELAND

Paweł Rafał Ostolski

War Studies University, Warsaw, Poland

Summary: *The developed article is an attempt to define a small homeland and security culture as an important factor influencing the construction of any security system. Values have been indicated as generators of national needs, goals and interests, as well as components of emotional intelligence, which is one of the components of the culture of security.*

The bibliography used and internet sources related to solved research problems may form the basis for further research.

Keywords: *Culture, security culture, homeland, small homeland, security, intellectual culture, emotional intelligence, security system*

Admission

The article Culture of security in a Small Homeland is the author's individual interpretation of selected theoretical issues of broadly understood security in micro-social conditions perceived as small homelands, but not only. Therefore, theoretical considerations seem to start with the solution to the first research problem, which is an attempt to define a small homeland and the transition to the second research problem, which is a general understanding of the culture category regarding the safety culture. This approach will give you a new perspective on individual components of broadly understood security, which is the main subject of knowledge and the most general category in security science, as one from eleven scientific disciplines in the field of social sciences in Poland since 2018[1].

Constructive interdisciplinary theoretical research and its results can be used as a methodological basis for the next stages of empirical research. They could be focused on assessing the level of security culture in relation to each individual, as a component of small groups and local communities, functioning in small homelands, and maybe even considered in the national and international context, as security systems with their components, called subsystems[2].

[1] See. Regulation of the Minister of Science and Higher Education of September 20, 2018 regarding fields of science and scientific disciplines, as well as artistic disciplines, Journal of Laws, item 1818. Eleven scientific disciplines in the field of social sciences have been identified, which include: 1) economics and finance, 2) socio-economic geography and spatial management, 3) security sciences, 4) social communication and media sciences, 5) science on politics and administration, 6) management and quality sciences, 7) legal sciences, 8) sociological sciences, 9) pedagogy, 10) canon law, 11) psychology.

[2] The Polish national security system consists of management subsystem and executive subsystems. The executive subsystems are divided into operational subsystems (defense subsystem and protective subsystems) and support subsystems (social subsystems and economic subsystems).

Small Homeland

Defining the category "Small Homeland" can begin with a reflection on the scope of understanding this concept. One can apply for an individual image of the territorial scope, however, this may constitute a significant limitation of considerations in relation to the research area, but on the other hand, in a sense, such range boundaries seem to be a necessary assumption in the research process, at least due to the population and the determination of the minimum number of the research sample, so that the results of the study estimate the entire population. Motives about a small homeland can be found in literature, where most poets identified her with the idyllic image of a small child, as a place (family village or city) filled with carefree, harmony, peace and family warmth, giving a sense of security. *"Small Homeland" can be called a kind of geographical, social and cultural space in which the individual lives and with which he is emotionally connected. Otherwise it is a space that is the closest surrounding, well known, safe and "tamed"*[3]**.**

A similar definition characterized by a significant degree of generality, but at the same time precisely defining the territorial scope is identified by opening the Great Polish Dictionary in which*"Small Homeland" is a place with which someone is emotionally connected because they were born, raised or lives in it*[4]**.** L. Kołakowski described it in the same way in 1993 during the ceremony of granting him the title of honorary citizen of Radom, saying**:** *The small homeland is the city or village in which we were born, is the center of the world. This is a small space in which we revolve - our houses, streets, cemeteries, churches, a small space built up with great human effort, destroyed and reconstructed by wars, it is the center of the world*[5]. The terms center of the world and center of the world used indicate that this is the most important place for the author of these words, due to the enormous effort of generations that shaped it in a variety of conditions, related to the constantly rolling circle of the history of the Polish nation and its local communities.

For many literature authors, their small homelands play an inspirational and myth-creating role, especially when they are remembered from a distance, nostalgically - after loss. Such a role is played by Lithuania in "Pan Tadeusz", Adam Mickiewicz, "Żmudź" in the works of Czesław Miłosz, Huculszczyzna in the prose of Stanisław Vincenz, or Wielopole in the work of Tadeusz Kantor[6]. Thinking about a small homeland always intensified after its loss, but not only. Childhood memories have always been a source of inspiration for poets, who in their works willingly return to images remembered for life. This is testified by a poem by Joanna Białobrzeska: "My little homeland":

There is a small dot on the map
I live here, you'll meet me here.
How interesting and cheerful
in my world around.

Three puddles in the yard,
lay down by the wall,
beater today whimsical -
a large carpet hangs on it.

The sun with shadow plays tag here,
the chimney sweep from the roof looks,
now probably everyone will admit
that she is beautiful has a homeland![7]

[3] http://eszkola.pl/wos/mala-ojczyzna-4481.html [access: 21.09.2019].
[4] http://wsjp.pl/index.php?id_hasla=40308 [access: 21.09.2019].
[5] http://teatrnn.pl/leksykon/artykuly/mala-ojczyzna/ [access: 21.09.2019].
[6] Ibidem.
[7] http://www.pogotowieflagowe.pl/wiersze_patriotyczne.html [access: 22.09.2019].

Summing up the brief considerations related to the attempt to define the category of a small homeland, it can be said with certainty that for every human being it is the place where he was born, raised and lives. Thus, the definition from the Great Polish Dictionary seems to be the most accurate. However, after a deeper reflection on the nature of a small homeland, images of other places appear in the mind that are associated with the daily functioning of each subject of the small homeland. These are places of study and work, cinemas and theaters, churches and museums, medical clinics and hospitals, small neighborhood stores and large shopping centers or supermarkets, stations and means of communication, which can be at least a few, several or several dozen in the local environment of each person in which verbal and non-verbal interpersonal contacts occur every day, where the soul and personality are shaped, where everyone leaves a part of themselves through attitudes, behaviors, actions and cooperation.

Culture and security culture

Explaining the importance of the general category of culture can be helpful to analyze and assess the level of security culture in a small homeland.

The sources of the term culture come from Latin - *the term is ambiguous, it comes from Latin. cultus agri ("soil cultivation"), it is interpreted in many ways by representatives of various sciences. Culture can be defined as the totality of people's products, both tangible and intangible: spiritual, symbolic (such as patterns of thinking and behavior)* [8].

Consequently, the term is developed and interpreted as follows: *Most often it is understood as the whole of the spiritual and material achievements of society. Sometimes identified with civilization. Also patterns of behavior specific to a given society, including what is learned in human behavior, as opposed to what is biologically inherited*[9].

This understanding of culture is usually dependent from the degree of civilization development, as a result of spiritual and material achievements, as independent variables of this development. Whereas civilization development itself is an independent variable of culture. In addition, independent culture variables can be identified, which are behavioral patterns and learned behaviors.

An extended definition of culture can be found in the "Polish Dictionary", in which ten points describe culture as:

1. *ability to interact with people, behave appropriately to the situation; culture, refinement, tact, familiarity;*
2. *material and mental activity of societies and its products;*
3. *society considered because of its material and mental achievements;*
4. *sufficiently high level of society development to some extent;*[10] (…)

The four point limitation is due to the fact that the remaining 6 refer to agriculture and biology. The above-mentioned records identifying culture have common parts in the field of mental (spiritual) and material output, as well as civilization (social) development and patterns of behavior (behavior in specific situations).

W. Okoń presents a similar proposal, who understands culture as: *all scientific, social, artistic and technical values created by people and processes of creating these values. (...) Nowadays, culture begins to be perceived broadly, i.e. as both effects and processes of creating goods, both as norms, values and patterns of behavior, as human-made works of art, as well as scientific and artistic values, as social and technical-civilization. The subject of specific controversy is the issue of elite culture and mass culture. According to some philosophical concepts, culture was treated as a product of exceptional groups or individuals with special predispositions, and they were only assigned the ability to experience the most*

[8] https://pl.wikipedia.org/wiki/Kultura [access: 22.09.2019].
[9] Ibidem.
[10] https://sjp.pl/kultura [access: 22.09.2019].

valuable cultural goods produced by humanity. The contemporary development of mass communication promotes the democratization of culture, gradually blurring the border between elite and mass culture[11].

The cited definition is the basis for thinking about security culture in subjective categories. In addition, it creates conditions for a dualistic perception of security culture as an elite security culture and mass security culture.

The perception of security culture depends on the culture level of the subject. This problem is anchored in the essence of a culture that, when developing properly, will always be the result of the cumulative efforts of a nation or community or group in intellectual, emotional and aesthetic terms. These variables, independent cultures, affecting intellectual, emotional and aesthetic potential to varying degrees, require a broader explanation to increase awareness of this impact not only on culture itself, but also on a broad understanding of security culture.

Intellectual potential can be seen, like A. Pieczywok as *an intellectual culture. Intellectual culture is the result of combining university and humanistic knowledge, acquired thanks to one's own interests (literary, music, theater, etc.) and one's own life experiences (life knowledge). Emotional culture includes the following:*

- *knowledge about society, culture and education;*
- *ability to logically and concisely formulate thoughts, inference, argue, critically evaluate facts and phenomena;*
- *ability to listen to and use the arguments of the other party (ability to discuss*
- *order of thinking and actions, clarity in the formulation of thoughts*[12].

The second independent cultural variable is emotional potential, which is suggested to be interpreted as *emotional intelligence*. This term was used for the first time by D. Goleman by isolating its components, which are emotional needs and drives, as well as the individual's value system. They direct the external behavior of each entity. An attempt to define emotional intelligence is also made by J. Wieczorek, who identifies it with consciousness in controlling his emotions, enthusiasm and perseverance in pursuit of the goal[13]. *Emotional intelligence (EQ) decides about the ability to adapt to the environment, successful interpersonal relationships and professional successes. Recent scientific research confirms that both intellect and emotional* intelligence *play an important role in achieving success in life*[14].

The level of emotional potential, and thus emotional intelligence depends on the subject's scope of possession of the features that it manifests and are at the same time indicators of this independent variable in the context of security culture. Using J. Wieczorek's proposal, we can state that emotional intelligence consists of a set of thirteen features, which are:

- *emotional energy;*
- *stress resistance;*
- *optimis;*
- *self-esteem;*
- *getting involved in work;*
- *care;*
- *change orientation;*
- *courage;*
- *self-reliance;*
- *assertiveness;*
- *tolerance;*

[11] W. Okoń, *New pedagogical dictionary*, Academic Publishing House "Żak", Warsaw 2007, p. 209.
[12] A. Pieczywok, *Professionalism of the academic teacher of education for security*, National Defense University, Warsaw 2016, p. 76.
[13] See. J. Wieczorek, *Employment and development of employees using the Assessment Center/Development Center*, Consultancy and Improvement Center for Personnel Sp. z o.o., Gdańsk 2010, p. 19.
[14] Ibidem.

- *caring for others;*
- *sociability*[15].

The third pillar of culture is *aesthetic potential*, which can also be interpreted as aesthetic effort or aesthetic culture. Taking into account its use for assessing the level of safety culture, it is suggested, however, to perceive it in the category of potential.

Explaining the concept of aesthetics can help you understand the aesthetic potential as a pillar of culture that has a significant impact on shaping the level of safety culture. Aesthetics - *from Greek – αί σθητική (aisthetikê), < sensual impression, perception > – the term aesthetics has several basic meanings. In colloquial language, it refers to everything that is beautiful. In philosophy, it is defined in three ways:*

- as a branch of science whose purpose is to consider the essence of beauty perception, it concerns the problems of fine arts (the most important);

- as relating to the theory of art;

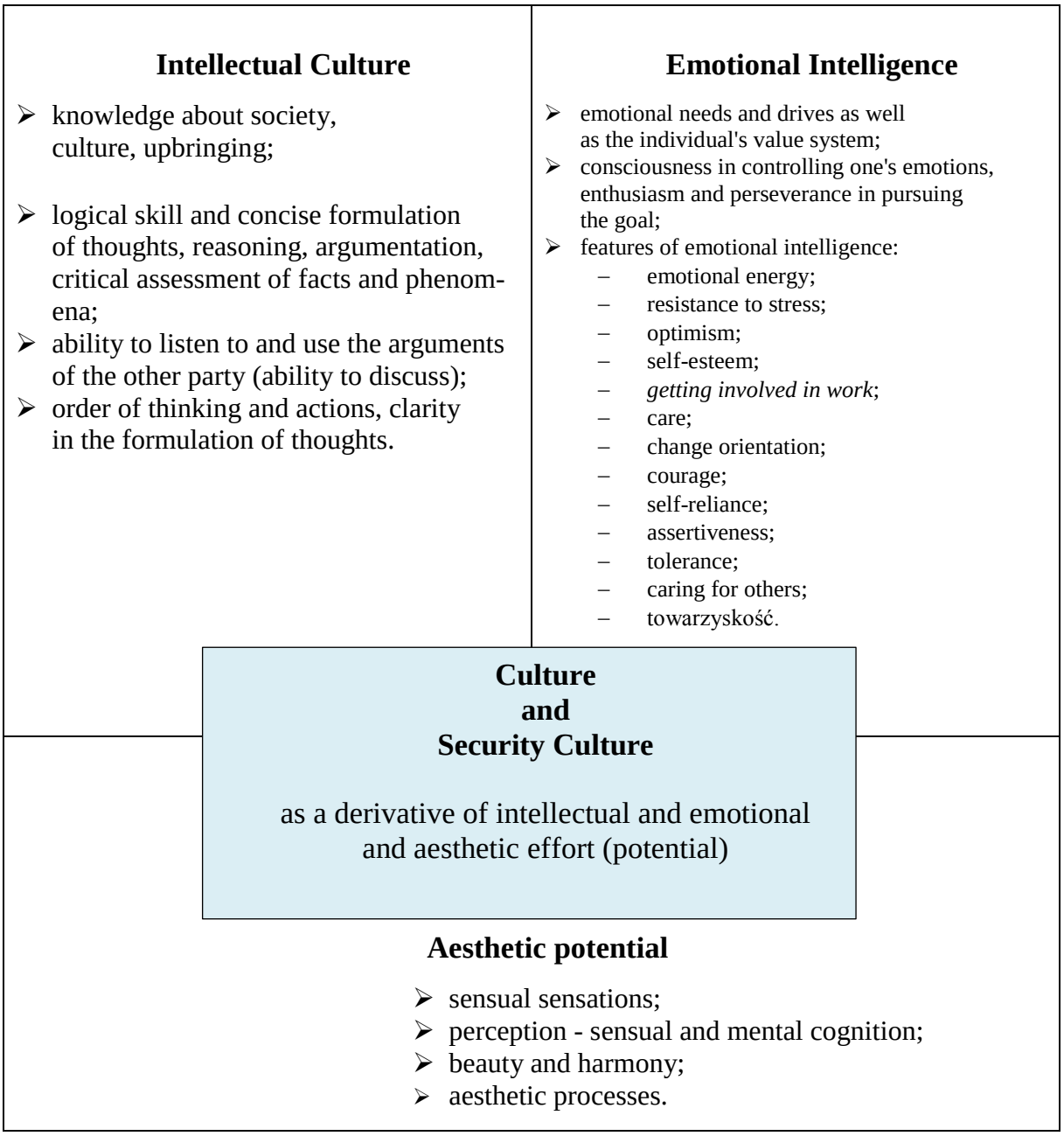
- as dealing with perception in a general way - both sensual and all other ways of perceiving reality[16].

In addition, selected problems arising from the evolution of civilization are important when considering aesthetics. *Throughout the 20th century, pragmatic (John Dewey), Marxist (György Lukács), phenomenological (Roman Ingarden), feminist (Carolyn Korsmeyer), ecological (Gernot Boehme) and neuroesthetics (Semir Zeki) aesthetics have appeared. The aesthetics of recent years is an area of interdisciplinary research. Particularly noteworthy are the concepts of Richard Shusterman's neopragmatic aesthetics and Wolfgang Welsch's anesthetics. The latter announced aesthetics as "modern first philosophy" - according to Welsch, the West is subject to the process of aestheticization of culture to an extent that raises fear, the reaction to aesthetization is anesthetization (blunting of the senses), the task of aesthetics is to study the processes of aesthetization and anesthetization*[17]. Complementing aesthetics is its philosophical interpretation, which treats it as a field dealing with issues of beauty and harmony[18].

A *summary* of considerations on the essence of culture, focused on the proper understanding of interaction with the level of security culture, is illustrated in Drawing1.

Aesthetic potential is the basis in shaping the level of safety culture regardless of the scale it will affect (small homeland in a narrow sense or wider, and even international). Sensory impressions and the ability to perceive in sensual and mental cognition is the starting point of all processes directed according to philosophical thought to achieve beauty and harmony. All activities in the field of building aesthetic potential are the subject of research into the complex aesthetic process. The threat is the phenomenon of dulling the senses, perceived by researchers, which results in the wrong and imaginary perception of reality. Erroneous sensual cognition results in providing unrealistic data to implement the process of mental cognition. The result of such action may be an individual and autonomous way of thinking about the subject of scientific cognition, which is security science, characteristic of each entity, and above all the way of feeling this security and the development of effective methods of action ensuring achieving and maintaining safety at the expected level.

[15] Ibidem, p. 19-20.
[16] http://ozkultura.pl/node/2429 [access: 23.09.2019].
[17] Ibidem.
[18] See. https://sjp.pl/estetyka [access: 23.09.2019].



Source: Own study.

Drawing 1. The essence of culture and security culture

Psychological literature does not facilitate the task of objectively assessing the level of safety culture. *It turns out that the same situation is perceived by two people completely differently. Each unit observing a given situation interprets, describes and remembers it differently, as well as differently evaluates the behavior of the participants in this situation*[19].

The result must be variously created images and images with a certain degree of divergence from reality that characterizes them. They form the basis for building knowledge, which, depending on the level of intellectual culture, is subject to a varying degree of critical assessment of facts, phenomena and processes. Additional determinants of such activities are the individual characteristics of each entity,

[19] https://www.edukuj.pl/percepcja-terminologia-psychologiczna.html [access: 23.09.2019].

which are perceived as indicators determining the variable, which is the level of emotional intelligence, but it should be noted here that they also directly affect the formation of values.

Theoretical studies and research indicate the basic elements on which any structure of the security system should be based. These are values previously recognized, as well as *the needs and goals of national security, in particular national interests*[20].

It is worth emphasizing the fact that values play a leading role in constructing the security system, because on their basis will be generated needs and set goals as well as determined national interests as determinants of each security system.

The final conclusions evoke reflection on the culture of security in small homelands, but also in a much broader respect. Since values as an independent variable affect emotional intelligence, which in turn is an independent variable of a safety culture, then the level of this culture will be a key determinant in the formation of any security system. The other factors will therefore be their derivatives, which should also be included in research focused on safety culture and security systems.

The consequence of the impact of many variables on the level of safety culture in a small homeland is the difficulty to make a reliable and objective assessment of this level. In addition, there is a reflection that such assessment should be the result of scientific research of an expert team. Members of this team should rather have high aesthetic potential, high intellectual culture and emotional intelligence (features and values). This conditions the selection of appropriate research methods, techniques and tools, and also allows for proper analysis and interpretation of the results of the research.

Recommendations and suggestions

This article is the result of theoretical reflection on problems related to security culture. It can be considered in individual, local, regional, national, international and global dimensions. I am completely convinced of the need to continue empirical and theoretical research, which may be based on the conclusions resulting from the presented content in the field of culture of security of small homelands. The research results contained in the article can be used to design subsequent and more complex processes with more variables.

In conclusion, I would like to inspire a whole group of scientists who are eager to take up challenges and see other security culture issues than those presented above, to cooperate in international research covering the Bucharest Nine (B9). I am thinking of people of science from all member countries of Bulgaria, the Czech Republic, Estonia, Lithuania, Latvia, Poland, Romania, Slovakia and Hungary, but not only because the high level of security of the small homeland and the B9 group is undoubtedly one of many measures of national, international and European security and global.

Bibliography

Gryz J., *Zarys teorii bezpieczeństwa państwa*, Akademia Obrony Narodowej, Warszawa 2015.

Krakowski K., *Współczesna dydaktyka wojskowa*, AON, Warszawa 2014.

Okoń W., *Nowy słownik pedagogiczny*, Wydawnictwo Akademickie „Żak", Warszawa 2007.

Pieczywok A., *Profesjonalizm zawodowy nauczyciela akademickiego edukacji dla bezpieczeństwa*, Akademia Obrony Narodowej, Warszawa 2016.

Szulc B. M., *Kształcenie, Nauka, Wartości,* Wydawnictwo Adam Marszałek, Toruń 2015.

Wieczorek J., *Zatrudnianie i rozwój pracowników z zastosowaniem metody Assessment Center/Development Center*, Ośrodek Doradztwa i Doskonalenia Kadr Sp. z o.o., Gdańsk 2010.

Rozporządzenie Ministra Nauki i Szkolnictwa Wyższego z dnia 20 września 2018 r. w sprawie dziedzin nauki i dyscyplin naukowych oraz dyscyplin artystycznych, Dziennik Ustaw, poz. 1818.

[20] J. Gryz, *Outline of the theory of state security*, National Defense University, Warsaw 2015, p. 48.

Internet sources

https://www.edukuj.pl/percepcja-terminologia-psychologiczna.html
https://sjp.pl/estetyka
http://ozkultura.pl/node/2429
https://sjp.pl/kultura
http://www.pogotowieflagowe.pl/wiersze_patriotyczne.html
https://pl.wikipedia.org/wiki/Kultura
http://wsjp.pl/index.php?id_hasla=40308
http://teatrnn.pl/leksykon/artykuly/mala-ojczyzna/
http://eszkola.pl/wos/mala-ojczyzna-4481.html

Benedictos Iorga,

PETROVTHE IMPACT OF 5G TECHNOLOGY ON CYBERSECURITY ENVIRONMENT

Benedictos Iorga

Spiru Haret University, Faculty of Engineering and Computer Science,
Bucharest, Romania
E-mail: *iorga.ben.mi@spiruharet.ro; iorgaben@yahoo.com*

Abstract:

The sustained evolution in the field of information technology, the ascending social necessity for permanent digital connection and worldwide accelerated information consumption determined the rapid development and operationalization need of a 5th generation digital communication technology, generically named 5G. The new technology which promises to revolutionize all digital technology, communications, data transmission and Internet access signify, will generate, in addition to immeasurable benefits and advantages (economic, industrial, technical, social, cultural), a profound impact on global cybersecurity.

I hereby set out to briefly determine and analyze the impact of the 5G communication technology implementation on current cyber environment, starting from the technical transformations induced by the new technology and using the current patterns of known, tested and documented cyber threats in the global network environment.

While apparently 5G technology promises to ensure a high level of security within the cellular communication environment by implementing the logical network segmentation (Network Slicing), adopting new dynamic end-to-end encryption tools (IMISI encryption) and operationalizing software-defined networks (SDN), I consider there is a high probability that the current cyber threats will benefit from a new developing environment and expansion at a global, insufficiently anticipated and known level.

Keywords: technology, 5G, cyber risk, internet, security threat, cyber vulnerability.

Introduction

It is for the first time in the modern history of the states when a mobile communications technology has determined the rethinking of strategic relations between the greatest technological powers, respectively the USA and CHINA, with chain effects on global security. In such a context, the question naturally arises: *What are the fundamentals of the dispute?* Certainly one of the main divergent elements is the subsequent economic and financial effect of the development and implementation of a new cutting-edge digital technology which promises a significant impact on the society transformation over the next 30 years.

Apparently, we deal with an economic conflict in order to take over the global communications market of the 5th generation with long term effects on the multi-spectrum evolution of society, on a global level. Although the economic element of the divergences cannot be neglected, any strategic dispute caused by the emergence of disruptive technology also has the security component, especially in the cybersecurity field and associated emerging risks.

Therefore, we witness the emergence of a new revolutionary technology whose initial development is apparently gained by the Asian profile industry (China) with two emerging effects represented by the economical impact (which imposes the standard, develops the systems and monopolizes the market of profile and subsequently creates technical dependency) and which controls the large volumes of data (global access to broadband communications systems, operational dependency, indirect control of critical communications infrastructure security of technology consuming states).

The 5th or 5G mobile communication technology theoretically represents a stage of the digital natural development by moving to the next level in mobile communications after the successful operation of 3G (2000-2010) and 4G (2010-present) technologies. Practically, however, from a technical point of view, there is a fundamental change in the philosophy, architecture and communication capabilities in mobile networks, compared to previous 3G/4G technologies (figure no. 1), as follows:

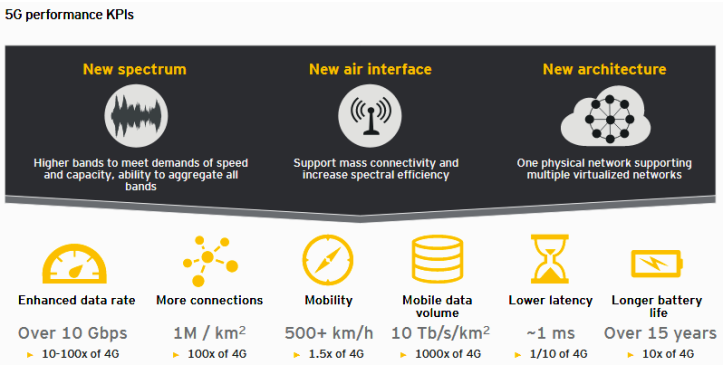


Figure no. 1 - *5G performance*
Source: **[1]** *https://www.ey.com/Publication/vwLUAssets/ey-china-is-poised-to-win-the-5g-race-en/$FILE/ey-china-is-poised-to-win-the-5g-race-en.pdf, pp.16*

a. Users' traffic speed. It is the main technical gain generated by 5G technology, along with bandwidth capacity. 5G will allow 10-20 Gbps traffic speed, with a real user experience of 100 Mbps (wide area, outdoor) and 1 Gbps (indoor) respectively, about 100 times higher than 4G technology. This feature will facilitate the Internet of Things, Machine to Machine Communication and Connection everywhere concept development.

b. Bandwidth. A 5G communications network will ensure a minimum bandwidth of 10 times greater than 4G, and the traffic capacity for a given geographical area is estimated to be at least 10Mb/s/m^2;

c. Communication latency. 5G networks promise to ensure communications between devices, with an optimal latency of 1 millisecond, compared to 4G networks that provide latencies of approximately 50 milliseconds**;**

d. Coverage level. 5G architecture aims at total urban coverage with an estimated connection density of 10^6 devices/km^2 by the use of „Massive MIMO" micro antennas, which utilize millimetric (very short) waves with low energy consumption and the use of a very high frequency spectrum (Ghz), which allows reducing radio interference.

e. Used frequencies. The used frequency bands will migrate to the higher spectrum (Ghz) being used depending on the operational scenario, as follows: 700 MHz band (690-790 MHz) for long distance coverage in rural/urban areas, 3400-3800 MHz band for urban clusters area coverage and the 26 GHz band (24.25-28 GHz) for densely crowded urban areas coverage in order to meet the broadband needs.

f. Security. 5G technology will implement 5 new concepts, theoretically aiming at developing the current security level, as follows: implementing a new network authentication system [16, 5G-AKA, EAP-AKA, EAP-TLS, pp.5-9], operationalization of „*software defined networks*" concept, implementation of network segmentation systems into dedicated sub-networks (*Network Slicing*), migration to network virtualization (NVF) and native cloud systems.

The above-mentioned capabilities generate a broad spectrum of applicability in the industrial, economic, technological and security environment, both in the area of technology producing and service consuming states. In this study, we start from the hypothesis that 5G technology, though it generates a new paradigm of the digital society equivalent to the period of Internet emergence, will most likely not cause an „apocalypse" in the cybersecurity field.

I consider that 5G networks transformations, induce in the network environment (figure no. 2) will require a new model of cybersecurity „business" and, at the same time, a rethinking of security strategies and policies in the online environment, especially at the level of critical communication infrastructures in each state. The size of security policies and technical measures adaptation and 5G implementation impact on the cyber environment will be determined primarily by the correct identification and extended analysis of security risks induced in the network environment and broadband communications infrastructures of the states on the way to the new era of global connection and artificial intelligence.

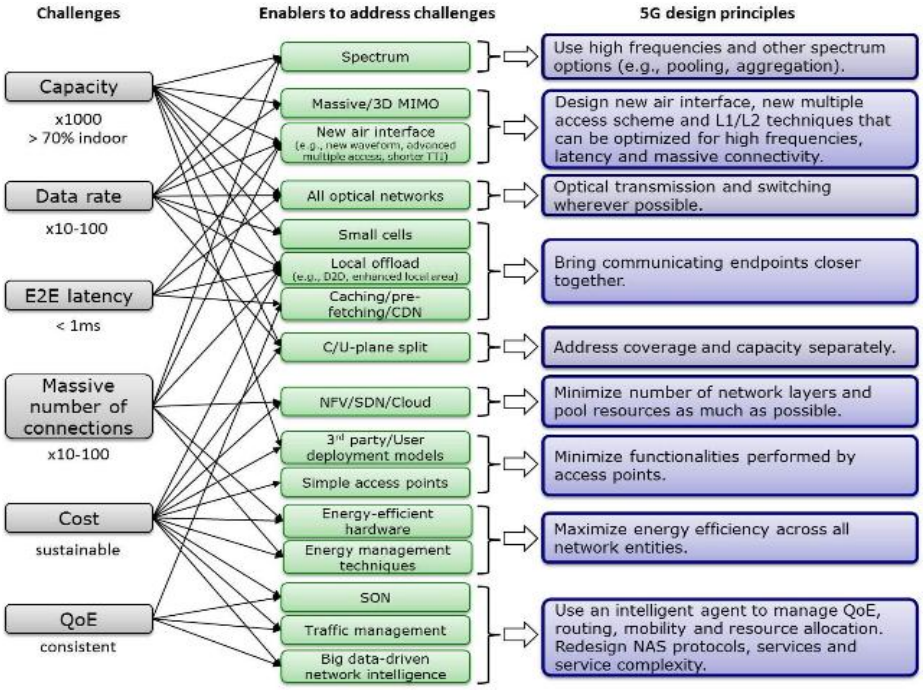


Figure no. 2 - 5G challenges

Source: **[2]** P. Agyapong, M. Iwamura, D. Staehle, W. Kiess, A. Benjebbour, *"Design considerations for a 5G network architecture"*, IEEE Commun. Mag., vol. 52, no. 11, pp. 65-75, 2014.

The cybersecurity environment in 5G technology.

Although the standard specific to 5G communication systems has not been completed yet (*IMT-2020, the name used in ITU for the standards of 5G, is expected to continue to be developed from 2020, according to ITU press release*), under the report on cybersecurity impact, numerous experts in the field of information technology have founded two divergent evaluations **[3].**

The first, mainly supported by the promoters of technological developments in the Asian space but also by a part of the European research area, stipulates that 5G technology is the safest communication technology ever developed and will not have a significant impact on the global cybersecurity environment. The induced insecurity risks are evaluated as being strict of technical nature and will be managed through "security by design" approaches and security policies adapted to each environment/network segment. Thus, they evaluate that the new emerging risks or the level of cyber insecurity risk induced by the operation of 5G mobile networks will be absorbed and limited by the innovative technical protection measures such as implementation of „Software Define Networks" systems, „end2end encryption solutions", securing the authentication process at the infrastructure level and implementing the virtualization tools and subnets logical segmentation - networks slicing. For example, the leader of Silverfort cybersecurity company, Hed Kovetz, declares that "*The 5G system incorporates secure identity management for identifying and authenticating users to ensure that only the genuine user can access services. Its new authentication framework enables mobile operators to choose authentication credentials, identifier formats and authentication methods for users and IoT devices*."

The second category of experts, especially from the US area but also from certain European states, estimates that 5G technology will generate a series of new technological threats **[4, William Chalk, CSO]** and will alter the actual level of cybersecurity within the network environment, mainly due to the domination and technological monopoly of Chinese companies (Huawei and ZTE) serving the strategic interests of Beijing authorities.

As an example, the American artificial intelligence and security expert at Brookings Institution, Chris Meserole, states that *"The fear ultimately is that China monitors the traffic that's passing through American networks, Western networks, and it's recording it and sending it back to China, and China has this gold mine of data. The bigger fear from a military perspective is that China builds in a back door and they selectively use it. The scale and scope of 5G technology make the threat exponentially greater. Just as 3G networks ushered in the smartphone and 4G revolutionized society by facilitating apps such as Uber, 5G will connect users like never before and bring about the fastest, most reliable wireless services in history*".

However, the two divergent positions are not transparently supported by scientifically based technical risk analyses or by concrete evidence available to the general public and academic environment.

Nevertheless, based on the historical experience generated by the implementation of 4G/4G LTE technology, together with the evolution of the society access to the Internet, we can recognize that there has been a significant global expansion of cyber risks and a transformation of the digital security environment. In this context, if we comparatively analyze the results of Deloitte's research **[5]** with regard to the evolution of cyber threats since 1990 *(figure no. 3)* and the result of 3GPP standardization organization study **[6** - 3rd Generation Partnership Project], as regards the evolution of mobile communication systems standards *(figure no. 4)* we can conclude that:

✓ Cybersecurity risks have evolved, along with the development of mobile communications systems;

✓ Risk explosion on cybersecurity and diversification of threats spectrum have been determined by the emergence and facilitation of the almost global access to the Internet network, using mobile data communication infrastructures (3G, 4G, 4G LTE networks, since 2010);

✓ The increase in the speed of access and capacity of data traffic in the mobile network environment has led to an increase of the users' interconnection level within the online environment and in the same time, to an increase of the cyber attack surface area within the digital society.

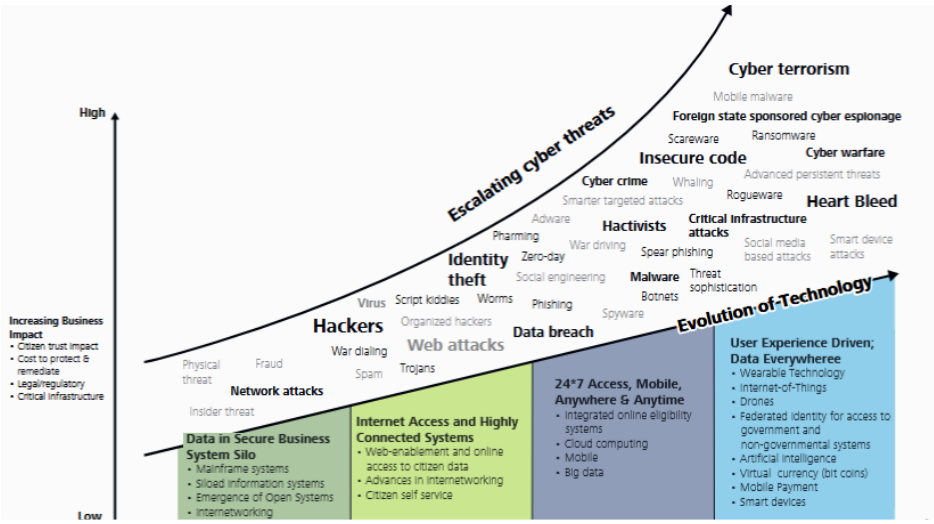


Figure no. 3 - *Evolving technology and cyber threats escalating*
Source:**[5]**
https://www.nascio.org/dnn/portals/17/2014Presentations/2014_Deloitte-NASCIO_Cybersecurity_Study_Overview _10_1.pdf

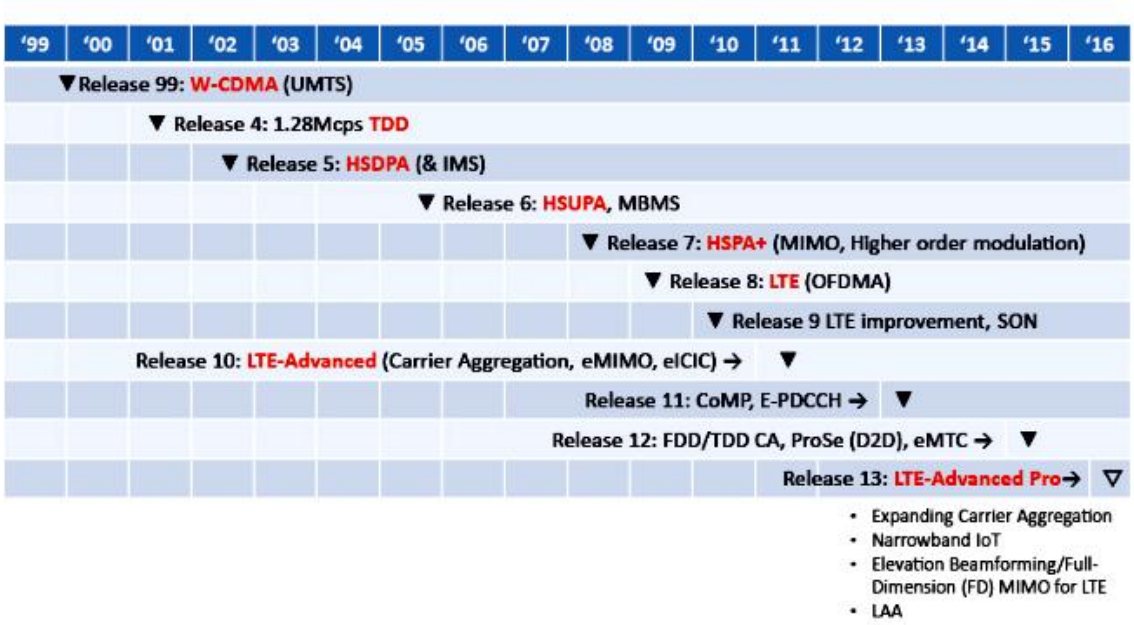


Figure no. 4 – *Networks Communication Standards evolution,*
Source: **[6]** 3GPP, *http://www.aec.mk/irc2018/irc2018_s3_02_1.pdf,* p.13

Thus, the diversification of cyber-attack tools and the attacks complexity are directly proportional with the users' capacity of access to the network environment and with the number of interconnected equipment. In the same time, the equation of threats in the digital environment depends on the capabilities offered by the communication channels. Therefore, the impact of 5G technology on the digital security environment will be a significant one, similar to a paradigm shift in the way of securing the network environment, argued by the persistence and enhancement of the vulnerabilities specific to the current 3G, 4G, 4G LTE networks that will continue to function, as well as by the emergence of new vectors threatening the global digital society.

In the new technological context, defined by a massive agglomeration of users, the lack of the systems interconnection boundaries, the critical infrastructures dependence of the mobile data, society dependence to the critical infrastructure networks and by the „Internet of Things" concept materialization, not only does the cyber threats taxonomy, but also the area they are generated from (Asia, USA, Europe, etc) gains significance. The importance of cybersecurity in the context of 5G networks operationalization derives mainly from the increased possibility of discharging relatively easy the critical communication services and infrastructures, using precisely the advantages of technological evolution, such as the possession of equipment production patent (firmware, zero-days errors, backdoors), the traffic speed, broadband transport capacity, mobility of network access, as well as the lack of centralized control and visibility of network environment.

Also, in the expected context of the increased number of connections to the Internet network from 7 billion hardware in 2019 to 21.5 billion in 2025, according to the analyses conducted by IoT Analytics **[7],** along with the „smart objects" and „IoT" technology implementation, the effects of the destructive actions to disrupt critical communications services will be rapidly visible and exponentially amplified.

5G technology implementation in the actual context of accelerated social and industrial processes digitization together with the emergence of a real technological cold war between mainly USA and CHINA but also Europe ((buffer zone or test area) will determine 6 (six) categories of effects on the digital security environment, with an impact on social security, as follows:

1. Increasing the dependence of states critical infrastructures on the major global technology producers:

From the beginning, 5G technology has been supported and promoted by Chinese multinational companies, such as ZTE and Huawei, that have strategically surprised the technology field by successfully developing and testing the 5G equipment since 2017, exceeding the efforts of the American profile industry. If in the situation of 3G and 4G networks there were about 10 major global manufacturers of technology (equipment, infrastructure, software) among which Siemens, Lucent, Ericsson, Alcatel, NEC, Nokia, Panasonic Marconi and Huawei, currently the development of 5G systems (complete cycle of operationalization and production) is mainly carried out by 4 major manufacturers, namely Nokia, Ericsson, Huawei and ZTE.

In terms of the primary components, chipsets and controllers required in 5G equipment (mobile terminals, smart equipment, servers), the technology is dominated by 4 global manufacturers, namely Qualcomm (USA), MediaTek (Taiwan), Samsung Electronics (South Korea) and HiSilicon (China, a subsidiary of Huawei).

Therefore, the next 5G infrastructure will depend on one of these equipment and technology providers. Thus, there is a reduction in the number of companies in the field of advanced technology capable of producing 5G communications systems and equipment, practically, the market is currently divided between the US, China and partly Europe (on certain network segments).

In the future context, „after 5G implementation", the critical communication infrastructures in each state will be significantly dependent on one of the 4 manufacturers of 5G systems as well as one of the chipset manufacturers, given the advanced level of technology and the existing discrepancy between them and the other communications companies in the profile industry.

Technically, the 5 facilities offered by 5G networks (traffic speeds between 1 - 10Gbps with 1 millisecond latency, minimum download speeds of 50 Mbps, the urban coverage level through MIMO antennas of approximately 10 times better than 4G networks, network interference discharge by customizing Beamforming, and implementing future full-duplex mobile communications in the future) will determine the gradual migration of the critical communications infrastructure of each state (government authorities, companies, medical systems, systems energy, banking systems) to the 5G network environment.

In addition, the increasing need for communications bandwidth, the limitations of 4G networks but also the fixed infrastructure to ensure mobile access and cloud-based real-time access to data and information will indirectly require the migration of applications, critical services and data traffic associated with the 5G mobile infrastructures. The two elements, corroborated with the complexity of high technology, will generate, as a consequence, the direct functional critical infrastructure dependence on the availability of 5G equipment and systems and on the capability and credibility of the system's manufacturer. Under the security and continuity of critical services, most technology-consuming states will have to choose between the dependence on the Asian technology and American technology, in the context where cybersecurity is no longer an exclusively technical issue.

From the perspective of induced security risks, besides the significant dependence on 5G systems and equipment manufacturers, the lack of transparency in the level of infrastructure, equipment production and maintenance cycle determined the European states (+ the USA) at the issuance, in a technical summit in Prague (May 5, 2019), of two recommendations indirectly intended upon high-tech developers.

As a future target, securing the critical communication infrastructure will inclusively imply the traceability growth of developing, implementing and operational processes of 5G technology communications infrastructure through:

- *„Shared responsibility of all stakeholders should drive supply chain security. Operators of communication infrastructure often depend on technology from other suppliers. Major security risks emanate from the cross-border complexities of an increasingly global supply chain which provides ICT equipment. These risks should be considered as part of the risk assessment based on relevant infor-*

mation and should seek to prevent the proliferation of compromised devices and the use of malicious code and functions".

- *Customer – whether the government, operator, or manufacturer -- must be able to be informed about the origin and pedigree of components and software that affect the security level of the product or service, according to state of art and relevant commercial and technical practices, including transparency of maintenance, updates, and remediation of the products and services"***[8]**

In the 5G technology generated context, cybersecurity acquires a new dimension represented by the transparency of the equipment (hardware) manufacturing processes, software products development, materialization of firmware updates and maintenance activities.

2. The need to adapt current cybersecurity technologies to the new network infrastructure and architecture framework - the emergence of a *„dynamic cybersecurity policy"* concept.

5G networks or „next generation of radio networks" in the network architecture level would mainly involve 4 innovative elements which require changing the current cybersecurity paradigm, based on standard security policies, as follows:

- *Facilitate the implementation of „software-defined network" networks and „software-defined radio"* to the detriment of traditional ISO/OSI networks. The security policy applicable to an ISO/OSI model network architecture will have to be redefined as **a dynamic security policy** adapted to a software network infrastructure (SDN - *Open Wireless Architecture*), which will work by alternatively modifying the traffic capabilities and the communication routes between users through fast dynamic allocations/deliveries of IP addresses, much more frequently than the traditional routine. For example, in the 5G infrastructure traffic situation, the number of nodal gateway equipment will increase by a factor of 20 to 30 times the original amount and the volume of distributed gateway equipment will decrease considerably **[9].**

- *The 5G network environment segmentation in 3 logically individualized networks,* as follows: radio access network (*radio access network - RAN*), *core network* (data centers networks) and „*transport network*" respectively. The principle will determine the change of a single technical infrastructure cyber protection concept and will ensure extended cybersecurity for the protection of a *network* function virtualization (***Network functions virtualization - NFV***), aimed at the simultaneous facilitation of several different functionalities, using the virtualization principles type IaaS. Thus, the perimeter cyber protection actions of the network environment will no longer be sufficient for traffic control and limitation of external threats, as it is necessary to combine active and passive protection measures.

- *Operationalizing the concept of network segmentation* - ***Network slicing*** into different segments of logical networks dedicated to a single set of functionalities. The high traffic speed estimated at 100Mbps/download/user and respective 50Mbps/Upload/user, the maximum latency estimated at 4 ms and the high level of coverage respectively, facilitates the segmentation of a common network platform into several subnets dedicated to different functionalities such as: networks dedicated to mobile communications (Mobile broadband network), networks dedicated to "machine to machine" communications, networks dedicated to government authorities (gov - networks), networks dedicated to the medical system (medical - networks), etc.

From the security point of view, these dedicated subnetworks (logically separated at the level of a single platform) will generate a high-security level, yet carrying significant resource consumption since different protection layers can be applied according to the importance and sensitivity of processed data, the network critical availability level or the subnetwork importance to the critical infrastructure. Although the cybersecurity level will significantly increase and will be adjusted based on the operational requirement, the complexity of measures and the personnel's knowledge level will become determinant.

The concept of networks logical segmentation depending on the destination or served need will most likely require the emergence of new equally customized communication protocols, depending on the subnet to which they are addressed, such as machine to machine type communication (MTC), Ultra-Reliable MTC (UMTC) or Extreme Mobile Broadband (xMBB)

- *Use of cloud computing infrastructure as native access infrastructure to applications*

and data resources. The notion of native cloud computing infrastructure is perhaps one of the greatest benefits of 5G technology. Migration to the cloud computing environment will not only become a necessity imposed by the need for instant data access but will also be a requirement to meet the standard levels of Quality of Service (QoS) and Quality of Experience (QoE) respectively. The new concept of "native cloud networks" will allow overcoming the current barriers regarding the migration of data and information in the cloud computing environment, but at the same time, it will require adapting cybersecurity processes to an "end to end security" approach, using especially the advanced software encryption and infrastructure resilience solutions through virtualization.

The impact on the security environment interpreted by the need to adapt actual cybersecurity policies and strategies indirectly generates a series of additional human, procedural and technical nature risks.

From the point of view of the personnel and security administrators who will manage the networks security in 5G technology, the need to adapt the training and constant education will increase substantially. Also, the complexity of actions and attacks on infrastructure will be permanently in an upward dynamic which will require not only the possession of highly specialized technical teams, but also the tools and resources of action in near real-time, to be able to cope speed of attacks. Although technology will allow online training execution through augmented reality platforms and innovative simulation techniques close to the real environment, security processes and defensive cyber actions will need the substantial support of cyber products controlled by artificial intelligence.

Whereas technology will allow online training forms execution by augmented reality platforms and innovative simulation technics close to the real environment, security processes and defensive cyber actions will need the substantial support of artificially controlled cyber products

Procedurally, the cybersecurity concept will become less standardized and will experience a permanent dynamic. Thus, cybersecurity static procedures, almost indispensable today, will be gradually replaced by experiences of good practices and knowledge bases operationally validated in simulation centers. The cybersecurity concept will migrate to a comprehensive cybersecurity approach.

3. Increasing and energizing the global platform for manifesting cyber attacks and the attack environment, by expanding IoT and M2M communications.

One of the most significant cybersecurity implications, generated by 5G operationalization, is evaluated as increasing the attack surface by facilitating mobile broadband connections to the Internet of all objects, equipment and systems that have an active network port, regardless of the environment provenance. The notion of „smart objects", an extension of algorithms and artificial intelligence almost anywhere (from industrial processes to household objects) but also the expansion of digital multimedia has created the need for permanent network connection and, implicitly, the concept of „Internet of Things". Each equipment connected to the network environment (IoT) will act as a user or consumer of connection services, but will also act as a sensor at the network level. The more the number of interconnected devices will increase, the greater the society dependence on the functioning of communication networks and the Internet environment will be.

In a 4G digital society, a harmful "botnet" network obtained by penetrating and taking control over a number of interconnected computers creates significant destructive effects on a digital infrastructure under attack, rendering services and access to data, information and applications unavailable. However, in the future 5G, hacking actions will be directed to the intelligent devices of a user in his social environment (TV, refrigerator, central heating, air conditioning, etc.), and these can be successfully used to mount large-scale DDOS attacks towards the critical communications infrastructures of the states. Moreover, in the future 5G world, most likely, the same network of penetrated and remote-controlled devices, which has become a botnet, will be used to shut down an entire network of vehicles or drones in a region, or to control the power supply processes of a city.

Technically, the existence of non-standard and hybrid operating systems at the level of various smart objects and equipment will make it almost impossible to detect malware software or virus tools stored and hidden in the software of IoT equipment. A large amount of data generated by the IoT environment in future 5G networks will make it much more difficult to identify anomalies in the behavior of

hacking actions or traffic anomalies in the digital environment, especially since the architectures and software applications have not yet implemented, under the restrictive effect of the law, the "security by design "concept.

Target diversification, new communication protocols capable of supporting M2M communications, as well as increasing the number of targets through vertical and horizontal digitization - Internet of Everything (IoE) and Smart City/Smart Society operationalization will increase the dependence of critical connection of infrastructure and environment and the "Butterfly effect" will be much easier to feel in the future security environment.

Ever since 2015, the company Wind River Systems (USA) in research for the security of IoT equipment **[10]** has drawn attention to the need to resize the concept of cybersecurity in the context of developing the three essential levels of digital society, namely smart cities, connected industry and connected buildings. The company's research concluded that there is no real solution, ideal for mitigating the risks generated by IoT development and the need to develop security standards unanimously accepted by the manufacturers of smart equipment and technology it is almost mandatory.

The emergent security risks arising from the IoT development, accelerated by 5G facilities derive from the fact that the operating systems used on smart devices are mainly based on Linux distributions and Open Source customizations such as FreeRTOS, Contiki/Contiki- NG, MBed OS and RIOT OS and equipment manufacturers use non-standard hardware architectures with short life cycles, replaced new versions relatively quickly, insufficiently tested for vulnerabilities and with minimalist security technical support.

According to security company Gartner **[11]**, over 25% of the cyber attacks by 2025 will be addressed to the IoT equipment or will have these systems as an intermediate target which will lead to a revaluation of risk analyzes on the digital environment.

The emergence of new vulnerable targets in the IoT environment which have not been considered essential up to now and the definition of the „smart home" digital environment as a vulnerability area, derives from the studies of the company NETSCOUT, which in the security report of 2018 **[12] Threat Intelligence Report, pp.2]** emphasized that "*five minutes is the average amount of time it takes for an IoT device to be attacked once connected to the Internet".*

4. Enhancing cyber attack capabilities for current vectors by increasing bandwidth and attack surface and decreasing latency of communication channels.

The report from 2018 elaborated by the European Networks Information Security Agency for (ENISA) **[13],** highlighted that, during the period 2017-2018, the number of "Denial-of-Service" (DOS), "Distributed Denial-of -Service "(DDOS)" cyber attacks, web-based "attacks and „botnet"cyber-tools has increased, becoming the main threat vector in the future.

Implementing 5G technology and facilitating broadband data transmissions with traffic capabilities estimated at an approximate potential level of 10 Gbps - 50 Gbps and a latency value of between 4ms-1ms will increase the success rate for DDOS cyber attacks, starting from the real premise that data exfiltration from the network environment will become inefficient as compared to the unavailability of the services of an entire network and critical infrastructures of a state. Improvement of DDOS attack tools and their operational testing in recent military conflicts (Estonia, Georgia, Ukraine) will determine that, in the context of increasing the cyber attack surface (IoT/smart society environment) and improving the speed of online traffic, they will be *the main cyber risk vector for the communication infrastructures of states.*

If actual DDOS attacks can be almost randomly performed at any OSI architectural level, in the context of 5G systems implementation, the volumetric and protocol DDOS attacks dedicated to level 3 and 4 of the OSI model but also those of the ones specialized in flow concentrators and nodal gateway equipment will be chosen, in order to discharge as many segments of the network as possible.

Although blocking legitimate data traffic on a 5G network becomes difficult in the context of existing connections diversity, this can be accomplished by diversifying attack vectors and combining DDOS techniques with other vectors such as web-based attacks on data management systems of 5G services of mobile operators or malware vectors, similar to the case law "*Mirai malware*" from 2016.

In 2016, „Mirai" generically named malware has successfully penetrated the networks of IoT-type devices that used the Linux operating system. On September 20, 2016, the Mirai malware was used in the largest ever Distributed Denial of Service (DDoS) attack, targeting French cloud computing site OVH and, later in the same year, the United States DNS provider „Dyn" **[13].**

Practically, the network facilities effect generated by the 5G technology on the DOS/DDOS/Botnet attack vectors will be a trampoline, enhancing in the event of such a successful attack, the future effects on the continuity of the access services to the critical digital applications. The solution, in the new digital context, can be represented by the division and sharing of security risk between technology/service consumers, equipment manufacturers and 5G service provider respectively, by implementing the concept of "security as a service" as part of the service contract (SLA - service level agreement).

5. The emergence of new attack vectors and new cyber attack opportunities in the global digital environment.

The 5G environment and the increased dependence on the advanced technology at society level, as well as on the producer's patents and technological standards offers reasonable indications about the possibility that, at one point, a technology producer could dismisses the communications infrastructure of a state, using constructive vulnerabilities specially designed or software elements gradually introduced in network architecture (exp: in SDN networks, as part of a firmware upgrade or as part of a legitimate maintenance process). In addition, large traffic capabilities through the 5G transport network nodes will create the real possibility of masking the exfiltration of confidential data from the network environment to the control servers of third parties or producers serving divergent security interests, without these exfiltrations to be quickly known and eliminated.

Therefore, the concept of cyber espionage, the possibility of data exfiltration from the network environment and the massive direct dependence on the technology of a certain developer may be the main new threats, not necessarily innovative in content, but in the form of manifestation and in the value of harm and destructive effects.

Another element of risk may be the accelerated development of online hacking platforms specialized for attacking GSM networks and infrastructure. A good example that can prove the effects of such a threat is the attack carried out by the online hacking platform „REGIN", which allowed in 2014 the penetration of critical communication infrastructures in countries such as Algeria, Afghanistan, Belgium, Brazil, Fiji, Germany, Iran, India, Indonesia, Kiribati, Malaysia, Pakistan, Syria and Russia. According to the Kaspersky Lab analysis *„A REGIN module was able to monitor the control systems of the GSM cells, collecting data on the GSM cells and network infrastructure and subsequently penetrating any GSM target cell. According to the information logged on the GSM cell control system obtained by Kaspersky experts during the investigation, the attackers were able to access data that allowed them to control the GSM cells inside the network of the respective penetrated telecommunications operator. The attackers had access to data about the calls processed by a particular cell and could facilitate the redirection of the calls to other cells or the activation of neighboring cells"* **[15].**

In addition to the mentioned threats, most likely 5G facilities will also diversify the applicability of ransomware threats as well as advanced and persistent attacks (APT) customized for communication systems, the motivation being provided on the one hand by the impact on the network environment but, on the other hand, by the successful procurement of illicit funds that will fuel the future development of new cybercrime tools.

Certainly, the assessment of emerging cybersecurity risks from the 5G operationalization will be subject to the analysis of each technology consumer state but also of cyber analysis environments considering that, the technical maturity of the 5th generation of mobile networks will be reached only between 2025-2030.

6. Migration of the cross-border organized cyber crime interest towards digital identities and personal data theft.

The 5G technology will boost the possibility of human communication in the social networking spectrum through the excessive use of virtual reality and, above all, of multimedia virtual communica-

tion, using augmented reality products. Although it may be considered futuristic, I evaluate that, in the near future, each individual, will be able to communicate in the social networking environment using one or more associated virtual identities. Thus we will find a parallel accelerated development of a new virtual human ecosystem associated with the social-terrestrial, similar to a new parallel world.

The limitations regarding these concepts development are due so far to the lack of band capacity, the slow/inconsistent traffic speeds and the limitations of mobile connectivity. The 5G infrastructure, as discussed above, will discharge these limits. In the new context of virtual human society, the importance and necessity of security of virtual identity/identities will become at least as significant as that granted to the protection of personal data or biometric data. In this respect, cybercrime will intensify the actions of illicit exploitation of virtual identities in the online environment in order to obtain illicit material benefits and resources in an innovative way, exploiting precisely the social evolutions generated by the technology. Most likely, the value of the fingerprint and virtual identity of each user will become a tradable resource, so that the protection of virtual personal data in terms of cybersecurity of the population and users will become a new field of activity.

Conclusions

The 5G technology alongside the artificial intelligence systems will redefine the society we know nowadays and implicitly, the cybersecurity environment. Even if the transformation will not be abrupt, the technological revolution will impose the following major directions of the transformation of the current cyber environment:

- The level of threats will be a permanent ascending one dictated by overly rapid implementation of certain insufficiently tested and documented technologies (5G) as well as by the developed criminal capacity of the cybercrime structures. **The effect:** cybersecurity of infrastructures can be ensured through governmental – private or consumer – technology producer cooperation.
- Dependence of critical communication infrastructure functioning on the major technology and equipment producers will increase significantly. **The effect:** on a short term, states will be faced with the dilemma of choosing between American and Asian technologies.
- Risks of losing sovereignty and freedom to choose the cybersecurity tools for new communications technologies and network systems will increase and responsibilities will gradually be transferred to equipment manufacturers. **The effect:** the concepts of *„security as a service"* and *„security by design"* will be operationalized, as part of the service contracts (SLA);
- Critical communications infrastructures of states will gradually migrate from the private/government data communication networks to the public 5G communications infrastructures. **The effect:** the spectrum of vulnerabilities will increase being dictated by the capacity of operators and the resilience of public telecom infrastructure.
- Cybersecurity field will no longer be exclusively technical, but it will represent a „cross" type domain on the border between technology - security strategy - artificial intelligence - governance. **The effect:** cooperation between states within the cybersecurity field becomes mandatory.

5G technology impact on the security environment, at the current state of knowledge, can be the most estimated, but a precise determination of possible effects and actions to limit them must become the subject of national security strategies for both European and other states that will define technology implementation in the first wave.

The level of risk assumed along with 5G technology implementation must be balanced with strategic advantages resultant from the operationalization of the 5th generation network in the pioneering period, as compared to implementation during its maturity period.

In conclusion, though it is premature to carry out a comprehensive risk analysis on a 5G communications infrastructure, for objective reasons related to the lack of technological knowledge, anticipating the main risks and assessing the likely impact on cybersecurity environment, it will facilitate network environment securing processes in the short and medium term.

References

[1] *,** *China is poised to win the 5G raceKey steps extending global leadership***,** *https://www.ey.com/Publication/vwLUAssets/ey-china-is-poised-to-win-the-5g-race-en/$FILE/ey-china-is-poised-to-win-the-5g-race-en.pdf*, p.12, 2018

[2] P. Agyapong, M. Iwamura, D. Staehle, W. Kiess, A. Benjebbour, *"Design considerations for a 5G network architecture"*, IEEE Commun. Mag., vol. 52, no. 11, pp. 65-75, Nov. 2014.

[3] Colin Lecher, Russell Brandom, Is Huawei a security threat? available at *https://www.theverge.com/2019/3/17/18264283/huawei-security-threat-experts-china-spying-5g*

[4] William Chalk, Privacy by design: *Cybersecurity and the future of 5G*, CSO, available at *https://www.idginsiderpro.com/article/3399000/privacy-by-design-cybersecurity-and-the-future-of-5g.html*

[5] ***, Deloitte-NASCIO *Cybersecurity Study "State governments at risk: Time to move forward"*, 2014, p.20, *https://www.nascio.org/dnn/portals/17/2014Presentations/2014_Deloitte-NASCIO_Cybersecurity_Study_ Overview_10_1.pdf*

[6] 3GPP, *http://www.aec.mk/irc2018/irc2018_s3_02_1.pdf*, p.13

[7] Knud Lasse Lueth, State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating, 2018, *https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/*

[8] *,** Prague 5G Security Conference: The Prague Proposals, Press release, *https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/*

[9]*** Huawei, 5G Network Architecture ,*https://www.huawei.com/minisite/hwmbbf16/insights/5G-Nework-Architecture-Whitepaper-en.pdf,.p.12, 2018*

[10] ****, Security in the Internet of Things- Lessons from the Past for the Connected Future, 2015, California, SUA*

[11] *https://www.computerweekly.com/news/450288414/IoT-to-play-a-part-in-more-than-a-quarter-of-cyber-attacks-by-2020-says-Gartner*

[12] ****, NETSCOUT Threat Intelligence Report, Dawn of the terrorbit Era-https://www.netscout.com/sites/default/files/2019-02/SECR_001_EN-1901%20-%20NETSCOUT%20Threat%20Intelligence%20Report%202H%202018.pdf, pp.2*

[13] *,** *http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisathreat-landscape-2018*

[14] *https://www.allot.com/blog/iot_cybersecurity_challenges_and_solutions/*

[15] *https://securelist.com/regin-nation-state-ownage-of-gsm-networks/67741/*

[16] ****, CableLabs, A Comparative Introduction to 4G and 5G Authentication,* pp.5-9, 2019, *www.cablelabs.com*

Adam Radomyski, Paweł Bernat,

ASSESSMENT OF IRAQ'S AIR DEFENSE SYSTEM IN THE IRAQI FREEDOM OPERATION

Adam Radomyski, Paweł Bernat

Department of National Security and Logistics, Polish Air Force University in Dęblin, Poland,
a.radomyski@law.mil.pl, p.bernat@law.mil.pl

***Abstract**: The paper presents a synthesis of research results that focus on identifying factors that affect the organization and functioning of Iraq's air defense system during the Iraqi Freedom operation and, as a result, contributed to Iraq's defeat. An important part of the considerations presented in the article are the results of research relating to the role and significance of the use by the coalition partners of the state-of-the-art air weapon systems, which facilitated carrying out very precise strikes on the most essential elements of the Iraqi air defense system beyond the reach of the anti-aircraft artillery and missile systems. The authors also indicate that of the vital importance in the lack of adequate protection of the most important objects, the so-called centers of gravity, located mainly in Baghdad, were organizational errors in the distribution of forces and resources, technological problems, and inept command. The paper is concluded with a reflection on the gained knowledge on the influence of the experience gathered from the Iraqi Freedom operation on the processes of technological modernization of the armed forces, and especially air defense that is still based on the technology from the 1960s and 1970s.*

***Keywords**: air defense system, centers of gravity, air attack, close air support, active defense.*

Introduction

Analyzing the concepts of conducting air operations at the end of the 20th and the beginning of the 21st century, one can see a change in the Clausewitzian victory paradigm – victory through destruction. This is since more and more advanced technologies allow for precise, even surgical strikes at carefully selected targets, the destruction of which should bring forth the breaking of the will of a given nation, government, or their subordination. As a result, the war and its conduct became more (although not spatially) limited (Świniarski & Wiatr, 1998). Despite a significant change in the paradigm of war and the dynamic development of airpower, the following words were spoken years ago by Sir Winston Churchill: "Air power is the most difficult of all forms of military force to measure, or even to express in precise terms" (MoD, 2015, p. 13) They have lost nothing of their relevance. In contemporary air operations, limiting the damage and losses not only of one's own but also of the opponent, including the civilian population, have grown into the basic canon of modern war (Kuriata, 1998). It also applies to the Iraqi Freedom operation.

In this context, it should be emphasized that after the rapid defeat of Iraq in the 2003 war, there are still many discussions on its main reasons. In this paper, the authors focused on the assessment of the organization and functioning of the air defense system in war conditions, which were recognized as one of the key elements that directly contributed to the final result. In this respect, based on the results of the research conducted at the Polish Air Force University in Dęblin, one can conclude that despite extensive organizational efforts, the Iraqis failed to properly prepare their air defense system to confront the air forces of the two leading countries of the Iraqi Freedom operation, i.e., USA and Great Britain. This resulted, among other things, from the fact that starting from 1991, in accordance with a UN Security Council resolution, an embargo was imposed on Iraq that banned the sale of any weapons by other countries. Among other things, it was for these reasons why Iraq found it very difficult to expand its aviation

potential and develop air defense. The Iraqi army had in its possession only old technologies – from the 1960s and 1970s that needed modernization and replacement for better quality anti-aircraft systems. It was, however, impossible to implement in a short time. Under these conditions, Iraq organized a provisional but relatively strong air defense system, which was based on a large number of various rocket and artillery systems deployed in the regions of Baghdad and Tirkit, as well as at several other important objects.

Preliminary studies carried out on the Iraqi air defense during the Iraqi Freedom operation confirmed the hypotheses that the state of knowledge in this area required more detailed examination and development. Most of the scientific publications describing activities during the Iraqi Freedom focus on their analysis from the point of view of ground forces or air forces, but not air defense, which is a basic determinant in maintaining the viability by the centers of gravity (which are also vital targets for a given state or its armed forces). The information, available in the subject literature, about the organization and operation of the Iraqi air defense in the Iraqi Freedom operation, is usually incomplete and fragmentary. That is why the authors assessed the current state of knowledge as unsatisfactory. In this situation, they decided that this is a sufficiently valid reason to investigate this problem in-depth, and the results of the research are presented in this paper.

From the above-presented problem, the subject of research has emerged, i.e., the Iraqi air defense system in the conditions of confrontation with the air forces of the coalition partners during the Iraqi Freedom operation.

Therefore, it was assumed that the research goal of the paper is to provide a characteristic of the organization and operation of the Iraqi air defense system in the conditions of airstrikes carried out by the coalition aviation during the Iraqi Freedom operation.

The analysis of the manner of achieving such a formulated goal led the authors to order the further research steps by formulating the main scientific problem with the following way: How was the Iraqi air defense system organized and operated during the Iraqi Freedom operation and what were the effects?

The methods used for the research were mainly theoretical; among the methods employed were analysis, synthesis, analogy, generalization, and deduction. The analysis was used because the subject of the study turned out to be too complex to be studied in its entirety.

Searching for answers to the main research problem and the purpose of a detailed understanding of the subject of research, critical literature analysis, and examination of documents were used. The analysis and synthesis were performed to obtain the most reliable information about the subject of the research. The implementation of these methods allowed for describing the strengths and weaknesses of the organization and functioning of the Iraqi air defense system during the Iraqi Freedom operation. Generalization and analogy were used to determine the group of factors that had the greatest impact on the organization and use of the anti-aircraft forces in the situation of mass air raids. The deduction was used in the process of drawing conclusions about the strengths and weaknesses of the Iraqi air defense system in the context of confrontation with modern air forces.

1. Characteristics of the coalition air forces operations in the Iraqi Freedom operation

It should be emphasized that the political and military situation prior to the commencement of Operation Iraqi Freedom was favorable to the commencement of the air operation, the purpose of which was to simultaneously win an advantage in the air and strike at the centers of gravity of Iraq. This was favored by, among others, by UN Security Council Resolution 688 that called on Iraq to cease ethnic cleansing on the Kurdish and Shiite people. As part of these actions, as early as August 26, 1992, the no-fly zones were introduced in Iraq. They were established to ensure the free carrying out of reconnaissance missions by the coalition air forces, and thus facilitate the constant control over compliance with the provisions of the UN Security Council Resolution. At the same time, they were forbidden zones for Iraqi aircraft of all types. The border of the designated zones was drawn above the 36th parallel in the north of Iraq and below the 33rd parallel in the south.

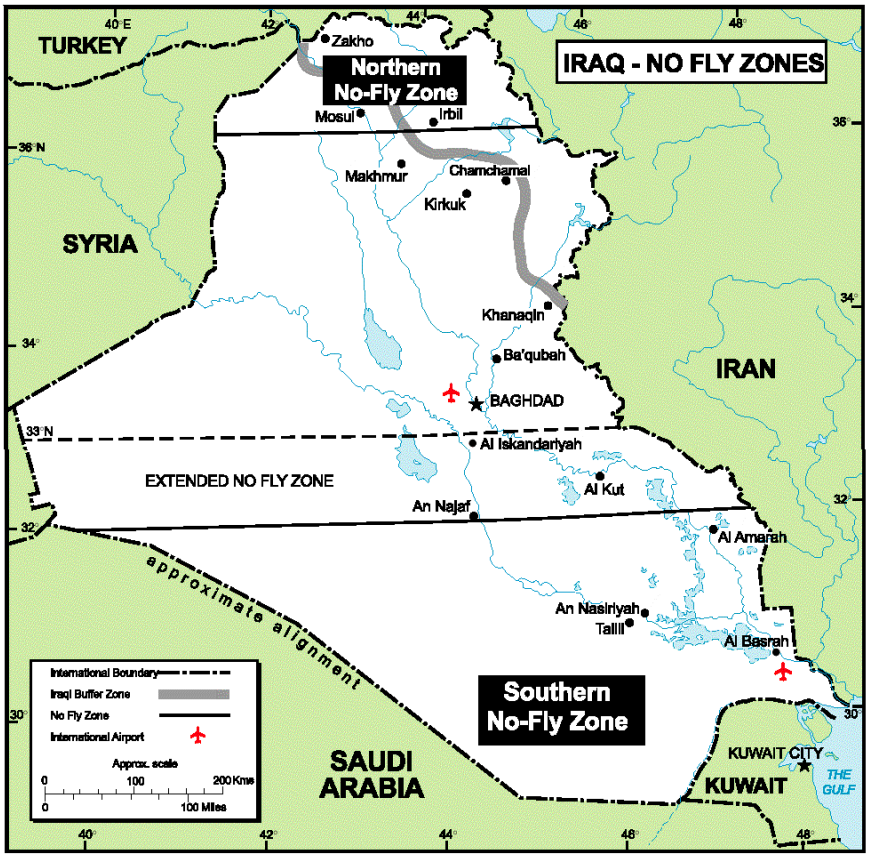


Figure 1: No-fly zones in Iraq
Source: https://www.globalsecurity.org/wmd/library/news/iraq/2000/45303.htm

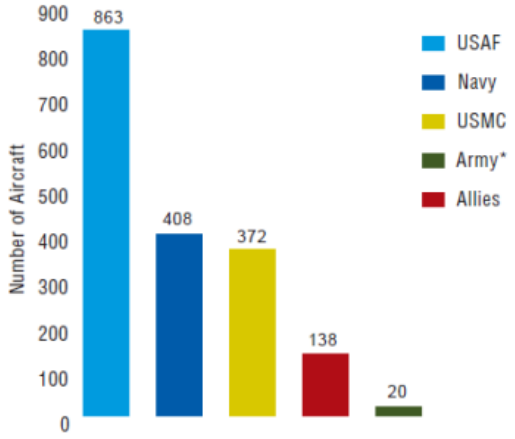
Operations carried out as part of the no-fly zone control were named "Operation Northern Watch" and "Operation Southern Watch." In order to coordinate the operations, the Americans formed Joint Task Force Southwest Asia, whose operational center was located in Al Udedi, Qatar, while air bases were located in Turkey, Saudi Arabia, Kuwait, and Bahrain. In total, until the start of the Iraqi Freedom operation, the forces involved in controlling the airspace over Iraq consisted of about 200 combat aircraft and 6,000 personnel (Heliński, 2003, p. 102).

The introduction of no-fly zones met with strong opposition from Iraq. Despite the coalition's warnings, Iraq did not withdraw its anti-aircraft systems from their positions and started firing at the coalition aircraft. The number of attacks on air targets was steadily increasing, as did the number of retaliation actions undertaken by the Allies. At the end of 1998, there was regular warfare taking place, not a mission aimed at controlling the implementation of the UN Resolution. In the period from December 1998 to January 2001 alone, Iraqi aircraft violated the southern zone more than 470 times, and over 670 accidents of targeting or firing at coalition planes by Iraqi anti-aircraft defense systems were recorded (Radomyski, 2009, p. 148). At that time, the coalition air forces carried out around 22,000 combat flights by opened fire over 350 times (Cordesman & Arleigh, 2003, p. 192). In this regard, one may conclude that even before the start of the Iraqi Freedom operations, both sides had already conducted regular acts of war. As a result of coalition air force strikes on the anti-aircraft systems, air control was obtained even before the start of the joint operation (Mosley, 2003). Airstrikes had intensified even more since the beginning of 2003 – there were around 170 rocket-bomb strikes almost exclusively with the use of precision ammunition. In some cases, these attacks went beyond the zone defined by the UN mandate, and the B-1B bombers were used to attack radar stations just before the outbreak of the conflict (Cordesman & Arleigh, 2003, p. 149).

Thus, the advantage gained by the coalition enabled them to redirect the effort from fighting for the control of the airspace to carrying out strikes at the centers of gravity of Iraq and to support the land

forces. Despite the Southern Watch and Northen Watch operations, it was expected that Iraq would still retain the command structure and control of the anti-aircraft systems that were located in underground shelters and bunkers.

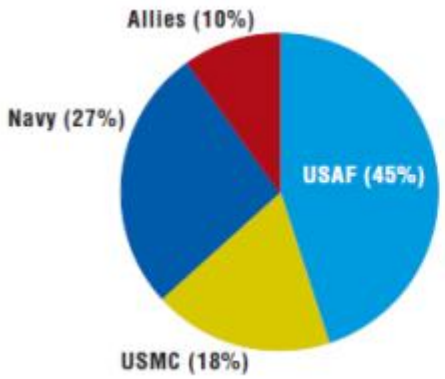
For the purposes of efficient conducting of a military operation against Iraq in the Persian Gulf region, a strong group of air, navy, and land forces was organized that amounted to about 300,000 soldiers with more than 1,000 tactical combat aircraft, 47 B-52N, B-1B, B2A strategic bombers, over 100 warships, of which 35 carried Tomahawk missiles. Military operations in Iraq were also supported by other forces, including satellite reconnaissance and guidance systems. In total, the aviation potential accumulated in the Persian Gulf consisted of 1801 combat and auxiliary aircraft. The US Air Force (USAF) provided 51% of the combat aircraft and all heavy bombers. Most refueling, transport, and reconnaissance aircraft came from the Air National Guard and Air Force Reserve Command (Grant, 2003, p. 10).



	Fighter	Bomber	SOF	ISR	C2	Airlift	Tanker	Other	Total
USAF	293	51	131	60	22	111	182	13	863
Navy	232	0	0	29	20	5	52	70	408
USMC	130	0	0	0	0	0	22	220	372
Army*	0	0	0	18	0	0	0	2	20
Allies	80	0	14	11	4	10	12	7	138

*Does not include helicopters.

Figure 2: Total number of coalition aircraft
Source: (Grant, 2003).



	Fighter	Bomber	Total	Percent
USAF	8,828	505	9,333	45.0%
Navy	5,568	0	5,568	26.9%
USMC	3,794	0	3,794	18.3%
Army	0	0	0	0
Allies	2,038	0	2,038	9.8%
Total	20,228	505	20,733	

Figure 3: Strike sorties
Source: (Grant, 2003).

On March 20, 2003, at 3.33, less than an hour after the deadline ultimatum given by President Gorge W. Bush to Saddam Hussein, the first raid on Baghdad started, and this is how the operation Iraqi

Freedom began. The objectives of the operation disclosed by Secretary of Defense Donald Rumsfeld were as follows:

- to end the regime of Saddam Hussein;
- to identify, isolate and eliminate Iraq's weapons of mass destruction;
- to search for, capture or drive out terrorists;
- to collect intelligence related to terrorist networks in Iraq and beyond;
- to collect intelligence on the global network of illicit weapons of mass destruction activity;
- to end sanctions and immediately deliver humanitarian relief to the displaced and the many needy Iraqi citizens;
- to secure oil fields and resources, which belong to Iraqi people;
- to create the conditions for Iraq's rapid transition to a representative government (Garamore, 2003).

In fact, the war against Iraq waged by the US and its allies from March 20 to April 15, 2003, boiled down to de facto control over one of the most important areas of oil production in the world. In this context, the US command in 2003, in a secretive and very detailed way, when planning a military operation including air operations, analyzed the real potential of Iraqi air defense capabilities. On that account, a combined air-ground operation was prepared.

The Iraqi Freedom operation began with the use of several BGM-109 Tomahawks and F-117A and F-16 aircraft that struck a bunker in the suburbs of Baghdad, which was believed to be the location of Saddam Hussein and other important commanders. On the day preceding the air-missile attack, US air forces attacked artillery positions in southern Iraq because they were considered a real threat due to the possibility of using chemical ammunition against the coalition land forces in Kuwait. In the earlier days preceding the war, coalition air forces using B-1B aircraft destroyed the elements of the Iraqi integrated air defense system located in no-fly Zones, including Soviet production radar stations P-15, a radar close to the H3 airbase, and a radar detecting small altitudes air targets in Ruwayshid, near the Saudi and Jordanian border (Kopp, 2003).

The main phase of warfare began with aircraft missiles strikes delivered by combat aircraft on selected targets in Iraq. Later on, these strikes were carried out in series; in total there were over 300 of them. Attacks took place both, during the day, and at night and targeted industrial, economic, and military facilities of the state control system, on the positions of the Iraqi troops, including the ground-based air defense systems and airports, which were systematically destroyed.

At that time, a wide range of precise weapon systems was used. For example, during the operation Desert Storm 282 Tomahawk missiles were used, while in the Iraqi Freedom, in only 15 days, over 1000 precision missiles and many thousands of self-guided bombs were fired.

Table 1: The number of precision combat weapon systems used during the Iraqi Freedom operation in 2003

Type of the air destruction agent									
TLAM *		Maverick		WCMD * *		LGB * * *		JDAM * * * *	
%	number	%	number	%	number	%	number	%	number
4	802	4.6	918	4.5	908	43.7	8.716	32.8	6.542

* Tomahawk Land Attack Missile;
** WCMD – Wind-Corrected Munitions Dispenser e.g., CBU-103/105,SFW/107;
*** LGB – Laser Guided Bomb, e.g., CBU-12/16/24/27/28 and EGBU-27;
**** JDAM – Joint Direct Attack Munition, e.g., GBU-31/32/35/37.

Source: Own elaboration

In total, coalition planes dropped 29,199 bombs, rockets, and missiles of all kinds on Iraq. The Second Gulf War was characterized by the intensive use of weapons guided by laser beams, satellites,

and other types of missiles guided by signal or TV image. Two-thirds, i.e., 19,948 of the used airborne weapons were precision-guided munition.

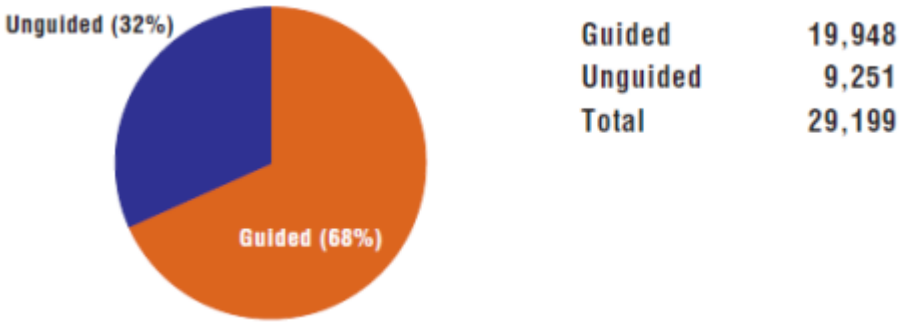


Figure 4: Munitions expended
Source: (Grant, 2003).

In attacks against Iraq, one of the most frequently used weapons were laser-guided bombs, joint direct attack munition, and Mk 82 bombs. These three types of means accounted for 71% of all types of munition used during the Iraqi Freedom campaign. The rest of the aviation weapon systems contained 16 other types.

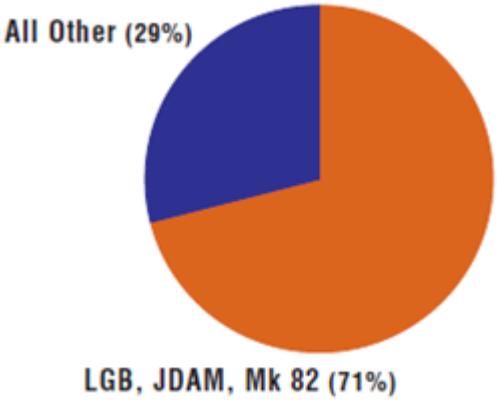


Figure 5: Most popular munitions
Source: (Grant, 2003).

The most effective was the rockets and bombs guided to the target with signals from the outer space radio navigation system NAVSTAR.

During the Iraqi Freedom operation, the precision-attack missiles HARM and MAVERICK also played a significant role in the disorganization of Iraq's air defense system. The latter is an American air-to-ground tactical missile manufactured by Huges Aircraft Corporation and Raytheon Corporation, and it is designed to fight tanks, combat transporters, surface ships, to destroy launch stations, and other tasks. The anti-radiation missiles AGM-88 HARM (high-speed anti-radiation missile) from Raytheon Corporation were introduced to the armament of American air forces in 1982. The HARMs significantly contributed to the destruction of many radar stations in combat operations in Iraq.

During the war against Iraq in 2003, American aircraft used the modernized variant of the "air-ground class MAVERICK AGM-56G2 missile. New software, including the targeting system with a thermal warhead (heat guided) allowed to detect the target and remember its location. The same type of missiles had already been used in operations in former Yugoslavia, where airstrikes were carried out not only on military equipment and facilities but also on military warehouses and bridges. The impact efficiency of this type of missiles was very high – it amounted to 97%. Most guided missiles were fired 6

kilometers or less from the target. During the entire Iraqi Freedom operation, more than 900 missiles of this type were used. They were carried by A-10 aircraft fighters; each of them could carry up to six such missiles. American air forces had 60 aircraft of that type in the Gulf region.

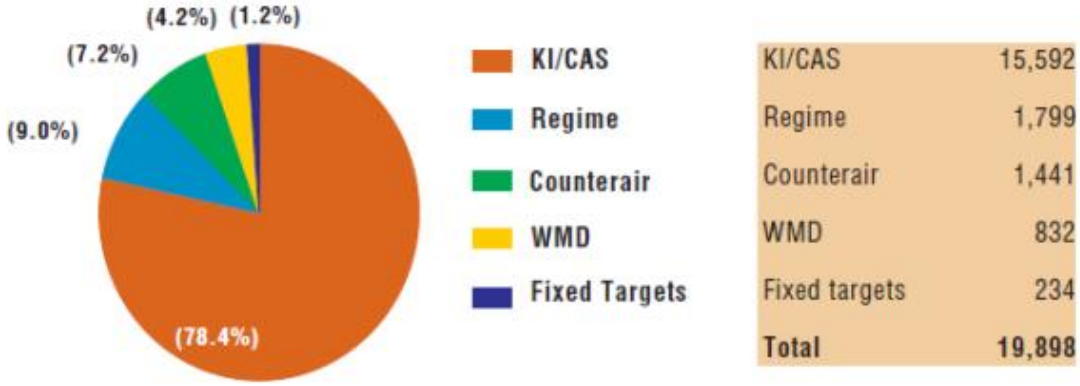
The appeared anti-radiation missiles HARM turned out to be the right choice for the campaign. Their 68 kg warhead caused great havoc among the Iraqi radar stations. The main carriers for these missiles were F-14, F-15, F-16 CJ, F/A-18, and TORNADO.

In Iraq, the main carriers of the HARM missiles were F-16 CJ, whose task under SEAD (Suppression of Enemy Air Defense) was to destroy the enemy's ground-based air defense systems. There were about 70 aircraft of this type in the American air forces, and they were based at the airports in Kuwait, Saudi Arabia, Qatar, and Turkey. The upgraded software and security equipment in the HARM missiles allowed to increase the accuracy in targeting the attacked objects.

In total, during the war, the coalition air forces used about 400 HARM anti-radiation missiles. They were also carried by F-117 attack aircraft, EA-6B electronic warfare aircraft, and F/A-18 combat jets. The greatest concern of Americans was the anti-aircraft shield of Baghdad, whose main core were medium-range anti-aircraft missile systems and high saturation of short-range anti-aircraft missile systems and anti-aircraft artillery, whose launch and fire positions were not accurately located. The Iraqi radars were turned on and off in very short time sequences, which made it difficult for the HARM missiles to reach the target. It showed the weaknesses of the HARM system – with the adopted tactics of Iraqi radar stations it had a problem with the proper location of the attacked object.

In the first part of the operation, the air and naval forces of the coalition struck the previously selected targets, including all Iraqi airports, which led to the elimination of many aircraft and airport infrastructure.

Based on the data, it can be stated that the air component focused the vast majority of its efforts, i.e., 78%, on air support for land forces, which was implemented under the Kill-box Interdiction/Close Air Support" (KI/CAS) strategy.



KI/CAS	15,592
Regime	1,799
Counterair	1,441
WMD	832
Fixed targets	234
Total	**19,898**

Figure 6: Strikes by category
Source: (Grant, 2003).

The effort of air forces to support land forces coincided with the ongoing strategic bombing that began with two-day "shock and awe" raids carried out with the use of B-2As, F-117As, and F-15E Beagles aircraft and several hundred of Tomahawk missiles that were fired from warships. As a result of these raids, Ba'ath Party facilities, Saddam's palaces, anti-aircraft stations, republican guard posts, and other targets in Baghdad were destroyed. The impact did not affect basic infrastructures, such as power plants and water intakes. Having analyzed air impacts, one can describe them as quite precise. The purpose of the raids in the initial period of the operation was to affect the civilian population and the Iraqi authorities psychologically and to disrupt the functioning of the state. After the initial phase of air raids, there were long and intense day and night attacks on the remaining government facilities in the city. These raids were part of the preparation for ground forces that were to engage in combat in the Baghdad region. Their goals were satellite links, buildings of the Ministry of Information, various Baath and mili-

tia and air defense facilities as well as republican guard positions and fire departments in Baghdad. As a result, airstrikes led to the disorganization of the defense system prepared by Iraq in the capital. The weapons used included laser-guided bombs Paveways and JDAMs. The uniqueness of this air force operation should be emphasized, because civilians, water and power supply systems, bridges, and government buildings that were not an integral part of the regime were not attacked during it.

The successes already achieved on the first day of the air operation and the lack of counteraction by Iraqi aviation enabled the early start of land operations. On the night of March 21/22, during the Shock and Awe operation, the coalition land forces began the strike. The lack of possibility to initiate the land attack from Turkey was definitely a disadvantage. It was also the reason why the main land component was deployed in Kuwait. The move forward of ground forces was accompanied by increased activity of air forces. The latter, closely supporting land forces (CAS), also successfully performed deep air support tasks (AI). Therefore, no classical, sequential course of operations was used, where land and air operations followed special and aerial operations, but individual phases of operations were carried out in parallel. At the same time, to ensure the offensive-raiding nature of land forces operations, special forces conducted intensive activities aimed at capturing important objects: airports, bridges, oil wells. It is estimated that air forces conducted as many as 4,278 strikes (Mosley, 2003, p. 5) to support special forces, and thereby opened them the way to take control over various strategically important places. From March 30 to the end of the operation, the difference between CAS and AI aerial operations blurred completely. In order to eliminate the resistance points at the entire depth of the task closer to the tactical relations with land forces, all air forces capabilities were used, and the depth of strikes of helicopters and close air support aircraft often went beyond the depth of strikes of strategic aircraft. It was also the first time when B-1B strategic bombers were used to carry out CAS tasks. These aircraft equipped with four powerful 2-ton BLU-113 bombs each performed frequent duty in the waiting zone over Iraq and were engaged when called from the battlefield. The use of unmanned aerial vehicles for reconnaissance purposes was also significant. The images transmitted in real-time were sent to the command of land forces, including the level of the company commander.

An analysis of the combat operations of the coalition air forces indicates the versatility and multidimensionality of the aviation usage that often had to take over the tasks of land forces. This situation was the result of a substantial, previously unforeseen pace of attack of the coalition forces, and thus the impossibility of introducing more and more troops.

In addition, air forces did not carry out a several-week "preparatory" air operation for the land attack, as was the case in 1991, but operated in parallel with the ground and special forces.

Close air support played (CAS) a significant role by clearly going beyond the area of tactical operations and covering the tasks of air interdiction (AI) and strategic strikes.

Over 50% of the overall effort was given to CAS. It was five times greater than in the Desert Storm operation. On the other hand, the Iraqi Freedom allocated more than twice as little effort, just 14%, to win and maintain the control in the air. Of course, the main reason here was the 12-year fight for control in the air, conducted almost continuously since the end of the war in 1991 and covering 70% of Iraq's airspace.

2. Organization and operation of the air defense system of Iraq during the Iraqi Freedom operation and the main reasons for the defeat

The Iraqi strategy of waging war in 2003 focused from the very beginning on the idea of defense based on the "city bastions," where the Republican Guard, Fedayeen, and other loyal units were deployed in urban areas, or the areas around them. The adopted defense model based on the cities was also supposed to provide better protection for soldiers against the consequences of air attacks and a certain limitation for the attacking air forces due to the possibility of large losses among civilians. Iraqis have deployed soldiers in schools, mosques, hospitals, historic sites, and in densely populated suburbs, which are excluded from bombing under the international law. In line with the adopted strategy, the Iraqis or-

ganized a layered defense around Baghdad based on Republican Guard troops, and to a large extent, it resembled the Soviet siege doctrine of 1941–43.

In the run-up to the Iraqi Freedom operation, out of the 220 combat aircraft at Iraq's disposal, only about 100 machines were fit for combat. That is why all Iraqi aviation was centered at eight airports (air bases). Before the start of warfare, Iraqis moved most of their combat aircraft: Mig-23, Mig-25, and Mig-29 (in sum around 50 units) near the Tammuz airbase (El-Habbania, 70 km west of Baghdad). On the basis of the directive of the commander-in-chief of Iraqi armed forces issued during the war, combat aircraft and helicopters were taken out of the command of the respective armed forces – their use, during the war, was governed by separate orders from Saddam Hussein himself.

Initially, it was assumed that aircraft stationed at the Tammuz airbase were important in the Iraqi concept of warfare. Moreover, the command of the Iraqi air force intended to use their aircraft to support their land forces from the al-Bark airport (about 80 km north of Baghdad) and the al-Hurrya airport (about 240 km north of Baghdad), where approximately 20 combat aircraft were located. However, this plan was not implemented. It should be noted that these forces, as Iraqi command declared, were best prepared for action and, at the same time, most strongly protected by ground anti-aircraft systems. Prior to the commencement of operations at the airport of the al-Bakr base, there were aircraft and their crews. That changed on April 6, when the base commander General M. Faruk ordered the officers to leave for homes and wait until they would receive a special order; an order that was never issued.

Such a decision resulted, among others, from the fact that the command of the Iraqi armed forces was aware of the fact that the coalition air forces would gain control in the air. Under these conditions, it was considered useless to use their own aircraft. However, it was predicted that they would be deployed during the defense of Baghdad, mainly when the enemy forces would approach the suburbs of the Iraqi capital. Again, for unknown reasons, it never happened. As a result, Iraqi air forces carried out only one reconnaissance flight from the Al-Bakr air base throughout the entire operation.

The main assumptions of Iraqi air defense tactics boiled down to a very short stay of anti-aircraft weapon systems at fire stations. Total control in the air of the US and UK air forces, which carried out missile-bomb attacks on objects located in Iraq, caused a significant weakening and the need to decentralize the command of Iraqi troops – subunits of anti-aircraft systems, which hindered, and in many cases even prevented the use of radar information from the stations that were located in the prohibited zones. The Soviet production anti-aircraft missile systems (S-75 and S-125) that were in possession of the Iraqi armed forces were not technologically modernized before the operations.

Before 2002, the Iraqi armed forces partly modified other air defense systems, which largely came from the Soviet era, with newer equipment that was obtained from various sources. As a result, before the outbreak of another war in the Persian Gulf, Iraq's air defense systems were a mixture of western and older Eastern European and Far East technologies. An important element of the qualitative improvement of Iraq's air defense system was technical assistance provided by China. It concerned the laying of fiber optic cables between various air defense nodes, especially in southern Iraq. As a result, it was supposed to limit electronic emissions of the air defense devices, which normally could be easily detected and located on the basis of standard reconnaissance activities carried out from the air. Despite these difficulties in detecting elements of the air defense system, American pilots were in a comfortable situation because they had the support of specialized aircraft specially designed to detect radar positions and anti-aircraft missile systems and disrupt their work. Moreover, American pilots could carry out attacks on radar stations from a distance of several dozen kilometers. In some parts of the country, Iraq was found to have attempted to block the global positioning system (GPS) that NATO forces used to target missiles at targets accurately. It was not entirely known whether those so-called GPS jammers were of domestic production or had been illegally purchased.

The analysis od Iraq's potential for air defense confirmed that in 1990 Iraq had 16,000 radar-guided surface-to-air missiles (SAM), mainly of Soviet production: SA-2, SA-3, SA-7, SA-8, SA-13, SA-14, and SA-16 and Roland produced by France and Germany. Iraq also had a wide range of Soviet mobile SAM systems, including SA-6 Gainful and SA-9 Gaskin. Of these, the most famous was Gainful, which inflicted heavy losses on Israeli air force during the Yom Kippur war in October 1973.

Table 2: Air defense command

SYSTEMS		1990 *	1995 *	2000	2002
AD GUNS		~ 4.000	~ 5.500	~ 6.000	~ 6.000
130mm		+	+	+	+
100mm		+	+	+	+
100mm	KS-19	+	+	+	+
85mm		+	+	+	+
57mm	S-60	+	+	+	+
57mm	ZSU-57-2 SP	+	+	+	+
37mm	M-1939	+	+	+	+
23mm	ZSU-23-4 SP	+	+	+	+
SAM				~ 2.300	~ 2.000
	SA-2	160	+	150	125
	SA-3	140	+	110	100
	SA-6	~ 300	+	150	125
	SA-8		0		
	SA-9 / -13		+	2.000	125
	SA-7 / -14	+	+		1.500
	SA-16	?	?	?	?
	Roland	100	+	+	+
	Crotale	5	5	5	+
	Aspide	-	-	+	+

Source: Own elaboration on the basis of https://www.globalsecurity.org/military/world/iraq/air-defence-equipment.htm

The most modern mobile SAM in the Iraqi army was the SA-8 Gecko short-range system. Its normal range of destruction of air targets was 1.1-5 nautical miles for targets flying between 100 and 16,500 feet. The most common tactic used against SA-8 was the use of anti-radar missiles or flying above its effective range. The self-propelled AAA ZSU-23/4 and MANPADS (Man-portable air-defense) systems supplemented the air defense. The portable anti-aircraft missiles sets MANPADS were equipped with missiles with thermal warheads that were designed to destroy targets at low altitudes and did not need accurate information from radar indicators. Iraq had an older type of MANPADS (SA-7, SA-14).

In addition, Iraqi air defense possessed more than 7,500 AAA units, which protected all the important military and civilian facilities. Some of these systems were located on the roofs of government facilities in Baghdad. 57mm and 37mm anti-aircraft guns, self-propelled AAA ZSU-23/4 and ZSU-57/2 systems, and hundreds of light anti-aircraft 14.5mm and 23mm machine guns constituted the backbone of the integrated air defense system. Based on the UN report, it can be stated that Iraq did not return a large amount of military equipment to Kuwait after the Gulf War in 1991, including one Hawk battery and 675 Russian surface-to-air missiles.

For major defense areas such as Baghdad, airports, chemical production complexes and nuclear facilities, air defense systems were particularly dangerous for aircraft operating below 10,000 feet.

To sum up, it can be said that the Iraqi air defense system was relatively well organized and combined the features of several systems. Multilayer air defense around Baghdad was more extensive than that surrounding most of the Eastern European cities during the Cold War and several times stronger than the one that defended Hanoi in the later stages of the Vietnam War. In the opinion of military ex-

perts, if it were assured that it would function as intended, that air defense system was able to protect key facilities in Iraq effectively.

Moreover, the quantitative and qualitative analysis of Iraqi air defense shows that it was one-third stronger in 2000 than during the first Gulf War in 1991. In 2002, Iraq already had an integrated air defense system (IADS) in which SAM systems of the various range covered all the area and created a protective umbrella. In particular, it was so in the Baghdad and Tikrit regions. In addition, air defense in the no-fly zones was mainly based on AAA, MANPADS, and a small number of SAMs. These were the means that could move quickly and organize ad hoc anti-aircraft ambushes. Command of the anti-aircraft resources in no-fly zones was decentralized. The information about air targets was received by radars deployed outside no-fly zones or from reconnaissance. Obtaining information from the radar indicators that were located at a fairly large distance from the anti-aircraft weapon systems resulted in its insufficient accuracy and timeliness for precise determination of the azimuth, distance, and altitude of the target.

In no-fly zones, apart from anti-aircraft artillery (AAA), MANPADS SA-7 and SA-14 were also used to fire at low-altitude aircraft. In this regard, it should be noted that Iraq did not have more modern MANPADS types like SA-16 and SA-18.

Although in the no-fly zones Iraqi air defense forces were much smaller than around Baghdad and Tirkit, where the main air defense forces were deployed, pilots of allied forces had to be very vigilant and careful. This was mainly due to the tactics of using the anti-aircraft weapon systems, which could unexpectedly appear in the no-fly zones, then open fire on the aircraft and quickly retreat to new positions. According to intelligence data, anti-aircraft systems arrived from the Baghdad region that was 80-100 km away from their operating areas and remained there for no more than two days, after which they returned to the areas of their permanent locations. Only in 2001, the coalition lost nine unmanned aircraft Predator over the territory of Iraq. The last such event took place in the northern part of Iraq in the no-fly zone on December 23, 2002, where the UAV was shot down by an Iraqi fighter.

According to the coalition's assessments, the air defense system in central Iraq was in a similar state of the organization as during the operation Desert Storm. The air defense operations center in Baghdad as well as the zone centers in Tai (central zone), Kirkit (northern zone) and Talili (southern zone) continued to operate. There was also the H-3 western center. These centers had the authority to command dozens of anti-aircraft weapons, SA-2, SA-3, SA-6 missile systems, and artillery systems organized in batteries or battalions. These centers commanded about 60 SAM (SA-2, SA-3, and SA-6) batteries and divisions. For comparison, there were 90 such subunits at the beginning of the Desert Storm. According to some estimates, there were 7,000-7,500 AAA 23mm or larger guns in these subunits (IISS estimates that there were about 6,000 such guns).

It should be noted here that despite the modernization of the command system, it did not have sufficient information capacity. It had just a few means, like KARI, which was produced by THOMSON-CSF (now TALES), before the Desert Storm operation. Despite the fact that 10-12 years ago, this system was difficult to disrupt, it could be effectively disorganized during the Iraqi Freedom.

As a result of extensive post-war control in 1991, as part of sanctions imposed on Iraq, the command decided that all the best anti-aircraft systems would be regrouped into an open zone for flights between 33 and 35 degrees latitude, where they would not be attacked by aviation.

The information that Iraq was in possession of SA-10 or SA-20 air defense systems was not confirmed. Moreover, the Pentagon has not released any information confirming the presence of these systems in Iraq.

It was also recognized that older SAMs: SA-2, SA-3, and SA-6 did not undergo any significant modernization. The reports that Iraq supposedly had a passive detection system, such as the Ukrainian Kolchuga, the Czech Tamara, or Trash Drum / Ramona were not confirmed either.

Conclusion

Air operations in the Persian Gulf during the Operation Iraqi Freedom in 2003 were of different nature to those that took place in 1991 war. They were strategic airstrikes of a sequential nature, which by destroying the highest value targets, consequently weakened the Iraqi defense system. A series of sequential attacks, the so-called "series warfare – sequential attack" on elements of the early warning system, airports, and anti-aircraft systems (missiles launchers and artillery) became the primary objectives. Each of these destroyed targets has opened a way to strike the next one.

Moreover, the Iraqi Freedom operation was carried out by relatively small land forces, with strong air support and significant involvement of the infantry and special forces. It is estimated that it was the first conflict of the 21st century in which the use of all components allowed to achieve a synergy effect.

Once again, the thesis has been confirmed that the best for air strikes (strategic and tactical) are air forces because they allow to achieve political and military goals the fastest, both, by themselves, and in cooperation with other types of armed forces (Zdrodowski & Marciniak, 1998). When assessing the predisposition of the air force to perform strategic attacks during Iraqi Freedom, one should turn attention to the need to have different air platforms with high combat capabilities (Szpyra, 1998).

Operation Iraqi Freedom has broken the standard that only obtaining control in the air is a prerequisite for starting a land or sea operation. In this case, the fight over control in the air was carried out simultaneously to strategic strikes and CAS. Offensive air operations and strategic strikes conducted at the same time as part of the air operations created particularly difficult and complex conditions for the Iraqi air defense system to undertake effective countermeasures. Difficulties in the efficient functioning of the anti-aircraft system stemmed, among other things, from a large number of objects (centers of gravity) in need of a strong shield. The complexity of operations of anti-aircraft forces in case of combined air operation also results from the diverse nature and variety of defended objects (of linear, point, or surface nature), as well as their location. Such a diverse nature, structure and location of centers of gravity requires air defense to have modern reconnaissance, fire, and command systems adequate to the predicted air threat. There are no doubts that only if Iraq had had state-of-the-art anti-aircraft systems, it would have been able to provide an effective defense to the center of gravity. What we mean here is also having the possibility of choosing the optimal method defending the given object, i.e., zone defense, object (direct) defense, or zone-object defense.

According to military experts, other factors also largely contributed to the successes of the coalition forces. One of them was that the defense was carried out in a situation of a disrupted and disorganized command system of the Iraqi armed forces. Moreover, desertations and escapes from the anti-aircraft positions were a big problem.

There are no doubts that the Iraqi air defense system in the first and second war in the Persian Gulf had to face the most modern air weapon systems that had been invented so far. An additional difficulty in its functioning was that it had to act alone without the support of an ally. The outcome of the first and second clash of the Iraqi air defense with the state-of-the-art air technology of the United States and other coalition countries proved to be catastrophic. It confirmed, at the same time, that the Iraqi system was largely an arsenal of outdated means of reconnaissance, command, and combat, which only seemed dangerous and threatening. In fact, it turned out that it was not able to resist modern airpower.

When assessing the course and results of the Second Gulf War, it can be concluded that many other, more technologically and organizationally advanced air defense systems would have survived. However, in all probability, with a better command organization, the Iraqi air defense could have been more efficient.

Despite the specificity of the environment in which the warfare was conducted, one can certainly draw conclusions of a universal nature that should be taken into account in the process of enhancing national air defense systems. It is pertinent especially to the armed forces of countries that have similar anti-aircraft potential. From the Polish perspective, this is important, because especially the armament of the Iraqi anti-aircraft system was, in many respects, analogous to the one we currently have in the Polish armed forces. Analyzing the weaknesses of Iraqi air defense, we have the opportunity to learn about our own shortcomings. In our opinion, both the First and Second Gulf War as well as subsequent military

operations in Libya, Ukraine, and Syria should provide a platform for serious reflection, mainly on choosing a rational development path for the national air defense.

In spite of a lot of sentiment for the S-125, KRUG, KUB or OSA sets, we believe that the currently undertaken "cosmetic" resuscitation attempts to modernize some parts of the anti-aircraft defense system cannot bring the desired results, because often over 30-year-old missiles sets in case of confrontation with modern air forces would never provide an effective defense of the endangered objects, regardless of their nature, type or location. Therefore, in many armed forces, it is necessary to replace outdated anti-aircraft defense weaponry, and it should not be put off in time. In our opinion, we should focus on mobile, multi-channel systems, resistant to interference, and capable of conducting independent (autonomous) operations in any battlefield environment.

References

1. Cordesman, A. H., & Arleigh, A. (2003). *The Lessons of the Iraq War: Main Report*. Washington: Center for Strategic and International Studies.
2. Garamone, J. (2003). *Rumsfeld List Operation Iraqi Freedom Aims, Objectives*. [U.S. Department of Defense]. Retrieved from https://archive.defense.gov/news/newsarticle.aspx?id=29253
3. Grant, R. (2003). *Gulf War II. Air and Space Power Led the Way: An Air Force Association Special Report*. Arlington: Aerospace Education Foundation.
4. Heliński, P. (2003). Strefy zakazane dla lotów w Iraku. *Przegląd Wojsk Lotniczych i OP (marzec)*, 98-112.
5. Kopp, C. (2003), Iraqi Freedom – The Hammer & Anvil. *Australian Aviation (May)*, 25-35.
6. Kuriata, R. (1998). *Obrona przeciwlotnicza w strategicznej operacji obronnej*. Warszawa: AON.
7. MoD [Ministry of Defence]. (2015). *British Air and Space Power Doctrine: AP 3000 Fourth Edition*. Retrieved from http://www.defencesynergia.co.uk/wp-content/uploads/2015/05/RAF-AP3000-Air-Power-Doctrine-4th-edition-2009.pdf
8. Mosley, M. T. (2003). *Operation Iraqi Freedom – By the Numbers: Assessment and Analysis Division.* Retrieved from https://www.comw.org/pda/fulltext/oifcentaf.pdf
9. Radomyski, A. (2009). *Użycie sił obrony przeciwlotniczej w sytuacjach powietrznego uderzenia strategicznego*. Warszawa: AON.
10. Szpyra, R. (1998). *Współczesna wojna powietrzna: Wybrane problemy*. Warszawa: AON.
11. Świniarski, J., & Wiatr, M. (1998). Koncepcje strategiczno-operacyjne. *Myśl Wojskowa, 4*, 47-63.
12. Zdrodowski, B., & Marciniak, M. (1999). *Doktryna powietrzna NATO*. Warszawa: AON.

DEFENSE AND SECURITY

Zhivko St. Yordanov,

EMPIRICAL RESEARCH OF INTERACTION BETWEEN BLGARIAN ARMED FORCES AND OTHER INSTITUTIONS IN THE PROTECTION OF INTERNAL SECURITY

Zhivko St. Yordanov

e-mail: sas_81@abv.bg

Abstract: *The internal security of a country is the most important for national security. That is why an empirical sociological research of the interaction between the armed forces and the other institutions was conducted in interest of the internal security of the Republic of Bulgaria. The subject of the study was the interaction between the various departments as a social relationship between them and their functioning in order to achieve a common goal of protecting the country's internal security.*

Keywords*: National security, Interior security, Counter terrorism, Military, Police, Interaction, Military operation, Police operation, Joint operations, Law, Law Enforcement, Research;*

ЕМПИРИЧНО ИЗСЛЕДВАНЕ НА ВЗАИМОДЕЙСТВИЕТО МЕЖДУ ВЪОРЪЖЕНИТЕ СИЛИ И ОСТАНАЛИТЕ ИНСТИТУЦИИ ПРИ ЗАЩИТА НА ВЪТРЕШНАТА СИГУРНОСТ НА РЕПУБЛИКА БЪЛГАРИЯ

Живко С. Йорданов

Анализът на военните конфликти през последните петнадесет години показва, че те първоначално възникват при наличие на вътрешнодържавна криза, която застрашава сигурността на съответната страна. В последствие, след като държавата се окаже неспособна да се справи с това състояние, кризата лесно прераства във военен конфликт, като не рядко в конфликта се включват и други държави в региона или страни, които имат политически, икономически и други интереси в съответния регион или страна. Това показва, че с нарастващите глобализационни процеси вътрешната несигурност на една страна не остава затворена в рамките на обществото, а често прераства в регионална несигурност, която може да доведе до глобална криза[3], поради което вътрешната сигурност на една страна е от особена важност за нейното нормално съществуване.

Един от най-важните аспекти на защитата на сигурността е взаимодействието между различните структури, ангажирани с нея.[10] За изследване на този проблем в периода от 10.09.2018г. до 19.12.2018г. беше проведено емпирично социологическо изследване на взаимодействието между въоръжените сили и останалите институции в интерес на вътрешната сигурност на Република България. **Обект** на изследването беше взаимодействието между различните ведомства като обществени отношения между тях и тяхното функциониране за постигане на обща цел – защита на вътрешната сигурност на страната. **Целта** на изследването беше да се провери сте-

пента на взаимодействие между различните институции и евентуално да се докаже една от следните работни хипотези:

- съществуват добре урегулирани обществени отношения, с точни правила за взаимодействие, здрави взаимовръзки и ясни правомощия на различните органи в системата;

- не съществуват добре урегулирани обществени отношения, поради което няма точни правила за взаимодействие и ясни правомощия на различните органи в системата;

- съществуват добре урегулирани обществени отношения, с точни правила за взаимодействие, но без здрави взаимовръзки и ясни правомощия на различните органи в системата;

- не съществуват добре урегулирани обществени отношения, поради което няма точни правила за взаимодействие и ясни правомощия на различните органи и въоръжени сили, но въпреки това има изградени взаимовръзки, които значително подпомагат взаимодействието между институциите при изпълнение на съвместни задачи;

Изследването се проведе по методика за провеждане на емпирично изследване, публикувана в сборник с научни трудове с ISBN: 978-954-9681-89-5., която включва в себе си следните основни методи: наблюдение, анкета, беседа (интервю), решаване на тест (въпросник). По време на изследването бяха проверени емпирични индикатори като познаване на нормативната база; познаване на участниците в системата за национална сигурност; познаване на специфичните функции на службите за сигурност; познаване на правомощията на различните органи в системата; познаване на специфичните правомощия на военнослужещите и органите на МВР; съществуване на единни планове; постоянен обмен на информация и съвместимост на комуникационно–информационните системи (КИС) на различните структури; и наличие на единни тактики, техники и процедури и провеждане на съвместни мероприятия по обучение и подготовка. В изследването участваха структури на Въоръжените сили, Министерство на вътрешните работи, Държавна агенция за бежанците, Министерство на транспорта, съобщенията и информационните технологии и др.

Изследването се проведе на три етапа. Първият етап включва провеждане на анкета относно личностните характеристики на анкетираните, за да бъдат причислени към една от фокус групите съгласно методиката. Вторият етап се заключава в провеждане на беседа, в която участниците се приканват да дадат мнение по съответната проблематика, както и да запишат своите реални впечатления и препоръки от работата си с други институции извън ведомствата, в които работят. На третия етап участниците решават въпросник от 39 въпроса, като дават цифрово изражение на основните емпирични индикатори съответно от 1 до 3 или от 1 до 5. След това въпросниците се обработват, като се разделят на три фокус групи, на които отговорите влизат с различен коефициент на истинност в зависимост от опита, реално прослуженото време и реалното участие в съвместни действия (учения, тренировки, операции и т.н.т.). След провеждане на анкетирането и обработката на данните от въпросниците бяха показани следните резултати:

1. Резултати от проведената анкета:

По време на изследването бяха събрани общо 254 /двеста петдесет и четири/ анкетни карти, които бяха разделени в три фокус групи. Във фокус група № 1 съгласно методиката бяха определени 68 /шестдесет и осем/ анкетни карти, на които им беше даден коефициент на истинност 0,5(Kt= 0,5) т.е. данните от техните въпросници следва да бъдат приети с известен резерв. В тази група влизат основно лица, кото никога не са изпълнявали съвместни задачи и/или имат изключително малък професионален опит. Във фокус група № 2 бяха определени 120 /сто и двадесет/ анкетни карти, на които им е даден коефициент на истинност 0,7(Kt = 0,7) т.е. данните от техните въпросници следва да бъдат приети за значително по-достоверни от предходната група. За да по-

паднат лица в тази група е необходимо да имат или голям брой съвместни дейности с други институции, или голям професионален опит, който да им позволява да бъдат запознати със съответната проблематика. В третата фокус група са включени останалите 66 /шестдесет и шест/ анкетни карти на анкетирани, които съчетават в себе си голям професионален опита, участие в съвместни дейности и високо ниво на познаване на теорията и практиката по въпроса на взаймодействието. Поради тази причина коефициента на истинност в техните въпросници е 0,9 (Kt = 0,9).

2. Реузлтати от проведените беседи:

Проведените беседи дадоха конкретни резултати относно взаимодействието между институциите и реалната ситуация относно проблемите, които са възникнали в реални ситуации на ниско тактическо ниво. Голям процент от анкетираните посочват като основен проблем липсата на комуникация между различните институции, непълната съвместимост между свързочните средства – като пример КИС на МО и КИС на МВР, липсата на единни понятия и изключително ограниченият кръг от правомощия на Въоръжените сили и неясните правила за използване на сила от тях при участие в операции по защита на вътрешната сигурност. Така на пример поради този факт по време на груповото нарушаване на обществения ред от бежанци в центъра за настаняване от открит тип в Харманли военнослужещите от механизирания батальон в Хасково са въведени едва на втория ден, а в първия ден докато се чака идването на жандармерия и тежка техника от ЗЖУ–Пловдив в управлението на центъра остават блокирани работещите от ДАБ през целия ден. Освен това служители от центъра, които са участвали в курсове и обучения в други държави споделиха опит, според които някои бежански центрове (от полузакрит и закрит тип) се охраняват от Въоръжените сили (армия, военна полиция) или от съвместни военно–полицейски сили както и факта, че поради културните особености на лицата от Близкия изток и Африка последните имат значително по-голям респект към военните сили от колкото към полицейските сили и частните охранителни фирми. Въпреки това по време на събитията в Харманли е постигнато задоволително ниво на взаимодействие между различните институции, което е довело до бързото овладяване на ситуацията, недопускане на нейното нарастване и разпространение в града и последващо преследване на имигранти на територията на страната.След овладяването на масовите безредици в центъра високото ниво на взаимодействие води до изключително бързото отстраняване на последствията и възобновяване на нормалната работа в центъра за бежанци. Освен това в беседата болшинството анкетирани лица посочиха, че недостига на правомощия, липста на обмен на информация или по-точно недостика на информация до оперативно-дежурните центрове и части, както и голямата централизация на някои дейности в голяма степен затруднява взаимодействието между различните звена, участващи в операция по защита на вътрешната сигурност.

Като цяло по-голямата част от анкетираните, независимо от институцията, в която работят, изразиха своето становище, че са необходими провеждането на повече съвместни мероприятия като занятия, тренировки и учения, по-добра комуникация между различните институции на различните нива, като е необходимо да се подобри разбирането за работата на институциите и в същото време да се определят ясни правила за употреба на сила и да се увеличат правомощията на въоръжените сили за участие в операции по защита на вътрешната сигурност.

3. Резултати от решаване на въпросника:

Решаването на въпросника показа сходни резултати с тези от проведената беседа с участниците в изследването. Чрез въпросника бяха определени емпиричните стойности на различните индикатори съгласно методиката, за да бъде доказана една от четирите хипотези. Според методиката една от четирите хипотези ще бъде доказана при следните стойности на емпиричните индикатори:

- Хипотеза 1 - **ИСТИНА** при : E_1= 5; E_2 = 1; E_3 = 5; E_4 = 1; E_5= 5; E_6= 5v 2; E_7=5; E_8= 5;
- Хипотеза 2 - **ИСТИНА** при : E_1 = 1; E_2 = 2; E_3 = 1; E_4= 2; E_5= 1; E_6= 1v 3; E_7= 1;, E_8= 1;
- Хипотеза 3 - **ИСТИНА** при: E_1 = 5v 4;E_2 = 1v 3; E_3 = 5v 4; E_4= 1v 3;E_5=5v 4;E_6= 1v 3;E_7= 1v 2;E_8= 1v 2;
- Хипотеза 4 - **ИСТИНА** при: E_1 =1v 2;E_2 = 2v 3;E_3 = 1v 2; E_4= 2v 3;E_5=1v 2;E_6= 5v 3;E_7=,5v 4;E_8= 5v 4;

Стойностите на първият емпиричен индикатор за различните фокус групи бяха следните:

ТАБЛИЦА						
С РЕЗУЛТАТИТЕ НА ПЪРВА ФОКУС ГРУПА						
ЗА ЕМПИРИЧЕН ИНДИКАТОР "ПОЗНАВАНЕ НА НОРМАТИВНАТА БАЗА"						
	Отговор №					
Въпрос №	**1**	**2**	**3**	**4**	**5**	Всичко
1	26	5	36			67
2	27	16	15	6	4	68
4	37	3	27			67
7	17	20	21	4	4	66
9	5	19	23	4	14	65
10	19	16	16	11	4	66
Общо:	131	79	138	25	26	399
Общо в %	**32,83**	**19,80**	**34,59**	**6,27**	**6,52**	**100,00**

*Таблица 1: резултати на първа фокус група за емпиричен индикатор **№1***

ТАБЛИЦА						
С РЕЗУЛТАТИТЕ НА ВТОРА ФОКУС ГРУПА						
ЗА ЕМПИРИЧЕН ИНДИКАТОР "ПОЗНАВАНЕ НА НОРМАТИВНАТА БАЗА"						
	Отговор №					
Въпрос №	**1**	**2**	**3**	**4**	**5**	Всичко
1	33	9	76			118
2	38	30	32	10	7	117
4	52	9	56			117
7	19	31	46	10	9	115
9	15	25	31	28	17	116
10	27	26	33	18	11	115
Общо:	184	130	274	66	44	698
Общо в %	**26,36**	**18,62**	**39,26**	**9,46**	**6,30**	**100,00**

*Таблица 2: резултати на втора фокус група за емпиричен индикатор **№1***

ТАБЛИЦА						
С РЕЗУЛТАТИТЕ НА ТРЕТА ФОКУС ГРУПА						
ЗА ЕМПИРИЧЕН ИНДИКАТОР "ПОЗНАВАНЕ НА НОРМАТИВНАТА БАЗА"						
	Отговор №					
Въпрос №	**1**	**2**	**3**	**4**	**5**	Всичко
1	33	5	25			63
2	10	15	16	8	16	65
4	40	5	20			65
7	5	17	21	9	13	65
9	5	10	21	10	19	65
10	10	17	12	6	19	64
Общо:	103	69	115	33	67	387
Общо в %	**26,61**	**17,83**	**29,72**	**8,53**	**17,31**	**100,00**

*Таблица 3: резултати на трета фокус група за емпиричен индикатор **№1***

От таблиците става ясно, че най-голям процент отговори е „**понякога"** или **„не мога да преценя**". След като приложим коефициента за истинност се получават следните резултати:

qт = Qn x Kt			**17,29**		
Qт =	**32,83**	**19,80**	**17,29**	**6,27**	**6,52**

qт = Qn x Kt			**27,48**		
Qт =	**26,36**	**18,62**	**27,48**	**9,46**	**6,30**

qт = Qn x Kt			**26,74**		
Qт =	**26,61**	**17,83**	**26,74**	**8,53**	**17,31**

Таблица 4: резултати на фокус групите след изчисляване на **Qт** *за емпиричен индикатор* ***№1***

Тези стойности се поместват в обобщена таблица (таблица 5), в която се изчислява средната стойност на процента отговори по формулата:

$$(1)\ \mathbf{E_n} = \frac{\mathbf{Q_{T1} + Q_{T2} + Q_{T3}}}{\mathbf{3}} \qquad \mathbf{E_n} \in (1:5)$$

ТАБЛИЦА						
С РЕЗУЛТАТИТЕ НА ПЪРВИ ЕМПИРИЧЕН ИНДИКАТОР E_1						
ЗА ЕМПИРИЧЕН ИНДИКАТОР "ПОЗНАВАНЕ НА НОРМАТИВНАТА БАЗА"						
	ОТГОВОРИ					
	1	2	3	4	5	
Qт1	**32,83**	**19,80**	**17,29**	**6,27**	**6,52**	
Qт2	**26,36**	**18,62**	**27,48**	**9,46**	**6,30**	
Qт3	**26,61**	**17,83**	**26,74**	**8,53**	**17,31**	
	28,60	**18,75**	**23,84**	**8,09**	**10,04**	
E_1 =	**28,60**					**E_1 = 1**

Таблица 5: обобщени резултати за стойността ***E_1*** *за емпиричен индикатор* ***№1***

От стойността на този емпиричен индикатор може да се направи извода, че според анкетираните лица или не съществуват правни норми по въпроса или съществуващите правни норми в нормативните и административните актове не регулират изчерпателно дейностите на институциите за провеждане на съвместни операции по защита на вътрешната сигурност.

По аналогичен начин се изчисляват стойностите на останалите емпирични индикатори. Емпирични индикатори **Е2** и **Е3** показват познаването на ведомствата и учрежденията, които участват в системата за защита на националната сигурност. Докато индикатор **Е2** показват познаването на органите на различните министерства, а индикатор **Е3** показва познаването на специфичните структури като службите за сигурност в Република България. Обобщените стойности на тези индикатори са показани в следните таблици:

ТАБЛИЦА						
С РЕЗУЛТАТИТЕ НА ВТОРИ ЕМПИРИЧЕН ИНДИКАТОР E_2						
ЗА ЕМПИРИЧЕН ИНДИКАТОР "ПОЗНАВАНЕ НА УЧАСТНИЦИТЕ В СНС"						
	ОТГОВОРИ					
	1	2	3	4	5	
Qт1	**39,39**	**14,02**	**23,30**			
Qт2	**41,70**	**10,64**	**33,36**			
Qт3	**56,12**	**6,84**	**30,80**			
	45,74	**10,50**	**29,15**			
E_2 =	**45,74**					**E_2 = 1**

*Таблица 6: обобщени резултати за стойността **E_2** за емпиричен индикатор **№2***

ТАБЛИЦА						
С РЕЗУЛТАТИТЕ НА ТРЕТИ ЕМПИРИЧЕН ИНДИКАТОР E_3						
ЗА ЕМПИРИЧЕН ИНДИКАТОР "ПОЗНАВАНЕ НА СЛУЖБИТЕ ЗА СИГУРНОСТ"						
	ОТГОВОРИ					
	1	2	3	4	5	
Qт1	**19,07**	**14,43**	**15,21**	**11,34**	**24,74**	
Qт2	**12,28**	**12,87**	**23,05**	**17,37**	**24,10**	
Qт3	**8,63**	**5,58**	**14,21**	**12,69**	**52,99**	
	13,33	**10,96**	**17,49**	**13,80**	**33,95**	
E_3 =					**33,95**	**E_3 = 5**

*Таблица 7: обобщени резултати за стойността **E_3** за емпиричен индикатор **№3***

От стойностите на тези емпирични индикатори може да се направи извода, че анкетираните лица познават институциите и техните органи, които участват в защита на вътрешната сигурност на Република България като познават не само основните министерства и ведомства, а и службите за сигурност в страната. Следователно с това е изпълнено едно от основните изисквания на взаимодействието–взаимно познаване между взаимодействащите структури[2].

Следващите два индикатора **E_4** и **E_5** определят до колко анкетираните познават правомощията на различните институции, както основните правомощия на въоръжените сили, органите на МВР, различните агенции в Министерство на транспорта и други така и на специфичните правомощия на различните институции. Техните стойности са показани в следващите две таблици:

ТАБЛИЦА						
С РЕЗУЛТАТИТЕ НА ЧЕТВЪРТИ ЕМПИРИЧЕН ИНДИКАТОР E_4						
ЗА ЕМПИРИЧЕН ИНДИКАТОР "ПОЗНАВАНЕ НА ПРАВОМОЩИЯТА..."						
	ОТГОВОРИ					
	1	2	3	4	5	
Q_{T1}	**20,75**	**19,00**	**39,50**			
Q_{T2}	**30,71**	**17,09**	**39,03**			
Q_{T3}	**51,89**	**19,39**	**22,96**			
	34,45	**18,49**	**33,83**			
E_4 =	**34,45**					**E_4 = 1**

*Таблица 8: обобщени резултати за стойността **E_4** за емпиричен индикатор **№4***

ТАБЛИЦА						
С РЕЗУЛТАТИТЕ НА ПЕТИ ЕМПИРИЧЕН ИНДИКАТОР E_5						
ЕМПИРИЧЕН ИНДИКАТОР "ПОЗНАВАНЕ НА СПЕЦИФИЧНИТЕ ПРАВОМОЩИЯ"						
	ОТГОВОРИ					
	1	2	3	4	5	
Q_{T1}	**18,33**	**21,95**	**14,59**	**14,48**	**16,06**	
Q_{T2}	**12,96**	**19,31**	**24,07**	**16,14**	**17,20**	
Q_{T3}	**8,92**	**14,42**	**28,15**	**19,45**	**26,16**	
	13,40	**18,56**	**22,27**	**16,69**	**19,80**	
E_5 =			**22,27**			**E_5 = 3**

*Таблица 9: обобщени резултати за стойността **E_5** за емпиричен индикатор **№5***

Стойностите на тези емпирични индикатори показват, че законите на страната дават основни правомощия на различните структури и техните органи, но не дават достатъчно правомощия за изпълнение на специфичните задачи по защита на вътрешната сигурност. Освен това понякога нормативната база позволява дублиране на правомощия и вменяване на задачи, които не са от ресора на съответното ведомство.

Останалите емпирични индикатори **E_6**, **E_7** и **E_8** имат пряко отношение към взаимодействието между институциите и техните органи на ниско ниво. Индикатор **E_6** показва дали има налични съвместни планове между отделните институции за извършване на съвместни дейности при различни кризи за защита на вътрешната сигурност. Стойностите на индикатора са определени в следната обобщена таблица:

ТАБЛИЦА						
С РЕЗУЛТАТИТЕ НА ПЕТИ ЕМПИРИЧЕН ИНДИКАТОР E_6						
ЗА ЕМПИРИЧЕН ИНДИКАТОР "НАЛИЧИЕ НА ЕДИННИ ПЛАНОВЕ"						
	ОТГОВОРИ					
	1	2	3	4	5	
Q_{T1}	**28,63**	**16,79**	**21,95**	**5,34**	**5,34**	
Q_{T2}	**26,54**	**17,76**	**32,70**	**4,61**	**4,39**	
Q_{T3}	**34,48**	**8,81**	**38,28**	**5,75**	**8,43**	
	29,88	**14,46**	**30,97**	**5,23**	**6,05**	
E_6 =			**30,97**			**E_6 = 3**

*Таблица 10: обобщени резултати за стойността **E_6** за емпиричен индикатор **№6***

Според този индикатор няма разработени планове между различните институции и техните органи, или ако има такива то анкетираните лица не са чували за тях. Като обобщение може да се посочи, че съвместен план се изготвя непосредствено преди конкретна операция, при което подчинените звена нямат достатъчно време и възможност да отработят дейностите по съответните планирани мероприятия.

Емпиричния индикатор $\mathbf{E_7}$ показва до каква степен има обмен на информация между различните ведомства и до колко КИС на различните ведомства са съвместими по между си. Резултатите на този индикатор са поместени в следната таблица:

ТАБЛИЦА						
С РЕЗУЛТАТИТЕ НА ПЕТИ ЕМПИРИЧЕН ИНДИКАТОР E_7						
ЕМПИРИЧЕН ИНДИКАТОР "ПОСТОЯНЕН ОБМЕН НА ИНФОРМАЦИЯ"						
	ОТГОВОРИ					
	1	2	3	4	5	
Qт1	**20,08**	**18,94**	**15,72**	**13,26**	**16,29**	
Qт2	**19,07**	**16,19**	**22,84**	**18,40**	**16,45**	
Qт3	**18,39**	**8,05**	**22,61**	**16,09**	**31,38**	
	19,18	**14,39**	**20,39**	**15,92**	**21,37**	
E_7 =					**21,37**	**E_7 = 5**

*Таблица 11: обобщени резултати за стойността **E_7** за емпиричен индикатор **№7***

Според стойността на този индикатор съществува постоянен обмен на информация между институциите и техните КИС са напълно съвместими. При резултатите на този индикатор наблюдаваме две аномалии. Първата аномалия е, че според въпросника съществува постоянен обмен на информация между органите на различните ведомства, а според данните от беседата обаче това не е така. Според беседата оперативните дежурни не само че не разполагат с цялата информация за дейностите на външните ведомства, а дежурните на различните ведомства почти не комуникират по между си освен при крайна нужда. Втората аномалия е, че докато според въпросника КИС са напълно съвместими, то според беседата КИС на различните ведомства изобщо не са съвместими. За да се определи кое е вярното твърдение на въпросника или резултатите от беседата следва да се прибегне до резултат от наблюдението на ведомствата и техните органи. Резултатите от наблюдението показват, че оперативните дежурни части и центрове не само че не обменят информация по между си, а често дори и не знаят конкретен начин за свръзка между тях. Това се потвърждава от някои случаи, при които наряди от различни ведомства оперират в един и същ район, но поради липса на информация започват да си пречат по между си. Относно съвместимостта на КИС е ясно, че различните системи са съвместими, но не на пълно.Това се обуславя от факта, че за да се свържат две свързочни средства от две различни системи по между си е необходимо да се прибегне до въвеждането на предварителен код за изход от съответната КИС или предварително трябва да се обменят радиочестоти в съответния УКВ или КВ диапазон и съответните позивни. Относно съвместимостта на КИС може би е възникнало заблуждение поради факта, че е възможно с щатните комуникационни средства на едно ведомство, при предварителна подготовка, да се свържем със съответните щатни средства на друго ведомство. Освен това съществуват инструкции като Инструкция № М-3 от 18 юли 2011 г. за взаимодействие между Министерството на отбраната и Министерството на вътрешните работи, обн. ДВ. бр.60 от 5 август 2011 г., изм. и доп. ДВ. бр.15 от 24 февруари 2015 г. и Инструкция № И-1 от 07 януари 2013 г. за условията, реда и организацията на взаимодействието между Военната полиция и структурите на Министерството на вътрешните работи, Обн. ДВ, бр. 7 от 25.01.2013 г., в сила от 25.01.2013 г. издадена от министъра на отбраната и министъра на вътрешните работи, които задължават ве-

домствата да обменят информация както между оперативно-дежурните центрове и части на високо ниво така и между оперативните дежурни на местно (областно и общинско) ниво.

Последният индикатор $\mathbf{E_8}$ показва наличие на единни тактики техники и процедури за общи действия при операции за защита на вътрешната сигурност на Република България както и провеждане на съвместни занятия, учения и тренировки. Обобщените стойности за този индикатор са показани в следващата таблица 12:

ТАБЛИЦА						
С РЕЗУЛТАТИТЕ НА ПЕТИ ЕМПИРИЧЕН ИНДИКАТОР E_8						
ЕМПИРИЧЕН ИНДИКАТОР ЕДИННИ ТАКТИКИ, ТЕХНИКИ И ПРОЦЕДУРИ						
	ОТГОВОРИ					
	1	2	3	4	5	
Q_{T1}	**25,93**	**21,61**	**18,76**	**10,02**	**4,91**	
Q_{T2}	**23,54**	**25,96**	**24,33**	**10,01**	**5,72**	
Q_{T3}	**25,86**	**26,86**	**24,71**	**13,50**	**6,08**	
	25,11	**24,81**	**22,60**	**11,18**	**5,57**	
$\mathbf{E_8}$ =	**25,11**					$\mathbf{E_8 = 1}$

Таблица 12: обобщени резултати за стойността $\boldsymbol{E_8}$ *за емпиричен индикатор* ***№8***

Резултатите на този индикатор показват, че не се провеждат достатъчно съвместни мероприятия като занятия, учения и тренировки между отделните институции. Освен това няма уеднаквени тактики, техники и процедури за еднакви действия. Това води до липсата на здрави взаимовръзки между различните институции и техните органи и изключително затруднява взаимодействието между тях. Следователно при провеждане на съвместни мероприятия обикновенно тактиките, техниките и процедурите се определят на място от ръководителите на групи и екипи.

Следователно емпиричните индикатори имат следните цифрови стойности:

$\mathbf{E_1 = 1; E_2 = 1; E_3 = 5; E_4 = 1; E_5 = 3; E_6 = 3; E_7 = 5; E_8 = 1;}$

Стойностите на индикаторите най-много се доближават до третата хипотеза а именно: **съществуват добре урегулирани обществени отношения, с точни правила за взаимодействие, но без здрави взаимовръзки и ясни правомощия на различните органи в системата.** Два емпирични индикатора обаче не отговарят на тази хипотеза, това са индикатори $\mathbf{E_1}$ и $\mathbf{E_7}$. За да бъде хипотеза 3 напълно изпълнена стойностите на на тези индикатори трябва да бъдат $\mathbf{E_1=4 \vee 5,}$ а $\mathbf{E_7=1 \vee 2,}$ т.е. нормативните и административните актове в Република България изчерпателно уреждат въпросите на взаимодействието и съответните органи познават своите правомощия, но въпреки това КИС не са съвместими по между си и няма обмен на информация между отделните институции. Резултатите от въпросника за съответните емпирични индикатори показват точно обратното или като стойности $\mathbf{E_1 = 1}$ и $\mathbf{E_7 = 5.}$ Като се вземе предвид резултатите от въпросника и резултатите от проведената беседа и като се съпоставят с резултатите от проведеното наблюдение върху институциите и техните органи участващи в системата за защита на националната сигурност може да се направи извода, че съществуват нормативни и административни актове, които регулират тези обществените отношения свързани с взаимодействието но тази регулация не е изчерпателна и не позволява ясно дефиниране на различните правомощия на институциите при изпълнение на съвместни задачи, а КИС на различните ведомства не е напълно съвместима, а обмена на информация е в изключително ограничен обем, който често пъти е недостатъчен за изпълнение на съвместните задачи.

От изложените до тук факти може да се направи извод, че съществуват изградени обществени отношения по силата на правни норми, които обаче не са изчерпателно урегулирани, поради което липсват ясни и точни правила за взаимодействие, поради което липсват и здрави взаймовръзки между различните органи в системата.

References

1. ГОЦЕВ, Г. (2012). *Защита на сигурността и обществения ред*: *Учебник за студенти*. София: Академия на МВР. ISBN 978-954-348-082-1;
2. ГОЦЕВ, Г. (2016). *Защита на сигурността и общественият ред*, София: ВТИ,. ISBN 978-619-90682-0-5.
3. ГЕОРГИЕВ, Х. (2011). *Политика на сигурност на Република България в началото на 21 век: теоретични и приложни аспекти*, София: ISBN: 9789545356926;
4. ДЕЛИБЕЕВ, И. (1987). *Теория и методи на емпиричното социологическо изследване*, София: БКП.
5. КОСТАДИНОВ, К. (2018) *Теоретични основи на оперативното използване на ВМС*, София: ВА. ISBN 978-619-7478-12-9;
6. МИХАЙЛОВ, С. (1980). *Емпирично социологическо изследване*, София:
7. МС: *Инструкция № М-3 от 18 юли 2011 г. за взаимодействие между Министерството на отбраната и Министерството на вътрешните работи*, обн. ДВ. бр.60 от 5 август 2011, изм. и доп. ДВ. бр.15 от 24 февруари 2015 г;
8. МО и МВР: *Инструкция № И-1 от 07 януари 2013 г. за условията, реда и организацията на взаимодействието между Военната полиция и структурите на Министерството на вътрешните работи,* Обн. ДВ, бр. 7 от 25.01.2013 г., в сила от 25.01.2013 г. Издадена от министъра на отбраната и министъра на вътрешните работи
9. РАДИЛОВ, Д., КОСЕВА, Д. & РУСЕВ, Ч. (1996) *Въведение в статистиката*, Варна: ТедИна.
10. СТОЯНОВ, Н. (2017) *Рискове и заплахи за сигурността на водната транспортно-преносна система*. Варна: Тера Балканика. ISBN 978-619-90844-0-3.

Atanas St. Atanasov,

TYPES OF EFFECTS IN JOINT OPERATIONS

Atanas St. Atanasov

ВОЕННА АКАДЕМИЯ "ГЕОРГИ СТОЙКОВ РАКОВСКИ"
СОФИЯ – 1504 БУЛ."ЕВЛОГИ И ХРИСТО ГЕОРГИЕВИ" № 82
КАТЕДРА "СУХОПЪТНИ ВОЙСКИ"

Abstract: *The report encompasses the main types of effects which are planned to be achieved in joint operations.*

***Keywords**: effects, artillery, joint operations.*

ВИДОВЕ ЕФЕКТИ В СЪВМЕСТНИТЕ ОПЕРАЦИИ

Атанас Ст. Атанасов

Въведение

Връзката между процеса на съвместно определяне на целите с желаните ефекти и от там с изпълняваните задачи за поддържане на плана на операцията, поставя ударението върху повишаване на способността да се въздейства върху поведението на противника и/или способностите му, чрез интегрирано прилагане на ударната и огневата мощ на съвместните сили или чрез прилагане на други средства (кинетични или некинетични) водещи до постигането на определени резултати, а именно промяна в поведението на противника в желаната посока и в определени ситуации до постигане на целите на операцията (кампанията). Този подход свързва оперативните и стратегически цели с оперативните и тактически ефекти за изпълнение на определени задачи, чрез определяне на желаните и нежелани ефекти в оперативната обстановка и поставя задачи на подчинените за постигането на ефектите чрез въздействие върху определени цели. Най-общо, мисленето, основано на постигане на ефектите е да се осигури логична последователна прогресия, като подкрепа към процеса на планиране на операцията, която в последствие да се развитие при вземането на решенията и поставянето на задачи към подчинените за постигане на оперативните цели.

Определянето на необходимите ефекти е дейност, която се извършват от групата за планиране и управление на съвместните ефекти в щаба на съвместните сили с цел да се подпомогне командващия в процеса на анализа на мисията и разработване на концепцията на операцията, като най-пълно този процес се вписва в разработваната концепция за огневата поддръжка и се проектира в разработваните списъци с целите за въздействие до подчинените щабове. Такива процеси протичат и в компонентните командвания и в маневрените формирования, където се прилагат определени процедури и техники за определяне на целите, тяхното разпределение за въздействие между средствата за огнева поддръжка и средствата с несмъртоносен ефект.

Съгласно доктрината за планиране на операциите (НП-5) под ефект се разбира „Промяна на поведението или физическото състояние на системата (или на елемент от системата) в резултат на едно или повече действия.

Ефектът позволява да се интегрира резултатът от различни действия (способности), провеждани от различни субекти. Това е ядрото на всеобхватният подход. Или с други думи ефекта е:

- Физическо и/или поведенческо състояние на системата, като резултати от действието, комплексността от действия или от други ефекти.
- Промяна на състояние, поведение или степента на свобода на системата.

Ефектите играят решаваща роля, защото те определят фокуса на действията и допринасят за постигане на целите и желаното крайно състояние. Действията имат за цел създаването на ефекти, които да водят както до промени в способностите, поведението или вариантите за отговор (действие на участниците в рамките на оперативната среда), така и в стратегическата среда. Ефектите могат да бъдат групирани в две категории – физически и нефизически (ментални/поведенчески). Независимо, че всички физически ефекти водят до някаква форма на нефизически ефекти, тяхната основна цел е оказване на влияние върху способностите на участниците.

Нефизическите ефекти по принцип са насочени към поведението на страните. Измененията в поведението или физическото състояние на дадена система (или на елементите ѝ), които са резултат от едно или повече действия или други причини, и могат да бъдат категоризирани, както следва:

- Желани ефекти – тези, които влияят положително на постигането на целите.
- Нежелани ефекти - тези, които прекъсват или застрашават постигането на крайните цели и като такива следва да бъдат намалявани (смекчавани).

Желаният ефект представлява условие за постигане на свързана цел, докато нежеланият ефект може да възпрепятства напредъка към същата цел. Ефектите и придружаващите ги причинно-следствени връзки свързват задачите с целите. Задачите и последиците във всяка причинно-следствена верига могат да произтичат от всеки елемент на националната мощ - дипломатически, информационен, военен или икономически - и може да възникне във всеки един момент от цялата военна операция. Една единствена цел може да изисква създаването на повече от един ефект.

Много от начините и средствата, свързани с процеса на съвместно определяне и поразяване на целите (СОПЦ) и използването на резултатите от поразяването (въздействието), водят до тактически ефекти спрямо избраните цели. Въпреки това, кумулативните резултати от тези целеви въздействия могат да допринесат за постигането на желаните оперативни нива и стратегически ефекти от съвместните сили (СС).

Командирът, който е отговорен за планирането на поразяването (въздействието) на целите в системата на СОПЦ, трябва да разбере не само конкретните желани целеви ефекти, но също така и целта и въздействието на поразяването на определените цели по отношение на създаването на желаните ефекти на старшият командир от СС и избягване на нежеланите ефекти. Командващият и щаба на СС трябва да обмислят нежелани ефекти при разработването на вариантите за действие и концепцията на операцията (КОНОП). Оперативните ограничения и ограниченията на СС и компонентите могат да бъдат коригирани, за да се предотвратят нежелани ефекти. Важно е желаните и нежелани ефекти да бъдат ясно съобщени, доколкото е необходимо, за да се гарантира, че тези ефекти се създават или избягват съответно. Правилното разбиране на връзката между ефектите на всички нива е важно за планирането и провеждането на всяка съвместна операция.

- Очаквани ефекти - тези, които са предварително определени и за които се предвижда да възникнат в резултат от определени действия;
- Неочаквани ефекти – тези, за които не се предвиждат да бъдат свързани с целите и предприетите действия и които могат да бъдат както желани, така и нежелани.

Ефектите могат да бъдат категоризирани по много начини. Едно важно разграничение е между преките и косвени ефекти.

- Преките ефекти са непосредствените последствия от военни действия (резултати от използването на оръжия и т.н.), които не се променят чрез събития или механизми. Те обикновено са незабавни и лесно разпознаваеми. Всеки войник е запознат с директното въздействие на своето оръжия. Противотанкистът знае, че снаряда, изстрелян от оръдието, генерира лесно разпознаваем директен физически ефект, когато прониква през защитна броня на вражеския танк и видимо изхвърля купола му във въздуха. По същия начин, преките последици от разхвърлянето на брошури могат да доведат до предаването на противниковите войници или увеличеното участие на местното население в изборите, но преди да се стигне до това заключение трябва да се направи повече от една оценка, тъй като други фактори могат да причинят противоречиво поведение. По същия

начин, прекият ефект от заглушаването може да бъде, че клетъчните телефони или други комуникационни устройства са неизползваеми от терористите, но този ефект няма да бъде незабавно наблюдаван и не трябва да се приема, че се случва без съответните достоверни доказателства. Обикновено този ефект се търси при заглушаване на устройствата с цел избягване на дистанционно задействане на импровизирани взривни устройства при преминаван на конвой или VIP лица през зона с увеличен риск.

• Косвените ефекти са забавените или изместени последствия от действие от втори, трети и по-висок ред, създадени чрез междинни събития или механизми. Тези ефекти могат да бъдат от физически или поведенчески характер. Косвеното въздействие може да бъде трудно да се разпознае, поради незначителни промени в поведението на системата, които могат да ги затруднят при наблюдението. Например, косвен ефект от унищожаване на комуникационен възел или задържане на куриер може да бъде, че това предотвратява командването и управлението на противниковите сили или лидери на терористични клетки и намалява тяхната ефективност срещу собствените сили; ефекти с реални ползи, които обаче трудно се измерват.

Ефектите от първи ред са тези които се появяват в резултат на прякото въздействие върху целта (поразяването на арт.батарея води до неутрализирането на целта за определен период. Пряк ефект – батареята не води огън. Или финансово подпомагане на определен член на групировка, го вербува за каузата на операцията). Примери за преки ефекти можем да открием в AArtyP-5 NATO FIRE SUPPORT DOCTRINE, а именно – неутрализиране, унищожаване, потискане, отклоняване, възпиране, канализиране, блокиране и т.н.

Ефектите от втори ред се появяват в резултат на невъзможността от изпълнението на задачите от целите/ефектите от първи ред (маневреното формирование не може да си изпълни задачата в следствие на поразената артилерийска батарея. Или решението за прекратяване на определена дейност е в следствие на въздействието оказано от вербуваният член)

Ефектите от трети ред са ефектите появили се вследствие от ефектите от втори ред (неизпълнението на задачата от маневреното формирование води до възможност за прегрупиране на собствените формирования, а от там до създаване на условия за изпълнение на други задачи. Или прекратяването на дейността на организацията създава условия за преминаване към началото на преговори)

Ефектите от втори и трети ред се явяват непреки ефекти, а когато са обвързани последователно стават каскадни ефекти.

Връзката между преките и косвените ефекти може да се види и в примера на атака срещу вражеската система за командване и управление. Унищожаването на един-единствен комуникационен възел чрез електронно подавяне или физическо унищожаване създава пряк ефект - този специфичен комуникационен възел е унищожен или престава да функционира. Косвеният резултат (непряк ефект) на множество удари срещу редица подобни и свързани цели може да доведе до постигането на истинската цел на планиращите - да подкопае способността на противниковият командир да командва ефективно военните сили. Както беше отбелязано по-рано, косвените ефекти обикновено се проявяват във времето и може да отнеме неопределен период от време, преди цялостната липса на комуникации да има вредно въздействие върху противника. Като цяло, комбинацията от преки и непреки ефекти може да постигне крайната цел на всяко действие - да принуди или да формира желания резултат.

• Кумулативни ефекти. Ефектите са склонни да се образуват, така че крайният резултат от редица преки ефекти е най-често по-голям от сумата на техните непосредствени последствия. По същия начин косвените ефекти често се съчетават, за да произвеждат по-големи ефекти от сумата на техните индивидуални последствия. Това може да се случи на всички нива, тъй като се постигат ефектите от по-нисък ред.

• Каскадни ефекти. Каскадните ефекти могат да се преплитат чрез целева система, често влияеща и на други системи; най-често чрез възли и връзки, които са общи и критични за съответните системи. Каскадните ефекти могат да са резултат и от преки въздействия. Каскадирането на преките и косвените ефекти, както подсказва името, обикновено преминава от по-високи към

по-ниски нива. Например, унищожаването на елемент от щаба или залавянето на висш лидер на терористична организация ще доведе до загуба на командване и управление и по този начин ще влоши ефективността на подчинените организации.

• Съпътстващи ефекти. Ефекти от поразяването на целите често се разпространяват, за да се създадат свързани ефекти, известни като съпътстващи ефекти или загуби, неволно или случайно нараняване или увреждане на лица или предмети, които не биха били законосъобразни военни цели при обстоятелствата, които са били в момента. Подобна загуба не е незаконна, доколкото тя не е прекомерна в светлината на общото военно предимство, предвидено от поразяването. Такива загуби могат да възникнат на собствени, неутрални и дори противникови сили. В такъв случай оперативните и стратегическите ефекти на СС и свързаните с тях странични ефекти обикновено не се отразяват като загуба, а като други видове резултати, които планиращите могат или не могат да очакват.

Съпътстващите ефекти често се разпространяват, за да създадат непредвидени последици, обикновено под формата на нараняване или увреждане на хора или предмети, които не са свързани с целите. В по-широк смисъл съпътстващите ефекти са всички ефекти, постигнати извън тези, за които е предприето действието, и могат да бъдат положителни или отрицателни за намерението на планиращите. В отрицателен смисъл, съпътстващите ефекти могат да бъдат случайни преки или косвени последици, които причиняват неволно и нежелано нараняване или увреждане на хора или предмети. Положителните съпътстващите ефекти могат да доведат до резултати, които да са от полза за продължаващите военни действия. Крайният резултат е, че планираните ефекти от първи ред неизменно ще генерират съпътстващите ефекти, които са нежелани или неочаквани. Важно е да се прави разлика между съпътстващи и странични ефекти. Разумното планиране следва да позволи отчитането на рисковете от непредвидени ефекти от втори и трети ред. Съпътстващите ефекти следва да бъдат основно, целево разглеждани при планирането, изпълнението и оценката на военните действия от всякакъв мащаб.

Освен като преките и косвени ефектите могат да бъдат категоризирани по начина на въздействие като смъртоносни и несмъртоносни.

• Използването на оръжейните системи могат да предизвикат смъртоносни и несмъртоносни въздействия върху целта. Смъртоносните ефекти се получават чрез някаква комбинация от взрив, фрагментация и кинетично проникване в избраната цел при което се получава летален изход. Освен с оръжейни системи този резултат може да се постигне и с други средства- некинетични (трябва да се прави разлика между смъртоносни и несмъртоносни и кинетични и некинетични. Не винаги кинетичните са смъртоносни както и не винаги некинетичните са несмъртоносни). Макар и изключително ефективни по предназначение, смъртоносните ефекти не винаги могат да бъдат подходящи за цялата военна операция.

Например, по време на военни действия, сътрудничество в областта на сигурността и операции за възпиране, прилагането на смъртоносни ефекти обикновено е силно ограничено и формированията могат да се ограничат до използване само на отбранителен огън. Използването на смъртоносни начини и средства по време на съвместни операции може да бъде ограничено от ограниченията в правилата за поведение. Командващият на СС може също да се наложи да обърне внимание на опасенията за причиняване на нежелани жертви сред некомбатантите и причиняване на съпътстващи щети на инфраструктурата и съоръженията, които ще са необходими за функционирането по време на другите фази на операцията (стабилизиране) . Тези опасения могат да бъдат разрешени чрез използване на несмъртоносни (нелетални) ефекти.

• Несмъртоносните ефекти като тези, произведени чрез електронна война, компютърна мрежова атака и определени насочени енергийни оръжия, се използват и могат да постигнат цели във всички военни операции и на всички нива на война. Те водят до невъзможност за използването на щабовете или определени съоръжения, като същевременно свеждат до минимум смъртните случаи, трайните увреждания на личния състав и нежеланото увреждане на собствеността и околната среда. Способността да произвежда несмъртоносни ефекти предоставя на командващият на СС редица гъвкави целеви решения. Мащабируемостта, избираемостта и способността за

реагиране на несмъртоносни способности предоставят на Командващият на СС средствата за въздействие към определени лица; неутрализиране или отхвърляне на използването от противника на целеви съоръжения без унищожаване. Несмъртоносните ефекти могат също да се използват за допълване на смъртоносните такива чрез приоритизиране или канализиране на враждебни сили в предварително избрани зони на поразяване. Те могат също така да допълнят или да предложат алтернатива на използването на високоточни боеприпаси, когато е необходимо предотвратяване на последиците от странични щети.

Използването на ефекти при планиране на операциите спомага за приоритизиране на усилията за постигане на политическите и стратегическите цели на държавата, като и за ефикасно разпределяне на ресурсите. Правилното определяне на ефектите е възможно само чрез добро познаване на кризисната ситуация, основните субекти и културните аспекти на средата, в която ще се провежда дадена операция. Ефектите трябва да бъдат измерими, ограничени по брой и неделими.

Ефектите трябва да бъдат формулирани по такъв начин, че ясно да представят промяна в поведението на противника или в промяната на способностите или състоянието на дадена система. Планиращите експерти трябва да са наясно, че за постигането на определени ефекти може да е необходимо продължително време. Задълбоченото разбиране на оперативната среда позволява да се определи кои ефекти ще бъдат създадени бързо и кои не. Неправилното разбиране на сроковете необходими за създаване на различни ефекти, води до чести, а някои случаи и до ненужни промени в плана.

За да се оценят ефектите следва да се въведат и съответните критерии за ефективност. Целта на критерия за ефективност е да бъдат описани конкретните промени в поведението или способностите на дадена система или подсистема, за да може да се определи дали желаните ефекти се постигат, или не се постигат. Затова командира трябва да определи критерии за ефективност за всеки ефект, за да може да се установи дали операциите създават желаните ефекти, или водят до нежелани последствия, които биха могли да изложат на опасност постигането на целта или изпълнението на мисията. Критериите за ефективност са много важни, защото тяхното прилагане при оценяване на напредъка може да повлияе на бъдещите решения относно провеждането на операции и разпределението на ресурси.

Използвана литература:

1. Доктрина за планиране на операции (НП-5).
2. Iliev, K. Nature and characteristics of the collateral damage. *International Scientific Conference*, collection of papers, 2015, pp 135-142, ISSN 2367-7902.
3. Stanchev S., Iliev, K. Methodology to reduce collateral damage. *International Scientific Conference*, collection of papers, 2015, p. 380 – 391, ISBN - 2367 – 7902.
4. Ръководство за планиране на операции, Част II – оперативно ниво
5. AArtyP-5 NATO FIRE SUPPORT DOCTRINE Edition B Version 1 NOVEMBER 2015
6. AJP-3.9 ALLIED JOINT DOCTRINE FOR JOINT TARGETING

Atanas St. Atanasov,

NEW ARTILLERY SYSTEMS AND CONCEPTS FOR USE OF ARTILLERY

Atanas St. Atanasov

ВОЕННА АКАДЕМИЯ "ГЕОРГИ СТОЙКОВ РАКОВСКИ"
СОФИЯ – 1504 БУЛ."ЕВЛОГИ И ХРИСТО ГЕОРГИЕВИ" № 82
КАТЕДРА "СУХОПЪТНИ ВОЙСКИ"

Abstract: *The report analyzes the need to change perceptions of the use of artillery generated by changing the technical capabilities of artillery systems. Attempts have been made to substantiate certain views on the use of artillery in the interests of performing tactical and fire tasks. The main point of the report is that it is not the technical capabilities of the systems that underlie the alignment of the battle order, but the commander's decision making on how to use the means of fire support.*

НОВИТЕ АРТИЛЕРИЙСКИ СИСТЕМИ И СХВАЩАНИЯТА ЗА ИЗПОЛЗВАНЕ НА АРТИЛЕРИЯТА

Атанас Ст. Атанасов

Въведение

Настъпилите демократични промени доведоха до постепенното съкращаване на армията, и респективно до съкращаване на артилерийските структури и броя на артилерийските системи. Идеята за изграждането на армия от нов тип (малка - но мобилна и с висок боен потенциал), показа необходимостта от преосмисляне на възгледите за количеството и качеството на артилерийските системи. В тази връзка предприетите промени за създаването на бригадни (батальонни) бойни групи постави като изискване, в маневрените формирования да се поставят мобилни и скорострелни артилерийски системи с автоматизирани системи за управление на огъня, за осигуряване на непрекъсната поддръжка на дълбочината на изпълняваната задача. Тежките буксирни артилерийски системи, както и реактивната система БМ 21 бяха изведени в състава на артилерийския полк.

На базата на приетите стандарти на НАТО по отношение на далекобойността на системите (осигурява непосредствена огнева поддръжка на маневрените формирования на дълбочина 40 км., и използване на съвременни артилерийски бойни припаси при всякакви климатични условия и способност за произвеждане на псевдозалп), както и възможността за интегрирането на артилерията в системата за огнева поддръжка с „Обща оперативна картина" и сухопътната разузнавателна (ISTAR) система, с възможност за интерфейс между „Съвместен център за координиране на огъня" и „Център за осигуряване на съвместен удар" и разпределение на целите до съответните средства за поразяване постави като изискване да се вземе решение за замяна на сега съществуващите артилерийски системи с нови или да се модернизират съществуващите. Към настоящият момент се предвижда за артилерията за непосредствена поддръжка в състава на маневрените формирования да се заменят сегашните 122 мм. системи с далекобойност 15 км., със системи с калибър 155мм, които да изпълнят изискванията на стандартизационните документи.

За артилерията за обща огнева поддръжка се предвижда модернизиране на системите БМ 21 чрез увеличаване на далекобойността на системите на 40 км и внедряване на система за управление на огъня, като на следващ етап може да се говори и за придобиване на нови системи, като едно от изискванията е далекобойния реактивен дивизион да осигурява съсредоточена огнева поддръжка на разстояние над 70 km, която трябва да бъде допълнително увеличена, чрез използването на специални ракети с далекобойност над 150 km.

По отношение на средствата за разузнаване целите са насочени към придобиване на нови разузнавателни средства като за артилерията за непосредствена поддръжка това са комбинирани прибори за разузнаване с дълбочина на засичане на целите 10-15 км с повишени характеристики по отношение възможностите им за интегриране в система за управление на огъня, а за артилерията за обща поддръжка съответно средства за разузнаване от типа на радиолокационни станции за контрабатарейна борба, и комплекси за звуково разузнаване, които да имат възможности за разузнаване за артилерийския звукометричен комплекс да покрива зона с размери 120 km x 30 km, а за радиолокационните станции за откриване на стрелящи системи да определят местоположението на цели на разстояние от 40 km или повече спрямо собствената позиция. На базата на тези съвременни постановки ще се развива и усъвършенства артилерията и следователно ще се мисли за нейното използване в съвременните операции.

Следва да си зададем въпроса „Какво би се променило с въвеждането на новите системи?". Едно от нещата което следва да се обмисли е промяната на параметрите на бойният ред (широчина и дълбочина на районите за използван, отдалечение от линията на съприкосновение) както и начина за използване на артилерийските системи (по взводно, по оръдейно) и т.н..

Съгласно сега действащите нормативни документи (които са на основата на старите документи от Варшавският договор, с леки преработки) дивизионите за непосредствена поддръжка се разполагат на дълбочина 4-6 км от предният край на отбраната, а дивизионите за обща поддръжка на отдалечение съответно 6-8 км. Сравнявайки далекобойността на системите (122мм 2С-1 с далекобойност 15 км и 152 Д-20 с далекобойност 17 км) се вижда, че при това разположение на бойното поле всички те имат една и съща досегаемост на огъня, при което изпълняват едни и същи задачи. В същото време дивизионите за обща поддръжка в състава си нямат АПНГ (което е разбираемо понеже тяхната задача е изпълнение на тактически задачи обща поддръжка и обща поддръжка усилване), но нямат и средства за дълбоко разузнаване, а далекобойността е в рамките на непосредствената поддръжка. Въвеждането само на средства за разузнаване (респективно средства за поразяване) не удовлетворява изискването за обща поддръжка т.е. трябва да се търси комплексно решение.

Повишаването на далекобойността на системите предполага и промяна на досегашното използване на артилерийските дивизиони. Въпреки, че в „Ръководство за използване на полевата артилерия – артилерийски дивизион" са посочени размерите на район за използване на артилерийски дивизион до 9 км по фронта и до 3 км в дълбочина (свързано основно с това, че единственият дивизион в състава на бригадата да има възможност да води огън и по фланговете на полосата за отбрана и възможност за маньовър), отдалечението от линията на съприкосновение си остава същата.

В района за използване на дивизиона батареите заемат райони за огнево позиции с размери до 3 км., по фронта и в дълбочина. Във всеки район за огневи позиции на батареите се избират не по-малко от 4 позиции които се заемат по лотариен способ.

Използваният термин „лотариен" способ не описва конкретно как става смяната, поради което по-добре реда да се избира в тактическия оперативен център (ТОЦ) на дивизиона, при използване на батареята в състава на дивизиона или в центъра за управление на огъня на батареята (ЦУОБ), при самостоятелно използване на батареята (в състав на батальонна бойна група и др.).[2]

Всичко това се налага от факта за избягване на шаблонност в действията с цел увеличаване на жизнеспособността на артилерийските формирования поради минималното време, през което огневото формирование изпълнява огневи задачи, което затруднява откриването на местоположението му и дезориентира противника.

При увеличаване на далекобойността на системите същите могат да се изведат на по-голяма дълбочина (зад резерва или вторият ешелон - за артилерията за непосредствена поддръжка и зад полосата за отбрана на маневреното формирование - за артилерията за обща поддръжка), където ще има по-голям простор за маньовър на бойното поле и ще се освободи тактическо пространство за маневрените формирования за изпълнение на задачите по нов начин или нови задачи. Доколко това е целесъобразно и ще окаже ли значение при изпълнението на задачите от артилерията следва да се провери.

Една от основните задачи на артилерията се явява борбата с противниковата артилерия или така наречената огнева задача – контрабатарейна борба. За засичането на целите в контрабатарейна борба се използват РЛС, звукометрични комплекси и дистанционно управляеми летателни апарати.

Основните ТТ характеристики на РЛС на въоръжение в армиите са разгледани в следващата таблица:

Характеристика	**AN/ TPQ-36(V)**	**AN/ TPQ-37(V)**	**EQ-36**	**AN/TPQ-48(V)2A**	**«КОБРА»**	**"Артур»**				**EL/M-2084**
						A	**B**	**C**	**D**	
Разтояние на засичане на огневи позиции, км										
минохвъргачки	3-18		0,5-20	10	20	30-35	30-40	35-40	16-40	до 10
артилерийски оръдия	0,75-14,5	30	3-34		20	15-20	20-25	25-30	25-30	до 50
РСЗО	8-24	50	5-60		50			45-60	45-60	100
летателни апарати									100	350
Сектор за наблюдение, град.				7						
по азимут	90-360	90-360	90 и 360	360	270	90	90	90	360	120
по ъгъл на мястото	2,45-6,95	1,65-7,65	60	30						80
Количество на едновременно съпровождани цели	10	10	50			8	8	8	8	200
Диапазон на работните честоти, ГХц	8-9	3-4	3-4	1-2	4-8	5-6	5-6	5-6	5-6	1-2
Количество на работните честоти	32	15								
Точност в определяне на координатите на огневите позиции, проц.	1-2,5 от разстоянието	0.9 от разстоянието			0,3 от разстоянието					на разстояние 50 км - 125-150 м
Точност в определяне на координатите, м: при сектор на наблюдение 90 град			30	75 (на разстояние 5 км)						
при сектор на наблюдение 360 град			100-270							
Тип на антенната система				ФАР	АФАР					

Количество приемопредаващи елементи			1024							
Боен разчет, човека			4	2	1-2					
Време за развръщане/събиране, мин					5/1-2	7	5	5	5	

Следва да се посочи, че радиолокационните станции AN/TPQ 36, AN/TPQ 37, 47 и AN/TPQ 64, руският комплекс за контрабатарейна борба 1L2218-Зоопарк времето за определяне на координатите на стрелящата батарея е в рамките на 15 sec, а 22 сек. след първият изстрел предават данните в центъра за управление на огъня на артилерийският дивизион. Това е времето което следва да се приспадне от общото време за изпълнение на задачата. Това време може и да не се отчита, при положение, че разузнаването се води с ДУЛС и данните се предават на центъра за управление на огъня в реално време. За съвременните артилерийски системи оставащото време може да се определи на базата на следващата таблица:

Сравнителни характеристики на 155 mm самоходни гаубици отговарящи на съвременните стандарти

Характеристики	Вертикален ъгъл на насочване	Макс. далекобойност	Скорострелност	Возим боекомплект	Време за престояване на ОП
PzH 2000	-2.5^{o}- +65°	40 km	10 изстрела за мин. 3 изстрела за 9,2 s.	60 снаряда	2,2 min (с 16 изстрела)
AS-90	-5°- +70°	40 km	6 изстрела за мин. 3 изстрела за 10 s.	48 снаряда	1 min (с 3 изстрела)
M 109 A6 "Паладин"	-3°- +75°	40 km	8 изстрела за мин.	48 снаряда	3 min (с 8 изстрела)
"Ceasar"	-5°- +70°	42 km	6 изстрела за мин. 3 изстрела за 18 s.	18 снаряда	3 min (с 1 изстрел)
2C19 МСТА-С	-4°- +68°	40 km	8 изстрела за мин.	50 снаряда	3 min (с 8 изстрела)
2C35 "Коалиция"	-	40(70) km	Над 10 изстрела за мин.	70 снаряда	-
M109I7 "SPARK"	-	41 km	3 изстрела за 15 s.	80 снаряда	2 min.
"Doher" M109	-5°- +70°	28 км.	4 изстрела за мин.	45 сн., допълнително 80 сн. в товарен автомобил	-

Анализът на данните посочени в таблицата показва, че времето за престояване на огнева позиция е в рамките на 1 до 3 минути, за което време се изстрелват в рамките на 1 минута от 5 до 10 изстрела. Този разход на бойни припаси за взвод е 20-40 снаряда, а за батарея респективно 40-80 снаряда. За поразяването на противникова самоходна артилерийска батарея на степен 25% с площ 6 хектара са необходими 210 снаряда. При положение че престоят на огнева позиция както е посочено е в рамките на 2 – 3 мин свързано с времето за заемане и времето за водене на огън, то за засичане на целта и вземане на решение и определяне на данните за стрелба и подготовка на стрелбата (с цел да се води огън по целта поне в рамките на 30 сек- при което на оръдие се падат около 3-5 снаряда на съвременните системи) остават около 30 сек до 1,30 мин. И това при положение, че целта се засече преди откриване на стрелбата. Ако целта е засечена по време на воденето на огън от нейна страна (отчитайки времето за засичане и предаване на данните от РЛС) то

времето намалява от 0 до 30 сек. За сравнение дивизион 122 мм 2С-1 въоръжен с автоматизирана система за управление на огъня „Вулкан“ изпълнява задача за водене на огън по цел от неподготвена огнева позиция в рамките на 3-4 мин. Това донякъде покрива изискванията за маневреност на бойното поле за да може огневата част да открие огън в рамките на 1 до 1,30 мин. От момента на разкриването на целта на бойното поле.

Отчитайки това оставащо време с цел постигане на някаква ефективност стрелбата трябва да се извършва с дивизион в рамките на времето за престой на целта на огнева позиция, и това е при положение, че не се отчитат другите фактори от които зависи поразяването на целта, а именно времето за засичане и предаване на данните, времето за вземане на решение и поставяне на задачата за изпълнение и времелетенето на снаряда (последното зависи изключително от разстоянието на стрелбата).

Като пример може да се посочи, че при разстояние на стрелбата 12 км времелетенето за 152 мм Д-20 на заряд пълен е 32 сек., а на заряд 2-ри 42 сек. Това време може да се окаже определящо за вземането на решение относно разположението на артилерийските системи.

Ако се премести отдалечението на бойният ред зад резерва или вторият ешелон на отдалечение 12 км. И отдалечението на противниковата артилерия е на същото отдалечение то тогава времелетенето на боеприпасите ще бъде около 1 -1.3 мин., което показва, че боеприпасите ще падат на местност където целите вече ги няма.

При това положение воденето на огън по батареите на противника от артилерията се обезсмисля и поразяването на артилерийските батареи следва да се предостави на авиацията, а артилерията да поддържа бойните действия на пехотата като поразява целите пред техният фронт за изпълнението на задачите им. Заемането на позиции зад резерва или зад вторият ешелон е оправдано с цел даване на възможност на пехотата да извършва маньовър на една сравнително голяма дълбочина без да се съобразява с маньовъра на артилерията, и в същото време артилерията може да извършва широк маньовър с подразделения без да се съобразява с маньовъра на пехотата. От друга страна такава дълбочина предоставя възможност артилерията да остане скрита от земното оптическо разузнаване, о и от разузнаване от тактически БЛА (с далечина на полета до 10 км от пулта за управление), да не се премества в дълбочина за продължително време, като в същото време запазва способността да поддържа непрекъснато маневрените формирования. Това ще окаже и влияние върху построението на бойният ред на маневрените формирования и начина за изпълняване на задачите от тях.

Използвана литература:

1. Градев К. Новите технологии - предпоставка за нови оперативни способности. - В: Съвременни предизвикателства пред сигурността и отбраната. Ч 1.Сборник доклади от годишната научна конференция на ФНСО 17-18 май 2018 г. София: ВА ,Г.С.Раковски“, 2018 ISBN 978-619-7478-05-1
2. Марков Д. Нов ли е способът за бойно използване на самоходната и реактивната артилерия – артилерийска вртележка. Велико Търново 2019г.
3. Станчев С. Списание „Всичко за оръжието”, бр. 9 (565), бр. 10 (566) и бр. 11 (567), 2014, кат. № 143.
4. Ръководство за използване на полевата артилерия- артилерийски дивизион
5. Таблица за стрелба със 152 мм оръдие –гаубица Д-20

Atanas St. Atanasov, Atanas Vl. Atanasov,

AERIAL SURVEYLLANCE EFFICIENCY DURING ARTILLERY FIRING SERVICE

Atanas St. Atanasov, Atanas Vl. Atanasov

ВОЕННА АКАДЕМИЯ "ГЕОРГИ СТОЙКОВ РАКОВСКИ"
КАТЕДРА "СУХОПЪТНИ ВОЙСКИ"

Abstract: *The report states the need to introduce air reconnaissance assets into artillery units. The RAVEN RQ-11B unmanned aircraft system, currently available in the ISTAR battalion, does not provide the precision required to service the firing on single-targets, but instead can be used for engagement of group-targets. The statement is based on the results of tests performed to determine the accuracy of target detection by the RAVEN RQ-11B unmanned aircraft system during a live fire exercise and a fire control training with 61 Artillery Battalion.*

ЕФЕКТИВНОСТ НА ВЪЗДУШНОТО РАЗУЗНАВАНЕ ПРИ ОБСЛУЖВАНЕ НА СТРЕЛБАТА НА АРТИЛЕРИЯТА

Атанас Ставрев Атанасов, Атанас Владимиров Атанасов

Въоръжените конфликти от последните десетилетия потвърждават, че в боя само огневото превъзходство създава решаващи предпоставки за победа над противника и постигане на набелязаните цели.

Технологичния напредък и качествените промени в характера на възможната съвременна война, от една страна пораждат тенденцията противника силно да увеличи ролята на огневото поразяване за постигането на набелязаната цел, с минимални загуби на сили и средства, с минимален разход за боеприпаси и с висока точност и от друга страна налагат специфични изисквания към собственото разузнаването. Тези изисквания са наложени от необходимостта за получаване на надеждни и навременни разузнавателни данни за противника, за вземане на информирано решение, както и за ефективното използване на собствените средства за непосредствена огнева поддръжка.

Реализирането на способностите на артилерията за осъществяване на огнево превъзходство, пряко зависи от ефективността на разузнаването на целите.

Съвременните анализи отнасящи се до възможностите на силите и средствата за разузнаване показват, че разузнавателната информация, получена от различните видове разузнаване, способства максимално ефективно да осъществи огневото поразяване на противника.

Основните усилия на всички видове разузнаване (включително артилерийското) трябва да се съсредоточат не само върху разкриването на плана за действие на противника, но и върху получаването на пълни, надеждни и точни координати на приоритетите цели, които са обект на огневото поразяване и с поразяването на които се намаляват бойните способности на противника, снижава се бойния му потенциал и се създават предпоставки за завоюване и удържане на инициативата.

Това налага усъвършенстване организацията на разузнавателните подразделения, въвеждането на нови, различни по възможности и тип технически средства и повишаване умението на командирите, щабовете и личния състав от подразделенията по организирането и воденето на разузнаването.

Съгласно визията за развитие на способности на сухопътни войски на сегашният етап се предвижда придобиване на средства за разузнаването от типа на радиолокационни станции за контрабатарейна борба и комплекси за звуково разузнаване за артилерията за обща поддръжка, а за непосредствената - осигуряване с комбинирани прибори за разузнаване с възможност за интегриране в система за управление на огъня и това в комплекта на брониранта машина за артилейийските предни наблюдатели.

Придобиването обаче на средства за разузнаване от типа на радиолокационни станции за контрабатарейна борба, и комплекси за звуково разузнаване с възможностите на системите да покриват зона с размери 120 km x 30 km. за артилерийските звукометричени комплекси и 40 km или повече за радиолокационните станции за откриване на стрелящи системи спрямо собствената позиция е възможност за повишаване на способностите на подсистемата за разузнаване, въпреки, че за съвременният високоманеврен огневи двубой засичането на целите след началото на огневата им дейност не гарантира успех поради факта, че поразяването на целите става само за времето през което те се намират на позиция. Като се премахне времето за обработка на данните и реакция на огневите системи + времелетенето на боеприпасите (което за средни разстояния на стрелбата на съвременните системи е около 40-45 сек) почти не остава време за въздействие по целите. Ето защо смятаме, че все повече ще нараства значението на въздушното разузнаване, със засичане на целите в реално време, и започване на въздействието по тях (за артилерийските системи) със заемането на позиция. Тук времето за предаването на информация зависи само от закъснението на сигнала от разузнавателното средство, а точността на засичане на целите (определяне на координатите) е сравнително точна и е в рамките на изискванията за артилерията.

Въздушното разузнаване с БЛС значително увеличава обхвата на земното разузнаване, като позволява по-широко проучване на определените за разузнаване обекти и същевременно намалява неизвестността за различните им характеристики. Разузнаването с БЛС в много голяма степен намалява ограниченията предизвикани от географията на бойното пространство или т.н. „невидими полета", които остават скрити за средствата за оптическо и техническо разузнаване. В същото време, при използването на БЛС, практически всички обекти, които са цел на разузнаването са разположени в линията на наблюдение. Това позволява в реално време да се изпълняват задачите за разузнаване и наблюдение, да се предоставя видео информация за противостоящите и за собствените сили и да се извършва реална оценка на резултатите от огневото поразяване.

Един от основните аспекти при използването на БЛА е теренът в зоната на операцията. Теренът играе ключова роля както в ефективността на сензора, така и в командването и контрола. Откритият (пустинен, равнинен) терен осигурява оптимални условия за сензора на БЛА да локализира активност или обект. Планинския и гористия терен значително намалява ефективността на сензора. По същия начин, равнинният терен облекчава проблемите с линията на наблюдение, докато планинският терен може дори да възпрепятства използването на БЛА.

Друг основен аспект при използването на БЛА е времето. Валежите, ветровете и екстремните температури влошават работните параметри на БЛА. Когато БЛА изпълняват задачи при температури до пет градуса по Целзий и при видима влага, има опасност от обледеняване и замръзване. Ледът се развива по крилата и фюзелажа, увеличавайки теглото на БЛА. Когато забележи първите ефекти на обледеняване, операторът трябва да изкара БЛА извън тази среда или да прекрати мисията.

Напречните ветрове, надвишаващи 7 m/s създават опасни условия за излитане и кацане. Силните ветрове (над 25 m/s) на експлоатационна височина също създават неблагоприятни условия за летене. БЛА може да изпълнява задачи при слаб дъжд. Слабият дъжд влошава качеството на изображенията, но въпреки това те са използваеми.

Мъглата и ниските облаци намаляват ефективността на сензорите. Инфрачервената камера може лесно да даде изображение в лека мъгла, но не и в гъста мъгла или облаци. В такива условия, за да изпълни задачата си е необходимо да лети на ниска височина, като по този начин увеличава уязвимостта си и се демаскира. Освен това мъглата прави кацането изключително трудно.

Предимствата на БЛС се заключават във възможността да събират разузнавателни данни в реално време и да предават директно на наземната станция чрез връзка през деня или през нощта. Тази способност намалява необходимостта от пилотирани въздухоплавателни средства. Транспортните и логистичните изисквания за разполагане на БЛС обикновено са по-малки от другите средства за събиране на разузнавателни данни във въздуха. Не се изисква задълбочено специално обучение за да се използват ресурсите предоставени от БЛА.

Главните недостатъци на БЛА са ограниченията за полет наложени от терена и изискването за линия на наблюдение между БЛА и наземната станция управляваща въздухоплавателното средство.

Бойните формирования го използват основно за търсене и проследяване на противостоящи сили и за осигуряване на сигурност по време на конвоиране. В тези случаи използването му е „просто наблюдение на хълма или зад ъгъла". Характерният му шум при прелитане често се използва с цел провокация и принуждаване на наблюдавания обект да разкрие своята позиция.[1]

Въздушното разузнаване с цел обслужване и коригиране стрелбата на артилерията не е нещо ново за Въоръжените сили на Република България. Преди да навлязат масово БЛС, тази задача се изпълняваше от вертолети. При невъзможност да се обслужва стрелбата от земните наблюдателни пунктове и когато целите са ненаблюдаеми и тяхното местоположение не е точно известно, беше предвидено да се привличат вертолети от разузнавателната авиация. В състава на екипажа на тези вертолети има щурман-коригировачи (артилерийски специалисти), на които конкретно се поставя задачата по обслужване на стрелбата. Те водят наблюдение, извършват необходимите измервания с технически средства и докладват за резултатите от огневото поразяване.

През 2014 година на въоръжение в състава на механизираната бригада беше приета безпилотна летателна система „RAVEN RQ-11B". Безпилотната летателна система „RAVEN RQ-11B" е предназначена за въздушно разузнаване, наблюдение и целеуказване. Същата има редица технически възможности, които позволяват водене на разузнаване от въздуха, определяне на координати на цели с достатъчна точност за незабавно извикване огъня на артилерията, както и за засичане на разривите от огневото поразяване. Изграждането и усъвършенстването на способности на базата на безпилотна летателна система „RAVEN RQ-11B" значително намалява дефицита от разузнавателни данни и допринася за осигуряване на ефективна огнева поддръжка на маневрените формирования.

БЛА „RAVEN RQ-11B" е малък и се транспортира лесно. Развръща се бързо, стартира се от ръка на разстояние не по-голямо от 10м и за приземяване не се нуждае от специално подготвена писта. Има ниско ниво на шум – шумът е основен демаскиращ признак за БЛА.

„RAVEN RQ-11B" разполага със система за навигация, оборудване за контрол и полезен товар. При изпълнение на стандартни задачи полезния товар включва цветна и инфрачервена камера. Може да се управлява дистанционно от наземната станция или да лети напълно автоматизирано по предварително зададени точки.

При дистанционното управление се използва телекомуникационна връзка между наземната станция и БЛА. Операторът изпраща полетни команди към БЛА, като същевременно получава обратно в реално време телеметрия и видеоизображения.

Автопилотът, използва данните от бордовите сензори и вграденият GPS приемник за да оцени текущото положение и ориентация на БЛА. На база на получените данни, осъществява контрол, въвежда необходимите корекции и управлява полета на БЛА. Има възможност да прекрати изпълнението на задачата и незабавно да се върне до точката на излитане с натискането само на един бутон на наземната станция.

Приземяването се извършва от оператора, който направлява БЛА така, че да се плъзне по земната повърхност върху долната част на фюзелажа си, а при вероятност от по-твърдо приземяване с възможност да се разглоби на ниска височина.

БЛС допринасят за общите усилия за събирането на разузнавателна информация. Обхватът и гъвкавостта на БЛС осигуряват на командира перспективата да вижда от „птичи поглед" бойното пространство, когато и където се нуждае от нея, без излишни рискове.

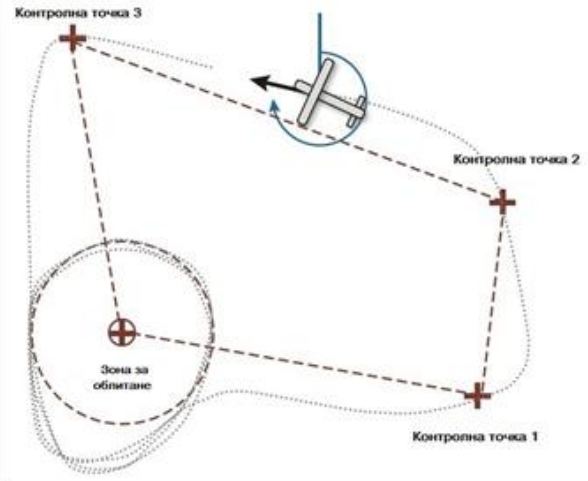
БЛС са достатъчно гъвкави, така че да бъдат използвани в цялата зона на операцията. Въпреки че бойното им използване е предварително планирано, техните задачи мога да се променят при изменение на обстановката, при изменение приоритетите на мисията или при идентифициране на нови цели.

Бойното използване на БЛА се определят в съответствие с плана за операцията така, че да се покрие заповядания район за разузнаване.

БЛА може да бъде пилотиран дистанционно с пулт за управление или да следва летателен план, зададен от оператора. Дистанционното пилотиране включва използването на пулт за управление с джойстиков контролер за маневриране и управление на БЛА. Операторът може да управлява БЛА или като използва камерата и телеметрията, или чрез директно наблюдение на БЛА от земята.

Ако се използва летателен план, операторът въвежда серия от точки, върху предварително заредено в компютъра разстерно изображение на зоната в която ще се използва БЛА. Тези точки са зададени с правоъгълни координати и височина, като по този начин се определя мястото им в триизмерното пространство. Тази информация е важна, за да се гарантира, че навигационната система на борда на апарата ще работи правилно. Като се приеме, че текущата позиция и желаната крайна позиция са известни, може да се изчисли траектория, за да може автопилотът да управлява БЛА до следващата точка.

След това БЛА изпълнява полета на автопилот (автоматично), като следва зададената последователност от точки. БЛА използва вградения си GPS, за да определи своята географска ширина, дължина и надморска височина. Като правило се задават контролни точки, които оформят необходимата траектория на полета и точките, които са обект на разузнаване (целите) и около които БЛА ще извършат разузнзвателния си полет. Летателният план може да бъде променян в реално време чрез добавяне, изтриване или преместване на точки. Има процедура, при която ако бъдат загубени комуникациите с БЛА, той самостоятелно прекратява изпълнението на задачата и се връща на изходна позиция.



„RAVEN RQ-11B“ не изисква голяма логистична поддръжка, което прави системата много гъвкава. Може да се превозва с ЛАПП, а цялото оборудването се събита в защитена кутия, която се носи от двама човека.

Той може да се използва денем и нощем. Изпълнява задачи по разузнаване, наблюдение и видео заснемане, като предава изображение в реално време на наземната станция за управление и изнесения приемо-предавател на видеосигнал. Това от своя страна позволява на оператора да управлява БЛА, да търси цели, да води разузнаване и да записва цялата информация за последващ анализ.

Използването на БЛА изисква допълнителна координация с всички бойните елементи и елементите за бойна поддръжка – авиация, ПВО, артилерия. Интергиране на БЛА във въздушното пространство се прави с цел ефективно и безопасно използване на системата.

Въпреки компактните си размери, безпилотните летателни системи са изключително сложни. Алгоритъмът за навигация приема командите на оператора, като дестинация, ъгъл на курса и

надморска височина, и ги превръща в команди за БЛА, които в този случай са височина, ъглова скорост и скорост на полета. Това, което е необходимо на оператора за да управлява БЛА е информация за положението и скоростта му, които данни се получават от GPS приемника. Този контрол в повечето случаи се осъществява в динамична среда, т.е. в условията на ветрове, течения, валежи и др., които напълно променят кинематичното състояние на БЛА в пространството.

Засичането на целта (разрива) се извършва на базата на получените в наземната станция изображения от видеокамерата на БЛА и данните от сензорите му. С получаването на тези данни, компютърът оценява положението на БЛА в пространството и изчислява местоположението на точката, която се засича. Същността на този процес е приемането на видеоизображенията за разпознаване на целта от наземната станция и позиционирането на целеуказателя върху целта. След това, като се използват координатите на БЛА, неговото положение в пространството, ъгълът на насочване на камерата от БЛА към целта, последващото измерване осигурява вектор на относително положение от БЛА към целта.

Резултатната срединна грешка при определяне на координатите на целта е сумата от грешките в местоположението на БЛА, ориентацията му в пространството и грешките от сензорите. При опростяване на уравнението на срединната грешка, то придобива следния вид:

$$\sigma_{TOTAL}^2 = \sigma_{x,NAV}^2 + \sigma_{\theta,NAV}^2 R^2 + \sigma_{x,SEN}^2 + \sigma_{\theta,SEN}^2 R^2 + \sigma_{\Delta T}^2 V^2 + \sigma_{\Delta T}^2 R^2 \omega^2$$

където

R - е относителното разстояние до целта;

V - е относителната скорост на БЛА спрямо целта;

ω - е ъгловата скорост на БЛА;

$\sigma_{x,NAV}$; $\sigma_{\theta,NAV}$ - са грешките от местоположението на БЛА;

$\sigma_{x,SEN}$; $\sigma_{\theta,SEN}$ - са грешките от сензорите на БЛА;

$\sigma_{\Delta T}$ са грешките в оценката на местоположението на целта.

Точността на задачите по засичане на цели от БЛА е в пряка зависимост от:

- възможностите на GPS приемника
- възможностите на сензорите отчитащи положението на апарата
- възможностите на алгоритъма за навигиране.

Грешката във всяка една от тези системи води до неточна оценка на положението на БЛА в пространството (например при отчитане на грешка в местоположението на апарата, тя се разпространява и в алгоритъма за навигиране), а от там и в определяне на координатите на засичаната цел.

„RAVEN RQ-11B" има и технически ограничения отнасящи се до камерите, които носи и съответно с изображенията изпращани към наземната станция. Първо, тези ограничения са свързани с това, че оптическата система на камерите е фиксирана, т.е. зрителното поле се измества с промяна на положението на БЛА в пространството. Това прави засичането и точното определяне на координатите целите (обектите) трудно, особено при наличие на силни въздушни течения. От друга страна, технически е заложено оптическата система да е ефективна при работна височина на полета от 45м до 300м над земната повърхност. При такава височина, разделителната способност на изображенията позволява обектите на разузнаването да се различават достатъчно ясно и да могат да бъдат получени достоверни координати. С увеличаване на работната височината над 300м. разделителната способност на засичаните цели (обекти) започва да намалява, с което намалява и точността. Яснотата на изображенията при използване в работна височина намалява също и в условия на мъгла, ниска осветеност, наличие на отражения от земната повърхност и др. При използване на височини от 300м до 4500м (таван на полета) задачите на „RAVEN RQ-11B" са свързани основно с наблюдение.

За определяне на точността на засичане на целите за нуждите на артилерията е проведено изследване на УЦ „Тюлбето" по време на тренировка по стрелба и управление на огъня.

Изследването е извършено при следните условия:

Отклоненията са засечени със следните разузнавателни средства:

- оптическото разузнаване – щатните разузнавателни АПНГ в артилерийския дивизион;
- въздушното разузнаване с БЛС „RAVEN RQ-11B" – от състава на батальон ISTAR.

Топогеодезическото привързване на бойния ред на оптическото разузнаване е извършено по карта с прибор със собствени сили и средства. Извършен е последващ контрол от контролна група.

Отклоненията на разривите при поразяването на всяка една цел са засичани едновременно с всички средства за разузнаване.

Данните от оптическото разузнаване в това изследване са използвани като контролни.

Данните получени от въздушното разузнаване са обобщени в табличен вид, като отклонения спрямо контролните данни.

Изследването е извършено като данните получени от въздушното разузнаване са сравнени с контролните данни.

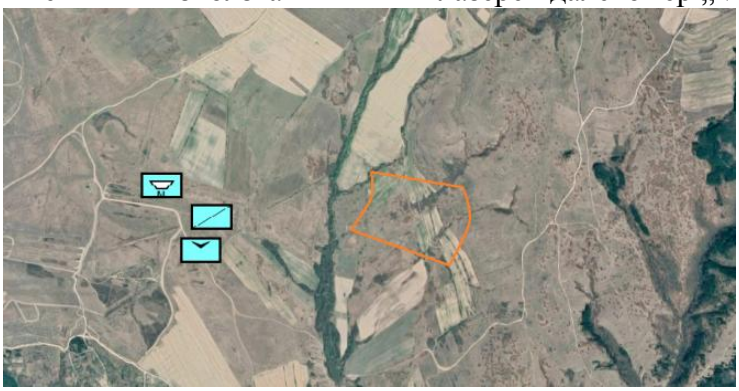
Основната цел е изследване на точността на БЛА „RAVEN RQ-11B“ при използването му като средство за обслужване на стрелбата на артилерията в хода на огневото поразяване.

С получените резултати при засичането на разривите в хода на огневото поразяване е направена оценка за възможността на БЛА „RAVEN RQ-11B“ за засичане на отделни цели.

По време на ТСУО основен разузнавателен орган е щатната АПНГ. За определяне на данните по целите се използва АСОУД “Вулкан“. Изпълнява се огнева задача №4 от КСУОА-98 – „Поразяване на неподвижна наблюдаема и ненаблюдаема цел с огън от закрита огнева позиция без пристрелка“. Данните за стрелбата са определени на базата пълна подготовка.

Наземната станция на БЛС е в района на КП.

За засичане на разривите АПНГ използва ПАБ-2А и лазерен далекомер „VECTOR 21“.



Резултатите от въздушното разузнаване са засечени при ръчно управление на БЛА. Оператора се намира в района на АПНГ на контролната група и участва в изградената КИС на послушване.

Цел	АПНГ	Въздушно разузнаване		
	Координати на целта	Засечени координати	Отклонения	
			В разстояние (метри)	В направление (ъгломерни деления)
1.	74136 21464	73996 21428	-137	-0-15
2.	74094 21742	- -	-	-
3.	74160 21350	74222 21363	60	0-05
4.	74115 21680	74112 21665	-3	-0-05
5.	74164 21317	74145 21017	27	-0-93
6.	74094 21820	74143 21667	44	-0-49
7.	74330 21628	74275 21667	-55	0-12
8.	74140 21190	74120 21385	-42	0-60
9.	74315 21763	74209 21730	-107	-0-09

В хода на анализа се търси отговор на следните въпроси:

Каква точност се постига при определяне на координатите на засечените разриви в хода на обслужване на стрелбата при използване на въздушно разузнаване с БЛА;

Сравнителната оценка за въздушното разузнаване е направена, като получените в изследването резултати са съпоставени със зададени условни размери на целите (отделни и групови).

Данните от засечените от БЛА разриви са обработени и чрез обратна геодезическа задача са изчислени отклоненията в разстояние и направление спрямо данните на контролната група.

За въздушното разузнаване съпоставка се извърши и за възможностите на БЛА за засичане на цели и определяне на техните координати, като целите условно са категоризирани в две групи – отделни и групови. Съответно размерите по фронт и дълбочина за отделните цели е приета за 25х25 метра, а за груповите – 150х150 метра.

№	Въздушно разузнаване			
	Отклонения		Размер на отделна цел (метри)	Размер на групова цел (метри)
	В разстояние (метри)	В направление (хилядни)		
1.	-137	-0-15	25/25	150/150
2.	-	-	-	-
3.	60	0-05	25/25	150/150
4.	-3	-0-05	25/25	150/150
5.	27	-0-93	25/25	150/150
6.	44	-0-49	25/25	150/150
7.	-55	0-12	25/25	150/150
8.	-42	0-60	25/25	150/150
9.	-107	-0-09	25/25	150/150

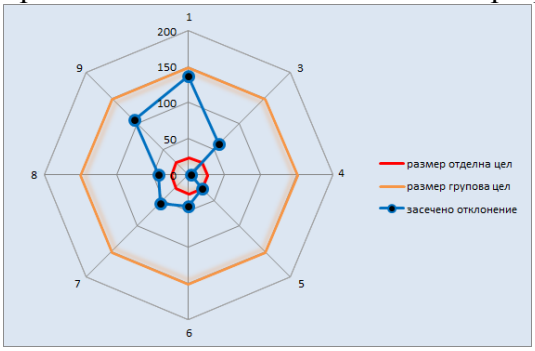
На базата на получените в таблица резултати е построена графика на отклоненията със следното съдържание:

За всяка една цел засечена от БЛА (от №1 до №9, без цел №2) са построени лъчи и дължината на всеки е изразена в метри;

Началото на всеки лъч (центъра на графиката) оказва засечените от контролната група разриви за всяка цел;

По дължината на всеки лъч са нанесени следните групи точки: засечени от БЛА отклонения; размер на групова цел; размер на отделна цел;

Точките от всяка група са свързани за всеки един от засечените разриви.



Построената графика дава визуална представа, какви са отклоненията на разривите засечените от БЛА, спрямо тези на контролната група. По-голямата част от разривите – 7 от общо 9 са засечени с грешка от 50м до 150м. Един е засечен с много голяма точност – до 3 метра и един от разривите не е засечен. Средно аритметичното отклонение от засечените разриви е приблизително

60 метра. Такива срединни отклонения не биха позволили да се обслужва стрелбата в хода на огневото поразяване с необходимата точност.

От настоящото изследване може да се направи още една връзка – с каква точност БЛА може да засече цел. Според стойността на засечените отклонения може да се направи препратка към възможностите на БЛА за засичане на цели. В тази връзка са зададени условните размери на целите – отделни и групови. От така построената графика и зададените размери на целите може да се обобщи следното:

В зоната на отделните цели (отклонение до 25м) попада един разрив, засечен от БЛА – разрив№4;

Всички останали отклонения попадат в зоната на груповите цели.

От броя на засечените отделни и групови цели към общия брой засечени цели може да се определи каква е вероятността БЛА да засече отделна и групова цел:

- за отделна цел вероятността е 0,1
- за групова цел вероятността е 0,9

и извода, който следва от тук е, че БЛА може да се използва основно при засичане на групови цели.

От графика става видно още, че 75% от засечените отклонения на разривите не превишават 50 метра, което от своя страна говори, че въпреки по-малката вероятност за засичане на отделна цел, БЛА сравнително точно може да определи координатите на групова цел.

От направеното изследване върху БЛС „RAVEN RQ-11B“ може да се заключи, че системата отчита по-големи отклонения в сравнение с другите използвани средства. Към момента в нормативните документи няма описани какви са допустимите грешки при обслужване на стрелбата в хода на огневото поразяване. Резултатите показват, че е целесъобразно БЛС „RAVEN RQ-11B“ да се използва за оценка на стрелбата в хода на огневото поразяване само на групови цели.

Използвана литература:

1. Марков Д., Чалъков Р. - Поразяване на цели и коригиране на огъня на дивизионитеза непосредствена огнева поддръжка с АСУОАД „Вулкан - С“ Пикис с помощта на безпилотни летателни апарати-Годишник на факултет „Командно-щабен“, ВА „Г. С. Раковски“, 2017
2. Илиев, К. Използване на безпилотни летателни системи в съвременните военни конфликти. Научна сесия на факултет “А, ПВО и КИС част I 2013, с. 131-137, ISSN 1313-7433.
3. Станчев С. Съвременни автоматизирани системи на полевата артилерия. Артилерийска научна конференция, “Полевата артилерия и новите технологии” Факултет “А, ПВО и КИС“ 2006, с. 207 – 211, ISBN-13:978-954-9681-24-6.
1. UAS: RQ-11B Raven® - https://www.avinc.com/uas/view/raven.

Kalin V. Gradev,

CHALLENGES TO LAND FORCES EMERGING FROM NEW TECHNOLOGIES

Kalin V. Gradev

Land force chair "G.S. Rakovski" National Defense College Sofia, Bulgaria
Phone: +35929226623, e-mail: k.gradev@armf.bg; kgradev@gmail.com

Abstract :*Victory in the modern battle requires the introduction of new weapons and technology to provide their own armies technical advantage over the enemy, thanks to which can reduce the number of victims and wounded on the battlefield. The rapid development of new military and non-military technologies inevitably leads to a change in the forms and methods of warfare, and the advantage will be on the side of the one who can first master and apply these technologies in action.*

Keywords*:new weapons and technology,*

ПРЕДИЗВИКАТЕЛСТВА ПРЕД ФОРМИРОВАНИЯТА ОТ СУХОПЪТНИТЕ ВОЙСКИ, ПРОИЗТИЧАЩИ ОТ НОВИТЕ ТЕХНОЛОГИИ

Калин В. Градев

Въведение

Усъвършенстването на технологиите през годините е оказвало пряко влияние върху развитието на способите формите за водене на бойни действия през различните етапи на човешкото развитие.Ужасяващото количество жертви от великите битки от древноста изглеждат като детска играчка пред унищожениео което ни предлагат съвремените технологии. Благодарение на технологиите, големи сражения могат да се водят в перод от не по вече от две, три години на ограничен участък от местноста (като в ,,Наполеоновите войни"), а на огромни пространства с изключително големи загуби и по няколко десетки на година (Втората световна война). В съвременната война (която е рожба на технологиите), ролята на икономиката и цивилните е решаваща.

За да може да се разгледат въпросите с възможностите за окомплектоване на формирование от Сухопътните войски за участие в съвремени операции трябва да се направи анализ на направленията в които работят водещите международни компании за производство на военна продукция. След като са проучат тези насоки за развитие ще е необходимо да се оценят възможностите на държавата и капацитета с който разполагат нашите фирми за производство на такава специална продукция. Защото е удачно оборудването и екипировката (или поне част от тях) на собствените формирования,участващи в съвремените операции да бъдат произведени в България.

Факт е че в момента разработките на новите оръжейни системи са насочени не толкова към оръжия за масово унищожение или както в началото на 20 век - оръжия за водене на ,,тотална война". Защото в днешно време никоя държава, трезво мислещ политик или военноначалник не би имал изгода от тоталното унищожение на ресурси, които ни предлагат оръжията за масово

унищожение, а така също и че ресурсите (човешки материални или природни) в днешно време са изключително ценни. И именно за това водещите компании и правителства са насочили усилията си за разработване на средства за водене на война, които биха позволили на победителя да се възползва от тази победа именно ползвайки ресурсите. Кой има полза от територия обхваната от ядрена зима?

Днес по света се работи в много различни направления за разработване и оборудване на формирования от въоръжените сили в зависимост от задачите които трябва да се изпълнят и целите които трябва да се постигнат. В тази насока усилено се включват имено технологиите, които бързо намират приложение (или случайно първо се експериментират) именно в армията.

По време на войната в Персийския залив през 1991 г. за пръв път бяха използвани вакуумните бомби "air-fuel", обявени от някои среди за истински триумф на военната наука. Обяснено простичко, новият тип бомби разпространяват облаци от силно запалим газ близо до терена и след няколко секунди газовата маса се запалва. При падането си върху позициите на иракската армия бомбите предизвикаха страховити поражения: кислородът бе изсмукван, смъртта на останалите без въздух нещастници е било почти мигновена, а малцината оцелели след този вакуумен ад са били овъглени от обвилата ги огнена топка.

Международната общественост се разтревожва, че жестоката ефикасност на новото оръжие надхвърляла приемливите граници за един военен конфликт. Пез седемдесетте години подобна реакция предизвиква и неутронната бомба, считана за символа на модерната война. При неутронната бомба радиоактивното съдържание на детонацията е увеличено за сметка на ограничената експлозивна мощ, което означава, че хората се премахват, но улиците и сградите остават непокътнати.

Стъпили в третото хилядолетие, правителствата започват да си дават сметка, че разрушенията в широк мащаб, както и изтреблението на хора и на средства трудно могат да се ограничат в определен регион. За да се предпазят собствените войници, (които са най-голямата инвестиция)от смъртоносното въздействиена съвременте оръжия се разработва широка гама от т.нар. несмъртоносни оръжия - потискащи психиката химични средства, инхибиторнипластмасови заряди, пушки, изстрелващи лепила, пяни, мрежи и пр. В рамките на доктрината "Унищожи нежно" се експериментират заслепяващи лазери, акустични автомати, радиочестотни оръжия, ултразвукови и микровълнови оръжия, поразяващи хора, радари и компютри и мн.

През следващите десетилетия войниците ще бъдат обличани с предпазни облекла от специални тъкани с отразителни свойства, правещи невъзможни за откриване телесната топлина и др. излъчвания. Проектират се индивидуални шлемове с вградени миниатюрни видеокамери за фиксиране на далечни изображения и за изпращането им чрез сателити до старшите командвания. Разработват се устройства, действащи вразлиния спектрален диапазон лъчи, посредством които наблюдениетои откриването на цели през нощта ще се сведе до елементарна дейност.

Според специалисти от водещите армии в света разработващи програми като „войник на бъдещето“ войникът на XXI век, освен със системи за прикритие, ще бъде снабден с остроумни оръжия като системата анти-снайпер например. Става дума за нов тип оръжие, свързано с портативен компютър, което е в състояние да открие изстрелян от скрит снайперист куршум, да го обезвреди, да локализира позицията на врага и незабавно с крайна точност да отговори на стрелбата. Традиционните оръжия също се автоматизират, роботизират, усъвършенстват и приспособяват към изискванията на „войната на бъдещето“ и дори стават автономни. Такъв например е "Арнолд" или Проект № 48 на американската армия, който е едно голямо роботизирано оръдие. "Арнолд" е снабден с мощен компютър, който на базата на нови технологии за оптически и акустични сензори локализира целта и я поразява с непропускаща точност. Оръдието само открива целите и само решава кога да открие огън и към коя цел. Разбира се, и "Арнолд" си има своята ахилесова пета: размерите. Тъй като е достатъчно голям, той лесно може да бъде засечен от сателити и атакуван от аероботи - самонасочващи се контейнери, хвърляни от роботизирани самолети.

Екипировката предвижда и усъвършенствани радио-управляеми лазерни оръжия. Лазерното оръжие "Стингрей", което вече е монтирано на бронетранспортьори на американската армия, е в

състояние да регулира количеството излъчена енергия, като може да заслепи врага или да "разреже" позициите му на две с лазерен лъч с висока концентрация на енергия.

Чрез акустичните оръжия също се постигат две степени на поразяване на целта. При ниско равнище на звуково излъчване те дестабилизират физически и психически противника, а с увеличаването на мощността предизвикват смъртта му.

Страховити слухове се носят и за качественото развитие на генетичните оръжия. Съвсем не са безпочвени опасенията на специализираната комисия към Международния Червен кръст, че генетиката ще се наложи като най-опасния инструмент за масово унищожение. Вече е постигнат значителен напредък в областта на вирусната генетика. Чрез генетични мутации се създават устойчиви на човешката имунна защита вируси и те могат да поразяват гените по специфичен начин. Да атакуват отделна раса на базата на определени генетични характеристики тези оръжия са в състояние да поразяват насочено и избирателно само африканци или само евреи, само корейци и т.н.

Роботиката също ще играе важна роля в бъдещите войни. Люис Франклин, висш служител във фирма за поръчки, свързани с американската отбрана, както и в доклади министерството на отбраната на Великобритания се предвижда, че до 10-20 години на пазара ще се появят т.нар. войници-роботи.[1] Според експертите железните воини ще бъдат проектирани съгласно изискванията на клиента и ще могат да оперират в екстремни условия при най-трудните бойни полета. Войниците-роботи ще бъдат умели, точни, добре въоръжени и конструирани с трайни материали. Тяхно преимущество ще бъде относително ниската им производствена цена в сравнение с конвенционалните оръжия.

С последните завоевания на нанотехнологиите стана възможно конструирането на електронен двигател с дължина само 1 мм, което развихри река от идеи в търсенето на нови военни приложения. Така бяха реализирани мравките-роботи.

Идеята, която стои зад мравките-роботи, е родена след внимателно изследване на истинските мравки в естествената им среда. Учените се убедиха в невероятната способност на мравките да се организират в ефикасни колонии и да транспортират маси с тегло 60 пъти по-голямо от теглото на телата им. Тези наблюдения бяха обобщени в микроелектромеханичната система мравка-робот. Моделирани по образ и подобие на истинските насекоми, миниатюрните машини имат по шест силиконови лапи и са специализирани да решават специфични задачи. Едни изгризват електрически кабели, други освобождават малки дози киселина и разрушават електрическите вериги, трети са програмирани за транспортирането на инструменти за комуникация, четвърти експлодират при контакт с вражеско превозно средство и пр. Експлозивният заряд на една нанотехнологична мравка не е достатъчен, за да разруши бронирана кола, но отряд от мравки е в състояние да се справи с каквато и да е цел независимо от нейната големина. Тъй като са толкова малки, те са трудни за откриване и обезвреждане, но дори и да бъдат поразени, производствената им цена е толкова ниска, че лесно и бързо се заменят с други.

Вече са факт и миниатюрните разузнавателни самолетчета, не по-големи от кутия за обувки. Екипирани с широк асортимент сензори и комплект "интелигентни" мини, бойните нановерсии ще могат да хвърлят миниатюрни заряди, които ще се позиционират сред терена в очакване на противникова жива сила и техника.

Израелски учени разработват амбициозен проект на боен робот-стършел, който ще открива и унищожава противника на бойното поле. Стършелът ще бъде снабден с видеокамера, чрез която ще се предава картина на пункта за управление на войските и ще носи боен заряд. Най-интересен нанопроект във Великобритания е MFI (Micromechanical Flying Insect 21– механично летящо насекомо). Работи се и върху процеса на събиране на подобни микророботи (пчели) в ято и обмяна на информация между тях за съвместни действия в различни видове бой. Някои от тези „насекоми” може да бъдат сгънати в кутия с размерите на пакет цигари. Когато те се освободят, те могат да летят за известно време в сграда и предават ценна оперативна информация към действащото подразделение. Друг робот може да бъде изработен под формата на змия или гъсеница с монтирани датчици за изображение за проучване на подземни съоръжения.

[21]https://people.eecs.berkeley.edu/~ronf/MFI/index.html

Множество научно изследователски институти22, компаниии специалисти създават високоякостни материали като „течната броня"23, мощни енергоизточници като „аморфния силиций", невидими и променящи цветовете си нанообекти, наноматериали за униформата на войниците, нови защити от оръжията за масово поразяване и др.. „Течната броня", която представлява гел от твърди наночастици и течен пълнител, може да се използва за усилване защитата не само на отделния войник (броне жилетка) а и на автомобили, вертолети, катери. Разработките са на единичен принцип целящи при рязък удар (попадане на куршум или парче от граната) частиците мигновено да се свързват една с друга, превръщайки гела в компонент възпрепятстващ проникването на чуждо тяло в прикривания обект.[2]

В челото на тази серия от нови военни стратегии е и кибервойната или информационната война, при която главни оръжия на воюващите страни ще бъдат компютърни програми и алгоритмични данни. Умелото манипулиране на закодираната информация през XXI век би могло да доведе до обръщането на въоръжените сили на врага срещу собствените му части. Предполага се, че който съумее да спечели информационната битка, ще спечели и войната.(Ако бъдещата война въобще може да бъде спечелена!)

Швейцарски учени успяха да създадат 9 частици антиматерия, просъществували само една 40-милиардна част от секундата. В момента в няколко секретни бази в света се провеждат изследвания за обуздаване на енергията на субатомните частици и използването й като оръжие. Антиматерията се активира, като се приближават две податомни частици с противоположен електромагнитен заряд, които се неутрализират взаимно, освобождавайки ужасяваща разрушителна енергия. В книгата си "Пътят към Армагедон" Питър Люис твърди, че еднокилограмова бомба с антиматерия може да предизвика експлозия с мощност 43 мегатона и разрушителна ефикасност, еквивалентна на експлозията на няколко десетки милиона тона тротил. Резултатът би бил доста по-страшен от разрушенията, предизвикани от уранова ядрена бомба. Въпреки, че специалисти твърдят, че ще е нужно много време и пари за осъществяването на такъв проект [3] самата възможнпст за използване на такава енергия е силно притеснителен.

Преразглеждането на технологиите на основата на аеростатите24, включват както малогабаритни, преносими системи, които използват прости и надеждни платформи за ефективно обезпечаване на радиорелейната свръзка, така и такива които да издигат във въздуха 170 т полезен товар и да го транспортира на разстояние до 5000 км., а дори и в системата за ПРО. [4]Съвременните технологии разкриват техния нов потенциал за нуждите на противоракетната отбрана, като голямата им и широка повърхност позволява да се монтират едновременно няколко антени и локатори, чрез които да се следи въздушно пространство с площ от хиляди квадратни километри, отчитайки евентуалните изстрелвания на ракети. В единен комплекс със спътникова орбитална групировка аеростатите се превръщат в потенциален елемент на противоракетната отбрана. Тук главният недостатък на дирижаблите – ниската им скорост – не играе роля.

САЩ също са оценили по достойнство потенциала, който дирижаблите разкриват в съвременната епоха. Разработеният от тях аеростат предлага голяма товароподемност (според някои оценки тя значително превишава възможностите на руския аналог), а плановете са и той да се използва в труднодостъпни райони за военни превози.Големи успехи във военното приложение на дирижаблите е постигнал Китай. През 2015 г. там е направен опит с истински гигант - аеростат запълнен с почти 20 000 куб. м хелий, които му позволяват да се издигне в атмосферата на височина до 100 км и да остане там до 2 денонощия. Използването на слънчеви батерии дава възможност на китайските инженери да увеличат полезния товар на летателния апарат.

Безпилотните средства трябва да бъдат неразделна част от арсенала на новите бойни единици, армиите на великите към монента държави отдавна работят по внедряването им. Такива безпилотни средства включват четири различни системи; БЛА (безпилотни летателни средства),

[22] Helios Global Technologies, BAE Systems, Chiron Global и Фондът за рисков капитал на МИЦ от Екатеринбург
[23]"Liquid Armor"
[24]По – познат като дериджабъл.

най-малко две UGV (Автоматични наземни средства) и UGS (Автоматични наземни датчици) разполагани на далечни разстояния и други специални сензори.

UGV и UGS – не са далечна перспектива. Във войските вече се използват някои от тези системи, компанията Aerovironment Raven, компанията "Elbit Systems, мини-робота за наземно разузнаване Pacbot на фирмата I-Robot и Dragon Runer, са вече използвани от морските пехотинци на САЩ.

Автоматичните наземни датчици (UGS) имитират скали, дърво или дънери, и може да работят тайно дълбоко в територията на врага в продължение на няколко месеца без никаква непосредствена поддръжка. UGS са били използвани по време на войната във Виетнам, но през последните години те станаха ,,по-умни” и са равнопоставени по дееспособност на действащи сложни разузнавателни системи.

Дистанционните Видео Терминали (RVT) могат да се свържат със съществуващите видео потоци за аналогови видео данни в реално време. По-съвременните централно мрежови системи, Advanced Information Architecture (AIA) на компанията Northrop Grumman може да извлече информация от бази данни, които идват от много предаватели и разузнавателни служби, осигурявайки по този начин достъп до огромен обем информация в реално време. Също така помага на потребителите да намират информацията която им трябва, както това се прави в Интернет.

Пример за ,,ускорена верига за унищожение" е използването на БЛА в операциите ,,Hunter-Killer". Тези операции се превръщат в основа на нова концепция ,,превъзходство във въздуха". Такива операции се осъществяват с датчици, въоръжение и БЛА за едновременното решаване на разузнавателни и щурмови задачи. БЛА са особено подходящи за такива операции, тъй като те са в състояние да обхванат големи площи в продължение на дълъг период от време. БЛА са в състояние да нанесат прецизни опустошителни удари по важни (внезапно открити) цели. Покривайки район за наблюдение и водене на огън, БЛА като Predator на компанията General Atomics, или Hunter, съвместнаразработка на израелската армия и Northrop Grumman, летят на височина от приблизително 3/5 хиляди метра, оборудвани са с електронно-оптични и РЛС със синтезирана апаратура и въоръжени с оръжия с лазерно насочване, Hellfire на фирмата " Lockheed Martin " или Viper Strike на фирмата Northrop-Grumman. Sperwer B, е френската версия на проверения в бой БЛА Sperwer, разработен от Sagem, може да бъде въоръжен с две оптикоелектронни управляеми ракети Spike LR производство на израелската фирма RAFAEL. Други БЛА, като Hermes 450 и IAI / MALAT Heron на компанията "Elbit Systems (и двете са на въоръжение в Израел ВВС) са демонстрирали възможността да носят значителен външен товар, но подробности за естеството на външния товар, които могат да пренасят тези устройства не са оповестени. Палестински източници заявяват, че израелските въоръжени сили често се използват БЛА срещу техни обекти в ивицата Газа.

Международната доброволческа общност InformNapalm отбелязва, че след началото на бойните действия на окупираните територии на Донбас са засечени и е потвърдено използването им на 8 вида руски дронове: «Гранат-1», «Гранат-2», «Гранат-4», «Форпост», «Орлан-10», «Елерон-3СВ», «Застава», «Тахион». Както и един тип съвременен руски БЛА с неустановено име.[5]По непотвърдени данни тежкият руски ударен дрон С-70 "Охотник" е с многофункционално предназначение и ще бъде предназначен основно за изпълнение на бомбардировъчни задачи, откриване и унищожаване на широк спектър от наземни, морски и въздушни цели, но също такаще може да съпровожда стратегически бомбардировачи от ново поколение (ПАК-ДА), т.е. - ще бъде в състояние да ги защити от вражески самолети. Една от най-важните функции на "Охотник" обаче ще бъде пробивът на вражеската ПВО и изпълнението на внезапни високопрецизни удари върху най-важните обекти, разположени в дълбочината на фронта.[6]

Това показва, че голямо значение се отдава на управляемите системи, чието използване допреди години се заключаваше единствено и само до наблюдение, а сега започват да се причисляват към космическите войски.

Разбира се възможностите на държавата и икономиката ни далеч не са на нивото на водещите икономики и компании които разполагат с огромен финансов ресурс осъществяване на своите

разработки. Но въпреки това има и ниши които ние също можем да развием въпреки натрупаното във времето изоставане.

Едно от направленията в които можем да постигнем резултати и трябва да се развива това са именно безпилотните летателни апарати. Може би е необходимо да се припомни, че в края на 60-те и началото на 70-те години България е била водеща в развитието на безпилотните летателни апарати и много от водещите в тази област държави в момента са се учили от нас като Израел например. В момента в България има няколко фирми които се опитват да развиват този вид самолети и при подходящата подкрепа на държавата и поръчки от армията биха могли да усъвършенстват продукцията си до ниво, което да е конкурентно на международното и полезно за армията. В подкрепа на това да се развива това направление могат да се посочат много фактори като:

- по ниската цена на безпилотния самолет в сравнение със стандартния пилотируем такъв;
- по-ниска поддръжка на същия:
- отпада необходимостта от скъпото обучение и поддържане на летателни способности на пилоти;
- несравнимо по малък риск от загуба на човешки живот при изпълнение на опасни мисии и др.

Комплектуването на една батальонна бойна група с БЛА при участието й в многонационална операция би дало на командира възможност за придобиване на разузнавателна информация която да го подпомогне във вземането на решение при планиране на дадена операция или в самия ход на операцията.

Автоматичните наземни датчици и други специални сензори разполагани на близки далечни разстояния, не изискват колосални инвестиции. Разположени в определена схема те могат способстват за охраната на оперативни бази разположени в противникова територия и значително да облекчат хората ангажирани с тази дейност, като в същото време тези хора да се ангажират в изпълнението на други задачи.

Формированията от Сухопътни войски участващи в многонационални операции ще изпълняват мисии в условия на ограничена видимост и нощем. Въпреки че се работи за комплектуването на формированията с индивидуални прибори за нощно виждане те все още са твърде не достатъчни, и трябва да се достигне такова ниво на комплектуване че всеки един войник участващ в определената мисия да бъде снабден с прибор за нощно виждане. Повечето бойни бронирани машини са снабдени със старите активни прибори за нощно виждане които са лесно откриваеми от противника на бойното поле и представляват заплаха за целия екипаж на машината. Крайно време е тези прибори да се подменят с такива от по ново поколение без активно излъчване. Тук е мястото на Института по отбрана в съчетание с български фирми които произвеждат и предлагат такава продукция да намерят точното направление за развитие на това направление.

За да не изостанем тотално от нашите партньори в НАТО и да бъдем съвместими с тях при изпълнение на операции от всякакъв характер, искаме или не, трябва да положим съответните усилия и да вложим необходимите средства за комплектуване на нашите формирования при участието им в многонационални операции с техника средства и въоръжение осигуряващи ефективно изпълнеше на поставените задачи. Не го ли направим рискуваме да сме в тежест на тях и на самите нас

В условията на все по голяма редукция на средства за отбрана една от алтернативите за гарантиране на националната сигурност на страната е създаването и участието в надеждни съюзи основаващи се на взаимната полза. Но не бива да се пренебрегва възможността за възникване на условия за самостоятелно справяне със дадена криза.

При участието на формирование от Въоръжените сили в многонационална операция е необходимо дасе направи задълбочен анализ от специалисти за оборудването му със средства съобразени със спецификата на задачите които изпълнява. В противен случай участието в такава операция може да доведе до негативни последици не само за нас но за съответните коалиционни партньори.

Ако направим ретроспекция на изложеното до тук може да да се твърди че развитието на формите и способите за водене на бойни действия са в пряка зависимост от развитието на технологиите. Промяната до началото промишлената революция от края на 18 век е ставало сравнително бавно, принципите за водене на бой са си оставали сравнително същите каквити са били от началото на древността.

Техническата революция променя всичко и завинаги и както се вижда от историческите данни особено в края на 20 век предимството във воденето на война е на този който владее по виско развита тенология, която му позволява да води и бойни действия на по-големи пространства, с по точно поразяване на целите , по добра комуникация и най важното с по-малко жертви от страна на собствените войски.

Тенденцията която се наблюдава от края на 20 век за устойчиво снижаване на разходите за отбрана в повечето държави от Европа опредля нови насоки за развитие на въоръжените сили от тази част на света, а именно провеждането на многонационални операции за постигане на определени политически или военни цели без да се получава ефекта на рухнали икономики и национални катастрофи на които са били свидетели нашите предци.

За да сме пълноправни участници в многонационални операции и това участие да бъде с възможно най малко негативни последици за нас е необходимо, формированията ни да бъдат комплектовани с въоръжение и техника които са съвместими с тези на нашите партньори и позволящи ни да участваме в многонационални операции при минимален риск за българския войник. Технологичната изостаналост на армията ни трябва да бъде преодоляна защото ако ние успеем да си намерим извинение за провал касаещ само нас, то един провал довел до загуби от коалиционните ни партньори няма да ни бъде простен.

Използвана литература:

1. https://www.independent.co.uk/news/uk/home-news/future-war-robot-soldiers-enhanced-humans-space-gene-editing-ministry-of-defence-a8583621.html
2. https://bg.performancegunworks.com/1436-liquid-armor-is-already-a-reality.html
3. https://indico.cern.ch/event/657393/contributions/3083471/attachments/1692611/2723617/Antimatter.pdf АнтиматерияВероника ЧобановаГалисийски институт по физика на високите енергииУниверситет Сантяго де Компостела25 юли 2018
4. https://bg.rbth.com/science/2017/06/29/ruskite-voenni-dirizhabli-zavladyavat-nebesata_791520
5. https://informnapalm.org/bg/rusiya-izpolzva-v-donbas-nad-8-vida-drono/
6. https://bg.rbth.com/science/329527-ohotnik-radar-identichen-s-tozi-na-su57

Lyubomir K. Duchev,

GOVERNANCE, COMMAND AND MANAGEMENT OF THE ARMED FORCES IN PARTICIPING IN DISASTER PROTECTION OPERATIONS IN THE COUNTRY

Lyubomir K. Duchev

*Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences,
Department "Management of Security Systems", l_duchev_2012@abv.bg*

***Abstract**: Optimization of the organization and the system for governance, command and management of the Armed Forces of the Republic of Bulgaria when participating in disaster protection operations in the country, based on the existing legal framework.*

***Keywords**: Governance, Command, Management, Armed Forces, Disaster*

РЪКОВОДСТВО, КОМАНДВАНЕ И УПРАВЛЕНИЕ НА ВЪОРЪЖЕНИТЕ СИЛИ ПРИ УЧАСТИЕ В ОПЕРАЦИИ ЗА ЗАЩИТА ОТ БЕДСТВИЯ В СТРАНАТА

Любомир К. Дучев

Въведение

По своята същност бедствието е значително нарушаване на нормалното функциониране на обществото, предизвикано от природни явления и/или от човешка дейност и водещо до негативни последици за живота или здравето на населението, имуществото, икономиката и за околната среда, предотвратяването, овладяването и преодоляването на което надхвърля капацитета на системата за обслужване на обичайните дейности по защита на обществото.

Природо-географската структура и местоположението на България в област на висока сеизмична активност прави региона уязвим към бедствия и аварии от природен и техногенен характер, които могат да предизвикат значителни човешки и материални загуби. Природните бедствия са следствие от опасни геологически, метеорологически, хидрологически и други процеси. Налице са и техногенни рискове, които са в резултат от дейността на съществуващите обекти с промишлено предназначение, новото промишлено строителство, което разрушава природни екосистеми и негативното въздействие на консервирани обекти с потенциално опасни свойства.

Възможни бедствия на територията на Република България:

- *Земетресения* - разрушителният ефект от земетресенията се дължи на процесите, протичащи на земната повърхност в района на епицентъра, както и на вторичните отрицателни ефекти, съпътстващи земния трус или получените в последствие – пожари и взривове в електрозахранващи и газозахранващи инсталации; наводнения, вследствие на огромни водни вълни – от разрушаването на язовирни стени и други хидротехнически съоръжения; епидемии, причинени от нарушения във водоснабдяването и канализацията; радиационна опасност при разрушаване на ядрено-енергетични обекти, свлачища и други.

- *Радиоактивно замърсяване* - радиационна авария в АЕЦ “Козлодуй”, съпроводена с изхвърляне на радиоактивни продукти в околната среда; - авария в АЕЦ извън страната и трансграничен пренос на радиоактивни продукти; - авария в други обекти с ядрени и радиоактивни материали.

- *Наводнения* - разливания на реки, рязко повишаване на нивото на Черно море, след интензивни снеговалежи и/или интензивно снеготопене, заприщване на течението в речно легло вследствие натрупването на отпадъци, скални материали и дървета.

- *Промишлени аварии, свързани с отделянето на опасни вещества* - технологични аварии с токсични химични вещества; - транспортни инциденти; - прекъсване на продуктопроводи, нефтопроводи и газопроводи; - разпиляване на пестициди; - нефтени разливи по реки и море.

- *Биологично заразяване* - производствено-икономически условия, влошената международна епизоотична и епифитотична обстановка, търговията, вносът и износът на живи животни, продукти от животински и растителен произход са условия за възникване на огнища на биологично заразяване**.**

- *Свлачища* - катастрофални явления, които се отразяват негативно върху състоянието на околната среда, техническата инфраструктура и материалните ресурси.

- *Масови горски и полски пожари* - възникват по различни причини, като не могат да бъдат прогнозирани, а броят им през последните години се увеличава. Характеризират се със заплаха за живота и здравето на голям брой хора, големи материални щети и замърсяване на околната среда.

- *Обилни снеговалежи, снежни бури и заледявания* - континенталният климат е в основата на възможни снегонавявания. Снежните бури и заледявания са често явление за нашата страна, като водят до разрушаване на въздушни комуникации, блокиране на пътища и могат да поставят в рискова ситуация живота на много хора.

- *Бедствия, вследствие на инциденти с плавателни съдове* - речният и морският трафик в териториалните води на страната, в прилежащата зона и в открито море, както и превозът на товари, в т.ч. опасни субстанции, са свързани с риск от аварии или инциденти с плавателни съдове.

- *Автомобилни, железопътни и авиационни катастрофи* - през територията на страната преминават основни международни железопътни, автомобилни и въздушни трасета, по които се транспортират различни по количества и вид химически, пожароопасни и взривоопасни продукти.

- *Терористични актове с употреба на оръжия за масово поразяване (ОМП)* - терористичните действия са предварително обмислени, детайлно планирани и се извършват от организации с различна структура. Обекти на терористични актове с използване на ОМП могат да бъдат публични личности, превозни средства, сгради и прояви с масово събиране на хора като зали, ритуални домове, транспортни средства, гари, летища, големи магазини, митинги, концерти на открито, спортни прояви и т.н.

- *Невзривени бойни припаси* - на територията на страната има неустановени по количество и месторазположение невзривени авиационни, артилерийски, морски и стрелкови боеприпаси. Значителна част са запазили бойните си възможности и представляват смъртоносна опасност при неправилно боравене с тях.

Промените в климата водят до нарастване на честотата и мащаба на бедствията, за което е необходимо обединяване на усилията на всички отговорни институции в България и включването им в дейности за намаляване на риска от бедствия и максимално ограничаване на човешките, социалните, икономическите и природните щети и загуби.

Изложение

Въоръжените сили на Република България включват: - Българската армия; - служба "Военна полиция"; - служба "Военна информация"; - военните академии и висшите военни училища; - Военномедицинската академия; - Националната гвардейска част; - Военно-географската служба; - Стационарната комуникационна и информационна система; - Централното военно окръжие; - Централния артилерийски технически изпитателен полигон; - Комендантство – МО.

Ръководството на въоръжените сили е дейност и отговорност на политическото и военно-политическото ръководство, а командването и управлението се осъществява от военните командири от всички нива по степени на правомощия. Системата за ръководство, командване и управление на въоръжените сили е изградена на три нива:

- стратегическо ниво (Президент, Министерски съвет, министър на отбраната, началник на отбраната, както и подчинените им щабове и служби);

- оперативно ниво (Съвместно командване на силите, Сухопътни войски, Военновъздушни сили и Военноморски сили);

- тактическо ниво – включва командирите и щабовете на формированията от въоръжените сили.

Държавното ръководство реализира ръководните си функции спрямо въоръжените сили: - *косвено* - закони и други нормативни актове, които въздействат с включените в тях правила, норми, ценности, мотиви и принципи; - *пряко* - заповеди, разпореждания, директиви, указания и др.

Ръководството е механизъм, който реализира идеите на управляващия субект по цялата йерархична верига в низходящ ред. По тази причина може да се приеме, че ръководство има и на военностратегическо, оперативно и тактическо ниво. Ръководството е акт на налагане на волята на управляващия субект спрямо управляваната система.

Командването и управлението са специализирани, експертни дейности, които обединяват всички управленчески функции във въоръжените сили и се осъществява по степени на правомощия. Командването и управлението се отнасят до всички нива на армейската структура в целия спектър от мисии и задачи. Чрез тях командирът упражнява предоставената му власт и носи пълна отговорност за изпълнението на задачите и постигането на поставените цели.

В мирно време въоръжените сили поддържат способности за участие в операции в отговор на кризи, кризисни ситуации и инциденти на територията на страната за осъществяване на: - дейности по контрола на въздушното пространство и морските пространства; - защита на стратегически обекти, включително на системите за производство, доставка и разпределение на енергийни ресурси; участие в операции по сдържане и неутрализиране на терористични, екстремистки и престъпни групи; - защита и подпомагане на населението при природни бедствия, аварии и екологични катастрофи; - неутрализиране на невзривени боеприпаси; - оказване на хуманитарна помощ; - съдействие за контрола на миграцията; - спасителни и евакуационни дейности; - помощ, при необходимост, на други държавни органи, организации.

Обществените отношения, свързани с осигуряването на защитата на живота и здравето на населението, опазването на околната среда и имуществото при бедствия в Република България се осъществява съгласно Закон за защита от бедствия и разработените документи във връзка с изпълнението му.

Дейности по защитата на населението при опасност или възникване на бедствия:

- предупреждение;
- изпълнение на неотложни мерки за намаляване на въздействието;
- оповестяване;
- спасителни операции;
- оказване на медицинска помощ при спешни състояния;
- оказване на първа психологична помощ на пострадалите и на спасителните екипи;
- овладяване и ликвидиране на екологични инциденти;

- защита срещу взривни вещества и боеприпаси;
- операции по издирване и спасяване;
- радиационна, химическа и биологична защита при инциденти и аварии с опасни вещества и материали и срещу ядрени, химически и биологични оръжия;
- ограничаване и ликвидиране на пожари;
- временно извеждане, евакуация, укриване и предоставяне на индивидуални средства за защита;
- извършване на неотложни аварийно-възстановителни работи;
- ограничаване на разпространението и ликвидиране на възникнали епидемични взривове, епидемии и епизоотии от заразни и паразитни болести;
- други операции, свързани със защитата.

Дейностите се изпълняват от единната спасителна система (ЕСС), която включва структури на:

- министерства и ведомства;
- общини;
- търговски дружества и еднолични търговци;
- центрове за спешна медицинска помощ, други лечебни и здравни заведения;
- юридически лица с нестопанска цел, включително доброволни формирования;
- въоръжените сили.

Структурите са съставни части на ЕСС, но запазват институционалната или организационната си принадлежност и определените им функции или предмет на дейност. Координацията на съставните части на ЕСС се осъществява чрез оперативните центрове на Главна дирекция "Пожарна безопасност и защита на населението" - МВР.

Въоръжените сили предоставят помощ при провеждане на спасителни и неотложни аварийно-възстановителни работи с разрешение на министъра на отбраната въз основа на искане от съответния държавен орган съгласно план на министерството на отбраната за защита при бедствия.

Взаимодействието и координацията между частите на ЕСС, участващи в изпълнението на дейности в района на бедствието, се извършва от ръководител на операциите, който се определя със заповеди на министър-председателя на Република България, на съответния областен управител или кмет на община в зависимост от обхвата на бедствието. Ръководителят на операциите организира и контролира изпълнението на одобрените решения на щабовете за изпълнение на плановете за защита при бедствия.

Държавната политика в областта на защитата при бедствия се формира и осъществява от Министерския съвет, който:

- осъществява общото ръководство на защитата при бедствия;
- приема Национална стратегия за намаляване на риска от бедствия;
- приема Национална програма за намаляване на риска от бедствия и годишни планове за защита от бедствия;
- приема Национален план за защита при бедствия;

- въвежда Национална система за ранно предупреждение и оповестяване на органите на изпълнителната власт и населението при бедствия;
- планира финансови средства за защита при бедствия.

За подпомагане изпълнението на тези дейности към Министерския съвет се създава Съвет за намаляване на риска от бедствия, който включва представители на ръководствата на министерствата, ведомствата, Българската академия на науките, висши училища, научно-изследователски институти, Националното сдружение на общините в Република България, Българския Червен кръст и юридически лица, включително юридически лица с нестопанска цел, имащи отношение към намаляването на риска от бедствия.

За изпълнение на Националния план за защита при бедствия със заповед на министър-председателя на Република България се създава национален щаб с поименно определени ръководител и членове: министри, заместник-министри, ръководители на ведомства или техни заместници и други, представляващи институции, които имат задължения за изпълнението на Националния план за защита при бедствия. Дейността на Националния щаб се обслужва логистично, комуникационно и административно от Главна дирекция "Пожарна безопасност и защита на населението" - МВР, както и от компетентните с оглед характера на бедствието министерства, ведомства и институции.

Във връзка със Закона за отбраната и въоръжените сили, Закона за защита при бедствия, Националната програма за защита при бедствия и Националния план за защита при бедствия, за създаване на организация за ефективно участие на ресурсно осигурени и подготвени сили и средства от министерството на отбраната и въоръжените сили, в действия по оказване на помощ на населението при бедствия на територията на страната, във взаимодействие с органите на изпълнителната власт, е изготвен План на министерство на отбраната за защита при бедствия, с който е създадена организация за:

- разпределение на задълженията между структурите от Министерството на отбраната и въоръжените сили за оказване на помощ на населението при бедствия;

- взаимодействие на силите и средствата от Министерството на отбраната и въоръжените сили с останалите части на ЕСС;

- ресурсно осигуряване действията на определените сили и средства от Министерството на отбраната и въоръжените сили.

Въоръжените сили подготвят и поддържат в готовност военни формирования за оказване помощ на населението при бедствия, съгласно утвърдени Планове за защита при бедствия, като:

- силите и средствата от Министерството на отбраната и въоръжените сили се привличат след изчерпване възможностите на другите съставни части на ЕСС, за нарастване на техните усилия;

- привличането на сили и средства извън определените в плановете за оказване на непосредствена помощ на населението, се извършва целево, само след разрешение от министъра на отбраната за всеки отделен случай;

- финансовите и материални средства, разходвани за осигуряване на дейността на военните формирования от Министерството на отбраната и въоръжените сили при оказване на помощ на населението при бедствия се възстановяват след приключване на операцията от Министерския съвет.

Органи за управление, сили и средства – вида и състава на формированията, техника и имущества от Министерството на отбраната и въоръжените сили при оказване на помощ на населението при бедствия са:

1. *Щаб за защита при бедствия на Министерството на отбраната* - подпомага министъра на отбраната по въпросите на защитата при бедствия при:

- организирането и контрола на превантивната дейност във въоръжените сили за преодоляване на последиците от бедствия;

- осъществяване на ръководство и координация за изпълнението на задачите от формированията и структурите от въоръжените сили, участващи при овладяването и/или преодоляването на последиците от бедствия;

- координацията и взаимодействието с останалите части на ЕСС на страната.

Съставът на Щаба се определя със заповед на министъра на отбраната и включва ръководен състав от структури на Министерството на отбраната, структурите на пряко подчинение на министъра на отбраната и Българската армия, имащи функционални задължения по защитата при бедствия.

Щабът изготвя проекти на заповеди на министъра на отбраната, относно:

- привеждане в изпълнение на плана за защита при бедствия на министерството на отбраната и участие на формирования от въоръжените сили в оказване помощ на населението при бедствия;

- провеждане на неотложни мерки от военните формирования на въоръжените сили дислоцирани в района на възникналото бедствие;

- провеждане на спасителни и неотложни аварийно-възстановителни работи от формирования на въоръжените сили;

- прекратяване участието на формирования от въоръжените сили в оказване помощ на населението при бедствия и за провеждане на дългосрочни мерки за ликвидиране на последствията от възникналото бедствие.

2. Българска армия (БА) - Военните формирования от Българската армия създават, подготвят и поддържат в готовност за действия „Формирования за овладяване и/или преодоляване на последствия от бедствия” (ФОППБ) по типове, състав, техника и имущества за оказване на помощ на населението за: - ликвидиране на последствията при авария в АЕЦ „Козлодуй”; - действие при промишлени аварии; - гасене на пожари; - действие при наводнение; - действие при земетресение; - действие при тежки зимни условия; - разузнаване и унищожаване на невзривени бойни припаси.

Основни задачи на БА:

- подпомагане на населението и изпълнителната власт при овладяване и/или преодоляване на последствията от бедствия;

- формиране, подготовка и поддържане в готовност на сили и средства, предназначени за участие в действията за защита на населението при бедствия на територията на цялата страна;

- поддържане на надеждна система за оповестяване и привеждане в готовност на определените сили и средства за участие в операцията;

- осигуряване и поддържане в готовност на система за командване и управление при водене на операция за оказване помощ на населението при бедствия;

- организиране на взаимодействието на силите и средствата от БА с определените структури на министерствата, ведомствата и органите на централната и местната власт при оказване на помощ на населението при бедствия.

На основание заповед на министъра на отбраната № ОХ-138/06.02.2019 г., ФОППБ изпълняват дейности по разузнаване, идентифициране, оценка, обезвреждане на място или транспор-

тиране за последващо унищожаване на открити невзривени боеприпаси на територията на страната, извън войсковите полигони, райони и обекти. Организацията за изпълнението, контрола и отчитането на дейностите на ФОППБ се осъществява съгласно заповед на началника на отбраната №ЗНО-148/11.07.2019 г. относно обявяване на стандартна оперативна процедура.

Информация за открит невзривен боеприпас постъпва с писмено искане (факс) от Министерството на вътрешните работи, други министерства и ведомства, областните управители и кметовете на общини до дежурния офицер във Военния команден център (ВКЦ) на БА. В зависимост от мястото на откриване на невзривените боеприпаси и прилежащия район на отговорност на ФОППБ, с разрешение на министъра на отбраната и резолюция на началника на отбраната, искането се изпраща до вида въоръжени сили, на която се разпорежда изпълнението на задачата. Командирът на вида въоръжена сила изготвя писмена заповед, която се изпраща до военното формирование за привеждане в действие на съответното ФОППБ. Командирът на военното формирование отдава своя писмена заповед, в която се указва реда за действие, изискванията и мерките за безопасност съгласно „Ръководство по подривните работи" и „Инструкция за действие при откриване на невзривени боеприпаси".

Охраната на намерените невзривени боеприпаси, до пристигането на модулна група и информирането на местното население за опасностите от тях се извършва от регионалните структури на МВР, а съпровождането на автомобилите на модула до подготвени площадки или полигони за последващо унищожаване на боеприпасите се извършва от структурите на Служба „Военна полиция" - МО.

Командването на ФОППБ се извършва по реда на подчиненост, а управлението се осъществява от ВКЦ по постоянно действащите комуникации.

3. Военномедицинска академия - основни задачи:

- извършва прогнозиране и оценка на общата и медицинска обстановка, възникващи в резултат на различни бедствия;

- подготвя подчинените си заведения и медицинските екипи за действие при бедствия;

- прогнозира медицинските загуби сред населението и структурите на въоръжените сили при възникване на бедствия;

- оказва специализирана и квалифицирана медицинска помощ на териториален принцип със специализирани екипи на ВМА и подчинените й многопрофилни бази за активно лечение.

4. Служба „Военна полиция" **- о**сновни задачи:

- ограничаване достъпа на лица, неучастващи в спасителните операции до пострадалите райони и обекти;

- наблюдение и събиране на информация за установяване на реалните граници на поражение;

- изпълнение на охранителни мероприятия в районите и обектите пострадали от бедствие;

- изпълнение на регулировъчни функции на пътното движение в пострадалите райони;

- ескортиране на колони от специализирани транспортни средства, участващи в аварийно-спасителните работи;

- контрол при превозването и разпределението на хранителни продукти за пострадалото население.

5. Изпълнителна агенция "Военни клубове и военно-почивно дело" - основни задачи:

- предоставяне на наличните инфраструктурни обекти и леглова база за настаняване на хора останали без подслон;

- нарастване на капацитета на държавните органи, държавната и местната администрация, след изчерпване на техните възможности.

6. Дирекция „Инфраструктура на отбраната" и Централно военно окръжие - осигуряват временно настаняване в освободени войскови райони на пострадали от бедствието лица.

Министърът на отбраната, чрез Щаба за защита при бедствия на министерството на отбраната осъществява ръководството и координацията за изпълнението на задачите на силите и средствата на структурите на Министерството на отбраната и въоръжените сили, участващи при овладяването и/или преодоляването на последиците от бедствия.

Началникът на отбраната осъществява общото ръководство на действията на ФОППБ в системата за командване и управление на въоръжените сили.

При привеждане в действие на ФОППБ от повече от един вид въоръжена сила, командването и управлението се осъществява от командващия Съвместното командване на силите (СКС) в общата система за командване и управление в Българската армия, а непосредственото - от назначените ръководители (командири) на формирования. При привеждане на ФОППБ само от пряко подчинените на СКС или от един вид въоръжена сила, командването и управлението се осъществява съответно от командващия СКС или от командира на вида въоръжена сила, а непосредственото – от назначените ръководители (командири) на формирования.

Взаимодействието между ФОППБ и силите и средствата на структурите на подчинение на министъра на отбраната, участващи при овладяването и/или преодоляването на последиците от бедствия се организира от Щаба за защита при бедствия на министерството на отбраната.

Взаимодействието между ФОППБ в зоната на операцията се организира от командващия на СКС (командира на СВ, ВВС или ВМС) и се осъществява от командирите на ФОППБ.

Практическите действия на ФОППБ преминават през 6 основни етапа:

1. Поддържане в готовност.

2. Подготовка и извършване на марш.

3. Развръщане в района на бедствието.

4. Участие в овладяването и/или преодоляването на последствията от бедствието.

5. Ротация.

6. Изтегляне в пункта за постоянна дислокация.

Действията на личния състав на ФОППБ за всеки един етап са описани в Плана на Българската армия за оказване помощ на населението при бедствия и Плановете на СКС и видовете въоръжени сили за оказване помощ на населението при бедствия.

Изводи

В България е възможно възникването на различни по вид бедствия, които могат да предизвикат значителни загуби на човешки и материални ресурси и да окажат неблагоприятно влияние на националната сигурност и стабилност в региона. Тяхното проявление би довело до сериозни затруднения в нормалната работа на инфраструктурата в районите на бедствия, като ще се нарушат жизненоважни системи за управление и нормалното функциониране на националното стопанство и условията за живот на населението. За овладяване на кризисните ситуации, намаляване на загубите и ликвидиране на последствията е необходимо предварително прогнозиране, планиране и съгласуване на мероприятията по защитата на населението и собствеността в рамките на ЕСС. Характерът на последствията от вероятните бедствия изисква готовност за използване на всички способи и средства за защита на населението и националното стопанство и провеждане на предварителни мероприятия за тяхното недопускане и намаляване на вредното им въздействие.

Важно значение за успешната защита на населението имат превантивните дейности и особено такива, които позволяват да се прогнозира появата и развитието на бедствените явления, както и за отстраняване на предпоставките за възникването им. Обемът и спецификата на спасителните и неотложните аварийно-възстановителни работи налагат подготовка и поддържане в готовност на сили и средства на държавните институции, които имат функционални задължения по тези проблеми.

Въоръжените сили притежават оперативни способности, органи за управление и ресурс от сили и средства да участват активно в оказване помощ на населението при бедствия на територията на страната.

За предотвратяване на възможните последствия за населението при възникване на бедствия се налага непрекъснато и целенасочено обучение по способите за защита и самозащита и своевременно информиране. За осигуряване провеждането на спасителни и неотложни аварийно-възстановителни работи и осигуряване условия за живот в бедстващи райони е необходимо наличието на запаси от материално-технически и финансови средства.

За прилагане на единен подход, намаляване на риска от бедствия, осигуряване на съгласуваност между отделните дейности и мерки, и рационално разходване на наличните ресурси в страната, както и за намаляване на съществуващите рискове от бедствия и недопускане възникването на нови такива е необходимо изготвяне и изпълнение на стратегията, програмите и плановете за защита при бедствия на съответните нива на управление в страната, съгласно Закона за защита при бедствия.

Реализирането на Националната стратегия за намаляване на риска от бедствия 2018 – 2030 г. и планиращите документи за защитата при бедствия в страната е важно, за да бъдем по-добре подготвени и устойчиви на предизвикателствата, което ще е основа за постигане на траен икономически, социален и екологичен просперитет.

Литература

1. Закон за отбраната и въоръжените сили, обн. в ДВ, бр. 35 от 12.05.2009 г., посл. изм. и доп., бр. 42 от 28.05.2019 г., в сила от 28.05.2019 г.
2. Закон за защита при бедствия, Обн., ДВ, бр. 102 от 19.12.2006 г., посл. изм. и доп., бр. 77 от 18.09.2018 г., в сила от 1.01.2019 г.
3. Национална стратегия за намаляване на риска от бедствия 2018 – 2030 г., РМС № 505 от 19 юли 2018 г.
4. Национална програма за защита при бедствия 2014 - 2018 г.
5. Национален план за защита от бедствия, РМС № 973 от 29 декември 2010 г.
6. Наредба за условията и реда за функциониране на Националната система за ранно предупреждение и оповестяване на органите на изпълнителната власт и населението при бедствия и за оповестяване за въздушна опасност.
7. План за развитие на въоръжените сили на Република България до 2010 г., ПМС № 382 от 30 декември 2015 г.
8. Доктрина на въоръжените сили на Р България, МО, С., 2017 г.
9. Национална отбранителна стратегия, МО, С., 2016.
10. Стратегия за национална сигурност, приета с Решение на НС от 25.02.2011 г., обн., ДВ, бр. 19 от 8.03.2011 г.
11. МЗ № ОХ-138/06.02.2019 г. относно организация за изпълнение на дейностите на ФОППБ при разузнаване, транспортиране и унищожаване на невзривени бойни припаси открити на територията на страната.

Radoslav B. Chalakov,

PLANNING OF THE FIRE SUPPORT IN THE PROCESS OF PLANNING ON OPERATIONS

Radoslav B. Chalakov

ВОЕННА АКАДЕМИЯ "ГЕОРГИ СТОЙКОВ РАКОВСКИ"
КАТЕДРА "СУХОПЪТНИ ВОЙСКИ", r.chalakov@rndc.bg

Abstract: *Dynamically noticeable on Monday, security is evident from the ever-changing element of conflict, the emergence of new technologies, and the opening up of new combat capabilities. You need to change the format for use of the Armed Forces, go out for planning, and check operations on the new Thursday to save, recommend looking at a new way of the process in order to use the format to manage your systems. the forces and means of fire support.*

ПЛАНИРАНЕ НА ОГНЕВАТА ПОДДРЪЖКА В ПРОЦЕСА НА ПЛАНИРАНЕ НА ОПЕРАЦИИ

Радослав Б. Чалъков

Нека нашето предварително безпокойство се превърне в предварително мислене и планиране. Уинстън Чърчил

Въведение

За подготовката и провеждането на една военна операция [25]е необходимо да се разработят оперативни планове, в които да залегнат всички фактори, от които зависи нейното ефикасно и успешно провеждане.

Освен това, ясното определяне и поставяне на подходящо ниво на правомощията за инициирането и изготвянето на оперативни планове на всички нива е от особена важност за осигуряване на необходимата политическа и военна експертиза за стартиране на процеса на планиране и разрешаване на военно-политическа криза. Това ще позволи на командирите от всички нива от ВС да провеждат адекватно планиране според техните компетенции. [4]

Съгласно "*Доктрина за планиране на операции*" *НП-05* планирането е организационно и функционално структуриран процес, извършван от командирите и щабовете чрез формиране на групи за планиране, който цели превръщането на намерението на командира в план за неговата реализация. Целта му е своевременно и ефикасно да се подготвят въоръжените сили на Република България за провеждане на/или участие в операции/кампании в отговор на текущи, развиващи се, вероятни или потенциални кризи. Резултатът от този процес е разработването на план или серия от планове. Субект на планирането са командирите (групите за планиране на операции от тяхно име), а обект на планирането – използването на силите. [2]

[25] *Военна операция са координираните военни действия на дадена държава като отговор на определена ситуация. Тези действия са проектирани и предначертани във военен план на операциите (военнооперативен план), който има за цел да разреши ситуацията в полза на дадената страна. [8]*

Планирането на операции е процес от аналитично последователни логически стъпки, водещи до уясняване на мисията, разработването, анализирането и сравняването на варианти за действие (ВД), избиране на ВД и изготвяне на план.

Този процес подпомага командирите и щабовете да вземат правилни решения за бъдещи действия, които да са адекватни на условията на обстановката, и от там и общото разбиране за същността на целите на операцията/кампанията. Процеса също подпомага разработването на различни варианти (опции), които ефективно да отговорят на предизвикателствата и осигурят правилното използване на военната мощ за постигане на стратегическите цели.

Процесът на планиране на операции е съвкупност от доказани в практиката процедури, прилагани от командира, щаба и подчинените структури при организиране на дейностите и разработване на планове, които по най-добрия начин осигуряват изпълнението на мисията.

В основата на планирането на операциите е правилната оценка на рисковете и конкретните действия за намаляването им. При разработване на различните ВД, целящи постигане на желаното крайно състояние, командирите и техните планиращи органи определят необходимите сили и средства за постигането на целите, сравняват наличните с необходимите способности и определят техния недостиг/излишък.

Целият процес е част от една система, която представлява съвкупност от взаимосвързани и работещи в синхрон военни и невоенни органи за управление, прилагащи общи политики, доктрини и процедури, използващи оперативно съвместими оборудване, съоръжения и комуникации и изпълняващи задачи за изготвяне, преглед и изпълнение на планове за съгласувани действия на въоръжените сили и невоенните компоненти (правителствени и неправителствени организации).

Тази система подпомага диалога и взаимодействието между различните нива на командване, така че да бъде осигурено пълното използване на военния инструмент на националната мощ в съответствие с националните приоритети, и осигурява непрекъснат преглед и обновяване на изготвените планове в съответствие с промените в стратегическите указания, ресурсите и оперативната среда.

За ефективно изпълнение на плана следва да се определи редът за формиране на необходимите сили и средства, тяхното активиране и развръщане, като им се възлагат отговарящи на способностите им задачи за разрешаване на кризата.

Планирането на операция е ориентирано към постигане на желано крайно състояние и стратегическите цели, установени от държавното ръководство и се извършва в рамките на политически и ресурсни ограничения. За всяко ниво на планиране ще се иска и определена цел за постигане. На стратегическо ниво целта е превръщането на политическите параметри във военни указания за командирите на оперативно ниво. На оперативно целта на планирането е да трансформира стратегическите указания в серия от интегрирани, с приемлив риск военни действия за ефективно постигане на целите. Изпълнението на оперативните цели допринася за постигане на стратегическите цели.

При планирането на огневата поддръжка като част от общия процеса е необходимо предварително да се извърши анализ на състоянието на модела за планиране на огневата поддръжка. По този начин е възможно да бъде ясно дефинирано мястото на процеса за планиране на огневата поддръжка като част от всеобхватния процес на планиране .

Планирането на огневата поддръжка е непрекъснат и едновременен процес на анализиране, разпределение и определяне на задачи с цел тяхното интегриране и синхронизиране с плановете на командирите, а така също и за максимизиране на бойната мощ.[3]

Целта на планирането на огневата поддръжка е да се постигне необходимата ефективност и ефикасност при изпълнение на изискванията на силите за огнева поддръжка, също така и да се определи правилното рапределение на средствата за огнева поддръжка.

Съществуват следните категории планиране на операциите, приложими за операции, както по чл. 5 на Вашингтонския договор, така и извън чл. 5 - предварително, непосредствено (в отговор на кризи) и детайлно.

Предварително планиране се извършва по време на предварителната подготовка и е процес на първоначално разработване и въвеждане на планове, базирани на сценарии в съответствие с прогнози, необвързани с времеви граници и ограничения. То се извършва в мирно време, посредством поетапен йерархичен работен процес и се провежда за по-продължителен период от време като може да протече в рамките на няколко месеца. Резултат на предварителното планиране са оперативните плановете за потенциални кризисни ситуации и/или постоянните отбранителни планове.

Непосредственото (кризисно) планиране е процес на планиране в отговор на текуща (развиваща) се криза. При него може да се използва по възможност съществуващ план, който да бъде в основата на разработването на оперативния план. То е процес на непрекъснато разработване и актуализиране на текущи и последващи оперативни планове в хода на разрешаване на кризата (военния конфликт). Използва се при разработване на оперативен план (оперативна заповед) за използване в предстояща операция или криза. Непосредственото планиране се основава на конкретни събития и се провежда в изострени кризисни ситуации и непредвидени обстоятелства.

Детайлното планиране се извършва в групите и подгрупите за планиране и координиране на огневата поддръжка, центровете за координиране на огневата поддръжка и елементите за огнева поддръжка на сухопътния компонент, в авиационния оперативен център на военновъздушния компонент, в морския оперативен център на военноморския компонент и щабовете на маневрените формирования. В тези органи за планиране се изготвят планове за огневата поддръжка и се поставят задачи на силите и средства за огнева поддръжка, като се указват: целите за въздействие (отделни и групови цели); целта на поразяването (унищожаване, неутрализиране, подавяне); времето за нанасяне на ударите и огъня; реда за оценка и докладване на бойните загуби на целите след поразяването им.

Детайлното планиране продължава при непосредствените изпълнители, които определят: какви сили да се привлекат за изпълнение на задачата; какви способи за изпълнение на задачите да се приложат; времето за нанасяне на ударите и огъня; разхода на ракети и боеприпаси; реда за оценка и докладване на бойните загуби на целите след поразяването им.

Планиращите огневата поддръжка са отговорни за изготвянето на целесъобразни предложения на командирите относно най-доброто използване на наличната огнева поддръжка, разработване на плановете за нейното провеждане, издаване на необходимите заповеди до подчинените командири и изпълнение на одобрените планове.

Процеса на планиране определя какъв тип цели ще бъдат поразени, кога и с какви средства. При планиране на необходимия брой цели, както и процеса на насочване, който е критичен елемент от процеса на планиране на огневата поддръжка е необходимо:

- да се оцени терена и ПС;
- да се индетифицират онези групировки на ПС, оборудването, съоръженията и обектите, върху които трябва да се въздейства, за да се гарантира успеха.

Едни от основните принципи както при планирането така и при разработване на плана за огнева поддръжка са:

- ранно и непрекъснато планиране;
- правилното използване на всички налични средства;
- използването на минималното количество средства, нужни за осигуряването на ефективна огнева поддръжка;
- използване на най-ефективните огневи средства;
- вида на огневата поддръжка;
- избягване на ненужното дублиране;
- координиране на въздушното пространство;
- осигуряване навременна огнева поддръжка;
- осигуряване на взаимодействието;
- определяне на линиите за координиране на огневата поддръжка;

- установяване на комуникационната поддръжка.

Ранното и непрекъснатото планиране.

За да се интегрира ефективно огневата поддръжка плана на маневрените формирования, планирането трябва да започне, когато командира посочи мисията и представи указания по планиране.

Обмислено използване на всички налични средства.

Да се гарантира, че информацията от всички налични ресурси се оценява бързо и се насочва към подходящите средства. Това включва информация от собствените, от съседни и поддържащи елементи и от по- старшото ниво.

Използване на минималното количество средства, нужни за осигуряването на ефективна огнева поддръжка.

Решава се какво е необходимо и ако определените в конкретния случай са недостатъчни, трябва да се поиска допълнителна поддръжка.

Използване на най-ефекритните огневи средсва.

При вземане на решение се разглежда естеството и важността на целта, времето за поразяване, наличието на средства за поддръжка и желаните резултати. Може също така да се обмисли и за средства за временно използване по целта, докато по-ефективното средство може да и въздейства. **Пример** *за това е ситуация, при която въздушната поддръжка е най-желаното средство, но е на около 20 минути. В този случай непряко огнево средство може да фиксира целта, докато пристигне самолетът.*

Вида на огневата поддръжка.

От намерението на командира се знае какво е необходимо относно приоритетните цели, настоящите и бъдещите потребности на огневата поддръжка. Но въпреки това може да се прецени искането на друго средство за огнева поддръжка.

Избягване на ненужното дублиране.

Основна задача е да се гарантира избягване на дублиране, а при необходимост на такова ще се използват само минимални средства, необходими за постигане на желаните ефекти.

Координиране на въздушното пространство.

При планирането на огневата поддръжка се предоставят данни относно използването на въздушното пространство от състава, участващ в управлението на въздушното пространство, а на по-ниски нива подобна координация може да включва въздушни наблюдатели и други ползватели на въздушното пространство.

Осигуряване на навременна огнева поддръжка.

Необходимо е да определи количествата и видовете огнева поддръжка, необходими за успеха. Тук също трябва да се информира командира на маневреното формирование, когато няма достатъчно ресурси в подкрепа на неговия план.

Осигуряване на взаимодействието.

Целесъобразно е да се знаят тактико-техническите характеристиките на различните средства за огнева поддръжка и да има информация за тяхната наличност. Също така е необходимо и наличие на информация за развитието на бойните действия, за да се въздейства както на планираните цели, така и други възникнали задачи.

Определяне на линиите за координиране на огневата поддръжка.

Мерките за координиране на огневата поддръжка са предназначени да улеснят бързото въздействие по целите и в същото време да осигурят предпазни мерки за собствените и съседни сили. Те гарантират, че огневите удари и атаки няма да застрашат безопасността на силите, ще взаимодействат с други огневи средства и/или няма да нарушат съседните операции. С изключение на границите/разграничителните линни/зони, мерките за координиране на огневата поддръжка са разрешителни или ограничителни. По същество основната цел на разрешителните е да се улесни въздействието върху целите. Следователно основната цел на ограничителните е да осигурят безопастност за съседните сили.

Така разгледаните принципи при планирането на огневата поддръжка в момента на взимане на решение от командира за въздействие върху ПС, не е необходимо да се създава значително превъзходство на сили и средства. Предполага се, че различните видове оръжия са съпоставими по отношение на приноса към крайния резултат от военните действия и затова на всеки от тях може да се придаде определена тежест. В таблица №1 е показано вариант на матрица на целите, чрез която се определя необходимото средство за въздействие към определена цел с определена тежест, който ще има най-голям ефект при използването му. Показаните данните в модела са примерни. Същите следва да не бъдат взимани по внимание.

Показания модел ще сведе до минимум вероятността за ненужно дублиране, както и осигуряване на навременна огнева поддръжка, чрез използване на най-ефекритното огнево средсво. Този модел ще подпомогне планирането на минималното количество огневи средства, нужни за въздействието по определена цел.

В заключение може да се каже, че е необходимо непрекъснато да се изучават, познават и целесъобразно да се избират в реални условия, основните принципи оказващи влияние при поразяване на ПС, на груповите и отделните цели при различни видове бойни действия.

Таблица 1

МАТРИЦА НА ЦЕЛИ (ВАРИАНТ)

ПРИОРИТЕТ		**1**	**2**	**3**	**4**	**5**	**6**
ГРУПИ ЦЕЛИ		**Системи за ПВО**	**Кораби за ОгП**	**Десантни кораби**	**С4I**	**Маневр. форм.**	**РЛС**
КОГА		**планови/по извик-ване**	**планови/по извикване**	**планови/по извик-ване**	**планови/по извик-ване**	**планови/по извик-ване**	**планови/по извикване**
ЕФЕКТ		**Унищожаване**	**Неутрализиране**	**Подавяне**	**Подавяне**	**Неутрализиране**	**Унищожаване**
СИСТЕМИ ЗА ПОРАЗЯВАНЕ	**Авиация**	избор с-ма **4** точност координ. 500м. време на поз. 30мин количество с-ми 2 неподвижна не	избор с-ма **1** точност координ. 500м. време на поз. 30мин количество с-ми 2 неподвижна не	избор с-ма **1** точност координ. 200м време на поз. 30мин количество с-ми 2 неподвижна не	избор с-ма **2** точност координ. 500м. време на поз. 30мин количество с-ми 2 неподвижна не	избор с-ма **3** точност координ. 500м. време на поз. 30мин количество с-ми 2 неподвижна Не	избор с-ма **3** точност координ. 500м. време на поз. 30мин количество с-ми 2 неподвижна не
	9К79	избор с-ма **3** точност координ. 100м време на поз. 17мин количество с-ми 1 неподвижна да	избор с-ма **4** точност координ. 50м време на поз. 17мин количество с-ми 1 неподвижна да	избор с-ма **4** точност координ. 50м време на поз. 17мин количество с-ми 2 неподвижна да	избор с-ма **1** точност координ. 50м време на поз. 17мин количество с-ми 2 неподвижна да	избор с-ма **4** точност координ. 50м време на поз. 17мин количество с-ми 1 неподвижна Да	избор с-ма **4** точност координ. 50м време на поз. 17мин количество с-ми 1 неподвижна да
	РСЗО	избор с-ма **2** точност координ. 150м време на поз. 15мин	избор с-ма **2** точност координ. 100м време на поз. 15мин	избор с-ма **3** точност координ. 50м време на поз. -	избор с-ма **3** точност координ. 50м време на поз. 15мин	избор с-ма **2** точност координ. 150м време на поз. 15мин	избор с-ма **1** точност координ. 50м време на поз. -

		количество с-ми	4	количество с-ми	8	количество с-ми	16	количество с-ми	8	количество с-ми	8	количество с-ми	4
		неподвижна	да	неподвиж-на	да	неподвиж-на	не	неподвижна	да	неподвижна	Да	неподвижна	не
	Нарезна Арт.	избор с-ма	**1**	избор с-ма	**3**	избор с-ма	**2**	избор с-ма	**4**	избор с-ма	**1**	избор с-ма	**2**
		точност ко-орд.	50м	точност коорд.	50м	точност коорд.	50м	точност ко-орд.	50м	точност ко-орд.	100м	точност ко-орд.	50м
		време на поз.	15мин	време на поз.	15мин	време на поз.	-	време на поз.	-	време на поз.	-	време на поз.	-
		количество с-ми	8	количество с-ми	24	количество с-ми	24	количество с-ми	16	количество с-ми	24	количество с-ми	16
		неподвижна	да	неподвиж-на	да	неподвиж-на	не	неподвижна	не	неподвижна	не	неподвижна	не

ЗАБЕЛЕЖКА:

избор с-ма точност коорд.	Приоритет при избор на система за въздействие Необходима минимална точност за постигане на желания ефект
време на поз.	Миним. необходимо време за реакция на избраната система за въздействие в зависимост от макс. време на целта на позиция
количество с-ми неподвижна	Препоръчително назначаване на системи за поразяване за постигане на желания ефект Този стандарт определя целта дали е стационарна или се движи

Използвана литература:

1. Атанасов А Ст. Марков Д К. Условия за единно управление, чрез интегриране на системите за огнева поддръжка при участие в многонационални операции., ВА “Г.С.Раковски”; София , 2016
2. Атанасов А Ст Органите за планиране на съвместната огнева поддръжка във всеобхватният подход при планиране на операциите. Шумен. 2011
3. Доктрина на Въоръжените сили на Република България НП -1 2018 г;
4. Доктрина за планиране на операции НП-052018 г.;
5. Доктрина за за съвместно определяне и поразяване на целите НП-3.9 2019 г.;
6. Костадинов К. Теоретични основи на оперативното използване на Военноморските сили, ISBN 978-619-7478-12-9, ВА „Г. С. Раковски“, София, 2018 г.
7. Илиев, К. „Съвместна огнева поддръжка” – фактор в съвременните операции. International Scientific Conference, Collectionofpapers, 2017, стр 120-127, ISSN 2367-7902.
8. Оперативно изкуство в съвременни условия, Учебник;
9. Ръководство за опер ативно планиране 2009 г

Radoslav B. Chalakov,

HISTORY AND CURRENT POTENTIALS NEEDED TO IMPROVE THEM

Radoslav B. Chalakov

ВОЕННА АКАДЕМИЯ "ГЕОРГИ СТОЙКОВ РАКОВСКИ"
КАТЕДРА "СУХОПЪТНИ ВОЙСКИ", r.chalakov@rndc.bg

***Abstract**: The modern stage of the development of military activity is characterized by fundamental changes in the forms and methods of war. This is due to the emergence of various types of precision weapons, effective means of intelligence, communications and command and control of troops (forces) and other factors caused by the modern information technology revolution that has embraced all aspects of society.*

ИСТОРИЯ И НАСТОЯЩЕ НА БОЙНИТЕ ПОТЕНЦИАЛИ - НУЖДА ЗА УСЪВЪРШЕНСТВАНЕТО ИМ

Радослав Б. Чалъков

Въведение

Военните конфликти са се променили в много аспекти въпреки, че воденето на мащабни войни днес не може да бъде изключено, но от друга страна са се появили редица местни конфликти и войни с уникалните за тях методи и условия на въоръжено съперничество, които се превърнаха в реалност. Всичко това изисква един процес от задълбочено теоретично разбиране, разработване на нови подходи за дефиниране на зони за отговорности, както и подобряване на оперативните методи за планиране, командване и управление на войските.

Увеличаващите се локални конфликти [26]и войни, в които се използва ограничено количество хора и техника, от своя страна налагат изменение в оперативното планиране и преди всичко на методите за оценка на бойните възможности на силите и средствата, тяхното съотношението в съвременните операции, както и определянето на необходимите сили и средства за водене на бойни действия. Всички тези изменения следва да доведат до дълбоко преосмисляне на процеса при определянето на бойния потенциал на въоръжението. Този процес води до актуалност и сложност в прогнозирането на хода и изхода на конфликта или операцията в зависимост от началното съотношение на силите на страните (бойния потенциал).

Важно място в този процес заема оперативното планиране и по точно методите за количествени оценки на бойните способности на войските, баланса на силите в съвременните операции и определянето на необходимия състав на силите и средствата за воденето на операции.

На този етап изменението на формите и способите за водене на операция е свързано с появата на различни видове високоточни боеприпаси, по съвременни средства за разузнаване, а и от там и по точно определяне координатите на целите и обектите на бойното поле, далекобойни системи, автоматизация на силите и средствата както за командване и управление, а така също на

[26] *Локалният конфликт е противопоставяне на две и повече държави с употреба на военна сила за постигане на ограничени политически цели. В локалният военен конфликт страните ще действат в рамките на територията на противоборстващите страни и ще се заключава в постигането на интересите в рамките на тези страни (териториални, икономически, политически и др.).[1]*

оръжията и ред други фактори в съвременния свят. Особено актуален и сложен е проблемът за прогнозиране на хода и изхода на конфликта в зависимост от началното съотношение на силите и средствата и условията за неговото водене. Най-правилният начин в този случай е разработване на математически модел на съвременните операции. Това от своя страна следва да доведе до изготвяне на много разчети в процеса на планиране, затова в практиката се използват два основни метода: *Метода на анализ на статистическите данни от операциите през Втората световна война и следващите войни и Метода на бойните потенциали.*

Тези два метода не са загубили своето значение и при планиране на операциите на съвременния етап, но следва да се преосмислят и усъвършенстват.

Методът на анализ на статистическите данни и определяне на закономерностите за въоръжената борба въз основа на изучаването на войните от миналото е бил и остава най-важен във военните и военно-исторические изследвания. Постигнатите резултати имат голяма практическа стойност, особено с експерименталното усъвършенстване и проверка на математическите модели.

Методът на бойните потенциали (БП) е основен за определяне на бойната мощ на войските, както собствени така и на противника. До настоящият момент използването му се отнасяше към традиционните форми за водене на операция – от стратегическа операция на различни театри на военните действия до тактически бойни действия. Така например в недалечното минало този критерии беше в основата на изграждането на въоръжените сили като с него се обосноваваше "Отбранителната достатъчност" т.е. поддържането на минимално необходимо количество и съответното качество на войските и въоръженията така, че да отговарят на определени изисквания.

Това е един от новите и най-ефективни инструменти в оперативната работа на стратегическите и оперативните щабове при планиране на операциите.

Каква е неговата същност?

Това е *„количествена характеристика, осреднена за условията на използването ѝ в операцията, която изразява резултата от измерването на бойната ефективност на разглежданата система с определена референтна единица, определяща единицата за скала. Измервания, и е средното съотношение на броя на референтните единици към еквивалентния брой разглеждани единици, където еквивалентността се разбира в смисъл на запазване на резултата от операцията след замяна на определен брой еталонни единици с разглежданите бойни единици. "*

Трудно е да се разбере горната дефиниция, особено, що се отнася повече до *коефициента на бойния потенциал*, а не към потенциала на въоръжението. Понятието трябва да бъде ясно, сбито, недвусмислено, в този случай има набор от не съвсем свързани, отклоняващи се фрази. Тук може да се кажем, че резултатът от операцията зависи до голяма степен от качеството на командването и управлението. *Защо* само командването и управлението и къде е осигуряването - бойното, логистичнот и т.н., както и човешкият фактор, което в общи линии пряко влияе върху хода и изхода на операцията?

Но да започнем с дефиницията за „боен потенциал". - *„Бойният потенциал в избрана точка във всяка ситуация трябва да се оценява чрез поне три основни изисквания, изразяващи определени граници на евентуални бойни способности на военните формирования: идеалния потенциал на оръжията; реален-потенциалът на бойните способности, като се отчита тяхното състояние и способност да действат по предназначение; към реалния-потенциал за готовност за водене на бой, като се вземат предвид мерките, предприети за подготовка за изпълнение на възложената задача.*

Размерът на реалистичността на бойния потенциал зависи както от вътрешни фактори (човешкият фактор и т.н.), така и от външни фактори (материална и техническа поддръжка, околна среда и др.).

За по-пълно и по-дълбоко разбиране на разглеждания въпрос ще дадем понятие, което е вградено в думата „потенциал". Потенциал - набор от сили и средства на системата, нейните ресурси и резерви, предназначени за постигане на определени цели. Потенциал - физическата единица, силата на системата. Всяка система, реализираща съществуващия потенциал, решава проб-

лемите, присъщи на нея и след като ги разреши, достига целта. В същото време пълнотата на реализацията на потенциала характеризира ефективността на системата и зависи от много фактори: външни условия, способността на системата, качеството на управление и поддръжка, т.е. нейните възможности. Когато се оценява ефективността на въоръжените понякога се среща понятието „възможност" (бойни способности, способности за откриване на цели, способности за преодоляване на противовъздушна отбрана и др.).

И така, какво е *„възможността"*? Възможността е нещо, което може да се случи и да стане реалност при определени условия (обстоятелства). Тази концепция включва две взаимосвързани страни: външна, т.е. заобикалящата я системата, и вътрешна, присъща на самата система. Ако вземем външната страна като основа, тогава „възможността" са условията (обстоятелствата), които допринасят за функционирането на системата или затрудняват и ако тя е вътрешна, то е нейната способност (потенциал). *Потенциалната възможност се* характеризира с условия, благоприятстващи максималната реализация на целия потенциал, заложен в системата (образец, оръжието). *Реалната възможност се* характеризира с реалните условия за използване на потенциала на системата. По този начин степента на постигане на целта от системата зависи не само от наличието на потенциал, но и от съответните възможности. Всъщност реалните възможности определят осъществимостта на потенциала.

Ще дадем някои обяснения на горната концепция за „боен потенциал на въоръжението" като основа, на която се основават изчисленията на потенциала на бойните системи. В тази дефиниция тактико-техническите характеристики на модела на оръжията се разбират като набор от показатели (характеристики), количествените стойности, на които недвусмислено определят неговия технически възможности и бойна ефективност.

Част от характеристиките е - скорост на движение, далекобойност, бойно натоварване, време за подготовка за данни, характеристики на точността на стрелба и т.н.

Характерното за бойното натоварване на използван модел оръжие в бойни условия зависи от брой на боеприпасите, скорострелност или броя на нанасяне на удари и др., които може да извърши в битка преди физическото му унищожаване.

Ефективността на използването на метода на бойните потенциали зависи от решаването на два фундаментални проблема:

- Коректно определяне на дела на различните типове въоръжения в резултат на бойните действия;
- Обективна оценка на допустимите области, в които може да се използва метода.

Анализът на проблемите по използването на метода на бойните потенциали възниква, когато в оперативните щабове се появява необходимост от съизмеримост на бойната ефективност на различните видове оръжия за определяне на общото съотношение на силите и средствата. Т.е появата на разнообразни оръжия с висока огнева мощ съществено изменя характера на бойните действия и общите възможности на формированията. Необходима е единна мерна единица, която да отчита бойната мощ на всяко оръжие или формирование и чрез съпоставянето на сумата от възможностите да се определя съотношението на силите и средствата и по-лесно да се прогнозират резултатите от изхода на операциите.

Или казано накратко, модерното въоръжение в различни типични формирования се формолира като бойна система (БС). Отличителна черта на които е интегрирането на подсистемите, подготовката и въоръжението в единна информационна и контролна система. В резултат на това обединение, бойните системи придобиха качествени нови свойства и увеличиха способностите си включваики следните функционални подсистеми: разузнаване, командване и управление, подготовка и техническа поддръжка на оръжия; въоръжението (оръжие и боеприпаси).

Всяка подсистема изпълнява функцията си и предава информация и команди за управление на други подсистеми. Взаимодействието на тези подсистеми в БС определя работния цикъл на бойното използване на системата.

Процесът на функциониране на БС обикновено е последователен процес на изпълнение на отделни операции, така че времето за отговор на БС е равно на сумата от времената на нейните операции: откриване на целта до въздеиствието върху него.

Това може да доведе до по-лесно и по-бързо определяне на необходимите сили и средства и други планови характеристики на операцията, да се прогнозират резултатите и в крайна сметка да се определи вероятния резултат от операцията.

Бойните потенциали се определят основно по експертен път, използвайки и количествени методи за сравнение. Този метод обаче има и определени слабости дотолкова, доколкото при определянето на бойния потенциал не са отчетени възможностите на разузнавателните сили и средства, управлението на войските и оръжията и осигуряването на бойните действия и за тях трудно се определят бойни коефициенти. За тях са се определяли коефициенти чисто субективно и те не са били потвърдени от никакъв боен опит. При това не са се вземали под внимание характера, формите, мащабите и условията за воденето на бойните действия.

Процесът на изчисляване на бойните потенциали може да се опише с нелинейни математически функции, като за критерий на оценката на дела на всеки вид оръжие се взема началното съотношение на силите и средствата, маньовъра и загубите на войските в жива сила и бойна техника. За разчетите са избрани най-характерните и възможни решения на операцията, направено е моделиране на операцията, при условие че двете страни водят бойните действия в съответствие с оптимални условия за управление на войските и постигане на целите на операцията.

M(Xа, Xб, Уа, Уб, Zа, Zб, La,Lб ,t) = K;

- където:

- Xа и Xб са вектори, характеризиращи състава, структурата и въоръжаването на страните в операцията;

- Уа и Уб - вектори, описващи тяхната експлоатационна конструкция, вид на терена и неговото експлоатационно оборудване, условия за започване и поддръжка на операцията и други параметри;

- Zа и Zб - вектори, които отразяват планове на страните и командването и управлението;

- La и Lб са матрици на бойната ефективност на огневата поддръжка на страните;

- t - продължителността на операцията, приета за изчисления.

Известно е, че постоянна величина за съизмеримост на различните типове въоръжения не съществува, защото бойния потенциал на въоръжението е променлива величина и се определя не толкова от бойните възможности на оръжията, но и от количеството и структурата на противостоящите групировки, вида на бойните действия, качеството на управлението, бойното и другите видове осигурявания, условията на местността, времето като сезон и част от денонощието, характера на оперативната обстановка и други фактори. Освен това, величината на бойния потенциал е сравнително устойчива на стратегическо ниво (**изменението на началния състав на страните е в пределите на 10-15 %**), но в същото време на оперативно и на тактическо ниво малките изменения в състава на страните влияят съществено на дела на различните въоръжения и оттам - и на изхода на операцията.

Най-приемливи за използване в оперативната работа на висшите щабове се оказват бойните потенциали на механизираните батальони, числените значения, на които са сравнително устойчиви и то в широки граници (**до 30 % изменение в началното съотношение на групировката на войските**). По такъв начин не са се оправдали очакванията за големи грешки при оперативното планиране от щабовете и мярката за определяне на коефициентите на бойните потенциали се е оказала коректно определена и е дала добри резултати за хода и изхода на операцията.

Методът на бойните потенциали е особено ефективен при оценката на общото съотношение на силите, необходимия състав на групировката на войските в операцията, а след това и при определяне на очаквания изход от бойните действия.

Появата на новите средства за водене на бойни действия, както изменение в геополитическата, геоикономическата и военната ситуация, наложиха нови форми и способи за воденето им, което пък налага да се преосмислят основни положения от военното изкуство и военната наука, в това число и такава категория като съотношението на силите.

С особена острота на дневен ред се поставя проблема за достоверността на оценката на съотношението на силите в типичните за съвременната реалност регионални конфликти и най-вече борбата с екстремистите в различни региони на света и др. Всички тези конфликти се различават съществено, но в общ план си приличат – създаването на военно преимущество, което не винаги може да реализира успех в една или друга степен. В тези конфликти като правило, слабата страна избягва прякото стълкновение с превъзхождащия противник, стреми се да му нанесе загуби с партизански или терористични методи, понякога даже и извън пределите на на зоната на конфликта. В тези случаи традиционното понятие “съотношение на силите”, отразява бойните възможности на страните, но не може да се използва за прогнозиране на хода и изхода на конфликта и следва да претърпи съществено уточнение.

Ето защо при планиране на дадена операция съотношението на силите може да бъде различно и то ще зависи преди всичко от региона, в който се води операцията, населението в региона, целите на операцията, готовността на по-слабата в технологично отношение страна да понесе определени загуби в хора и инфраструктура и др. А това ще доведе до определяне на такова съотношение на силите, което да доведе до изпълнение на целите на операцията. Затова е важно да се разгледа в бъдеще същността, съдържанието и методите за определяне на значението на „бойния потенциал” на образците въоръжение, бойна техника и формированията.

Използвана литература:

1. Атанасов А Ст. Използване на артилерията за непосредствена поддръжка в съответствие с новите организационни промени в българската армия НВУ "В.Левски", факултет "Артилерия, ПВО и КИС" Шумен 2010
2. Градев К. Подход за оценка на бойните потенциали и бойните възможности на тактическа бойна група от Сухопътни войски в процеса на трансформация. Годишник на факултет "Командно щабен", 1/2010, 124-132 стр. 2010
3. Костадинов К. Влияние на процеса на превъоръжаване върху необходимитеоперативни способности на ВМС - международна научна конференция на Военна академия „Г. С. Раковски”, 11-12.април 2018 г.
4. Илиев, К. Определяне бойния потенциал на образците въоръжение и бойна техника. International Scientific Conference, Collection of papers, 2018, стр 88-92, ISSN 2367-7902.
5. Брезгин В.С., Буравлев А.И. О методологии оценки боевых потенциалов вооружения и военной техники и воинских формирований// Военная мысль. 08/2010.
6. Бонин А.С. О боевих потенциалах образцов ВВТ, формирований и соотношениях сил групировок сторон.// Военная мысль.04/2010.

Radoslav B. Chalakov, Dimitar Shomov,

EFFECTIVENESS OF REACTIVE ARTILLERY IN DESTROYING DIFFERENT OBJECTIVES OF THE FIELD

Radoslav B. Chalakov, Dimitar Shomov

ВОЕННА АКАДЕМИЯ "ГЕОРГИ СТОЙКОВ РАКОВСКИ"
КАТЕДРА "СУХОПЪТНИ ВОЙСКИ", r.chalakov@rndc.bg

Annotation: *Despite the overall warming of international relations, there has been a tendency in the last decade to increase the number, scope and intensity of local wars and armed conflicts. As shown by historical experience, in almost all such "small wars" artillery formations play a significant role in solving the tasks of impacting targets and objects of different nature.*

ЕФЕКТИВНОСТ НА РЕАКТИВНАТА АРТИЛЕРИЯ ПРИ ПОРАЗЯВАНЕ НА РАЗЛИЧНИ ПО ХАРАКТЕР ЦЕЛИ НА БОЙНОТО ПОЛЕ

Радослав Б. Чалъков, Димитър Шомов

Нищо в живота не е толкова ободряващо, колкото да стрелят по теб и да не улучат.

Уинстън Чърчил

Въведение

Факта, че поразяването на целта ще зависи не само от големината на нанесените материални щети, които се характеризират с показателя за ефективност на стрелбата, но и от моралното въздействие върху целта, което не може да се определи от този показател. При определяне големината на показателя за ефективност на стрелбата се разглеждат конкретните условия на стрелбата и резултатите от поразяването на целите.

Под конкретни условия на стрелбата се разбира: калибър, **разход на снаряди**, разстояние на стрелба, способ за подготовка на данни и водене на огън. След което се изчислява големината на показателя за ефективност на стрелбата – вероятност за поразяване на единични цели или математическото очакване на процента поразени елементарни цели от групова цел.

В „Доктрината за полевата артилерия" са определени значения на показатели за ефективност на стрелбата за надеждното унищожаване, неутрализиране и подавяне на различни по характер цели. Под норма за разход на снаряди се разбира разхода снаряди, които осигуряват при конкретни условия получаването на желаната степен на поразяване.

За определяне на нормите за разход на снаряди бе проведено експериментално изследване за поразяване на различни по характер цели на бойното поле. С помощта на на система за компютърни симулации JCATS. Бяха поставени две задачи за изследване. Първата е проверка ефективността на стрелбата по различните видове цели появяващи се на бойното поле с вече възприети норми разход на снаряди съгласно („Единните норми разход на снаряди утвърдени за формиро-

ванията от реактивната артилерия (ЕНРС)", а втората - проверка ефективността на стрелбата по различни видове цели с норми за разход на снаряди съгласно формулен апарат.

Първоначално се определят необходимите норми разход на снаряди по различните видове цели съгласно ЕНРС и по разгледан математически апарат. Впоследствие резултатите получени от системата за компютърни симулации JCATS се сравняват с тях.

В изследването е създаден модел на различните видове цели. На база сравнение и анализ на получените загуби (отчитане загубите във въоръжение, техника и личен състав) на поразените цели от симулиране на огневото поразяване ще са определи основата за крайния резултат.

Целия процес на изледването се извършва в „Център за дистанционно обучение и компютърни симулации" във Военна академия „Г. С. Раковски" предвид наличието на симулационна система JCATS.

В резултат на проведеното изследване е разработен алгоритъм включващ: Определяне и събиране на необходимите литературни източници [1,2,3,4,5,6,7,]; Създаване на модел на различните по характер цели; Определяне на района за изпълнение на задачата (характера на местността); Определяне на нормата разход на снаряди за унищожаване на различните видове цели на степен на поразяване 30 % съгласно ЕНРС; Изчисляване на нормата разход на снаряди за унищожаване на различните видове цели на степен на поразяване 30 % съгласно математическия апарат; Определяне на компонентите на изследване разхода на снаряди в зависимост от степента на укритост и степента на поразяване; Извършване на изследването (n на брой пъти); Сравняване на получените резултати.

Разгледните по долу примери са извършени в условия при който извършването на залпов огън преди всяка стрелба е необходима промяна на броя снаряди заредени в РСЗО, изходните данни за стрелба се подготвят на пълна подготовка, разстоянието на стрелбата се води от 13000м до 16000м, противостоящите сили не противодействат по време на провеждане на експеримента.

В пример № 1 се поразява бронирана батарея САУ открита. При фронт на целта (Фц) равен 400м и дълбочина на целта (Дц) равна 300м, където Nсн=540сн съглсно ЕНРС и Nсн=1087сн съглсно формулния апарат. Способ за водене на огън е на 1 мерника и 1 ъгломер. Получените резултатите са показано в таблица 1 и 2.

Таблица.1

Поразяване на бронирана батарея САУ открита с разход на снаряди по ЕНРС

Вид техника и личен състав	По списък	Безвъзвратни загуби	Процентно съотношение
2С-1	8	0	0 %
Личен състав	70	0	0 %
КЩМ	2	0	0 %
ТАПП	2	0	0 %
Общо	82	0	0 %

Таблица 2.

Поразяване на бронирана батарея САУ откритас разход на снаряди по формулния апарат

Вид техника и личен състав	По списък	Безвъзвратни загуби	Процентно съотношение
2С-1	8	1	12 %
Личен състав	70	6	9 %
КЩМ	2	0	0 %
ТАПП	2	0	0 %
Общо	82	7	10 %

В пример № 2 се поразява на буксирни гаубици на позиция в окопи.При Фц=400м и Дц=300м, където Nсн=360сн съглсно ЕНРС и Nсн=758сн съглсно формулния апарат. Способа за водене на огън е на 1 мерника и 1 ъгломер. Рвзултатите са показани в таблица 3 и 4.

Таблица. 3.

Поразяване на буксирни гаубици на позиция в окопи по ЕНРС

Вид техника и личен състав	По списък	Безвъзвратни загуби	Процентно съотношение
105мм М119	8	5	62 %
Личен състав	73	5	7 %
КЩМ	3	0	0
ТАПП	8	5	62 %
Общо	92	15	24 % (60%)

Таблица. 4.

Поразяване на буксирни гаубици на позиция в окопи по формулния апарат

Вид техника и личен състав	По списък	Безвъзвратни загуби	Процентно съотношение
105мм М119	8	8	100 %
Личен състав	73	17	23 %
КЩМ	3	1	33%
ТАПП	8	4	50 %
Общо	92	22	31 % (100%)

При пример № 3 се поразява буксирни гаубици на позиция в открито разположени. С Фц=400м и Дц=300м,където Nсн=300сн съглсно ЕНРС и Nсн=159сн съглсно формулния апарат. Способа за водене на огъня е на 1 мерника и 1 ъгломер показано на таблица 5 и 6.

Таблица. 5.

Поразяване на буксирни гаубици на позиция открита по ЕНРС

Вид техника и личен състав	По списък	Безвъзвратни загуби	Процентно съотношение
105мм М119	8	2	25 %
Личен състав	78	25	44 %
КЩМ	3	0	0 %
ТАПП	8	2	25%
Общо	97	29	35 %

Таблица. 6.

Поразяване на буксирни гаубици на позиция открита по формулния апарат

Вид техника и личен състав	По списък	Безвъзвратни загуби	Процентно съотношение
105мм М119	8	1	12 %
Личен състав	78	19	24 %
КЩМ	3	0	0 %
ТАПП	8	2	25 %
Общо	97	22	20 %

Пример № 4 включва поразяване на ВОП. При Фц=500м и Дц=300м. Където Nсн=750сн съглсно ЕНРС и Nсн=2772сн съглсно формулния апарат, при способ за водене на огън на 1 мерника и 1 ъгломер. Същият е показано на таблица 7 и 8.

Таблица. 7.

Поразяване на ВОП по ЕНРС

Вид техника и личен състав	По списък	Безвъзвратни загуби	Процентно съотношение
БМП-1	3	0	0 %
Личен състав	14	0	0 %
ПКМ	2	1	50 %
РПГ-9	3	0	0 %
Снаипер(7,62)	2	1	50 %
Общо	97	2	8 %

Таблица. 8.

Поразяване на ВОП по формулен апарат

Вид техника и личен състав	По списък	Безвъзвратни загуби	Процентно съотношение
БМП-1	3	1	30 %
Личен състав	14	5	30 %
ПКМ	2	1	50 %
РПГ-9	3	2	60 %
Снаипер(7,62)	2	1	50 %
Общо	97	10	40 %

От пример № 5 в който се поразяван пехота и бронирани средства открито разположени чрез системата за симулация с БМ-21 „ГРАД" и с Фц=500м Дц=400м. Където Nсн=600сн съглсно ЕНРС и Nсн=190сн съглсно формулния апарат и способ за водене на огъня на 1 мерника и 1 ъгломер се получават резултати показан в таблица 9 и 10

Таблица. 9.

Поразяване на пехота и бронирани средства по ЕНРС

Вид техника и личен състав	По списък	Безвъзвратни загуби	Процентно съотношение
Личен състав	14	14	100 %
БМП-1	3	0	0 %
ПКМ	2	1	33 %
РПГ-9	3	2	66 %
Снаипер(7,62)	2	2	100 %
Общо	97	19	100 %

Таблица. 10.

Поразяване на пехота и бронирани средства по формулния апарат

Вид техника и личен състав	По списък	Безвъзвратни загуби	Процентно съотношение
Личен състав	14	14	100 %
БМП-1	3	0	0 %
ПКМ	2	0	0 %
РПГ-9	3	0	0 %
Снаипер(7,62)	2	1	33 %
Общо	97	15	90 %

Пример № 6 е за поразяване на РЛС на полевата артилерия открито разположени с Фц=150м и Дц=150м. При Nсн=338сн съглсно ЕНРС и Nсн=38сн съглсно формулния апарат. При способ за водене на огъня на 1 мерника и 1 ъгломер. Резултатите са показани в таблица.11 и 12

Таблица. 11

Поразяване на РЛС на ПАрт. по ЕНРС

Вид техника и личен състав	По списък	Безвъзвратни загуби	Процентно съотношение
Личен състав	6	3	50 %
M9 CDR	1	0	0 %
Q37	1	0	0 %
ZIL WMRadar	2	1	50 %
Общо	10	4	50 %

Таблица. 12.

Поразяване на РЛС на ПАрт. по формулния апарат

Вид техника и личен състав	По списък	Безвъзвратни загуби	Процентно съотношение
Личен състав	6	2	33 %
M9 CDR	1	0	0 %
Q37	1	0	0 %
ZIL WMRadar	2	1	50 %
Общо	10	3	50 %

При пример № 7 се разглежда поразяването на РЛС на полевата артилерия укрито разположени. При Фц=150м и Дц=150м. При Nсн=405сн съглсно ЕНРС и Nсн=98сн съглсно формулния апарат. Способ за водене на огъня на 1 мерника и 1 ъгломер е показано на таблица.13 и 14

Таблица. 13.

Поразяване на РЛС на ПАрт. укрити по ЕНРС

Вид техника и личен състав	По списък	Безвъзвратни загуби	Процентно съотношение
Личен състав	6	4	66 %
M9 CDR	1	1	100 %
Q37	1	0	0 %
ZIL WMRadar	2	2	100 %
Общо	10	7	100%

Таблица. 14.

Поразяване на РЛС на ПАрт. укрити по формулния апарат

Вид техника и личен състав	По списък	Безвъзвратни загуби	Процентно съотношение
Личен състав	6	4	66 %
M9 CDR	1	1	100 %
Q37	1	1	100%
ZIL WMRadar	2	1	50 %
Общо	10	7	70%

От разгледаните до сега примери е ясно, че в резултат на огъня на дивизиона с БМ-21 „ГРАД" по пехота и бронирани средства на открито целта се поразява с вероятност 24%. Получения резултат означава, че при проведени голямо количество стрелби в аналогични условия по пехота и бронирани средства на открито, целта ще бъде поразена средно на 24%.

Също така и по бронирани САУ на позиция открито разположени се поразяват с вероятност 20%. Получения резултат означава, че при проведени голямо количество стрелби в анало-

гични условия по бронирани САУ на позиция открито разположени, целта ще бъде поразена средно на 21%.

Това е само една част от резултатите от разгледаните примери, всички резултати са обобщени в таблица 15 в която са сравнени резултати от получените степени на поразяване при различни норми разход на снаряди.

От разгледаните примери и резултатите посочени в таблица 15 се забелязва, че при поразяване на някои от целите с норма разход на снаряди съгласно ЕНРС не се постига зададената степен на поразяване от 30 % от личен състав и техниката. А при поразяване на същите цели с норма разход на снаряди изчислени чрез формулния апарат за дадената степен на поразяване от 30 % на личен състав и техниката се постига. Това дава направление за преразглеждане на нормите за разход на снаряди по определени видове цели.

От казаното до сега може да се направи извод, че РСЗО е целесъобразно да бъдат привличани за поразване на не бронирани, открито или укрито разположени групови цели. Тоест по цели на които с големина над 100 м^2. С което ще се допринесе за повишаване ефикасността на използване РСЗО определяйки необходимата норма разход на снаряди за получаването на определената степен на поразяване. при поразяване на различните видове цели появяващи се на бойното поле.

.

Таблица 15

Таблица със сравнителните резултати от получените степени на поразяване при различни норми разход на снаряди

	Бронирани самоходни гаубици на позиция открити	Бронирани самоходни гаубици на позиция открити	ВОП	ВОП	Буксирни гаубици на позиция в окопи	Буксирни гаубици на позиция в окопи	Буксирни гаубици на позиция открити	Буксирни гаубици на позиция открити	Пехота и бронирани средства на	Пехота и бронирани средства на	РЛС на артилерията укрита	РЛС на артилерията укрита	РЛС на артилерията открита	РЛС на артилерията открита
Nсн по методика	45 сн/ха		50 сн/ха		30 сн/ха		25 сн/ха		30 сн/ха		180 сн		150 сн	
Nсн изчислени		91сн/ха		184 сн/ха		63сн/ха		14сн/ха		10сн/ха		44сн		16сн
Зададена степен на поразяване	30%	30%	30%	30%	30%	30%	30%	30%	30%	30%	30%	30%	30%	30%
Получена степен на поразяване	0%	10%	8%	40%	24%	31%	35%	23%	100%	90%	100%	70%	50%	50%

Използвана литература:

1. Атанасов А.С. „Едно виждане относно степените за поразяване на целите в огневите удари“ ВА "Г.С.Раковски" София 2008;
2. Атанасов А.С „Действие на артилерията за обща поддръжка в операциите“ ВА "Г.С.Раковски" София 2009;
3. Марков Д., Поразяване на цели от артилерийски формирования, въоръжени със 122 mm СГ 2С-1 „Гвоздика“ в близост до зоната за координиране на въздушното пространство, Сборник доклади от международна научна конференция, НВУ, Факултет „Артилерия, ПВО и КИС“, с. 143-153, Издателски комплекс на факултет „Артилерия, ПВО и КИС”, Шумен, 2017, ISSN 2367-7902
4. Петров В.П. Теоретични обосновки на огневото поразяване. Шумен. 2007г.глава 7;
5. Правила за стрелба и управление на огъня на земната артилерия, Първа част, Издателство на МО, София, 1998г., Раздел пети;
6. Ръководство за използване на полевата артилерия – артилерийски дивизион, София, ВИ, 2009 г.;
7. Тактическа доктрина на полевата артилерия, ГлЩ на СВ, София, 2005;
8. Теория на стрелбата в земната артилерия. Държавно военно издателство София – 1968.
9. Katsev, I. Evaluation method of the Artillery's effectiveness against unitary target. International scientific conference “CONFSEC 2018”,vol 2, pp 208-210, ISSN: 2603-2945.

Yordan Petkov,

BASIC GUIDELINES FOR INCREASING THE SKILLS OF RECONNAISSANCE FORMATION PERSONNEL

Yordan Petkov

Военна академия „Г. С. Раковски", yorpet@mail.bg, тел. 26626

Abstract: *Intelligence is the main battle function. It is designed to provide commanders and staffs of all levels with up-to-date, accurate and reliable information at any time of the day for the entire duration of the operation and, in some cases, after it is completed. In order to be able to perform these tasks, it is necessary for reconnaissance units to obtain this information to be equipped with well-trained and motivated personnel. The purpose of this article is to point out some possible guidelines for enhancing the skills of the command and staff of reconnaissance units so that they can fulfill their duties in any type of operations.*

Keywords: *reconnaissance, training, preparation, skills*

ОСНОВНИ НАСОКИ ЗА ПОВИШАВАНЕ НА УМЕНИЯТА НА ЛИЧНИЯ СЪСТАВ НА РАЗУЗНАВАТЕЛНИТЕ ФОРМИРОВАНИЯ

Йордан Петков

Въведение

В рамките на бъдещата война се очаква да се водят едновременно или независимо едни от други, обхващащи огромни пространствени, географски и климатични области, както динамични, с висок темп и интензивност бойни действия, така също и множество по-малки, но продължителни във времето операции. Друга отличителна черта на бъдещите операции е свързана с отсъствието на фронтова линия, такава, каквато я познаваме в сегашната й форма – фронтът няма да изчезне като понятие, но ще придобие съвсем нов смисъл като вече няма да има онзи вид на развърнати формирования на местността. [4] Принципите за водене на бойни действия като определяне на географски зони на отговорност, преобладаващото използване на обикновени боеприпаси, близък бой, физическата защита, огромните складови запаси, вертикалните връзки на управление вече се заменят от функционални зони на отговорност, високоточни боеприпаси, удари в дълбочина, информационна защита, гъвкава и целенасочена логистика, мрежова среда за управление. [1] В такава среда повишаването на ефективността на личния състав на разузнавателните формирования придобива все по-нарастващо значение за успеха на операцията. Но дали този разузнавач от бъдещето ще бъде по-боеспособен използвайки технически иновации и информационни технологии или ще се разчита повече на способностите му да се адаптира, оценява и взема решения в непозната среда? Технологиите сами по себе си са наистина може би са ефективни, но проблемът е, че те биха подложили боеца на допълнително напрежение, както физическо така и психическо. За-

висимостта от техническите средства вероятно биха ограничили свободата на действията на отделния военнослужещ, биха го направили неспособен сам, без помощта на технологиите, да анализира и да взема решение, да не говорим, че тези технологии не могат да намалят или ликвидират стресовите фактори, а напротив – могат да създадат нови такива.

Всъщност, в основата на всяка успешна операция, както сега, така и за в бъдеще ще продължават да стоят индивидуалните умения на военнослужещите. От всеки войник ще се изисква да притежава специални познания, способности и умения, които да са предпоставка за успешния край на дадена операция и които осигуряват основата за справяне с нови ситуации при непрекъснато променящи се условия на средата. Ето защо, основната цел на обучението трябва да бъде насочена към това, да се научи отделния войник да действа самостоятелно и бързо да се адаптира към промените в ситуацията дори и в сложни ситуации. Бойните умения гарантират способност за оцеляване и устойчивост на собствените сили и трябва да останат във фокуса на основните възможности на войниците като не бива да се пренебрегва и друг ключов фактор в обучението - да се научат войниците непрекъснато да се справят със стресови ситуации.

Умения, необходими на разузнавателните формирования

Човешките ресурси са най-важният елемент и основен капитал на на всяка една армия. За посрещане на изискванията на постоянно променящата се оперативна среда, нарастващите нужди от професионално военно обучение и навлизащите нови технологии, военно-образователната система трябва да се поддържа на съвременно ниво. Системата на военно образование и обучение следва да се развива като гъвкава и комплексно развиваща се. Тя следва да се осъществява като индивидуална военна подготовка, колективна подготовка в щатните формирования и съвместна подготовка в рамките на създадени национални или многонационални военни формирования за бойно използване. В тази връзка, при планирането и провеждането на подготовката, с която се цели повишаване на уменията на разузнавателните формирования следва да се обръща внимание на две основни категории – командирите на формирования и личния състав.

Основни умения необходими на командирите на разузнавателни формирования

Доктрините и публикациите отнасящи се до обучение включват теми по задачите, които се изпълняват от разузнавателните формирования, като в същото време не се обръща нужното внимание на това, какво следва да се направи по отношение на обучението и образованието за развитието на гъвкави и адаптивни лидери. [5] Като цяло не са чести моментите, когато се обръща внимание на това, дали командирите от всички нива притежават нужните знания и умения. По скоро на тези умения се гледа като на даденост и не се подлагат на съмнение. Всъщност, за да подготвим командирите на разузнавателни подразделения така, че те да могат да управляват своите подчинени адекватно при всякакви ситуации, трябва първо да се разбере това, което ги отличава от другите командири от останалите родове войски. От въпросните командири се очаква да притежават множество качества и да владеят до съвършенство основни умения, които са от съществено значение за планиране на дейността, придвижването, докладването, насочването на средствата за поддръжка и запазване на свободата на действие. Притежаването на основни знания и умения за ориентиране на непозната местност е само отправна точка за разузнавачите, но в никакъв случай не е приемливия минимум. Поддържането на непрекъсната комуникация и докладване на резултатите от разузнаването също са от съществено значение за изпълнение на задачата и включват притежаването на технически умения, свързани с познаване на техническите параметри на комуникационната техника, както и своевременно свеждане на получена информация. Първоначалният анализ на ситуацията на бойното поле е основата за формиране на нужната предварителна осведоменост на командирите и щабовете и е основно умение за командирите на разузнавателни формирования.

Тъй като от разузнавачите се очаква да първи да научат за противника това, което ще е необходимо на командира и щаба означава, че командирите на разузнавателни формирования трябва винаги да са наясно, защо командирът има нужда от тази информация и да не забравят, че

решенията му зависят от нея. Информацията, отнасяща се до маршрути, райони, зони и определяне местоположението на разкрити цели, трябва да е прецизна и актуална тъй като на тази основа командирите вземат решения за това как, кога и къде да разположат своите сили.

Командирите на разузнавателни формирования трябва да имат нужните познания, благодарение на които непрекъснато да се оценява влиянието на терена, противника и дейността на местното население върху собствените операции. От съществено значение за изпълнението на задачите от един разузнавателен взвод в пълен обем са техническите познания и ясното разбиране на ситуацията, особено що се касае за мястото на взвода на бойното поле, което от своя страна е свързано с възможността за огнева поддръжка, от гледна точка на разстояние и обсег. Ето защо от тях следва да се очаква да познават в детайли и то без помощта на съответните специалисти, наличните огневи системи, възможностите им за наблюдение и водене на огън, като това се отнася в пълна сила и за въздухоплавателните средства.

Крайният резултат от обучението трябва да бъде осигуряването на разузнавателните формирования с командири, които не само са усвоили нова информация, тактики, техники и процедури, но и които могат да подготвят по най-добрия начин подчинените им формирования. Командирите на разузнавателни формирования трябва да развият умения, чрез които сами да разрешават възникнали проблеми и то в ситуации, които не са описани в нито едно наставление, да имат по-голямата увереност, инициативност, способността и творческо и управление на риска свързано с изпълнението на дадена операция. Тези нематериални активи не са предварително количествено определени и нямат измерими стандарти в същия смисъл, както чисто техническите задачи.

Основни умения необходими на личния състав на разузнавателните формирования

Личният състав е другият основен елемент от който се очаква да притежава нужните знания и умения за справяне в сложна и непрекъснато променяща се среда. Тяхното придобиване, обаче, е свързано най-вече с провеждане на пълноценна и качествена подготовка. Удачен вариант е подготовката на тези военнослужещи е да се раздели на четири части: начална (която всеки войник придобива при влизане в армията); базова (конкретна начална подготовка за всеки военнослужещ в разузнавателно формирование); основна (усъвършенстване на придобитите умения и получаване на нови такива); поддържаща (поддържане на придобитите навици и умения и усвояване на нови). Ако кандидатът за разузнавателно формирование вече е влязъл в армията, то той ще следва да преминава само последните три етапа; ако не е част от въоръжените сили – следва да премине всичките четири етапа.

За времето на *началната подготовка* от всеки един войник би следвало да се очаква да придобие такива знания и умения като сигурно боравене с личното въоръжение; отлична физическа подготовка; запазване на физическата и психическата издръжливост; умения за оказване на неотложна медицинска помощ на себе си и на други военнослужещи; основни познания по ЯХБЗ и основни умения за водене на наблюдение и докладване.

Като следващ етап, от *базовата подготовка* следва да се очаква придобиване на първоначални разузнавателни умения, които да са адекватни за широк спектър от операции като акцента следва да се поставя не само върху подобряване на уменията на отделния военнослужещ, а на бойното сглобяване на формированията. С приключвне на този етап от подготовката военнослужещите би следвало да са усвоили такива умения като своевременно откриване и преодоляване на засади; използване специални географско-информационни продукти; придвижване в пеши строй, особено в градските райони, през деня и при ограничена видимост, както и използване на навигационни средства; бойни животоспасителни мерки, включително помощ за себе си и други членове на формированието; спешното евакуиране от не-медицински персонал; взаимодействие с медицински персонал; комуникация с месното население; основни познания на съответния местен език; владеене на системите за комуникация; обща култура и междукултурна компетентност. Тези умения трябва да бъдат допълнени от придобиване на практически знания и умения по отношение на използването на личното и колективното въоръжение, както и на

познания относно последствията от използването на принудителна сила и правните последсвия от това.

По време на *основната подготовка* следва да бъдат придобити умения, които се отнасят до значително повишаване за знанията и уменията на личния състав на разузнавателните формирования. По време на това специализирано обучение от всеки един разузнавач би следвало да се очаква че ще придобие умения извършване на скокове с парашут и десантиране от зависнал вертолет по въже; перфектно познаване на военната топография, което означава да умее да се ориентира на непозната местност по компас, по карта и по местни предмети; бързо и правилно да определя местоположението на конкретни обекти и да свежда точно координатите на разкрити обекти посредсвом радиосредствата; определяне вида на оръжието на разкрития противник и познаване на неговите ТТД; познаване тактиката на действие на подразделенията на вероятния противник и умения за използване неговото оръжие и техника; определяне на принадлежността на противника по неговия външен вид, форма на облеклото и опознавателни знаци; умения да се маскира и да се придвижва безшумно в непозната местност; умения за скрито и безшумно да преодолява инженерните заграждения от всякакъв тип и преодоляване на водни прегради в брод или чрез подръчни средства; умения да прави дълги преходи пешком и на ски във всякакви условия; притежаване на познания относно военната терминология на езика на противника, да има умения да превежда документи и да разпитва пленници; умело използване на взривни вещества и средства за взривяване; да умее да изготвя взривни вещества от подръчни материали; притежаване на навици и умения за оцеляване в екстремални условия; умения за управление на колесна и верижна техника – своя и на противника; умения за насочване авиацията към стационарни и движещи се обекти на противника; разпознаване на контраразузнавателните мероприятия на противника и познаване на способите за заблуда, използвани от противника. [3]

Естествено е, че не може да се предвиди всичко, което ще е необходимо на разузнавача. На практика, тези знания, способности и умения, се разпределят между всички войници от групата, но в идеален вариант те трябва да се владеят от всеки боец, независимо каква е неговата щатна длъжност.

От *поддържащата подготовка* се очаква да затвърди придобитите знания и умения под различна форма. Това може да става чрез непрекъснато участие в тактически занятия, участие в допълнителни курсове, участие в реални операции и т.н.

Основен елемент от подготовката на командния и личния състав на разузнавателните формирования са *психофизическата и медицинската подготовка –* тези подготовки задължително трябва да започват от първия етап и да продължават непрекъснато.

На физическите показатели по време на бой до голяма степен влияние оказва психическия фактор. Ето защо, психиката на всеки един военнослужещ трябва да се тренира така, че той да се научава да преодолява страха в най-трудните за него моменти. Страхът е защитна функция на организма. В съвременната война войникът е длъжен да умее да контролира своя стрес и да помага на околните. От тези му умения зависи овладяването на дадена ситуация. Справянето с т.нар. стресори (събития или ситуации, които изискват нерутинна промяна в адаптацията или поведението) е важно условие за оцеляването на бойното поле. Бойни стресори са всички стресори, на които военнослужещия е изложен през време на изпълнение на свързаните с бойната дейност задължения, независимо дали са свързани или не с действията на противника. [2] Много стресори на бойната дейност са свързани с командира, подразделението или изискванията на изпълняваните задачи. Самите стресори могат да бъдат разделени на физически и психически.

Физическите стресори имат директен ефект върху тялото. Те могат да бъда външно условие на средата или вътрешно физическо или физиологическо искане на човешкото тяло. Към тях се отнасят стресорите на средата - горещина, студ, влага, вибрации, шум, хипоксия (недостатъчен кислород), дим, отрова, химикали, инфекциозни агенти, физическа работа, силна светлина, тъмнина, мъгла и др.

Физиологичните стресори са свързани с недостатъчен сън, дехидратация, недохранване, лоша хигиена, мускулна умора, отслабена имунна система, свръх използване или недостатъчно използване на мускулите, болест или нараняване и др.

Психичните стресори са тези, за които достига информация до ума без директно влияние върху човешкото тяло. Тази информация обикновено е свързана с когнитивната или емоционалната система, въпреки че най-често стресовата реакция е провокирана и от двете. Психични стресори са когнитивните стресори, като твърде много или твърде малко информация, сензорно претоварване, неяснота, несигурност, изолация, недостиг на време или чакане, непредсказуемост, организационна динамика, труден избор или отсъствие на избор и др. Емоционалните стресори са свързани със заплаха от нараняване, болест, болка, провал; загуба, предизвикваща страх и тревожност, загуба на близки, предизвикваща тъга и печал; заплаха, вина, водеща до раздразнение, гняв и омраза; загуба на вярата или духовна конфронтация; и др.

От друга страна, стресът не винаги е вреден и с негативно влияние върху човека. Позитивния стрес е тази степен на стрес, която е необходима за поддържане и подобряване на толерантността (търпимостта) към стрес без изтощително стресово преживяване. Определени нива на стрес са необходими за здравето. Това се отнася най-вече за някои физически стресори, към които тялото трябва да се аклиматизира. За да се постигне по-голяма търпимост или аклиматизация към физически стресор е необходимо прогресивно излагане на неговото влияние. Това излагане би трябвало да бъди достатъчно за предизвикване на нещо повече от рутинен стрес рефлекс. Типичен пример за позитивен стрес са аклиматизацията на топлина и увеличаването на мускулната сила. Този процес на повишаване на толерантността към стресорите чрез прогресивно излагане на тяхното влияние е също валиден и за когнитивно емоционалните стресори.[2]

Потенциалните стресори трябва да се предвидят и оценят още преди началото на изпълнение на мисията. Войникът трябва да е готов да посрещне опасността с ясното съзнание за произтичащите рискове и заплахи. Съвременното военно обучение трябва да включва изпълнението на комплексни и трудни, физически и психически задачи под голямо напрежение, недоспиване, недостатъчно храна и вода, физическа умора. Обучението трябва да дава на отделния войник увереност в собствените сили, а също така и разбиране как стреса действа върху него и останалите войници. [6] Обучението трябва да учи не на намаляване на стреса, а на контролирането му.

Без отчитането на психологическите измерения на съвременния бой всеки проект за навлизане на технологиите в подготовката на отделния войник за водене на бойните действия, както и съвместното им използване в реална обстановка, би бил обречен на провал. Функционирането на човешката психика в екстремални условия се променя. Би могло да се предскаже с достатъчна степен на сигурност, че военнослужещия ще изпълнява успешно поставените задачи в реална бойна обстановка само ако мирновременната им подготовка е била възможно най-близка до бойната, а командирите и щабовете отчитат психологическите ефекти на бойната интензивност върху военнослужещите.

В бъдещите войни разузнавателните формирования следва да притежават адекватна екипировка и умения, които да им позволяват да изпълняват отговарят на изискванията на информационната война и да съдействат за създаване на превъзходство на противника, чрез откриване на целите за кратко време, както и да бъдат първите сили, които ще бъдат прехвърлени при възникване на криза и да притежават гъвкави системи за командване и управление. Въвеждане на съвременни образци въоръжение, екипировка, оборудване и комуникационни средства за разузнавателните формирования, изискват и изграждане на модерна учебно–материална база и полигони, които да осигуряват необходимите възможности за подготовка за изпълнението на специфичните задачи от войсковото разузнаване. Едновременно с усъвършенстване на учебно-материалната база е необходима и целенасочена учебна програма, която да включва следните основни направления: подготовка и мотивация на личния състав; разработване на социални програми; обучение; бюджет и материални средства. Необходим е

специален подход при подбор на личен състав за нуждите на разузнавателните формирования, като същите следва да притежават много добра физическа и психическа подготовка.

Използвана литература:

1. Берковиц, Б., Новото лице на войната, Военно издателство, 2003 г.;
2. Карастоянов, Г., Боен стрес, статия за списание Военен журнал, бр. 4, 2000 г.;
3. Заруцкий Ф., Тарас А., Подготовка разведчика, 1997 г.;
4. NATO, „AJP-3.2 Allied Joint Doctrine for Land Operations”, October 2009;
5. Perry, Robert C., McEnery, Kevin, Army Reconnaissance Course: Defining the Aim Point for Reconnaissance Leader Training — ARMOR July-August 2009;
6. US Army Field Manual 8-51 (FM 8- 51), Combat Stress Control In A Theater Of Operations Tactics, Techniques, And Procedures, May 1994;
7. US Army Field Manual 22-51 (FM 22- 51), Leader’s Manual for Combat Stress Control, September 1994.

Hristo A. Hristov, Veliko P. Petrov,

MILITARY COUNTERINTELLIGENCE IN THE INTELLIGENCE COMMUNITY OF RUMANIA

Hristo A. Hristov, Veliko P. Petrov

Shumen university ,,Bishop Konstantin Preslavski’’, Shumen city, Faculty of technical sciences,
Department ,,Management of security systems’’
Faculty of Artillery, Air Defense and Communication and Information Systems,
National Military University, Shumen, Bulgaria, veliko_pp@abv.bg,

***Abstract**: Military Counterintelligence is an element of the National security of each country. In order to analyze the role, the place and the tasks of the bodies of the military counterintelligence (MCI) in our country and the need to improve their structure and functions, it is appropriate to analyze the development of these bodies in different countries.*

With respect to this, the research provides a summarized outlook of theoretical and practical issues related to the development and positioning of the National Security Protection System in Rumania, one of its elements - Military Counterintelligence.

***Key words:** security, intelligence, counterintelligence, intelligence community, national security, intelligence center, military staff, population.*

ВОЕННОТО КОНТРАРАЗУЗНАВАНЕ В РАЗУЗНАВАТЕЛНАТА ОБЩНОСТ НА РУМЪНИЯ

Христо А. Христов, Велико П. Петров

Въведение

Разузнавателните и контраразузнавателни служби са част от тази държавна система, които са специално създадени и предназначени за опазване на националната сигурност и недопускане на нанасянето на вреди върху нея [1].

Ролята и мястото на дадена специална служба в системата за защита на националната сигурност се определят от целите на функциониране в системата за сигурност и основните задачи за защита на националната сигурност, които се възлагат за изпълнение на конкретната служба, разкритите от нея външни и вътрешни заплахи за националната сигурност и от структурата на тази служба [2].

Контраразузнаването има за своя основна задача да разкрива и неутрализира конктретни посегателства, организирани и осъществявани от чужди разузнавателни служби, а също така и от антиконституционни организации, групи и нелоялни лица в страната, които нанасят вреди на националната сигурност [3].

Сигурността на въоръжените сили е динамично състояние на защитеност на личния състав, материалните средства, информацията и мероприятията, както и на мерките и структурите, необходими за постигането на това желано състояние. [4]. Специалните структури, осигуряващи тази сигурност, са органите за военно контраразузнаване (ВКР).

С цел анализ на ролята, мястото и задачите на органите на ВКР в разузнавателната общност на Република България е целесъобразно да се анализира развитието на органите за сигурност на въоръжените сили в различни държави. Една от държавите, чиито служби през годините са оказвали влияние на развитието на специалните служби на държавите от Балканския полуостров е Румъния. Съгласно авторитетния сайт за световната класацията за военна сила на Global Firepower от 2018 г. [5], при население от 21 529 967 души Румъния има 72 500. военни (без резервистите) и има присвоен индекс Power Index 0,7205, което я нарежда на 40-то място по военна мощ сред 136 държави от света, обхванати от тази класация.

Разузнавателна общност на Румъния

На съвременния етап румънската разузнавателна общност се състои от [6], [7], [8]:

1. Върховен съвет за национална отбрана (Consiliul Suprem de Aprrare a Tarii – CSAT).
2. Парламентарни комисии за контрол над специалните служби.
3. Служба за външно разузнаване (Serviciul de Informatii Externe – SIE) [9].
4. Румънска разузнавателна служба (Serviciul Roman de Informatii – SRI).
5. Генерална дирекция за военно разузнаване (Direcţ ia Generală de Informaţ ii a Apărării – DGIA) при Министерството на отбраната.
6. Служба за защита и охрана (Serviciul de Protectie si Paza – SPP) [10].
7. Служба за специални телекомуникации (Servicii de telecomunicaţ ii speciale – STS) [11].
8. Главно управление за разузнаване и вътрешна защита (Directia Generala De Protectie Interna – DGPI) при Министерството на вътрешните работи [12].

Върховният съвет за национална отбрана (CSAT) има за основна задача ръководство и контрол върху специалните служби. Осъществяването на парламентарния контрол над дейността на специалните служби на Румъния се реализира от създадената смесена комисия по отбраната, националната сигурност и обществения ред. През 1993 г. в парламента на страната е създадена и специална парламентарна комисия за контрол на SRI.

Първата румънска тайна служба се създава през 1924 г. Включва разузнавателни и контраразузнавателни структури. След края на Втората световна война в Румъния през 1944 г. е създадена служба „Народна сигурност“, известна като „Секуритате“ (Departamentul Securitatii Statului – Sekuritate). През 1990 г. Съветът на Фронта за национално спасение изгражда Център за външна информация, който през същата година прераства в Служба за външно разузнаване (SIE). Основна задача на SIE е да извършва разузнаване, като придобива, обработва и предоставя на държавни органи политическа, икономическа и военна информация зад граница [6], [7].

Службата за външно разузнаване е военизирана, като всички данни, които касаят дейността ѝ, са държавна тайна и огласяването им се наказва най-строго. На SIE са вменени разузнавателни и контраразузнавателни функции по защита на личния състав на службата. Службата осъществява техническите свръзки със задграничните представителства и осигурява защитата им, включително чрез разработката и прилагането на шифри и кодове за пощенския канал и радиоканалите за обмен на информация.

Румънска разузнавателна служба (SRI) е най-голямата специална служба на Румъния. Тя е

специализиран държавен орган в областта на информацията за националната сигурност, съставна част от националната система за отбрана, чиято дейност се организира и координира от CSAT на страната. Службата не е в структурата на МВР, а е самостоятелно звено с ранг на министерство. Тя се състои от: ръководство, централен апарат (управления и самостоятелни отдели) и териториални отдели в окръжните градове, съставени от по-малки звена, дублиращи структурно управленията в централния апарат на службата [7], [8].

Централният апарат се състои от следните управления:

- Управление „Контраразузнаване" осъществява контраразузнавателно противодействие на чуждестранните специални служби;
- Управление „Контрасаботаж" защитава националната сигурност от действия, дестабилизиращи вътрешната обстановка и сигурност. Противодейства на организирането на саботажни действия на вътрешни опозиционни и антиконституционни сили;
- Управление „Защита на конституцията" наблюдава с оперативни методи и средства анархистки, терористични, националистически и други организации, като се стреми да не допуска нарушения на конституцията и извършване на враждебни, екстремистки и терористични актове. Към управлението е формирана антитерористична бригада с център и ръководство в Букурещ;
- Управление „Икономическа сигурност" разработва висшия и средния ръководен ешелон на държавата по проблеми, свързани с корупцията, контрабандата, прането на пари и др.;
- Управление „Вътрешна сигурност" е структура, осигуряваща контраразузнавателната защита на самата служба;
- Управление „Оперативна техника" провежда мероприятия с използването на специални разузнавателни средства.
- Управление „Регистрационно-документално и административно" обединява няколко служби – „Кадри", „Обучение", „Планиране", „Управление на автоматизираните системи", „Архив" и други;
- Департамент за връзки с местните власти и неправителствените организации (Departamentul de Legatura cu Autoritatii Publice si Organizatii Neguvernamentale) е създаден с цел подобряване на двустранната комуникация с оглед подпомагане на решаването на задачите на службата.

На службата са вменени информационни и технически дейности за противодействие на тероризма. В тази връзка осигурява антитерористична защита на румънски и чуждестранни висши държавни представители, на висши държавни служители, охранявани от Службата за защита и охрана, когато те са заплашени от терористични актове, освобождаване на заложници и възстановяване на законовия ред. SRI съчетава разузнавателната и контраразузнавателната функция по отношение на румънските малцинства в съседни държави. Специализирано звено извършва радиоразузнаване, радиопеленгация и дешифриране. Националната академия по информация (Akademia Nationala Informatii – ANI) към SRI осигурява подготовката и усъвършенстването на действащите и запасните кадри за нуждите на SRI и другите специални служби и институции, изпълняващи функции във връзка със защитата на националната сигурност [7].

Служба за защита и охрана (SPP) е създадена през 1990 г. като самостоятелна структура в държавния апарат. Службата осигурява лична, постова и техническа охрана, специализиран транспорт и пропускателен режим по месторабота, местоживеене, пребиваване в страната и чужбина на висшите представители на законодателната, изпълнителната и съдебната власт. Към нея действа специален отдел за оперативна информация, който е контраразузнавателната структура в службата.

Службата за специални телекомуникации (SCS) е създадена на базата на оперативно-техническото управление на Sekuritate „Тонола". Извършва радиоелектронно наблюдение и осъ-

ществява държавните комуникации и свръзки, като осигурява тяхната защита чрез засекретяване.

Главното управление за разузнаване и вътрешна защита (DGPI) при Министерството на вътрешните работи осъществява контраразузнавателната защита на кадрите от структурите на МВР, проникване в средите на организираната престъпност (местна и международна), събиране на информация за остри социални недоволства и десни радикални организации.

Други специални служби са Независима служба за защита и борба срещу корупцията (Serviciul Independent de Protectie si Anticoruptie – SIPA) към Министерството на правосъдието, и Департамент за работа с външните румънци (Departament Pentru Romanii in Strainatate – DPRS) при Министерството на външните работи.

Следните румънски институции имат военен статут, но не са част от въоръжените сили – Румънска жандармерия, Гражданска отбрана и Главен инспекторат на Военно-пожарната бригада.

Служби за военно разузнаване и контраразузнаване

В системата за защита на националната си сигурност румънската държава има създадена единна автономна система за сигурност във ВС, един орган оторизиран с разузнавателни и контраразузнавателни функции за защита – Главно управление за отбранителна информация при Министерството на отбраната, пряко подчинено на Генералния щаб на румънската армия. Този функциониращ модел, обединяващ в едно цяло Дирекция „Военна информация" (Directia Informatii a Armatei – DIA) и Дирекция „Защита на военната сигурност" (ДЗВС), гарантира по-лесна и своевременна обработка и анализ на военна, военнополитическа и военноикономическа информация от чуждестранни открити източници, повишаваща ефективността на контраразузнавателното обезпечаване на въоръжените сили на Румъния [6], [7].

Главното управление за разузнаване и вътрешна защита (DGIA) е военноразузнавателна агенция на румънските въоръжени сили, подчинена на Министерството на националната отбрана. Управлението е създадено в края на 1999 г. на базата на обединяване на Дирекция „Военна информация" и Дирекция „Защита на военната сигурност". То е пряко подчинено на Генералния щаб. Състои се от следните звена:

1. Дирекция „Военна информация" (Directia Informatii a Armatei – DIA). Основни задачи на дирекцията са:

- разкриване на евентуална военна заплаха от съседните държави;
- своевременно разкриване на външни заплахи и рискови фактори за националната сигурност;
- противодействие на организирана престъпност, имаща отношение към военната и националната сигурност;
- придобиване на военна разузнавателна информация;
- провеждане на стратегическо и оперативно-тактическо разузнаване в районите на евентуалните бойни действия на румънската армия;
- оперативно ръководство на военните аташета, осигуряване и поддържане на връзките с тях;
- обезпечаване сигурността на личния състав и техниката на войски, участващи в операции зад граница;
- обработка и анализ на текуща информация;
- подбор и обучение на кадрите.

Служба „Техническа" (при румънските специални служби е специфично, че научно-техническото разузнаване се намира във военното разузнаване, а не в цивилното, както е в повечето разузнавателни системи);

Отдел „Ръководство на военните аташета" – координира разузнавателната работа зад граница, изгражда и ръководи резидентури;

Отдел „Сигурност на личния състав и противодействие на организираната престъпност";

Отдел „Войсково разузнаване", който извършва разузнавателна дейност в тила на против-

ника по време на война;

Отдел „Радиоразузнаване" – извършва техническо разузнаване на чуждестранни излъчващи системи.

Организационно-управленски структури:

- служба „Обработка на текущата информация" – изготвя ежедневен информационен бюлетин за правителството;
- служба „Обработка на информацията";
- служба „Регистър";
- отдел „Обучение на личния състав";
- отдел „Кадрово и материално обезпечаване";
- отдел „Управление на кризи".

Четири отдела са пряко подчинени на началника на дирекцията:

- „Международни връзки";
- „Оперативна техника";
- „Автоматизирани информационни системи";
- „Финанси".

2. Дирекция „Защита на военната сигурност" (ДЗВС)

Дирекцията е военното контраразузнаване на страната, създадено през 1990 г. на базата на Пето управление на Sekuritate.

1. Основната задача на ДЗВС е контраразузнавателното осигуряване на армията. Неин контингент са военизираните и цивилните служители в структурите на Министерството на отбраната. ДЗВС разкрива и предотвратява действия на чуждестранни разузнавания, насочени към придобиване на военна информация. Дирекцията предотвратява проникването на чуждестранни специални служби във военни обекти и вербовката от чуждестранни разузнавания на военни и граждански лица, работещи в системата на МО [6], [7].

Заключение:

Направеният преглед на развитието на органите на военно контраразузнаване в Румъния показва, че военното контраразузнаване присъства като неизменна част от разузнавателната общност на страната и този преглед може да бъде използван за извеждане на аргументирани предложения за ново, по-ефективно позициониране на органите за военно контраразузнаване в системата за защита на националната сигурност на Република България.

References:

1. Казаков, К., 2016: Управление на системата за защита на националната сигурност, Информация и сигурност, Първо издание, С., ISBN 978-954-334-181-8.

2. Любов, Е. и др., 2017: Роль и место МЧС в системе обеспечения национальной безопасности государства. [on-line, прегледано ноември 2018]. https://cyberleninka.ru/article/v/rol-i-mesto-mchs-rossii-v-sisteme-obespecheniya-natsionalnoy-bezopasnosti-gosudarstva.

3. Иванов, Д., 2009: Кой кой е в Държавна сигурност. millenium, С., ISBN 978-954-515-039-5.

4. Великов, И., 2008: Контраразузнавателна защита на въоръжените сили. Академия на МВР, София.

5. Global Firepower [on-line, прегледано ноември 2018]. https://www.globalfirepower.com/countries-listing.asp.

6. Бакалов, Й. Специални служби на Република Румъния. https://www.google.bg/search?source=hp&ei=XqdMXPyiFoO2sQGj7KD4Cg&q

7.Трифонов, Т. Специални служби на държави от Европа, Азия Африка. Академия на МВР, София. ISBN 978-954-348-022-7.

8. Георги В. Камарашев, Специални войскови действия в антитерористични операции, НВУ „Васил Левски“, Велико Търново, 2003 г.

9.Трифонов, Т., Ралчев, Г. Специалните служби – теория и практика. Фондация „Национална и международна сигурност“, София. 2001. 524 с. ISBN 954-90695-3-2.

10. SIE. https://www.sri.ro/

11. http://www.spp.ro/#/

12. https://www.stsnet.ro/

13. http://dgpi.ro/dgpi_blk_fe.html

Hristo Al. Georgiev,

PARTICIPATION AND SPECIFIC TASKS OF THE SOF IN PEACETIME CRISIS MANAGEMENT OPERATIONS

Hristo Al. Georgiev

Факултет „Командно-щабен", ВА „Г.С.Раковски, София, bizbez@abv.bg

Abstract: *The current security environment is characterized by a large dynamic of risks and threats to the security of human society, and to national security as well, which creates the right conditions for the peacetime crisis establishment. This is a broad meaning concept, with a tendency to evolution, requiring adequate countermeasures. Thus, it highlights the role of Special Operations Forces in dealing with different crises.*

Key words: *security environment, crisis, special forces*

УЧАСТИЕ И СПЕЦИФИЧНИ ЗАДАЧИ НА ССО В ОПЕРАЦИИ ПО ПРЕОДОЛЯВАНЕТО НА КРИЗИ В МИРНО ВРЕМЕ

Христо Ал. Георгиев

Въведение

Промените в геополитическото пространство, настъпващи в резултат на глобализацията и информационните технологии, увеличаващите се предизвика телствата пред сигурността на отделните страни и международната стабилност като цяло, принуждава държавите да се съобразяват с тях и да търсят решения за тяхното успешно преодоляване. Постепенно се формира идеята за търсене на нови подходи за намиране на баланс между заплахите за сигурността и възможностите за противодействие. Така се е стига до разбирането, че постоянно трябва да се изграждат способности за своевременно разкриване и неутрализиране на опасностите за сигурността, съчетани в съвременни системи за сигурност, осигуряващи нейната защита при всякакви условия.

Съвременната средата за сигурност се характеризира с голяма динамика на рисковете и заплахите за сигурността на човешкото общество и в частност за националната сигурност. От съществено значение за сигурността на държавата, обществото и на всеки отделен гражданин имат политическите, икономическите и военните сътресенията в заобикалящия ги свят, проявите на тероризъм и организирана престъпност, етническите и религиозните конфликти, нерегламентираното разпространение на оръжия за масово унищожение, бежанските и миграционните проблеми, трафикът на наркотици и на хора, стихийните природни бедствия, технологичните аварии и екологичните катастрофи. Всичко по-горе изброено носи като следствие възможността

от възникването на криза. Това е едно понятие носещо в себе си широк смисъл с тенденция към постоянна еволюция в своето съдържание поради ново възникващите заплахи за националната сигурност. Има написани не малко определения на понятието, имайки предвид обаче неговия обхват като параметър е необходимо да се разгледа определението за криза записано в ЗОВС: „*нестабилност в политическата и обществената сфера, предизвикваща рязка промяна на установеното състояние на икономиката и общест-вения живот".[3]*

Като правило кризите съчетават различни типове събития, от които един е централен и определящ елемент. В зависимост от това коя част от системата е засегната най-тежко, кризите като явление могат да бъдат определени като природни, екологични, технологични, финансово-икономически, политически, информационни, социални, военни и т.н. Спецификата на войната като обществено явление, което коренно променя организацията на функциониране на държавата, налага тя да се разглежда като особен вид криза, управлението на която е предмет на отделна наука. В този смисъл обикновено се говори за две големи групи кризи - ***кризи от военен и кризи от невоенен характер. [1]***

В зависимост от причините за тяхното възникване и основните фактори, които ги предизвикват, кризите могат да бъдат сведени до няколко вида:

- военнополитически кризи с различна степен на интензивност - състояния на междудържавните отношения, при които съществува реална заплаха от употреба на военна сила срещу суверенитета, териториалната цялост и независимостта на някои от засегнатите държави;
- вътрешнополитически кризи – вътрешнодържавни обществени състояния, застрашаващи жизненоважни интереси на отделната личност, различните човешки общности и на обществото като цяло, стабилността, вътрешната сигурност и обществения ред в държавата;
- външнополитически кризи – кризисни състояния, причинени от влошени междудържавни отношения или проблеми с български граждани и материални активи на страната в чужбина;
- хуманитарни кризи, предизвикани в резултат на стихийни природни бедствия, технологични аварии, екологични катастрофи и засягащи живота, здравето и интересите на хората;
- кризи, вследствие на терористична дейност. Те са разновидност на посочените по-горе, но поради високата обществена опасност от тяхното проявление и спецификата на противодействието им, през последните години се класифицират като относително самостоятелен вид кризи. [1]

Участието на силите за специални операции (ССО) като част от ВС на РБ за справяне с различни видове кризи в мирно време от своя страна се свежда до:

- участие в превантивната и непосредствената защита на населението при бедствия, аварии и катастрофи;
- участие в противодействие на тероризма и преодоляването на последиците от тероризъм;
- участие в защита на застрашени стратегически обекти и обекти от критичната инфраструктура. [2]

В разглеждания контекст, тъй като операциите по охраната на стратегически обекти в повечето случай се разглеждат като следствие от терористична заплаха, то те могат да бъдат разгледани в контекста на тероризма, като по този начин в тази разработка основно внимание ще бъде обърнато на участието на ССО в операции в мирно време в две основни направления: участие на ССО в операции по противодействие на тероризма и участие на ССО в операции по защита на населението при бедствия , аварии и катастрофи.

1. Участие на ССО в операции по противодействие на тероризма

С новите промени в законодателството на РБ, ССО на БА (формированията за противодействие на тероризма), има своето ново и много по-значимо място в усилията на държавата в борбата срещу тероризма. Съгласно плана за противодействие на тероризма на БрСпС, са декларирани определен брой военнослужещи за участие в такъв вид операции. Тази численост е около две трети от общата численост на всички екипи (от МО и МВР), за противодействие на тероризма.

Участието на ССО в борбата срещу тероризма следва да се определи в зависимост от мащабите на неговото проявление. В тази борба участието, може да бъде пасивно и активно. Пасивно участие се заключава в строгия контрол на собствените въоръжения и недопускане тяхното нелегално разпространение към отделни лица, организации и държави. Активното участие се заключава в използването на силов потенциал, при наличие на терористична заплаха на територията на страната.

На основата на съществуващите регламентиращи документи, може да се приеме, че участието на ССО на БА в операции по противодействие на тероризма, ще кореспондира с мисията „принос към националната сигурност в мирно време". В този случай е необходимо ясно да се подчертае, че ангажиране на ССО на ВС на БА, може да стане само на основата на политическо решение за това. Участието на Българската армия в тези случаи се регламентира в чл. 99 на Доктрината на ВС на РБ, чл. 49 на Военната доктрина на Република България и чл. 57 от Закона за отбраната и въоръжените силии по Закона за противодействие на тероризма, съгласно които въоръжените сили могат да изпълняват операции по противодействиев на тероризма.

От гледна точка на операциите в отговор на терористична кризи мястото на ССО в борбата с тероризма може да бъде дефинирано като участие в „операции в подкрепа на органите за сигурност". [4]

Основна роля и мястото на ССО, може да се търси при решаването на задача по ликвидират последствия от терористичен акт. Ясно трябва да подчертаем, че ССО нямат водеща роля при изпълнение на тази задача.

Участието на ССО в операции за противодействие на тероризма на територията на страната, съгласно настоящите планове, следва да се разглежда единствено и само, като съвместна такава с специализираните органи на МВР. Министерството на вътрешните работи и частност СОБТ, жандармерия имат оперативни способности за противодействие на тероризма, основно в градски условия и затворени пространства, сгради и други. ССО имат по- големи оперативни способности за действия в открита среда, като по този начин допълват и повищават способностите на органите на МВР при провеждане на съвместни операции за противодействие на тероризма.

При обявено извънредно положение, освен мерките и ограниченията по чл. 30 от закона за противодействие на тероризма, с решение на Министерския съвет държавните органи и въоръжените сили извършват следните дейности:

- охраняват обекти, застрашени от тероризъм;
- ограничават или забраняват полети на граждански въздухоплавателни средства и въвеждат особен режим на корабоплаване в териториалното море и вътрешните морски води на страната;
- ограничават движението по основни пътни артерии, а също така и през държавната граница;
- ограничават движението на железопътния транспорт и установяват контрол върху пътниците и товарите;
- ограничават свободното придвижване и установяват контрол върху гражданите и превозните средства;
- контролират обектите от критичната инфраструктура на страната;
- ограничават или забраняват достъпа до държавни учреждения;

- забраняват провеждането на събрания, митинги и манифестации. [4]

Специфични задачи на силите за специални операции при участие в съвместни контратерористични операции.

Като участник в съвместна КТО на територията на страната, БрСпС могат да бъдат включени в операции при внезапно възникнал терористичен акт или в операции при които има предварителна информация за подготовка на терористичен акт със следните задачи:

- локализиране на терористи;
- задържане на терористи;
- освобождаване на заложници;
- унищожаване на терористи;
- за противодействие на разпространението на оръжия за масово поразяване;
- охрана на важни обекти и други.

Специфични задачи на МСРО

Морските формирования от ССО приоритетно ще участват в КТО в черноморското крайбрежие и дунавската брегова зона, но това не изключва техни действия и в райони, които се намират навътре в сушата. Тези формирования провеждат операции под и на повърхността на водни басейни или на брега, които се характеризират със скритост, бързина и прецизно прилагане на сила.

Освен основните задачи на ССО, морските формирования се специализират върху изпълнение на следните задачи:

- инфилтрация и ексфилтрация по/под вода;
- разузнаване на обекти в крайбрежната зона;
- подготовка на направленията за навлизане на сушата и атака преди провеждане на амфибийни операции и други офанзивни действия за противодействие на тероризма;
- овладяване и(или) защита на кораби похитени от терористи;
- овладяване и защита на обекти в крайбрежната зона от терористи;
- други специфични действия в поддръжка на амфибийни или морски операции.

Военновъздушен елемент за СО

Към момента не съществуват формирования ССО на военновъздушните сили. За поддръжка на сухопътните и морски формирования за ССО е необходимо да се задели авиационен ресурс – летателни средства и екипажи, усвоили процедурите за осигуряване на ССО. Те ще провеждат и поддържат всички основни и допълнителни задачи на ССО, които могат да бъдат осигуряването на въздушна мобилност – специализирани транспортни задачи със самолети и вертолети, интегриране на действията по въздух и суша за инфилтрация, ексфилтрация, непосредствена поддръжка от въздуха, нанасяне на въздушни удари, екстрена или медицинска евакуация на сухопътни, морски формирования от ССО или сили и средства на авиационния ресурс, осигуряващ ССО. [5]

2. Участие на ССО в операции по защита на населението при бедствия, аварии и катастрофи

Бедствията са стихийни природни явления и/или причинени от човешка дейност инциденти, които водят до негативни последици за живота, здравето и имуществото на хората, и като цяло нарушаващи нормалното функциониране на обществото и пораждащи кризи в него. [1] Стихийните природни явления могат да бъдат класифицирани като: земетресения; наводнения; ураганни ветрове; пожари; снегонавявания; епидемии по хората и животните и др. Към бедствията в следствие на човешка дейност могат да се причислят технологичните аварии в промишлени предприятия с рискови производства, катастрофите с транспортни средства, екологичните инциденти и т.н.

Като цяло защитата при този вид кризи се извършва на национално, областно и общинско ниво, и се осъществява чрез:

- провеждане на превантивна дейност;
- провеждане на дейности по защитата при възникване на бедствия;
- подпомагане и възстановяване;
- ресурсно осигуряване;
- преодоляване и приемане на помощи.[1]

Операции при този вид кризи от невоенен характер са организирани целенасочени действия на формирования от силите за специални операции (ССО), насочени за предотвратяване, овладяване и ликвидиране на последствията от възникналите бедствия аварии и катастрофи.

Участието на ССО в такива операции на територията на страната се заключава в изпълнение на мероприятия по превантивна и непосредствена защита на населението и обекти от националното стопанство при природни бедствия, аварии и катастрофи, крупни промишлени аварии, опасни замърсявания на околната среда и други подобни.

При ликвидиране на последствия от аварии и стихийни бедствия се изпълняват и задачи по изясняване на радиационната, химическата, биологическата, екологическата, пожарната, инженерната, хидрометеорологичната и друга обстановка в района на бедствието, провеждане на специална и санитарна обработка и дегазация, дезактивация и дезинфекция в огнища на аварии, гасене на пожари, разчистване на разрушения и срутвания, провеждане на мероприятия по възстановяване на околната среда и други. Конкретните задачи и дейности зависят от характера и мащабите на кризата.

Силите и средствата от БА, в частност от ССО за участие в операции по защита на населението при бедствия, аварии и катастрофи се определят ежегодно със заповед на министъра на отбраната.

Те водят подготовка и поддържат готовност за участие в действия по защита на личния състав, въоръжението, техниката, обектите на Министерството на отбраната, населението и националната инфраструктура при бедствия, аварии и катастрофи.

Изграждат се модулни формирования, сформирани на териториален принцип и с отчитане на дислокацията на поделенията, които водят специализирана подготовка за действия при различните видове природни бедствия и промишлени аварии.

В операциите по защита на населението при кризи от невоенен характер се извършва единно планиране на дейността в национален мащаб, подготовка на формированията, организиране на взаимодействието, управлението и осигуряването на операциите.

За участие на Силите за специални операции в действия по защита на населението при възникване на кризи от невоенен характер, в хода на ежедневната планова дейност, се поддържа необходимата готовност и ресурс за действие.

За тази цел се води планова специализирана подготовка на личния състав за участие в действия при възникване, развитие и овладяване на инциденти и кризи от невоенен характер и преодоляване на последствията от тях. Поддържат се в готовност необходимите технически и материални средства. Организират се и се провеждат различни по мащаб и съдържание тренировки и учения за усвояване на плановете и подготовка на определените формирования, води се радиационно и химическо наблюдение и контрол. Поддържа се готовност за оповестяване с дежурните модулни формирования. От друга страна постоянна връзка се поддържа както със Военния команден център, така и с общините в районите за действие на модулните формирования.

Основните дейности на ССО се реализират в два случая: при заплаха от инцидент или признаци за възникване на криза от невоенен характер и при възникване на самата криза.

При заплаха от инцидент или признаци за възникване на криза от невоенен характер се усилва наблюдението върху предполагаемата зона на кризата в съответствие с възможностите на силите и средствата, събират се данни, анализира се и се прогнозира характера и хода на прояв-

ление на кризата и обстановката, която може да възникне. Уточняват се плановете за действие. Определят се необходимите сили и средства за овладяване на кризата.

При възникване на самата криза се оповестява дежурното модулно формирование, предприемат се незабавни мерки за защита на личния състав, въоръжението, техниката и имуществата, ако са застрашени, и се привеждат в готовност определените за участие сили и средства. При поискване от държавните органи за управление на кризи, определените сили и средства вземат участие в действията за овладяване на инциденти и кризи и преодоляване на последствията от тях, съгласно плановете.

Практиката показва, че най-често те биват привличани за провеждане на операции при възникнали земетресения, наводнения, срутвания, пожари, сложна зимна обстановка и др.

Задачите, които подразделенията от ССО най - често изпълняват са следните:

- разузнаване на предполагаемата зона (район) на възникване на кризата;
- устройване на магистрални и странични проходи през районите, затрупани с разрушения;
- откопаване, разкриване на затрупани скривалища и подаване на въздух в тях;
- спасяване на пострадалите под разрушения и от горните етажи на сгради с разрушени пътища за евакуация;
- осигуряване на хората и техниката с вода и необходимите материални средства;
- оборудване на пунктове за събиране на пострадалите и медицински пунктове;
- приспособяване на запазените части от здания и съоръжения за пунктове за отопление, почивка и хранене, а понякога и за временно живеене и противорадиационна защита на личния състав на формированията;
- закрепване или срутване на конструкциите на здания застрашени от събаряне;
- гасене на огнищата на пожари в местата, където се извършват тези работи и др.

Всички тези задачи, както и други възникнали в хода на операциите подразделенията от ССО ще изпълняват в тясно взаимодействие с други органи, служби и ведомства от страната.

Последователността и сроковете на изпълнение на различните по характер работи в огнището на поражение зависят от характера на разрушението на зданията и съоръженията, от пожарната обстановка, от степента на радиоактивно заразяване на местността и от възможността за продължителен престой на хората под разрушенията (срутванията).

Приоритетни са мероприятията, свързани със спасяването, оказването на медицинска помощ и евакуирането от огнището на поражение на хората, оказали се в частично разрушените и запазени здания, под разрушенията, както и работите по предотвратяване на възникването и локализиране на последващите (вторичните) разрушения, взривове, пожари, насищането с газове, наводняването на територията и др.

Възникващите съвременни кризи, променящата се военно-политическа среда в световен мащаб, дават основание да се смята, че ролята, правомощията, задълженията и отговорностите на силите за специални операции на национално ниво ще става все по-значима. Компонентът ССО ще играе все по-важна роля във все повече дейности касаещи националната сигурност. За разрешаването на различни съвременни кризи и противодействие на терористични прояви се изискват на свой ред мобилни, отлично подготвени и екипирани специални военни формирования, които своевременно и адекватно да реагират на възникналите заплахи. Тези реалности налагат ССО да бъдат развивани в всички аспекти на необходимите им способности да поддържат висока степен на бойна готовност за изпълнение на целия спектър от мисии, стоящи пред тях при разрешаване на кризи от невоенен характер, създавайки по този начин необходимите условия за поддържане на една стабилна среда за сигурност.

References

1. Гоцев, Г., Защита на сигурността и обществения ред, Троян, 2016 г.
2. Доктрина на ВС на РБ(НП-1), С., 2018 г.

3. Закон за отбраната и ВС на РБ, С., 2017 г.
4. Закон за противодействие на тероризма, София, 2016 г.
5. Концепция на Силите за специални операции, 2012 г.
6. Манев, М., Управление при кризи и конфликти, София, 2005 г.

Dimo V. Ginev,

MISSION, FUNCTIONS, AND TASKS OF THE NON-MILITARY COMPONENT IN THE COLLECTIVE DEFENSE

Dimo Velichkov Ginev

Department „Natioional security and defense", Rakovski National Defense College, Sofia, dimoginev@abv.bg

Abstract: *Using the analysis of the national defence system, the report outlines its elements. The centre of gravity of the research has focused on one of these elements - the non-military component. In the report has been defined the mission of the civilian component as regard its participating in the collective defence, also has been presented its functions and basic tasks during defence of the country. Based on the activities specialization, has been created prerequisites for the division and concretizing of the tasks in three categories: tasks in the interest of collective defence; tasks in the interest of specific operations, combined with the armed forces; and tasks performed in the communications area. The results of those analyses could be used for building up a catalogue of non-military ensuing tasks for its preparation for participation in the national defence.*

Key words*: national defence system, non-military component, mission, functions, tasks*

МИСИЯ, ФУНКЦИИ И ЗАДАЧИ НА НЕВОЕННИЯ КОМПОНЕНТ В КОЛЕКТИВНАТА ОТБРАНА НА СТРАНАТА

Димо Величков Гинев

В съвременната среда на сигурност все по-често се забелязва формирането на нови източници на дестабилизация на системата за международна сигурност, генерирани главно от провежданите политики от геостратегическите играчи; бурното развитие на технологиите и разработването на нови оръжия; нарушаването на утвърдени във времето договори; традиционните, замразени регионални конфликти и социални противопоставяния, изразяващи се в граждански войни и др. Резултатите, от който са ерозия на държавността в определени страни; миграционни процеси; нарушаване на стабилността в международните организации; радикализация, провокиране на сепаратизъм и национализъм и други подобни. Както Георги Димов обобщава „страните в съвременния конфликт не се концентрират върху традиционните резултати – победата или поражението. Те сякаш са изместени от целите на военните операции и визират косвените намерения за обединяване на определени групи от хора или просто за икономическа изгода".[1] Наблюдаваните процеси водят до многократно повишаване и усложняване на рисковите и заплахите за националната сигурност и международната стабилност. Успешното противодействие на дестабилизиращите фактори отдавна надхвърля държавните граници и възможностите на националната политика, която отделните държави могат да провеждат самостоятелно. Това от своя страна налага тези държави да участват в съюзи и/или коалиции за гарантиране на общата си и националната си сигурност и отбрана.

В частност през призмата на военната наука *отбраната* най-често се определя като основен вид военни действия, насочени за защита на определена територия и противодействие на външна агресия. Но в настоящия момент понятието е придобило много по-дълбоко и комплексно съдържание. Ръководните документи на страната разкриват еднозначно, че отбраната на страната е широко обхватна, общодържавна дейност с единно ръководство, планиране, финансово и ресурсно осигуряване, обединяваща дейностите на държавните органи, институции, организации и гражданите за изграждане и използване на отбранителни способности за разкриване, възпиране, предотвратяване и противодействие на заплахи, застрашаващи независимостта, суверенитета и териториалната цялост и националните интереси на страната. Съгласно съвременните схващания отбраната на страната се планира, подготвя и осъществява в рамките на Системата за колективна отбрана на НАТО и Общата политика за сигурност и отбрана на ЕС, с ефективно използване на националните отбранителни способности, включващи военните и невоенните компоненти.

За да реализира тази дейност държавата изгражда *система за отбрана на страната,* чиято същност можем да определим като сложна съвкупност от множество разнородни институции, обекти, субекти и ресурси, взаимодействащи чрез официални и скрити механизми при осъществяването на целите на отбраната на страната. Системата за отбрана е сложна и динамична социална система от смесен тип, притежаваща характеристики както на отворените системи (силно влияещи се от външни фактори), така и на затворените системи (значително устойчиви на външни фактори).

Изградената у нас система за отбрана условно може да бъде разделена на военен и невоенен компонент. Възприето е, че системата за отбрана е съставена от *въоръжените сили* и *невоенен компонент*, най-вече поради отчетливата разлика между предназначението и организационната структура на двата компонента. Разсъждавайки в тази посока, за изграждане на ефективна система за отбрана на страната е необходимо формиране, развитие и поддържане на стабилно ядро – базирано на способностите на военните формирования на въоръжените сили, и гъвкава и устойчива периферия, включваща способностите на другите държавни органи, държавната администрация, обществените организации и гражданите (невоенния компонент), които взаимно да се допълват при създаването на общата отбранителна способност на страната. Те трябва да могат да си взаимодействат ефективно, както за превенция и възпиране, така и при необходимост за противодействие или отстраняване на последиците от съвременните рискове и заплахи за сигурността на страната. Както отбелязва Петко Петков „националните въоръжени сили и невоенния компонент следва да са в постоянна готовност за реакция на най-ранен етап, както и да притежават необходимите отбранителни способности. Това изисква съществуване на изградена система от военностратегически възгледи, обхващащи всички въпроси касаещи националната сигурност и отбраната на страната".[2]

От гледна точка на функциите и задачите, които ще изпълняват отделните органи, структури, организации, сили и средства в отбраната, в състава си невоенния компонент може да включва следните *елементи*: органи за стратегическо ръководство и управление; структури на министерства и ведомства, осигуряващи отделните сектори на сигурност; държавни агенции и комисии; териториалните органи на изпълнителната власт; юридическите лица, организациите и гражданите. Може да се обобщи, че невоенният компонент в своята *същност* включва „силите на всички държавни органи, които имат възложени военновременни задачи, освен тези от военните формирования на въоръжените сили".[3]

Отбраната на страната по принцип е функция на военния инструмент на държавата, но в резултат на хибридния характер на съвременните рискове и заплахи за сигурността, тя отдавна не се изчерпва само с дейността на въоръжените сили. Успехът на отбраната в съвременните условия все повече зависи от интегрираното използване на всички инструменти на държавната и колективната мощ, при отчитане на конкретните фактори и условия.

Не е тайна, че както в НАТО, ЕС, така и в Република България в настоящия исторически период осигуряването и поддържането на националните или съюзните въоръжени сили, участващи в учения или в операции, свързани с отбрана на страната, разчитат все по-осезаемо на

граждански ресурси и помощ, които са продукт на невоенния компонент. Известен факт е, че по време на Студената война в нашата страна голяма част от инфраструктурата като железопътни линии, пристанища, летища, комуникационни мрежи и въздушно пространство са част от държавния монопол. Това предполага бързо и безпроблемно прехвърляне на контрола/управлението им при провеждане на военни операции. По данни на електронното списание NATO Review magazine „Днес ситуацията е коренно различна: 90% от доставките и логистиката на НАТО се движат от частни компании, а 75% от поддръжката от страната домакин на силите на НАТО е на база договори в частния сектор".[4] Анализирайки фактите се вижда прогресивно нарастващата роля на невоенния (граждански) компонент по отношение на системата за отбрана и нейните задачи.

Принципно, *мисията* представлява цел и обща задача или задължение, възложени на лице или група хора, структури или организации. Чрез нея се прави ясно, кратко и обосновано изложение на целта и произтичащите от нея задачи, базирано на отговорите на 5 (пет) основни въпроса, „кой (с кого)", „какво" „къде", „кога" и „защо", но не и въпроса „как" да бъде постигната съответната задача.

Анализът на множество литературни източници и нормативни документи разкрива, че за разлика от въоръжените сили, за невоенния компонент не е ясно формулирана мисията за отбрана. Това е показателно за отношението на нашето общество към войната. Видимо не се допуска възможността страната да бъде въвлечена във военен конфликт или да се достигне до състояние на война. Всъщност тази възможност доказано съществува. Ето защо, ще се опитаме да предложим един приемлив отговор на този въпрос и да заострим вниманието на обществото върху безусловното ангажиране на невоенния компонент във функциите на системата за отбрана на страната.

Отчитайки основните постановки в закона за отбраната и въоръжените сили на Република България относно целта и задачите на отбраната на страната и нейните дейности, отразени в националната отбранителна стратегия, бихме могли да формулираме ***мисията на невоенния компонент*** за участие в колективната отбрана като: *изграждане, поддържане и използване на граждански отбранителни способности за осигуряване на достатъчен ресурс от човешки, материални, информационни и финансови средства за отбрана на страната, а при необходимост във взаимодействие с ВС, силите на НАТО и други международни организации, да гарантират устойчиво управление и функциониране на държавата, в условията на военнополитическа кризи и военен конфликт, с оглед гарантиране на националния суверенитет, независимостта и териториалната цялост.*

Така формулираната мисия на невоенния компонент е показателна за големия обхват и сложни зависимости на невоенния компонент в системата за отбрана на страната, които са обект на вземането на решение от държавното ръководство.

Възможен подход за дефиниране на функциите на НВК в интерес на отбраната на страната, е да се придържаме към съществуващия в държавата регламент за участие на НВК в отбраната на страната. Това на практика са основните дейности, най-важните приложни области и ключовите роли, които е предвидено да изпълняват елементите на невоенния компонент в интерес на отбраната на страната. Фундаментът на този регламент са възложените военновременни задачи по отбраната на страната на държавните институции, органите на местното самоуправление и местната администрация и на юридическите лица съгласно закона, които са конкретизирани в *„Списък на основните отбранителни способности на страната (граждански компонент)"*. Съгласно приложение 2 от Постановление на Министерския съвет № 286 от 18 октомври 2011 г. ***основните функции***, които държавата възлага на НВК за участие в отбраната на страната са четири: *управление; защита; осигуряване и поддържане, възстановяване и изграждане.* [5]. Следователно по всяка от посочените функции е необходимо да се изграждат и развиват конкретни невоенни способности, които да гарантират изпълнението на широкия кръг от мирновременни и военновременни задачи.

Първата функция ***„Управление“*** е базова за съществуването на сложна социална система, каквато е системата за отбрана на страната. Функцията се реализира с помощта на редица органи, структури, сили и средства, чрез които се изпълняват дейностите за осигуряване на държавното управление, ръководството на отбраната, командването и управлението на ВС, ръководството на министерствата и ведомства от централната администрация, местната власт, търговските дружества и организациите на гражданите. Функция „Управление“ включва дейностите по: формиране на отбранителната политика; разработването на прогнози, анализи, оценки и препоръки за вземане на решения в областта на отбраната; изготвянето на стратегически планове и директиви за привеждане на въоръжените сили и НВК в готовност; изграждане на връзки и механизми, необходими за осъществяване на взаимодействие както между отделните елементите на НВК, така и между НВК и ВС и други за постигане на общата цел на отбраната на страната.

Министерският съвет формира държавната политика, а министерствата и ведомствата от централната администрация, ръководителите на подчинените структури на министерствата и ведомствата на територията на страната, областните управители и администрации, кметове на общини подпомагани от съвети по сигурност и щабове, а също така и юридическите лица с възложени военновременни задачи и техните структури, са инструментите за провеждането на тази политика. В този ред се осъществява подготовката на отделните сфери, касаещи НВК и отбраната на страната.

Ефективността и ефикасността на управлението в голяма степен зависи от всестранното осигуряване на процесите по планиране, организиране и осъществяване на контрол на подготовката, развръщането, използването и взаимодействието между въоръжените сили и НВК в интерес на изпълнение на задачи по отбраната.

Втората функция ***„Защита“*** обхваща дейностите и задачите по планиране и осигуряване на защитата на държавните органи и личния състав от държавната администрация и на стопанските субекти, защитата на населението, защитата на обектите от критичната инфраструктура, защитата на транспортната, енергийната, информационната и друга инфраструктура, екологичната защита. Също така дейностите по спасяване, евакуация и временна закрила; запазване и съхранение на културните ценности при кризи, учения и операции, касаещи отбраната на страната.

Третата функция ***„Осигуряване“*** има изключително важно отношение към отбраната на страната, защото е свързана с изхранването на населението, осигуряването с питейна вода и доставката на основни хранителни и нехранителни стоки при положение на война и при военно положение. Друг аспект на тази функция са поддържането и развитието на отбранителната индустрия и осигуряването на военновременния производствен комплекс, за производство и ремонт на необходимите материални средства, техника и въоръжение. Все по-важни са въпросите касаещи производство на топло- и електроенергия, преноса, разпределението и доставката на енергоносители и комуникационно – информационното осигуряване. На следващо място са геодезично и топографско осигуряване, транспортното осигуряване и транспортната логистика, пощенско осигуряване, здравеопазването и осигуряването на медицински услуги, ветеринарномедицинско осигуряване, митнически услуги и митнически контрол, социално подпомагане и социално осигурителни дейности. Не по-малко важни са осигуряването на съдопроизводство и функциониране на съдебната система, обучение, квалификация и научна поддръжка на сигурността и отбраната. Рамка за тези дейности са финансовото осигуряване и гарантиране на устойчивостта на банковата система на страната.

Четвъртата функция **е *„Поддръжка, възстановяване, изграждане“***. Тази функция обхваща дейности, касаещи невоенния компонент, свързани с поддържане, възстановяване и изграждане на инфраструктурата свързана с транспортните, с комуникационните и с енергийните системи. Дейностите по техническо прикритие, възстановяване и изграждане на административни и икономически обекти, урбанизирана инфраструктура и ВиК системи. На последно място, но не и по важност - изграждане и поддържане на полева хуманитарна инфраструктура и други.

Посочените четири функции обхващат основните области, в който невоенния компонент има възложени задачи в интерес на отбраната на страната самостоятелно или във взаимодействие

с въоръжените сили. Анализирайки нормативната база можем да заключим, че възложените задачите на НВК за участие в отбраната на страна са формулирани единствено в класифицирани документи, касаещи въпросната проблематика, което представлява сериозен проблем. Още повече, че голяма част от служителите от НВК не са допуснати до работа с класифицирана информация. Проблем, оказващ негативно и възпиращо въздействие, е познаването, подготовката и усвояването на общите и специфичните задачи, задължения и отговорности на персонала на НВК, касаещи военновременния режим на работа на всяка една организация. Точно поради това и с цел изясняване важността и отговорността на НВК, на база вече формулираната мисия и функции на структурите и елементите от НВК могат да бъдат изведени и групирани основните задачи касаещи участието им в колективната отбрана на страната.

Във връзка с мисиите на въоръжените сили можем да определим ***задачите на невоенния компонент*** в три категории: задачи в интерес на колективната отбрана; задачи, изпълнявани в интерес на конкретни операции, съвместно с въоръжените сили; и задачи, изпълнявани в зоната на комуникациите:

- Задачите в интерес на колективната отбраната на страната произтичат от базовите изисквания за устойчивост на гражданската готовност в НАТО. Те са приети от Комитета за гражданско планиране при извънредни ситуации (Civil Emergency Planning Committee – CEPC) [6] и включват: осигуряване на устойчиво държавно управление; гарантиране на непрекъснатост на енергийните доставки за съюзните сили; ефективно справяне с интензивни миграционни кризи; гарантиране на доставките на храна и вода; ефективно справяне с масови жертви; осигуряване на надеждна и непрекъсната работа на гражданските комуникационни системи; гарантиране функционирането на гражданската транспортна система; осигуряване на граждански ресурси в интерес на колективните сили, съгласно възприетите задължения като страна домакин;
- Задачите, изпълнявани в хода на конкретни операции съвместно с въоръжените сили включват: разузнаване и наблюдение; контраразузнаване; участие в прикриването на застрашен участък от държавната граница и осигуряване на благоприятни условия за развръщане на съюзнически сили и средства на НАТО за провеждане на последващи операции в условията на чл. 5 от Вашингтонския договор; участие в охраната на държавните граници с неучастващите във военния конфликт съседни държави; участие в охраната и отбраната на особено важни обекти на територията на страната; участие в дейностите по контрола на въздушното и морските пространства; борба с десантите, диверсионно-разузнавателните и терористичните групи на противостоящите сили; осигуряване на граждански ресурси в интерес на отбраната; поддържане, възстановяване и техническо прикритие на националната инфраструктура; конвойна и съпроводителна дейност извън зоната на бойните действия; спасителни и евакуационни дейности на населението от зоната на военните действия и обекти на икономиката участие в изграждане и поддържане на военнопленническа инфраструктура; възстановяване на разрушения [7] и др.;
- Задачите, изпълнявани в зоната на комуникациите се осъществяват извън зоната на бойните операции или учения, в интерес на националното стопанство, територията и инфраструктурата и населението. Такива задачи могат да включват: осигуряване на устойчиво държавно управление; осигуряване на ранно предупреждение за потенциални рискове и заплахи; гарантиране на непрекъснатост на енергийните доставки за населението и икономиката; осигуряване функционирането на националното стопанство за военно време; поддържане на необходимите държавни запаси от материални средства и хранителни продукти; гарантиране функционирането на гражданската транспортна система и логистиката; гарантиране на надеждна и непрекъсната работа на комуникационно и пощенско осигуряване на населението и икономиката; гарантиране на киберотбрана и киберсигурност; осигуряване на медицинска помощ и здравеопазване за населението; гарантиране на обществения ред и вътрешната сигурност в страната; организиране на гражданска отбрана в това число и защита и подпомагане на населението при пожари, природни бедствия, аварии и екологични катастрофи; оказване на хуманитарна помощ; осигуряване на режимно снабдяване на населението с хранителни продукти и стоки от първа необходимост; поддържане на благоприятна психологическа среда сред населението на страната и др.

На основата на посоченото до тук и отчитайки тенденциите и опита на водещите страни, по отношение на съвременните конфликти, можем да обобщим, че ролята и отговорностите на невоенния (гражданския) компонент непрекъснато нараства. Участието на невоенния компонент в отбраната страната се организира на базата на дефинирана мисия, конкретни функции и задачи, като по този начин се създават условия за успешно неутрализиране най-вече на съвременните нетрадиционни и асиметрични рискове и заплахи.

В условия на динамично променяща се среда на сигурност, невоенният компонент се оказва не просто източник на допълнителни отбранителни ресурси, а ключов инструмент за гъвкаво реагиране на нетрадиционните заплахи за сигурността на страната и за обогатяване на съюзните способности за колективна отбрана. Налага се извода, че в съвременни условия следва да бъде извършвано системно и непрекъснато планиране, изграждане, развитие и поддържане на невоенни способности, ориентирани към мисиите на въоръжените сили. За да бъде постигнат измерим резултат в това отношение са необходими ясни и проверени в практиката нормативни актове, качествен контрол на дейностите, реално ресурсно и финансово осигуряване при регулярно осъществяване на ведомствени и съвместни тренировки и учения.

References

1. Димов, Г. Д. (2017г.) „Науката и съвременната употреба на военна сила“, Съвременни предизвикателства пред сигурността и отбраната, сборник доклади от годишната научна конференция на факултет „Национална сигурност и отбрана“, 18-19 май 2017 г., първа част, ВА, ISBN 978-954-9348-92-7, стр.66.

2. Петков, П.И. (2018г.)„Значението на военностратегическите възгледи в подготовката на населението за отбраната на страната“, Военен журнал, брой 1, ВА, стр.32.

3. Гоцев, Г.Г. (2016г.) „Защита на сигурността и обществения ред,“ Троян: ВГЦ, ISBN 978-619-90682-0-5, стр. 402.

4. NATO REVIEW magazine: “Resilience: a core element of collective defence” - https://www.nato.int/docu/review/2016/also-in-2016/nato-defence-cyberresilience/en/index (24.10.2018 -16:40 ч.)

5. Постановление № 286 на МС от 18.10.2011 г. за възлагане на военновременни задачи по отбраната на страната на държавните органи, органите на местното самоуправление и местната администрация и на юридическите лица - бюджетни организации, обн. ДВ, бр.83 от 25.10.2011 г.

6. Концепцията за развитие на системата на отбранително-мобилизиционата подготовка на страната, МО, София, 2018 г.

7. Национална отбранителна стратегия, МО, София, 2016, стр.12

Milen N. Kisyov,

CROSS-BORDER MIGRATION AND THE RECEIVING COMMUNITY: MECHANISMS AND PRACTICES FOR MUTUAL ADAPTATION

Milen N. Kisyov

Rakovski National Defence College, “National Security and Defence” Faculty

***Abstract**: The article addresses the problems of of cross-border migrants and the host society. Particular attention is paid to a study of the migration situation in Europe. The focus is on the specifics of regional migration policy, the role of the media, the impact of migrants on regional labor markets, the role of intermediaries in adapting migrants, and the dynamics of 'ethnic markets' development.*

***Keywords**: Mutual adaptation, Migration situation, Regional migration policy, Cross-border migration*

ТРАНСГРАНИЧНА МИГРАЦИЯ И ПРИЕМАЩО ОБЩЕСТВО: МЕХАНИЗМИ И ПРАКТИКИ ЗА ВЗАИМНА АДАПТАЦИЯ

Милен Н. Кисьов

*Военна академия „Г. С.Раковски“,
Факултет „Нацинална сигрност и и отбрана“
e-mail: latin002@mail.bg*

Въведение

Дали в търсене на по-добър живот и възможности, далеч от бедността, глада, експлоатацията и несправедливото разпределение на световните ресурси, или за да избягат от военни конфликти и преследване, хората са принудени да мигрират. Освен това, заради липсата на сигурност и възможности за развитие те напускат родните си места, оставяйки зад себе си дома си, родните си, приятелите си, спомените си, семейството си. Диаметрално разположено е мнението, че **потоците на миграцията** могат радикално да променят етносоциалната и дори държавната структура на цели страни и региони с трудно прогнозируеми и трудно управляеми последствия. Определени основни вектори и обеми на миграционните потоци, тяхната структура и въздействие на икономиката, социалното и демографското развитие на страните. Агенцията за бежанците на ООН осъжда призивите в социалните медии, подчертавайки, че нелегалното преминаване на границата е рисково и опасно. В декларация, в която се предупреждава за фалшиви информации и слухове в социалните медии, Върховният комисарят на ООН за бежанците заявява, че не окуражава нередовни движения и отбеляза, че държавите имат право да охраняват границите си. Но нелегалното преминаване и превеждане на хора през границата, наричано още „нелегална миграция”, е най-често санкционираното трансгранично престъпление по границите на страните от ЕС.

За разлика от трафика на хора, нелегалното преминаване и превеждане през границата е полесно за доказване, тъй като не се налага прокуратурата и разследващите органи да доказват цел-

та, с която е извършено деянието. Достатъчно е да бъдат доказани фактът на преминаване на границата и съответно липсата на разрешение (когато такова се изисква) или неспазване на определените за преминаване на границата места (гранично-пропускателните пунктове). Поради тази причина често разследващите органи, изправени пред опасността да не успеят да съберат достатъчно надеждни доказателства за престъпната цел, с която е извършено деянието, го квалифицират като нелегално преминаване или превеждане, дори да има данни, че в конкретния случай може да е налице трафик на хора.

Този извод се подкрепя и от многократно по-големия брой наказателни производства, образувани за нелегално преминаване или превеждане, в сравнение с производствата, образувани за трафик на хора. [3]

1. Особеностите на трансграничната миграция

Какво е трансгранична миграция? Това е важен междусекторен регионален проблем с продължаваща нарастваща тенденция и рискове, водещи до съществени обществено-политически структурни промени, свързаното с тях дълбоко социално преструктуриране и нарушения в колективната (трансграничната) и индивидуалната сигурност.

Към въпросите, които все повече и повече трябва да ни вълнуват днес, са инициативите за решението на проблемите на миграциите и движенията на хората, както и ситуационни и структурни фактори, влияещи върху миграцията. В страните, намиращите в преходен етап, се наблюдават най-общо три основни миграционни тенденции: вътрешна миграция от изостанали, разрушени или тотално обеднели райони към големите агломерации[1], трансгранична миграция между съседни страни и емиграция[2].

Редица изследвания в това направление вземат предвид определени страни и региони, както и големите обеми мигранти, което е макроанализаторска дейност. При тях преимуществено се използват средствата и подходите на статистическия анализ и количествената социология. Но този подход работи съмнително (и не в достатъчен обем) за целите и задачите, които се поставят в интерес на прогнозите и анализите за другите два вида миграции. Когато например се установи, че миграционните потоци оказват влияние на приемащото общество на локално и регионално ниво, се търси отговор на въпроса в действителност каква е ролята на държавата, властта, обществото и всички обществено-политически фактори, създаващи равновесие в обществат. Образуването на диаспори в резултат на миграционни процеси практически може да доведе и до конфликти, липса на върховенство на закона, лошо управление, корупция, липса на достойни условия на труд, както и до повишаване на безработицата в приемащите страни.

Посочените рамки на това явление се определят и доизясняват до известна степен и от ролята на миграцията на личностно-групово ниво. Без пълноценен коректен анализ на това ниво, не е възможно да се градят жизнени стратегии и практики, да градят или защитават културни ценности, поведенчески норми и стереотипи и всичко, което съставлява и определя социокултурният аспект на миграционните и диаспоралните процеси.

Опитът учи, че на практика, изчерпването на обществената толерантност към нивото на очевидна престъпност, миграции и обществената неудовлетвореност от способността на правозащитната система резултатно да им противодейства, са фактори с пряко и конкретно влияние върху икономическа, обществено-политическа, духовна, нравствена и демографска криза. Тъй като разходите за постигане на сигурност се плащат от данъкоплатците, срещу това те очакват от управляващите и повече сигурност, очакват по-големи възможности и подходи, които да гарантират ефективно задоволяване на обществените потребности на национално и международно ниво.

[1] В градоустройството е селищно образувание, възникнало в резултат от свързване на големи градове и разположени около тях по-малки селища в обща урбанизирана територия. Агломерация понякога се нарича и процесът на агломериране, създаващ агломерации.,

[2] Доброволното или насилствено напускане за дълъг период от време на страната на обитаване и заселване в друга страна. Обикновено това е причинено от някаква отрицателна промяна в живота, била тя природна, икономическа или военна.

Във връзка с това, на основата на ясно осъзнати национални икономически и обществени цели и интереси, при отчитане на ресурсните възможности на страната могат да бъдат построени значими управленски решения и в крайна сметка да бъдат постигнати нужните икономически резултати. В противен случай, ще нараснат както преките, така и косвените заплахи за икономическата и за националната сигурност на страната.

Друг важен аспект на трансграничната сигурност е, че трудностите у дома като основни причини за миграция и търсене на убежище варират както от една мигрантска общност до друга, така и от един миграционен тип до друг вътре в мигрантските общности. Емблематичен пример е сирийската, причините за която през 70-80-те години са образователни, през 90-те - предприемачески и трудови, а след началото на конфликта –търсене на убежище.

От 20-те години на миналия век големи движения на населението – някои от тях принудителни, в Съветския съюз подкрепиха индустриалното и селскостопанското развитие в дванадесетте републики. Подхранвана от геополитически събития, които до голяма степен са засегнали човешката мобилност в глобален мащаб, връзката между миграцията и развитието се превърна в централно място в съвременните политически, икономически и социални дебати. Миграцията се превърна **в основен стълб на развитието** в няколко региона в рамките на проекти за регионална интеграция и развитие, по-специално Европейската икономическа общност, наследена от Европейския съюз. От 70-те години на миналия век миграцията е от основно значение за развитието чрез регионални системи за свободно движение в Централна, Източна и Западна Африка. Днес, трансграничната миграция в Африка представлява важна стратегия за оцеляване и приспособяване към екологичните проблеми и икономическите спадове и това се оказва ключова характеристика в процесите за разбирането и прогнозиране на възникването и развитието на хуманитарни катастрофи.

Изследванията на трансграничните миграции[3], новата картина на света, формирана на тяхна основа, наскоро се превърнаха в една от водещите „тенденции" в световните научни и анализаторски изследвания. В същото време, това е и модерен сюжет за средствата за масова информация, неразделна част от масовите настроения, инструмент за идеологическа и политическа мобилизация, приоритет на държавните политики и вече най-важното поле за взаимодействие в областта на международните отношения. Говоренето и писането за миграцията[4] и мигрантите[5] стана обичайно, познато, почти тривиално.

Причината е очевидна. Интензивно се описват и обсъждат оценяваното явление и свързаните с него последствия и това се е превърнало в най-важното явление на световното развитие.[6] Прогнозите за 21 век са направени както за целия свят, така и за неговите макрорегиони и отделни държави, казват, че през настоящия век ролята на миграциите[7],[8]и свързаните с тях процеси на диаспоризация ще бъдат само растат.

1.1. Германия: най-голям брой имигранти[9] и емигранти[10]

[3] Тенденции в трансграничната миграция на работна сила и свободното движение на хора – ефекти за България, Институт „Отворено общество", София, ISBN 978-954-9828-95-5, 2010, http://www.osf.bg/cyeds/downloads/OSI_Report_Migration_2010_MEW.pdf

[4] Преместване на хора с цел смяна на местоживеенето.

[5] Човек, който мигрира, т.е. придвижва се и се преселва от едно населено място в друго или от една страна в друга. Речник на българския език

[6] https://www.coe.int/bg/web/compass/migration

[7] Статистически данни за миграцията и мигрантите https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Migration_and_migrant_population_statistics/bg

[8] Миграционни потоци: 2 милиона имигранти от държави извън ЕС, https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Migration_and_migrant_population_statistics/bg

[9] Човек, който се заселва за постоянно или поне за дълъг период от време в друга страна и дори получава ново гражданство.

[10] Човек, доброволното или насилствено напуснал за дълъг период от време на страната на обитаване и заселване в друга страна.

Данните показват, че през 2016 г. Германия е отчела най-голям общ брой мигранти (1 029 900), следвана от Обединеното кралство (589 000), Испания (414 700), Франция (378 100) и Италия (300 800). През 2016 г. Германия е отчела и най-голям брой мигранти (533 800), следвана от Обединеното кралство (340 400), Испания (327 300), Франция (309 800), Полша (236 400) и Румъния (207 600). През 2016 г. общо 21 държави — членки на ЕС, са отчели по-голяма миграция, отколкото емиграция, но в България, Хърватия, Латвия, Литва, Полша, Португалия и Румъния броят на емигрантите е надвишил броя на имигрантите.[11]

Спрямо броя на пребиваващото население, през 2016 г. Люксембург е отчел най-голям процент на имиграция (39 имигранти на 1 000 души), следван от Малта (38 имигранти на 1 000 души). През 2016 г. най-високи проценти на емиграция са били отчетени за Люксембург (23 емигранти на 1 000 души), Малта, Литва и Кипър (всяка от които с 18 емигранти на 1 000 души), и Ирландия (13 емигранти на 1 000 души).

1.2. Интеграцията на мигранти в Европа

Расизмът, ксенофобията и анти-имигрантските настроения са проблем в много държави. Мигрантите са лесна мишена на расистки и ксенофобски настроените политици, които ги обвиняват за социалните и икономическите проблеми в техните общности. „Мигрантофобията" се превръща в проблем, който възпрепятства интеграцията и взаимното разбирателство и води до отчуждаване на и насилие срещу мигрантите в много европейски държави. Редица висши политици, включително и лидери на европейски държави, заявиха, че мултикултурализмът[12] се е провалил. В Европа се случват важни демографски промени със степени на многообразие, определяни от миграционните движения. Съществуващите подходи към интеграцията и управлението на културното многообразие са поставени под въпрос. „Както разбираме днес, мултикултурализмът дава възможност обществата в една и съща държава да се развиват успоредно… Това трябва да бъде спряно." Това каза Торбьорн Ягланд – генерален секретар на Съвета на Европа.[13] [14]

След като **мултикултурализмът** (като механизъм) се провали, какво е решението? Отговорът може да бъде нещо, което се нарича „междукултурализъм", който популяризира индивидуални права за всеки, без дискриминация. В културното общество, хората имат право да запазят своята етническа, културна, религиозна и социална идентичност, а тези идентичности трябва да се толерират от останалите. Въпреки това, цялата общност трябва да уважава стандартите за правата на човека, а културните различия не могат да бъдат приети като извинение за нарушаване правата на други групи индивиди. Според критиците на мултикултурализма, Европа е допуснала прекомерна имиграция без да изисква достатъчно много интеграция – неудачно решение, в резултат на което социалното сцепление е ерозирало, националните идентичности са били подкопани, а общественото доверие – силно понижено. Защитниците на мултикултурализма, от друга страна, отговарят, че проблемът е не в прекомерното разнообразие, а в прекомерния расизъм. Може уверено да се твърди, че хаотичният процес на принудително преместване на огромни маси от хора от „периферните" към привилегированите страни изглежда като истински реванш срещу преобърнатата структура на съвременния несправедлив свят. „Разпространението на страх и доверие" в манипулирания западен свят се превръща в средство за администриране на включването и изключването в западното общество и за асимилацията на имигрантите. ЕС е спокоен със своята Агенция за охрана на границите „Фронтекс", с Глобалния подход към миграцията и мобилността, Стокхолмската програма и Дъблинския регламент, който връщаше мигранта в първата страна от ЕС, в която е получил статут и с обемистото си безсмислено мигрантско законодателство. За последните десетина и повече години

[11] Пак там.
[12] Понятие, с което се описват общества, в които съжителстват много на брой различни култури без една от тях да е господстваща или поне преобладаваща.
[13] Съветът на Европа предупреждава за мултикултурализма, Финеншъл Таймс, 16 февруари 2011; http://www.ft.com/intl/cms/s/0/72c02d9a-39c6-11e0-8dba-00144feabdc0.html#axzz1bhKInsit
[14] От 2009 г до март 2015 г.

бяха похарчени стотици милиони за програми за засилване охраната на границите, за интегриране на бежанците, но без особен ефект.

Този подход гарантира **максимум** толерантност и разбиране към индивидуалния избор и **минимум** толерантност към идеи, които могат да подронят самите основи на демократичното общество.

1.3. Реакциите в Европа

„Ислямът е смъртта на Европа”: Хиляди на протест срещу мигрантите[15]. През септември 2015 г., няколко хиляди демонстранти се събраха днес във Варшава, за да протестират срещу мигрантите, с лозунги като „Ислямът е смъртта на Европа!”, предаде АФП. Демонстрации от същия тип, със стотици участници, се състояха в Прага и Братислава. Демонстрации, но значително по-малобройни, бяха организирани по същото време в трите столици в подкрепа на приемането на бежанците.

Във Варшава около 5000 антимигрантски активисти (според кореспондентите на АФП на място, 10 000 според организаторите), се събраха в центъра на града. Те носеха полски национални знамена и скандираха под дъжда: „Днес бежанци, утре терористи!” и „Полша - свободна от исляма!” Повечето се представиха като католици, които са против приижданието на мюсюлмани. Акцията започна с молитва към Богородица. Източноевропейците искат затваряне на границите. И са прави! „Тук сме, за да може нашият глас да стигне до правителството и решението за приемане на мюсюлманите да бъде отменено”, заяви един от ораторите, качен на камион-платформа. Варшава на този етап е приела 2000 бежанци и отказва да се съгласи с квотите. Полицаи в снаряжение за борба с безредици следяха за реда по време на акцията, организирана от крайнодесни групировки като „Рух народови” (национално движение) и Национално-радикалния лагер (ОНР). Радикални десни демонстранти налетяха да бият тъмнокож пешеходец по време на демонстрацията, но охранителите на акцията се намесиха навреме.

Привържениците на приемането на мигранти, които се събраха близо до Варшавския университет, бяха около пет пъти по-малко. „Добре дошли, бежанци!” и „Да се питаме как да помогнем, а не трябва ли да помогнем”, са техните лозунги.

Полската полиция отказа да даде оценка за броя на участниците. В Братислава около 1500 души според АФП протестираха против приемането на мигранти по призив на антиислямско движение, водено от активиста на крайната десница Лукаш Копач, с одобрението на националистите от партията „Наша Словакия”. „Мултикултурализмът е утопия!” и „Не отваряйте границите!”, „Вие не се добре дошли, вървете си у дома!”, гласят плакатите им. Друга демонстрация с мото „Апел за хуманност”, събра симпатизанти на бежанците - около 500 на брой, в словашката столица.

В чешката столица Прага също имаше две демонстрации, като тази на противниците на мигрантите беше видимо по-многобройна - с около 800 участници според полицията. „Вървете си у дома!” и „Защитете границите!”, скандираха те, докато ораторите призоваха правителството да подаде оставка и страната да напусне ЕС. Около 2000 привърженици на отварянето на границите за мигранти, събрали се в съседство, носеха плакати, пожелаващи „Добре дошли, бежанци!” и „Миграцията не е престъпление”.

През месец юли 2019 г., хиляди протестиращи излязоха по улиците в Германия, за да изразят солидарност с мигрантите, опитващи да прекосяват Средиземно море, и екипажите на спасителни плавателни съдове, предаде ДПА. Сьорен Мойе, член на екипажа на кораба "Сий уоч-3", призова германските градове да участват повече в приема на спасените в морето бежанци. "Средиземно море сега е най-опасната граница в света", каза Мойе пред множеството, събрало се в северния германски град Олденбург. Събраха стотици хиляди евро за арестуваната германката, капитан на хуманитарния кораб.[16]

[15] https://dariknews.bg/novini/sviat/islqmyt-e-smyrtta-na-evropa-hilqdi-na-protest-sreshtu-migrantite-1498127

[16] https://dariknews.bg/novini/sviat/mnogobrojni-protesti-v-germaniia-za-migrantite-i-spasitelite-v-sredizemno-more-snimki-2175374

Протести на организацията "Зебрюке" ("Морски мост") имаше и в Берлин и Хамбург, където според полицията в акцията са участвали 3000 души. Общо протести е имало в стотина германски града с участието на над 30 000 души, предаде АФП, като се позова на организаторите. Според тях в Берлин са се събрали 8000 души, а в Хамбург - 4000.

Германският министър на вътрешните работи Хорст Зеехофер (от 14 март 2018 г.) призова в писмо италианския си колега Матео Салвини да отвори пристанищата. През 2019 г. убийството на официален служител, подкрепящ мигрантите, е „аларма“ за Германия. Това предупреди Зеехофер, като категорично подчертава, че десният екстремизъм е „сериозна опасност за нашето общество.“ Убийството на Валтер Любке е „аларма, насочена към всички нас", повтори Зеехофер на пресконференция, ден след като прокурорите заявиха, че подозират десен екстремистки мотив в смъртта на началника на градската администрация в Касел. През месец юли 2019 г. Матео Салвини наложи забрана на хуманитарни кораби, превозващи мигранти, да акостират на италианска територия. Въпреки министерската забрана, няколко кораба на неправителствени организации я пренебрегнаха и пуснаха котва до пристанището на остров Лампедуза. „Не можем да не бъдем отговорни за корабите със спасени хора, които седмици наред се носят из Средиземно море, защото не могат да намерят пристанище“, пише Зеехофер в писмото си и призовава за европейско решение. „Затова ви призовавам да преразгледате позицията си на отказ от отваряне на италианските пристанища“, допълни той. „Заради общата европейска отговорност и общите ни християнски ценности не трябва да има никакво значение от коя организация са били спасени мигрантите в Средиземно море, откъде е екипажът и под какъв флаг плава съответният кораб“, заяви германският вътрешен министър.

2. МЕХАНИЗМИ И ПРАКТИКИ ЗА ВЗАИМНА АДАПТАЦИЯ

Глобалният пакт за миграцията[17]**,** наричан пакт за безопасна, организирана и законна миграция е първата международна и правно необвързваща рамка за сътрудничество по въпросите на миграцията. Той е резултат от широкообхватен процес на обсъждания и преговори между всички държави — членки на Организацията на обединените нации, който започна с Декларацията от Ню Йорк от 2016 г., приета с единодушие от Общото събрание на ООН през 2016 г. Европейският съюз и неговите държави членки участваха в разискванията относно Глобалния пакт за миграцията от самото начало, като резултатът бе глобален пакт, който до голяма степен отразява европейските цели.

2.1. Какви са целите на Глобалния пакт за миграцията?

Миграцията е реалност в глобален мащаб и нито една държава не може да се справи с нея сама. Тя изисква глобални решения и споделяне на отговорността в световен мащаб на основата на международно сътрудничество. Глобалният пакт за миграцията има за цел да насърчава международното сътрудничество, определяйки ръководни принципи и осигурявайки многостранна политическа рамка. Той обхваща комплексния характер на международната миграция, като засяга множество аспекти, свързани с миграцията, като управлението на границите, контрабандата и трафика на хора, документите на мигрантите и връщането и обратното приемане, както и диаспорите и паричните преводи.

Прилагането на Глобалния пакт за миграцията се ръководи от десет принципа, сред които са универсалният характер на правата на човека, националният суверенитет, както и правно необвързващият характер на документа. В него са очертани 23 конкретни цели за безопасна, организирана и законна миграция, които да служат като отправни точки за държавите при провеждането на национални политики в областта на миграцията.

2.2. Какво ще е въздействието на Глобалния пакт за миграцията върху незаконната миграция? Ще се увеличи ли миграцията?

[17] https://europa.eu/rapid/press-release_MEMO-18-6417_bg.htm

Целта на Глобалния пакт за миграцията е миграцията да се осъществява по безопасен, организиран и законен начин. Той съдържа конкретни действия, които ще помогнат на държавите да намалят незаконната миграция, например чрез засилено сътрудничество за справяне с причините за миграцията, борба с трафика на хора и контрабандата на мигранти, управление на границите и улесняване на връщането. Той също така ще спомогне вниманието да се съсредоточи върху законните канали за миграция. Пактът, като международна рамка за сътрудничество, ще бъде основа и за вече извършваната съвместна работа на ЕС и трети държави и международни организации, като Международната организация по миграция (МОМ) и Върховния комисариат за бежанците на ООН (ВКБООН). Всички тези аспекти съответстват до голяма степен на приоритетите и целите на ЕС.

Как ще се осъществи приемането или подписването на Глобалния пакт за миграцията? Текстът на Глобалния пакт за миграцията е приет по време на междуправителствената конференция в Маракеш, Мароко, която проведе на 10 и 11 декември 2018 г. Няма да има подписване, приемането на текста ще се осъществи с консенсус или с гласуване с необходимо мнозинство от поне две трети. След това Общото събрание на ООН ще бъде приканено да приеме официално Глобалния пакт за миграцията под формата на резолюция.

Какво точно съдържа пактът за миграцията, който България отхвърли?[18]

В този пакт няма нищо подмолно, нищо тайно, нищо опасно. Мигрантите няма да станат още повече, както твърдят неговите противници. Едва ли е имало друг проект на ООН, който да е предизвиквал толкова много спорове. Сега той все пак е официално приет от представителите на над 150 държави. Както е известно, България реши да не се присъединява към пакта. На същата позиция застанаха и държави като САЩ, Австралия, Австрия, Чехия, Полша и Унгария. Във всички тези страни противниците на пакта проведоха целенасочена кампания с внушението, че този пакт ще даде право на мигрантите и бежанците да се заселват където си искат. А това е лъжа, твърдят мнозинството специалисти и наблюдатели. Ето за какво всъщност става дума.

2.3. Защо този пакт е важен и полезен?

В своя уводна статия германският седмичник „Ди Велт" пише: „Този пакт е нещо наистина напредничаво. В него няма нито някаква тайна, нито някаква заплаха. И той изобщо не въвежда някакво ново „човешко право на миграция". Идеята на тази глобална договорка е колкото проста, толкова и смислена. В момента четвърт милиард души по цял свят бягат от някакви неволи, като тенденцията е към увеличаване. Те бягат от безработицата, от гражданските войни, от насилията, от изменения климат. Те са изселници, които търсят сигурност, препитание и по-добро бъдеще. Няма страна на този свят, която да може сама да се справи с проблемите на тези хора - и с проблемите, които те създават по пътя на своето бягство. Ако тази задача изобщо има решение, то може да бъде само международно. В това са убедени всички държави, които се включиха в споразумението и така се договориха за принципите, според които в бъдеще трябва да се регулира миграцията.

Тази регулация не се е родила в главите на някаква клика от елитарни глобалисти. През есента на 2016 г., Общото събрание на ООН взе решение за изработването на този пакт. В консултациите се включиха огромен брой участници: правителствата на богати и бедни страни, учени, неправителствени организации, кметове от цял свят, дори Папата. Проведоха се онлайн-семинари, изписаха се безчет доклади, внесени бяха какви ли не предложения.

Дълго време никой не се интересуваше от тези преговори, но те бяха много важни и полезни. Дипломатите също така отбелязаха, че в първоначалния проект „дискриминационната власт между мигранти и бежанци на много места е твърде неясна“.[19]

[18] https://www.dw.com/bg/a-46488432

[19] Wie der UN-Migrationspakt wirklich ausgehandelt wurde, https://www.welt.de/politik/deutschland/article193853001/Streit-der-UN-Wie-der-Migrationspakt-wirklich-ausgehandelt-wurde.html?wtrid=onsite.onsitesearch

Както винаги в подобни процеси, главното беше да се намерят компромиси, но и ясно да се посочат различията. Само за пример: **пактът прави ясна разлика между обичайната и извънредната миграция**; той взема предвид и факта, че държавите, от които идват мигрантите, често пъти имат съвършено различни цели от държавите, към които тези мигранти са се отправили. Пактът изрично подчертава както суверенитета на отделните страни, така и първостепенната валидност на националните им законодателства. В него е вписано още, че онези мигранти, които се завръщат в родината си, имат правото да бъдат приети и да получат документи. С две думи: 23-те принципа на пакта са формулите на едно глобално здравомислие, което сега трябва да се осъществи на практика.

При това юридически пактът няма обвързваща сила. Никой не може да се позове на него в съда. Целта е той да развие собствена политическа динамика и да упражнява натиск - точно както световните климатични цели. Дали в резултат от този пакт броят на мигрантите ще намалее? Едва ли. Или пък мигрантите ще станат още повече, както твърдят противниците на пакта? Защото бежанците и мигрантите тръгват на път не под влиянието на някакви договори, а заради войни, суша и бедност. И най-вече, защото става дума за хора, които се опитват да вземат в собствените си ръце своя живот и живота на семействата си", пише „Ди Цайт“.

2.4. Абсурдни аргументи срещу пакта

Вестник „Тагеспшигел" се спира на аргументите, които привеждат (включително и в България) критиците на пакта: „Те изкарват направо тежката артилерия: пактът давал на мигрантите от цял свят правото свободно да мигрират и отменял правото на суверенните държави сами да решават миграционните въпроси. Това не е вярно. Подобни упреци само помагат на политическите подстрекатели и насърчават конспиративните теории. Абсурдното е, че с настояването си за отхвърляне на пакта тези критици всъщност увреждат собствените си национални интереси, които уж искат да закрилят. (…) Сигурната, уредена и легална миграция е в интерес на всички засегнати - на изходните и на приемащите държави, на самите мигриращи хора. През последните години става все по-очевидно, че индустриалните държави имат нужда от миграция, за да задържат равнището на производителността и на благоденствието. И обратно - със своите инвестиции и парични преводи мигрантите помагат за подобряване на положението в своите страни", коментира "Тагесшпигел".

Германският канцлер подчерта важността на Пакта. Според нея той е голяма стъпка в борбата с трафикантите на хора. **Ангела Меркел, канцлер на Германия казва: „**За първи път, на глобално ниво, съгласувахме общ политически пакт за миграцията. Добър знак е, че се заехме със съдбата на милиони мигранти и още веднъж подчертахме, че универсалните човешки права са за всички граждани, на всяка една държава на планетата.“

Редица държави - Словакия, Австрия, Чехия, Израел, отказаха да подпишат пакта, а заради него се разпадна управляващата коалиция в Белгия. Глобалният пакт за миграцията, е трябвало да бъде одобрен от Общото събрание на ООН на 19 декември 2018 г. През 2018 г., Пакта доведе до правителствена криза в Белгия. Пактът обаче предизвика и остри критики, най-вече сред националисти и привърженици на затварянето на границите. Според тях влизането му в сила ще доведе до още по-сериозен наплив на мигранти в развитите страни. А опасенията на редица правозащитни организации са, че пактът не защитава достатъчно правата на мигрантите.

След провала с Истанбулската конвенция българското правителство обяви, че България няма да стане част и от друг актуален международен документ - Глобалния пакт за миграция на ООН. Позицията на правителството и парламентарните групи на партиите в управляващата коалиция е да не се подписва документът, срещу който се заформи остра съпротива през последните няколко седмици. България се въздържа от присъединяване към Глобалния пакт за миграцията. Министерският съвет реши Република България да се въздържи от присъединяване към Глобалния пакт за безопасна, регулирана и редовна миграция, но страната ни запазва правото си да прилага „онези части от документа, които обслужват интересите ѝ “.

Еврокомисарят по миграцията Димитрис Аврамопулос отправи „последен апел" към държавите, които не желаят да гласуват за Пакта за миграцията на ООН, да променят позицията. Документът ще се приеме идната седмица на Конференция в Маракеш, но няколко държави, сред които наблюдателите слагат и България, не желаят да се присъединят. Българското правителство все още не е обявило официална позиция, макар че преди 10 дни съветът на коалицията реши пактът да не се подкрепи. „Съжалявам, че някои страни не само се оттеглиха от споразумението, но и за това, че реагираха късно", коментира Аврамопулос, който ще представлява ЕС на форума в Мароко.[20] Според него, „пактът не е покана за миграция в Европа", а ще позволи да се намали нелегалната миграция, ще гарантира принудителните връщания и ще предостави закрила на тези, които се нуждаят от нея. "Правя последен апел към тези страни да преосмислят позицията си, защото пактът е в интерес на ЕС, на всички страни членки и на страните, които пряко или косвено са въвлечени в миграцията", заяви еврокомисарят в Брюксел днес.

Засега никоя членка на ЕС не е отказала официално да подкрепи документа, но Унгария, Австрия, Полша, Чехия и Хърватия направиха подобни анонси. Правителството в Белгия се бори за оцеляване в момента заради спорове в управляващата коалиция за националната позиция по пакта. Междувременно Европейската комисия съобщи, че незаконната миграция в ЕС от началото на годината е паднала под предкризисните нива. До октомври 2018 г., незаконните влизания са общо 116 000 по всички граници на ЕС. Навсякъде бройките намаляват с изключение на пътя от Мароко и Алжир към Испания, както и по сухопътната граница между Турция и Гърция. По Западносредиземноморския маршрут от началото на 2018 г. нелегално са влезли 57 000 души. Тези през Турция са около 23 000. Еврокомисията предупреди, че Босна и Херцеговина се превръща в преразпределителен център, откъдето незаконните мигранти се насочват към Западна Европа. По данни на Комисията в Босна в момента има 6000 мигранти, пристигнали през Гърция, Албания и Черна гора.

Еврокомисарят за миграцията Димитрис Аврамопулос призова в Брюксел през 2018 г. министрите на вътрешните работи от ЕС да приемат поне договорените до момента промени в общата система за убежищата, за да може да се ускори работата по вече пристигналите в Европа мигранти. Още през лятото на 2018 г., страните-членки постигнаха принципно съгласие по 5 от 7-те законодателни предложения на Комисията. Липсата на консенсус по процедурите за убежище и по Дъблинското споразумение[21] обаче блокират цялостната миграционна реформа. Предвид европейските избори през май Еврокомисията сега настоява да се приемат поне регламентите за условията за предоставяне на международна закрила, за агенцията за убежището на ЕС, за регистъра за пръстови отпечатъци "Евродак" и за презаселването, както и директивата за условията за приемане, където се смята, че преговорите с Европейския парламент могат да завършат преди изборите и те да бъдат окончателно приети.

За да се гарантира, че сътрудничеството в рамките на регламента[22] почива на солидна основа, както и за да се развие взаимното доверие между държавите членки във връзка с политиката в областта на убежището, следва да се установи процес за ранно предупреждение, подготвеност и управление на кризи в областта на убежището, който да има за цел да предотврати влошаване и сривове на системите за предоставяне на убежище, и в който ЕСПОУ да играе ключова роля чрез правомощията си съгласно Регламент (ЕС) № 439/2010. Този процес следва да създаде условия Съюзът да бъде предупреждаван възможно при опасения, че безпрепятственото функциониране

[20] Брюксел: Размислете за пакта за миграцията - Новопристигналите в ЕС - под предкризисните нива https://www.dnes.bg/notifikacii/2018/12/04/biuksel-razmislete-za-pakta-za-migraciiata.395576

[21] Регламент, определящ коя членка на ЕС е длъжна да проучи кандидатурите за бежански статут, за хората, търсещи защита по Женевските конвенции и Квалификационната директива на ЕС, в рамките на Европейския съюз. https://eur-lex.europa.eu/legal-content/BG/TXT/HTML/?uri=CELEX:32013R0604&qid=1561550021182&from=EN

[22] Регламент (ЕС) № 604/2013 на Европейския парламент и на Съвета от 26 юни 2013 г. за установяване на критерии и механизми за определяне на държавата членка, компетентна за разглеждането на молба за международна закрила, която е подадена в една от държавите членки от гражданин на трета държава или от лице без гражданство. https://eur-lex.europa.eu/legal-content/BG/TXT/HTML/?uri=CELEX:32013R0604&qid=1561550021182&from=EN

на създадената с настоящия регламент система е застрашено поради особено силен натиск върху системите за предоставяне на убежище и/или поради недостатъците на същите системи на една или повече държави членки.

Един такъв процес би дал възможност на Съюза да насърчава превантивните мерки на ранен етап и да отдава необходимото политическо внимание на такива ситуации. Солидарността, която е основен елемент в общата европейска система за убежище върви ръка за ръка с взаимното доверие. Чрез засилване на това доверие процесът за ранно предупреждение, подготвеност и управление на кризи в областта на убежището би могъл да подобри насочването на конкретни мерки на действителна и практическа солидарност към държавите членки, за да се помогне на засегнатата държава членка като цяло и на кандидатите в частност. В съответствие с член 80 от ДФЕС, винаги когато е необходимо актовете на Съюза следва да съдържат подходящи мерки за прилагането на принципа на солидарност, този процес следва да бъде придружен от такива мерки. Заключенията относно обща рамка за действителна и практическа солидарност с държавите членки, чиито системи за предоставяне на убежище са изложени на особено силен натиск, включително предизвикан от смесени миграционни потоци, приета от Съвета на 8 март 2012 г., предвижда инструментариум, съставен както от съществуващи, така и от потенциални нови мерки, като този инструментариум следва да се взема предвид в контекста на механизма за ранно предупреждение, подготвеност и управление на кризи.[23]

Европейският икономически и социален комитет (ЕИСК)[24] в свое становище[25], припомня, че Глобалният пакт е инструмент с незадължителен характер, който не поражда никакво ново задължение за държавите членки и в чийто текст са включени изцяло принципите и ценностите на Европейския съюз.

Изразява се съжаление, че Пактът не беше одобрен от всички държави-членки, и счита, че това щеше да бъде отлична възможност да се постигне напредък в изграждането на единна позиция на ЕС на световната сцена по въпросите на миграцията. Затова ЕИСК счита, че той трябва да бъде ратифициран от всички държави — членки на ЕС, като същевременно приканва ЕС да конкретизира и доразвие неговите цели посредством подходящи механизми. ЕИСК счита, че би било интересно да се проучат възможностите за участие в процеса на междуправителствени консултации и преговори за развитие на Международния форум за миграцията (International Migration Review Forum — IMRF), както и в самия форум, който ще бъде инструментът на ООН за мониторинг на Глобалния пакт.

ЕИСК отдава признание на усилията на гражданите, социалните партньори и организациите на гражданското общество в ЕС, които чрез своята ангажираност и действия показаха как да се прилагат на практика ценностите на ЕС и, съответно, как да се реализират целите на Пакта.

[23] https://eur-lex.europa.eu/legal-content/BG/TXT/HTML/?uri=CELEX:32013R0604&qid=1561550021182&from=EN

[24] Европейският икономически и социален комитет (ЕИСК) е консултативен орган на ЕС, в който влизат представители на организации на работниците и работодателите и на други групи. Той представя становища по свързани с ЕС въпроси пред Европейската комисия, Съвета на ЕС и Европейския парламент, като по този начин действа като мост между вземащите решения институции на ЕС и гражданите на Съюза. https://europa.eu/european-union/about-eu/institutions-bodies/european-economic-social-committee_bg

[25] https://webapi2016.eesc.europa.eu/v1/documents/EESC-2019-01355-00-00-AS-TRA-BG.docx/content

2.6. Миграцията в Европа – голямото разминаване между гражданите и политиците[26]

Неконтролираните миграционни потоци разкриха слабости в управлението на външните граници на ЕС. Ключов елемент в подкрепата на ЕС за държавите-членки е оперативната подкрепа, предоставяна в рамките на системата за горещи точки. Това включва идентифициране и регистриране на всички пристигнали търсещи убежище лица, както и осигуряване на адекватни условия на приемане и капацитет. Въпреки, че има напредък в снемането на пръстови отпечатъци на мигрантите и според данните, предоставени от Комисията, то вече достига близо 100%, условията за прием продължават да пораждат сериозна загриженост. През 2017 г. и през 2018 г. бе отчетен значителен спад на разкритите незаконни преминавания по външните граници на ЕС, главно по миграционните маршрути през Източното и Централното Средиземноморие, но цялостният натиск върху външните граници на Европа продължава да е относително висок. Освен това пътуването до ЕС може да бъде изключително опасно, а контрабандистите често излагат живота на мигрантите на рискове. Предотвратяването на загуба на човешки живот, особено в Средиземно море, изисква операции по издирване и спасяване, както и борба срещу мрежите за трафик и контрабанда на хора.

Прогресивна и всеобхватна европейска имиграционна политика, основана на солидарност, е ключова цел за Европейския съюз. Имиграционната политика има за цел да установи балансиран подход както към законната, така и към незаконната имиграция. Целите са определяне на балансиран подход към имиграцията: целта на ЕС е да се установи балансиран подход за управлението на законната миграция и борбата срещу незаконната имиграция. Правилното управление на миграционните потоци предполага гарантирането на справедливо третиране на граждани на трети държави, законно пребиваващи в държавите членки, засилване на мерките за борба с незаконната имиграция, включително трафика и контрабандата, и насърчаване на по-тясно сътрудничество с трети държави във всички области. ЕС има за цел уеднаквяване на правата и задълженията на законните имигранти, които да бъдат съпоставими с тези на гражданите на ЕС. Като принцип на солидарност за тази политика се посочва Договора от Лисабон, съгласно който имиграционните политики следва да се уреждат на принципа на солидарност и справедливо споделяне на отговорността между държавите членки (член 80 от Договорът за функционирането на Европейския съюз), включително неговите финансови последици.

„Държавите членки все още не са намерили точния баланс между отговорността, която всяка държава трябва да поеме на своята територия, и необходимата солидарност помежду им. Те обаче трябва да демонстрират тази солидарност, ако искат да запазят Шенгенското пространство без вътрешни граници. Противник съм на вътрешните граници и ще продължавам да бъда против тях. Там, където междувременно отново ги има, те трябва да бъдат премахнати. Ако останат, това ще бъде неприемлива стъпка назад за европейското настояще и бъдеще", заявава Жан-Клод Юнкер в реч за състоянието на Съюза през 2018 г. [4]

Европейска имиграционна политика разглеждат трите основни компонента на всеобхватния подход към управлението на миграцията:

- действия с партньорите извън Съюза;
- действия по външните граници;
- действия вътре в Съюза.

Извън ЕС трябва да продължи работата с партньорите: да се намерят решения на първопричините за незаконната миграция, да се сътрудничи за подобряване на управлението на миграцията и борбата с контрабандата на мигранти, да се гарантира, че хората, които нямат право да останат в ЕС, могат да бъдат върнати, да се демонстрират алтернативи на незаконната миграция под формата на легални пътища и да се вземат предвид специфичните потребности на разселените при конфликт лица и на тези, подложени на преследване. За да е силна външната граница, трябва да се поддържа непрекъснато надеждно равнище на контрол и сигурност чрез висока степен на координация и постоянен мониторинг за идентифициране и преодоляване на слабостите. Тези

[26] http://cios-bg.com/index.php/2017-07-08-23-55-16/61-2018-02-24-01-14-34

цели трябва да бъдат допълнени от съгласуван и хуманен подход в рамките на Съюза, като процедурите на държавите членки в областта на убежището и връщането трябва се укрепват взаимно и да се предприемат решителни действия срещу престъпните мрежи, наред със справедлива и последователна уредба на ЕС, основана на солидарност и отговорност.

Стана очевидно, че мигрантите вече са тук и ще продължат да пристигат. Но въпросите и дискусиите вече стават съвършено други - за ролята им в икономиката и обществения живот сега, днес и утре. Въпроси за това как да се разбираме, да съжителстваме и да си взаимодействаме всеки ден с хора, които не са много свикнали с това, не знаят как и често, не искат да правят това. В условия, когато практически няма създадени - или бавно създадени чрез механизми, опитите и грешките в социално и държавно регулиране на тези невероятно сложни, фини и потенциално експлозивни процеси са съществено значение. Дали само идентифицирането на количествените и качествени изменения в обществото зависи или направо засилва динамиката на миграционните потоци в големи мащаби за цели страни и региони? Дали само големината на въздействието на миграционния фактор ще окаже съдействие в развитието или спада на икономическия живот на страните. Ето това е изключително важния въпрос, предоставящ огромно поле от концептуални, практически и държавни задачи, които все още не са решени, а и скоро няма изгледи да бъдат трайно и окончателно решени. Във всеки случай, Европа се превръща в общество на мигранти, т.е. придобива ново качество и този процес по условие не е просто жизнено важен и необходим, но и болезнен и конфликтен.

Основните вектори и обеми на миграционните потоци, както и техните структура, икономически, социални и демографски тенденции оказват въздействие върху развитието на страните и радикално променят етно-социалната структура на много региони, като трудно можем да си представим последствията. Бързото възникване на ново явление като нов елемент в културната, етническата, социалната картина на света неизбежно нарушава стария баланс, формира почвата за появата на нови проблеми и нови конфликти. Отношението към мигрантите вече стана най-болезненият момент в общия комплекс на международните и междуетническите взаимоотношения.

Освен чисто научно значение, това стана важен фактор на въздействие върху развитието на държавна политика за миграцията и в по-малка степен - върху формирането на обществените мнения и настроения. В същото време, именно това създава възможност и диктува необходимостта да се задават нови въпроси, да се поставят задачи и да се разширява тематичното и проблемното поле за изследвания. Да не говорим за факта, че динамично променящата се ситуацията с миграцията прави задачата за наблюдение абсолютно необходима и осмисляне на бързо възникващите нови тенденции и явления. Мощната миграционна динамика и интензивното развитие на нейното разбиране практически премахват (или изтласкват в „идеологически застои") поранните интензивни дебати дали дадена страна или ЕС като цяло има нужда от външни мигранти.

В резултат на всичко това, както обществото като цяло, така и мигрантите в процеса на взаимна адаптация са изправени и непрекъснато ще се сблъскват с няколко социокултурните задачи с висока степен на сложност. Първо, това е задачата за взаимно уважение към тези „крайни" културни ценности, провалът на които ще бъде възприет от всяка от страните като заплаха за нейната идентичност. Второ, задачата за разработване на толерантни форми на взаимодействие, което включва елиминиране на взаимноизключващи се практики от общуването норми на поведение. Трето, приемащото общество е изправено пред предизвикателството да признае мигрантите и диаспорите в процеса на икономическа активност на социалните практики, не противоречащи на нормите на закона, а мигрантите и диаспорите са изправени пред задачата за асимилация и спазване на тези стандарти и норми.

Като правя връзка с изложеното по-горе, бих искал да спомена само няколко извода.

Трансграничната миграция е феномен, който е неразделна част от човешката история, явление, което е все по-засегнато от глобализацията, икономическото и социалното развитие. Нека, както призовава папа Франциск, „да бъдем разумно отворени към сложното явление миграция и да улесняваме интеграцията с дължимото спазване от страна на мигрантите на законите на приемащата ги държава, както и да предизвикаме подновен ангажимент на обществото за истинска

култура на прием и солидарност, за да могат всички да бъдат обичани като деца и да се чувстват у дома в голямото човешко семейство“, в нашия „общ дом“.

При такива глобални проблеми като миграцията или изменението на климата е необходимо и задължително да се работи за транснационални решения за трансгранична сигурност, да се определят общи принципи и да се приемат компромиси. „Пактът си заслужава, защото е ангажимент за многостранността", казва Меркел. Много голямо мнозинство от страните-членки на ООН избраха този ангажимент. Ангела Меркел обаче е права: пактът, е нещо повече от самия пакт, а и как световната общност иска да се справи с големите проблеми на бъдещето в бъдеще.

Използвани източници:

1. United Nations Global Compact for Migration, https://refugeesmigrants.un.org/migration-compact

2. Международната организация за миграция, https://www.iom.bg/

3. Укрепване на правосъдието и правоприлагането в граничните райони, Център за изследване на демокрацията, 2007, ISBN: 978-954-477-152-2, , с. 34, www.csd.bg, csd@online.bg

4. Съобщение на комисията до Европейския парламент, Европейския съвет и Съвета - Управлението на миграцията във всичките ѝ аспекти: Напредък по европейската програма за миграцията, com(2018) 798 final, Европейска комисия, брюксел, 4.12.2018 г., https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-migration/20181204_com-2018-798-communication_en.pdf

Nikolay Y. Dosev, Vladislav S. Savov,

CHALLENGES FOR DEFENSE POLICY IN THE NATIONAL SECURITY STRATEGY

Nikolay Y. Dosev[1], Vladislav S. Savov[2]

1. Faculty of Artillery, Air Defense and Communication and Information Systems, Shumen
2. Service"Military Police", Varna

Abstract: *The report examines and analyzes the priorities related to the defense policy in The National Security Strategy of the Republic of Bulgaria. Positions are presented and targeted activities are proposed to address the current issues related to the implementation of defense policies.*

Keywords: *defense, strategy, policies,the armed forces.*

ПРЕДИЗВИКАТЕЛСТВА ПРЕД ОТБРАНИТЕЛНАТА ПОЛИТИКА В СТРАТЕГИЯТА ЗА НАЦИОНАЛНА СИГУРНОСТ

Николай Й. Досев, Владислав С. Савов

Въведение

Стратегическата цел на отбранителната политика е защитата и утвърждаването на националните интереси чрез изграждане, поддържане и използване на адекватни на средата на сигурност отбранителни способности и изграждане на оперативно съвместими модерни въоръжени сили с единна система за командване и управление в мирно време и при кризи.

Реализиранто на тази цел не е възможно с използването само на военния инструмент, а ще изисква прилагането на всеобхватен подход с използването и на дипломатически, политически, информационни, икономически, финансови, разузнавателни и правни инструменти.

Изследването има за задача да покаже предизвикателствата, които стоят на дневен ред в отбранителната политика и тяхното преодоляване. Докладът не е задълбочен, но представя актуални теми и проблеми в областта на отбранителната политика в стратегията за национална сигурност, която по същество се организира в рамките на девет точки, указващи принципите и приоритетите съставляващи цели и задачи за изпълнение на същите. Основните направления по които е нужно своевременно и приоритетно развитие се фокусират върху:

- отбраната на страната, справянето с некомплекта в Българската армия (БА);
- изпълнение на споразумението между страните членки на НАТО от срещата на върха в Уелс 2014г.;
- модернизация на отбранителните способности в БА;
- подбора и кариерното развитие на военнослужещите;

- създаването на доброволната военна подготовка.

Първо предизвикателство - справянето с некомплекта в БА:

Некомплекта от личен състав в Българската армия към 2018 г. е в порядъка на около 25%. В немалко формирования обаче особено от състава на сухопътни войски той стига до 30%, като причините за това са комплексни. Тази ситуация предизвиква допълнителни компромиси при изпълнение на поетите съюзни ангажименти и увеличава дефицита от отбранителни способности на военните формирования. Въпреки увеличените средства за възнаграждения на военнослужещите, все още не може да се достигне приемлив обществен баланс за осигуряване необходимата социална устойчивост в армията. Това води до системен отлив на подготвени кадри и спад в мотивацията на военнослужещите.

Възможни политики за намаляване броя на напускащите военнослужещите, може да бъдат реализирани чрез:

- увеличения на възнагражденията - през 2018 г. и 2019 г. са налице увеличения на възнагражденията на военнослужещите, промени се и механизмът за формиране на основното месечно възнаграждение. Това разбира се е една чакана стъпка в правилна посока.
- Необходимото обновяване и извършване на капиталови ремонти на материалната база на ведомствените жилища за нуждите на военнослужещите, както и изграждане на нови такива.
- Актуализиране на компенсационните суми за свободен наем.
- Подобряване на материалната база във военно почивните домове.

Второ предизвикателство - постигането на 2% от БВП на разходите за отбрана съгласно споразумението между страните членки на НАТО от срещата на върха в Уелс (2014 г.).

Актуализираната Стратегия за национална сигурност залага поетапно увеличаване на бюджета за отбрана до 2% от брутния вътрешен продукт на страната. Отчетена е необходимостта от реализиране на инвестиционните проекти за придобиване на нови основни бойни платформи и модернизация на Въоръжените сили, както и от създаване на система за прозрачен, ясен подбор и кариерно развитие на военнослужещите и цивилните служители, която да включва и ефективен пакет от мерки за мотивация. В тази връзка през 2017 г. Министерския съвет прие „Национален план за повишаване на разходите за отбрана на 2% от брутния вътрешен продукт на Република България до 2024 г.", с който се посочват способите за реализиране на нарастването на разходите за отбрана до 2024 г.

Ако този план бъде реализиран успешно, то това би довело до:

- Спазване на поетите ангажименти към НАТО за постигане на 2% от БВП на разходите за отбрана.
- В резултат от увеличението на бюджета за отбрана и при наличие на правилното организиране и разходване на средствата по съответните направления, ще се създаде възможност за надграждане и реализиране на следващи приоритети в отбранителната политика.

Трето предизвикателство - модернизацията на отбранителните способности в БА.

Българските военнослужещи изпълняват задълженията си с физически и морално остаряло въоръжение и техника. Усеща се липса на достатъчна поддръжка и ремонт на въоръжението, техниката, оборудването и инфраструктурата. Всичко това силно затруднява изпълнението на задачите по опазване на националната сигурност и участието в мисии на НАТО. Дългосрочността на процеса на придобиване на способности и оперативните ангажименти на въоръжените сили налагат разширяване обхвата на плана до 2018 г. Десетгодишният хоризонт за планиране създава стабилност и управляемост на процеса на планиране на способностите и синхронизира националното отбранително планиране с това на съюзниците. Опитът от изпълнението на Плана за организационното изграждане и структурата на Българската армия 2010 г., на Плана за организационното изграждане на въоръжените сили на Република България 2004 г. и на Плана за организационно изграждане и модернизация на въоръжените сили 2015 г. показва безалтернативно, че подходът за планиране с фиксиран краен срок не е достатъчно ефективен. Той не е адекватен на динамичните изисквания на средата на сигурност. В хода на изпълнението и на трите плана се доказа, че

на всеки две до три години е необходим преглед на постигнатите резултати, адаптиране на планирането към промените и конкретизиране на дейностите, предстоящи за изпълнение в следващите две или три години. Динамиката на процесите в областта на сигурността и отбраната, високата степен на непредсказуемост на рисковете и заплахите в днешната и утрешната среда на сигурност налагат цикличността на прегледа като необходимо условие за повишаване ефективността на планиране, а оттам и на разходване на предоставения ресурс за отбрана. Съюзната практика показва, че на всеки две години е целесъобразно да се извършва преглед на резултатите от изпълнението на десетгодишния план, които да се използват за адаптиране на заложеното в него, а на всяка четвърта година да се удължава хоризонтът на планиране с четири години. По този начин се осигурява непрекъснатост, гъвкавост и реалистичност на планирането и управлението на процеса на изграждане на необходимите способности. Предимствата на този подход налагат въвеждането му и в българските въоръжени сили. Възможните ползи от така организираните мероприятия може да се характеризират с :

- Поставяне на дългосрочни цели и ясна визия за развитието на отбраната на Република България;
- Реално изпълнение на поставените цели за модернизация и придобиване на нови и модерни отбранителни способности от СВ, ВВС и ВМС;
- Разширяване дейността на военно-промишления комплекс, неговото производство и задоволяване на нуждите на въоръжените сили с необходимата техника и елементи за СВ, ВМС и ВВС. Това би спомогнало до създаване на нови работни места, както и икономически растеж на държавата.

Четвърто предизвикателство - проблемите свързани с подбора и кариерното развитие на военнослужещите.

Кариерното развитие на военнослужещите е трудоемък процес, а правилното му провеждане води както до създаване на необходимите способности на военните формирования за изпълнение на възложените им мисии и задачи, така и до ясна визия на военнослужещите за техния професионален живот. Мащабът на заплахите и реалните щети от неефективния модел за кариерно развитие, които се нанасят на организационната структура на въоръжените сили, безспорно извежда тези въпроси сред най-значимите приоритети за ефективно управление на човешките ресурси. В модела за кариерно и кадрово развитие на военнослужещите от въоръжените сили, кариерата се определя като баланс между интересите на военнослужещите и потребностите на въоръжените сили и се влияе от придобитите от тях образование, професионална квалификация, умения, опит, лидерски качества, участие в мисии в чужбина и заемане на международни длъжности. Процесът на управление на човешките ресурси изисква да се осигурява организационно-щатно изграждане на въоръжените сили, проектиране и планиране на длъжности, изграждане на структурите на системата за управление на човешките ресурси, изграждане и подготовка на резерва, привличане, набиране, подбор и селекция на персонала, обучение, оценяване/атестиране, кариерно развитие, заплащане, социално партньорство, социална адаптация на освобождаваните военнослужещи.

Основни принципи на процеса на планиране на кариерното развитие на военнослужещите са:

- **Единност** – изразява общото състояние на процеса на планиране като част от системата за управление на човешките ресурси. Планирането на кариерното развитие на военнослужещите или на група от тях е на основата на цялостното планиране състоянието на човешките ресурси в Министерството на отбраната като организация с определена цел;
- **Адекватност** – съобразяване на процеса по планиране на кариерното развитие на военнослужещите с условията, при които той се извършва, и факторите, които влияят: съществуваща нормативна уредба, органи за управление и ръководство, автоматизирана система за управление на човешките ресурси, национално и международно състояние на човешките ресурси на „пазара на труда";

- **Прозрачност** – планирането се осъществява със знанието на съответните военнослужещи и командири (началници, ръководители);
- **Целенасоченост** – изразява се в целенасочена дейност за максимално удовлетворяване стремежа на военнослужещите, максимално използване на създадени компетенции и достигане на определено състояние на организацията;
- **Ротация на военнослужещите** – преназначаване на военнослужещите на други длъжности, които могат да са по хоризонтала (в обхвата на едно военно звание) или по вертикала – „нагоре" (с повишаване във военно звание), или „надолу" (на длъжност, изискваща по-ниско военно звание);
- **Обвързаност** – планирането на кариерното развитие на определен военнослужещ или определена група военнослужещи е функция от планирането на кариерното развитие на друг военнослужещ или друга група военнослужещи;
- **Оптималност на престоя в длъжност и във военно звание** – изразява потребността на системата за управление на човешките ресурси да се създава възможност натрупаните практически опит и знания да водят до съответните промени по „кариерната стълбица", както и възможността да не се задържа развитието на военнослужещите с определени военни звания. В резултат са установени минимален и максимален престой в длъжност и минимален и максимален престой във военно звание;
- **Обективност** – намаляване или премахване на възможността за субективно, еднозначно влияние върху планирането на кариерното развитие на военнослужещите на някой от вътрешните фактори: командирите (началниците, ръководителите), военнослужещите, структурите по управление на човешките ресурси (личен състав), организацията. Този принцип изисква съпоставяне на нужните компетентности за длъжността, наличните компетенции на военнослужещите и възможността за реализиране.

Ако е така организиран и прилаган, процесът на кариерно развитие, би бил изключително ефективен по отношение на:

- Подборът на качествени военнослужещи назначени на длъжности отговарящи на техните компетенции;
- Стимул за работа, всеотдайност и признателност от страна на личния състав.

Пето предизвикателство - създаването на доброволната военна подготовка.

В политическата рамка с Решение на Народно събрание от 14 март 2018 г. за приемане на актуализирана Стратегия за национална сигурност на Република България, във връзка с чл. 86, ал. 1 от Конституцията на Република България, чл. 16, т. 5 от Закона за отбраната и въоръжените сили на Република България и във връзка с чл. 7, ал. 1, т. 2 от Закона за управление и функциониране на системата за защита на националната сигурност, е регламентирано: „Въоръжените сили и невоенният компонент на системата за отбрана на страната съсредоточават усилията си за:

- подготовка и използване на доброволен резерв на въоръжените сили за тяхното докомплектоване;
- създаване на система за доброволна военна подготовка на български граждани за защита на Отечеството".

Автоматично това би довело до:

- Разширяване на възможностите за комплектоване на въоръжените сили за мирно и военно време;
- Повишаване на способностите на въоръжените сили за изпълнение на националните и съюзните ангажименти. Засилване на военно-патриотичното възпитание на българските граждани.

В резултат на направения анализ, с въвеждането на обучение по военна подготовка на български граждани за защита на Отечеството на доброволен принцип, в съответствие с приетите приоритети и мерки, се очакват следните резултати и ползи:

- Създаване в Министерството на отбраната на единна политика по управление на планирането, подготовката и отчета на ресурсите от резерва и запаса, обучението на българските граждани за защита на Отечеството и доброволна военна служба;
- Повишаване на възможностите за комплектоване на военновременните формирования с обучени и мотивирани млади офицери, сержанти и войници от резерва и запаса;
- Разширяване на доброволното обучение на пълнолетните български граждани чрез придобиване на практически умения при действия за оцеляване при кризи от военен характер, терористични актове, природни бедствия и оказване на първа помощ;
- Увеличаване на ресурса от обучени български граждани по начална и специална военна подготовка;
- Назначаване на служители в структурите по сигурността и отбраната след преминаване на начална и специална военна подготовка;
- Формиране на доброволчески батальони в състава на Единния център за начална военна подготовка – Плевен и Центъра за подготовка на специалисти – Сливен.

Заключение

Разгледаните проблеми показват нуждата от своевременни, адекватни и стратегически действия за решаване на предизвикателствата в отбранителната политика. Процесите в армията са взаимосвързани и е необходимо да вървят ръка за ръка. Дори и да бъде осигурен финансов ресурс за закупуване и на най-модерната техника, то липсата на личен състав, който да борави с нея, това води до неефективност. Ако пък сме се осигурили финансово за много кратко време с най-модерното въоръжение и попълним в кратки срокове личен състав, то той не би могъл да борави с въпросното въоръжение, поради недостатъчната подготовка на военнослужещите. Ето защо в бъдеще, функционирането на Българската армия е немислимо без добре мотивиран и подготвен личен състав. Стремежът към добре окомплектовани и модерни въоръжени сили, които да бъдат гарант за националната ни сигурност, изисква непрестанно прогнозиране и планиране на нашето развитие. За жалост, от поставените цели за развитие на въоръжените сили на Република България са реализирани само тези свързани със съкращаване на числеността на армията с цел тя да бъде по-модерна, боеспособна и компактна. Състоянието на основното въоръжение и техниката остава критично, независимо от повишените инвестиции за поддръжка и ремонт на основни бойни средства. Същите се експлоатират с редица ограничения, водещи до понижаване на бойната им ефективност, като по този начин крият риск за здравето и живота на личния състав. Някои системи са толкова остарели, че дори и осигуряването на достатъчно финансови ресурси няма да може да реши проблемите с тяхната поддръжка и експлоатация. Недостигът на финансови средства, липсата на ремонтни органи и квалифициран персонал, обслужващ техническите съоръжения, остарелият и амортизиран граден фонд, са основните проблеми при мотивацията в личният състав, поддържането на военната техника и инфраструктура. Затова усилията за справяне с предизвикателствата и проблемите във въоръжените сили, е нужно да бъдат насочени приоритетно към тях.

References

1. Актуализирана стратегия за национална сигурност на. Република България. Приета с Решение на НС от 14.03.2018 г., обн., ДВ, бр. 26 от 23.03.2018 г.

2. Лекция на началника на отбраната генерал Андрей Боцев, https://www.mod.bg/bg/doc/NO/speeches/20180903_Lekci%D0%B0_VA.pdf

3. Актуализиран план за организационно изграждане и модернизация на въоръжените сили, https://strategy.bg › FileHandler

4. Кариерно развитие на военнослужещите подп. д-р Галин Иванов, http://rnda.armf.bg/wp/wp-content/uploads/vjournal/2015_4/Galin_Ivanov.pdf

5. Визия за доброволна военна служба полк. Милен Илиев, http://rnda.armf.bg/wp/wp-content/uploads/2019/03/%D0%A1%D0%9E%D0%A1%D0%97%D0%A0.pdf

Zhaneta St. Georgieva-Panayotova,

SECURITY SYSTEMS IN THE COMMERCIAL BANKS

Zhaneta St. Georgieva-Panayotova

Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, Department “Management of Security Systems”, janeta.st.georgieva@gmail.com

***Abstract**: The need to manage and evaluate risk is largely dictated by the need to give assurance to the bank's shareholders that its activities are within reasonable risk levels and their interests as owners are protected. Regardless of the nature of the investment, the profit and the effect of the investment, timely and objective reporting information, as well as the lawfulness and compliance with the legal provisions are of major advantage for the investor.*

***Keywords**: Security systems, Risk management*

СИСТЕМАТА ЗА СИГУРНОСТ В ТЪРГОВСКИТЕ БАНКИ

Жанета Ст. Георгиева-Панайотова

Въведение

С развитието и налагането на дадена финансова институция на банковия пазар, риск апетита й неимоверно бързо нараства. Ефективното управление на риска гарантира запазване на доходността на банката и същевременно води до повишаване на качеството на предлаганите от нея услуги и продукти. Изграждането на система за сигурност е провокирано от необходимостта от защита на организацията в частност, както и на интересите на нейните клиенти и служители.

Структурирането на звената за сигурност в банките изисква на първо място да дефинираме понятията сигурност и риск.

Изложение

Сигурност в енциклопедичният речник е "спокойно душевно състояние на онзи, който смята, че няма нищо, от което да се страхува". Сигурността може да бъде разгледана като състояние на отсъствие на страх или липса на риск от настъпване на нежелано събитие.

Думата "риск" произхожда от латинското "risicare" и означава решавам. Терминът "риск" започва да се употребява през средновековието. Преди това хората свързвали опасностите и бъдещи събития със суеверните вярвания и въздействието на "висши сили". Употребата на думата риск започва да се употребява по-масово едва когато за хората осъзнават отговорността си от вземането на дадено решение. В тълковния речник рискът е определен като "възможна опасност", негови синоними са угроза, заплаха, опасност, несигурност, фаталност, шанс, късмет, отговорност, вероятност, случайност, съдба.

Рискът се явява следствие от решенията на субекта, който прави своя избор и преценява вероятността от настъпване на дадени събития, както и размера на последствията от тяхното настъпване. Рискът е потенциална, числено измерима вероятност от настъпване на загуба, щета, нереализиране на печалба и т.н. Неопределеността е специфична характеристика на понятието

"риск". При състояние на "риск" съществува възможност за възникване на нежелани ситуации или последици от реализацията на предприети решения.

Необходимостта от управление и оценка на риска е продиктувана до голяма степен от потребността да бъде дадена увереност на акционерите на банката, че осъществяването на дейността й е в разумни нива на риск и техните интереси като собственици са защитени. Независимо от характера на инвестицията, основен превес за инвеститора имат печалбата и ефекта от вложението, навременната и обективна отчетна информация, също така правомерността и съблюдаването на законовите разпоредби.

Дейността на системата за сигурност на банките, гарантира набавянето и анализа на необходимата икономическа информация, установяване на несъответствията, предприемането на незабавни коригиращи действия, и стартиране на дейности за превантивен контрол с цел недопускането на повторно настъпване на рисково събитие.

Звената за вътрешна сигурност и контрол, базират дейността си прилагайки основно два подхода на действие - традиционен или риск-ориентиран.

И при двата подхода се изисква детайлно познаване и прилагане на нормативните изисквания за осъществяване дейността на търговската банка, познаване и оценка на риска и прилагане на адекватни мерки за снижаване на последствията от настъпване на рисково събитие

При традиционния подход се следи да не бъдат нарушени основни изисквания в приложимото законодателство, стремеж към ефективност на структурите за вътрешна сигурност и даване на увереност на ръководството, че дейността на банката се осъществява в разумни от гледна точка на риска граници.

Извършват се проверки на извадков принцип на отделни операции от различен тип и съществени в различни клонове на банката /териториално разграничени/.

Целта е да се гарантира спазването на законовите изисквания на дадена операция и прилагането на вътрешни методики и процедури, одобрени от конкретната банка.

При този подход обикновено банката приема предварително регламент за дейността на системата за вътрешна сигурност, одобрява процедури за работа и формуляри на документите, отразяващи дейността на звеното. Регламентирани са правомощията на служителите по сигурността.

Във връзка с осъществяването на дейността си звената по сигурността имат ясна визия за техническата си обезпеченост с компютърна и друга специализирана техника, както и план за нейната автоматизация и надграждане във връзка с развитието на технологиите, и потребностите от прилагане на иновации в областта на сигурността.

В резюме традиционния подход гарантира прилагането на законовите разпоредби, спазване изискванията на вътрешните норми и методики на банката и подпомага управлението на риска от страна на висшия мениджмънт, предоставяйки му точна и проверена отчетна информация за оперативната дейност. Преодоляването на кризи се осъществява прилагайки предварително одобрени модели и процедури за противодействие на риска.

Риск-ориентираният модел включва проучване и анализ на всяка рискова ситуация и събитие в конкретната банка. Дава се определение на рисковите събития и се набелязват обектите , които следва за бъдат одитирани в процеса на осъществяване на ежедневната дейност на банката, както и се дефинират факторите, обуславящи вероятността от настъпване на рисково събитие. Всеки потенциален обект на проверка, следва да има извършен анализ и присъден рейтинг/ниво/ на риск. Структурата по сигурността, приема методика за оценка на рисковете, определя нивата на риск и изготвя програма за дейността /предимно се планира на годишна база/. Утвърдените от ръководството методика и годишен план, се обсъждат и свеждат до знанието на всеки един служител.

Обект на одит са както материални/ сгради, техника, специализирано оборудване и др./, така и нематериални активи като право на ползване на земи и сгради, лицензи, стандарти по качество и т.н. Акцент при одита имат основните предлагани от банките.услуги и продукти, обуславящи основния паричен поток, както и всички съпътстващи дейности като контактите с клиентите във връзка с промотиране на нови продукти, привличане на нови клиенти и капитали, както и предоставяните чрез използването на технологии продукти и услуги.

В управлението на финансовите институции е изградена ясно изразена структура на функциониране /организационна система/, в която дейността, взаимовръзките между отделните структурни единици и различните нива, са регламентирани, както и информационния поток и нивата на достъп до информация. Стъпвайки на тази организационна база, звеното за сигурност има за цел да внедри работеща система, съобразена с особеностите на конкретната банка и прилагайки гъвкав подход, да осъществява контрол на риска, основан на анализ на всяко настъпило рисково събитие.

При риск-ориентираният подход познатите дефиниции за риск и методите за преодоляването му, следва да бъдат прилагани при възможност, но за всяко събитие извън гореспоменатите се прави индивидуален анализ и се търси адекватно снижаващо риска действие. Това е обусловено от факта, че финансовата среда в глобален мащаб е една от най-динамично развиващата се и в технологичен и социален аспект. Всяка иновация води след себе се както ползи от прилагането й, така и създава предпоставки за риск, които следва да бъдат предвидени и на които трябва да се противодейства.

Добре работещата системата за сигурност гарантира създаването на бази данни с достоверна информация за характера и степента на рисковите събития, прилагането на ясни и точни процедури, регламентиращи работния процес по видове операции и направления, данни от системите за мониторинг, както и постоянен контрол върху документооборота в банковите институции.

Изводи

Динамиката на риск-ориентираният подход ни дава увереност за по-добрата адаптивност на метода и гарантира неговата всеобхватност. Възможността да се вземат адекватни и навременни мерки за справяне с проблеми и да се променят условията за работа и оценка на риска, спомага за постигане на синхрон както с целите на организацията /в частност банката/, така и с запазване и защитаване на интересите на акционерите, клиентите и служителите.

Прилагането на високотехнологични иновативни системи за наблюдение, ранно известяване и превенция на злоупотреби е до голяма степен ключово за недопускането на критични събития и минимизиране на финансови загуби. Ефективността на търговските банки, се свързва до голяма степен с присъден висок финансов рейтинг, постигната нетна печалба, добрата репутация, но също така и с не по-маловажно значение е нейната устойчивост на външни и вътрешни операционни рискове и способността на организацията да се справя с тях, претърпявайки минимални загуби.

References

1. Управление деятельностью коммерческого банка, под ред. О.И.Лаврушина.М : Юристь, 2005
2. Ong M.K.Internal credit risk Models. Capital Allocation and Performance Management. London : Risk Books, 1999
3. The Joint Forum "Operational risk transfer across financial sectors" August 2003.

Svetlin E. Stefanov,

JUDICIAL REVIEW OF THE SECURITY SECTOR - A GUARANTEE FOR HUMAN RIGHTS PROTECTION

Svetlin E. Stefanov

*Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences,
Department "Management of Security Systems", svetlin.stefanov65@abv.bg*

***Abstract**: Accountability for the work of the Security Sector is exercised through the control of various actors, including the judiciary, expert bodies, parliamentary committees and data protection authorities. This control is crucial: it helps to ensure that services are accountable for their actions, and encourages the development of effective internal safeguards within the services. Control is not a lack of confidence, but a desire to make things clear.*

***Keywords**: Judicial review, Security Sector, Human Rights Protection*

СЪДЕБНИЯТ КОНТРОЛ ВЪРХУ СЕКТОРА ЗА СИГУРНОСТ – ГАРАНЦИЯ ЗА ЗАЩИТА ПРАВАТА НА ГРАЖДАНИТЕ

Светлин Е. Стефанов

Въведение

Отчетност върху работата на сектор „Сигурност" се осъществява чрез контрол от различни субекти, включително съдебната власт, експертни органи, парламентарни комисии и органи за защита на данните. Този контрол е от решаващо значение: той спомага да се гарантира, че службите носят отговорност за своите действия, и насърчава развитието на ефективни вътрешни предпазни механизми в рамките на службите. Контролът не е липса на доверие, а желание нещата да са ясни.

Контролът е част от управленческия процес и има за цел да провери дали определена система е в нужните параметри, за да изпълнява предназначението и функциите си. В зависимост от гледната точка и функциите си, контролът бива външен и вътрешен; предварителен, ат-хок и последващ; финансов, одитен, функционален или с цел сертифицирането на дадено звено за определен вид дейности и т.н.

Изложение

Според чл. 21 от Закона за управление и функциониране на системата за защита на националната сигурност, върху дейността на органите и структурите от системата за защита на националната сигурност се осъществява парламентарен, административен, съдебен и граждански контрол [1].

Контролът в службите за сигурност се осъществява на няколко нива както следва:
- ръководител на служба за сигурност;
- изпълнителна власт;
- съдебна власт и прокуратура;
- парламентарен контрол;
- контрол от гражданския сектор, осъществяван от граждани и неправителствени организации /НПО/.

Специализираните парламентарни комисии обикновено акцентират върху оценяването на правителствените политики в сектора. Органите за защита на данните разполагат с правомощия над сектор сигурност – главно поради залегналото в законодателството провомощие за контрол при използване на личните данни.

Съдебната власт и експертните органи участват най-често в контрола върху мерките за наблюдение. Съдебният контрол обхваща използването на специални разузнавателни средства от институциите в сектора за сигурност, прилагането на решенията на Европейския съд за правата на човека, тълкувателни решения на върховните съдилища, решения на Конституционния съд и решения на други съдилища, компетентни да разглеждат съответните дела.

Законодателна дейност в Република България се осъществява прозрачно и с обществено обсъждане, законът винаги се публикува и става известен на всички, преди да започне прилагането му. Самото създаване и развиване на правна рамка за дейността на службите за сигурност неизбежно ги поставя в положение на по-голяма прозрачност. Това означава и контрол – от политическото представителство в държавните институции, от една страна и пряко от гражданите – от друга [2].

Правилата за опазване на държавната тайна днес са прозрачни и общодостъпни чрез обнародвания Закон за защита на класифицираната информация (обн. ДВ, бр. 45 от 30.04.2002 г.). Процедурата по опазване на държавната тайна на Република България бе ревностно опазвана от обществения поглед дори през 2002 г., когато „Програма достъп до информация" (ПДИ) я поиска по реда на Закона за достъп до обществена информация. Министерският съвет разсекрети документа, в който се съдържаха тези правила, едва през 2004 г. под натиска на заведеното във Върховния административен съд дело срещу отказа (а.д. № 11243/2003 г. по описа на ВАС петчленен състав).

През 2009 г. Европейският съд по правата на човека, промени предишната си практика, според която чл. 10 от Европейската конвенция за правата на човека (ЕКПЧ) не задължава държавите да предоставят информация на желаещите да я получат. В същата година бе отворена за подписване и ратификация от държавите, членки на Съвета на Европа, първата в света Конвенция за достъпа до официални документи. През 2013 г. Комитетът на министрите на държавите, членки на Съвета на Европа, прие Препоръка относно националната сигурност и достъпа до информация, последвана от резолюция на Парламентарната асамблея, към държавите членки да подобрят баланса между правото на обществото да знае и защитата на легитимните интереси на националната сигурност. През 2015 г. бе приета резолюция на ПАСЕ и съответно препоръка относно подобряване на защитата на информаторите (whistleblowers), която се позовава на посочения документ и реферира изрично към случая „Сноудън". Достъпът на гражданите до информация и защитата на личните им данни са неразривно свързани. Често се сочи, че тези права представляват двете страни на една и съща монета. В демократичните общества по правило гражданите имат широк достъп до информацията, която се съхранява от институциите, а последните имат ограничен достъп до данните на гражданите.

Правната уредба при използване на специални разузнавателни средства от институциите в сектора за сигурност след 1990 г. :

С разпоредбата на чл. 34 от Конституцията от 1991 г. бе гарантирано правото на неприкосновеност на кореспонденцията и другите съобщения. Според алинея втора от тази разпоредба намесата в това право може да е осъществявана единствено с разрешение на орган на съдебната власт, когато е наложително за предотвратяване или разкриване на тежки престъпления. През 1994 г. е приет първият Закон за специалните разузнавателни средства (ЗСРС). През 1997 г. е от-

менен с новоприетия и сега действащ ЗСРС. Основен принцип на закона е използването на СРС след издаване на съдебно разрешение. Изключение от този принцип е допустимо само при непосредствена опасност за извършване на тежко умишлено престъпление или за националната сигурност. Непосредствено след приемането на ЗСРС (1997 г.) е поставен въпросът за конституционосъобразността на отделни разпоредби. Главния прокурор поставя четири въпроса, по които се произнася Конституционният съд. Това са съответства ли на Конституцията: 1. съществуването на хипотеза в ЗСРС, при която съдът се произнася впоследствие, а не преди използването на специалното разузнавателно средство (СРС)? 2. правомощието на министъра на вътрешните работи да прекрати прилагането на СРС преди срока? 3. правомощието на министъра на вътрешните работи да вземе решение за използване на СРС при получаване на резултати извън направеното искане? 4. задължението на министъра на вътрешните работи да осъществява контрол по използването на СРС? С решение от 1998 г. Конституционният съд отхвърля искането [3].

През 2001 г. е изготвен доклад от ВКП относно използването на СРС през периода 1999-2000 г. Според доклада през периода януари 1999 – януари 2001 г. съдилищата са разрешили използването на СРС в 10 000 случая, като за изготвяне на доказателства в наказателни производства са послужили едва 2 – 3 % от тях. Данните са цитирани в решение на Европейския съд по правата на човека от 28 юни 2007 г. [4]. Достъп до доклада бе отказан по реда на ЗДОИ на Българския хелзинкски комитет (БХК), като за основание за отказ прокуратурата посочи обстоятелството, че е маркиран с гриф за сигурност „за служебно ползване" и представлява служебна тайна. Състави на Софийския градски съд и на Върховния административен съд отхвърлиха жалбата на БХК, подадена със съдействието на „Програма достъп до информация" (ПДИ), като се позоваха на чл. 33 от ЗСРС, според който информацията за факти и сведения за прилагането на СРС по реда на закона, както и събраните данни не подлежат на разгласяване. Отхвърлен е доводът, че междувременно е изтекъл предвиденият в ЗЗКИ срок с мотива, че декласифицирането се извършва само от компетентния служител [5].

През 2000 г. въпросът за съобразността на ЗСРС с Конвенцията за защита правата на човека и основните свободи бе поставен в Страсбург [6]. С решение на ЕСПЧ от 28 юни 2007 г. (окончателно от 30 януари 2008 г.) по делото на „Асоциация за европейска интеграция и права на човека и Екимджиев срещу България" [7] редица положения от ЗСРС бяха обявени за водещи до системно нарушение на чл. 8 от Европейската конвенция за правата на човека, според който всеки има право на зачитане на личния му живот и кореспонденция. В решението на ЕСПЧ се отбелязват редица дефекти в системата за тайно следене, установена със ЗСРС, които водят до системно нарушение на правата на гражданите по чл. 8 от ЕКПЧ. Отбелязва се липсата на независима институция, осъществяваща контрол върху дейността по прилагането на СРС, извън министъра на вътрешните работи. Посочена е липсата на орган, който да проверява спазват ли се условията в разрешенията за използване на СРС, добросъвестно ли се възпроизвеждат оригиналните данни в писмените записи и унищожават ли се в срок тези данни. Липсват правилници, определящи със съответната степен на точност начина на проверка на данните, получени чрез използване на специални разузнавателни средства, или процедурите за запазване на тяхната цялост и поверителност и процедурите за тяхното унищожаване. Не е описан начинът, по който министърът на вътрешните работи осъществява контрол. Съдията, издал разрешението, не се уведомява впоследствие за резултатите от използването на СРС и не осъществява последващ контрол върху законосъобразността му. Нито министърът, нито някое друго длъжностно лице е задължено да докладва редовно на независим орган или на обществото за цялостното функциониране на системата или за мерките, прилагани в отделни случаи. Ако събраните данни попадат извън обсега на искането за използване на специални разузнавателни средства, министърът на вътрешните работи е този, който решава, по свое усмотрение и без никакъв независим контрол, какво трябва да бъде направено с тях. Не на последно място, в коментираното решение ЕСПЧ отбелязва, че съгласно българския закон лицата, по отношение на които са използвани специални разузнавателни средства, не са уведомявани за този факт по никое време и при никакви обстоятелства. По този въпрос

жалби подават в Страсбург и други български граждани. България е осъдена за същото нарушение на чл. 8 на ЕКПЧ и по делата „Хаджиев с/у България" и „Нацев с/у България" [8].

Законодателни изменения в ЗСРС през 2008 – 2009 г. В резултат на решението на ЕСПЧ бе предприето изменение в закона. С изменението и допълнението на ЗСРС през 2008 г. се създаде Национално бюро за контрол над специалните разузнавателни средства. Бюрото просъществува едва няколко месеца, като при смяната на политическата власт през 2009 г. с ново изменение и допълнение на ЗСРС контролът бе предоставен на създадена парламентарна подкомисия към Комисията по правни въпроси. Националното бюро за контрол на СРС бе отново създадено през 2013 г., като смяната на властта след изборите през октомври 2014 г. не доведе до рокада на състава. С изменението през 2009 г. се въведе задължение за последващо информиране на съдията, дал разрешението за прилагане на СРС. Той обаче не се произнася по законността на това прилагане. Създаде се парламентарна подкомисия към Комисията по правни въпроси, която да осъществява контрол, основно като събира информация и подготвя годишен доклад по въпросите на прилагането на СРС. Подкомисията не бе натоварена с функции да налага санкции, но получи правомощието да информира гражданите за незаконно прилагане на СРС спрямо тях. С изменение в Закона за отговорността на държавата и общините за вреди се предвиди възможност да се търси обезщетение за незаконно приложени СРС. Промените бяха в правилната посока, но развитието през следващите години показа, че не са достатъчни.

Изменения на ЗСРС през 2013 – 2019 г. В резултат на активния дебат през годините ЗСРС бе изменен и допълнен през 2013, 2015, 2016, 2017, 2018 и 2019 г. С измененията от 2013 г. на ЗСРЗ Националното бюро за контрол над СРС е определено като постоянно действащ орган за външен контрол по приложението на ЗСРС. Създадено бе изискване в исканията за разрешаване на СРС да се включва пълно и изчерпателно посочване на фактите и обстоятелствата, даващи основание да се предполага, че се подготвя, извършва или е извършено тежко умишлено престъпление. Бяха изчерпателно изброени престъпните състави, съставляващи тежки престъпления, за разследването на които може да се използват СРС, с което се стесни законово допустимото приложение на намесата в личното пространство по реда на ЗСРС. Освен определянето на срок за използването на СРС, се предвиди задължение за мотивиране на продължителността му. Мотивите трябва да съдържат и обосновка за невъзможността необходимите данни да бъдат събрани по друг начин или описание на изключителните трудности, с които е свързано събирането им. През 2013 г. се обособи като самостоятелна дейността по техническото прилагане на СРС и особено на подслушванията, които са най-големият дял от тях. За целта бе създадена отделна институция на изпълнителната власт, пряко подчинена на Министерския съвет – Държавна агенция „Технически операции" (ДАТО). При изключението, според което СРС може да се използват преди разрешението от съда, решението се взема от председателя на ДАТО, ДАНС или секретаря на МВР. Целта очевидно е да се неутрализира силната политическа фигура на министъра на вътрешните работи.

Статистика относно използването на СРС. През годините неколкократно се стигна до скандали, твърдения или данни за подслушване със съмнителна законност. Още през 2001 г. се коментираше монтирането на подслушвателно устройство в дома на тогавашния главен прокурор и разработката „Гном". Един от най-нашумелите скандали с подслушване през 2008 г. бе свързан с разработка под названието „Галерия" на ДАНС, по която обект на подслушване са били журналисти и политици. Скандали около подслушванията имаше по време на първото правителство на ГЕРБ (2009 – 2013 г.), като за основно отговорна политическа фигура се сочеше тогавашният министър на вътрешните работи Цветан Цветанов, впоследствие подсъдим за отказ да бъдат използвани разрешени от съда СРС. Всяка следваща година се увеличаваше бройката на разрешенията за използване на СРС. В доклада на прокуратурата от 2001 г. са отчетени 10 000 разрешения за периода 1999 – 2000 г., т.е. средно по 5000 годишно. В решението си от 2008 г. ЕСПЧ сравнява тази бройка с данните за Великобритания, показващи цифрата 400 за телефонни подслушвания и 100 за отваряне на кореспонденция. Десет години по-късно, т.е. за 2009 г., новосъздадената парламентарна подкомисия докладва 9600 разрешения у нас. Това показва, че разрешенията са се удвоили за период от десет години. През 2010 г. се оказва, че броят на разрешенията за прилагане

на СРС стига до рекордното число от 15 864. За следващата 2011 г. те са около 14 000, като в доклада на подкомисията изрично се подчертава, че намалението е изкуствено – вследствие на включването на повече способи в едно искане по инициатива на председателя на Софийския градски съд Владимира Янева. За сметка на това броят на лицата, спрямо които са приложени СРС през 2011 г., е с 30 % по-голям от този през 2010 г. Съществено за всички тези данни за периода 1999 – 2011 г. е, че броят на използваните в съда доказателства, събрани чрез СРС, е изключително малък като процент от общия брой на разрешените – 2 – 3 % през 1999 – 2000 г. и 5 – 6 % през 2011 г. В Доклада на Националното бюро за контрол над СРС от 2015 г. не се сочи броя на разрешенията, а брой на „лицата, поставени под секретен контрол". За 2014 г. броят им е 4202, за 2013 г. – 4452, за 2012 г. – 5902, за 2011 г. – 8184, а за 2010 г. – 5763. Изводът на бюрото е, че след 2011 г. има тенденция към намаляване на броя на лицата, спрямо които са използвани СРС. Доминиращата форма на прилагане на СРС през всичките години са подслушванията. За 2014 г. са издадени 6475 разрешения за подслушване. От тях реално приложени са 4927, т.е. доста по-малък брой. Изводът е, че се ползва възможно най-дълбоко навлизащото в личното пространство средство, а резултатите от него не са значителни (следва да се има предвид, че липсва статистика колко от делата са приключили с осъдителна присъда).

В доклада на Националното бюро за контрол на специалните разузнавателни средства за извършената дейност през 2017 г. [9] и 2018 г.,[10] се посочва, че през 2017 г. са осъществени процедури със СРС по отношение на 2748 лица, през 2016 г. на 2749 лица. Наблюдава си трайна тенденция към намаляване на броя на лицата, контролирани със СРС, спрямо предходни години. Поисканите за прилагане оперативни способи са общо 17714 бр. като през 2016 г. те са били 14382 бр. В Доклада са отразени броя на поисканите видове оперативни способи. В 261 случая СРС са използвани по отношение на обекти за установяване самоличността на лица, за които е имало данни за участието им в престъпна дейност, съгласно чл. 12, ал. 1, т. 4 от ЗСРС. За 640 лица прилагането на СРС е започнало по реда и условията на чл. 17 от ЗСРС и за 28 лица по чл. 18 от ЗСРС. През 2016 г. лицата са били съответно 685 и 49. През 2017 г. исканията за използване на СРС са 5939, по които са постановени 1315 откази и 4624 разрешения. Националното бюро е констатирало, че през 2017 г. съдебният контрол върху използването и прилагането на СРС е значително завишен, за което свидетелства по-големият брой и добре мотивирани откази. По отношение на информацията, не послужила за изготвяне на веществени доказателствени средства е направен извод, че същата се унищожава в законоустановения срок, в резултат на своевременно упражняван контрол от ръководителите на органите по чл. 13 и 20 от ЗСРС. В резултат на прилагане на СРС са изготвени 1670 бр. веществени доказателствени средства, при 1431 бр. през2016г.

През 2018 г. са използвани СРС по отношение на 3046 лица. Поисканите за прилагане оперативни способи са общо 16002 бр. В Доклада са отразени броя на поисканите видове оперативни способи. В 279 случая СРС са използвани по отношение на обекти за установяване самоличността на лица, за които е имало данни и основание да се предполага, че подготвят, извършват или са извършили тежко умишлено престъпление по чл. 12, ал. 1, т. 4 от ЗСРС, чиито анализ на данни показва относителна стабилност на тези специфични процедури. За 607 лица прилагането на СРС е започнало по реда и условията на чл. 17 от ЗСРС и за 7 лица по чл. 18 от ЗСРС. През 2018 г. исканията за използване на СРС са 6099, по които са постановени 771 откази и 5328 разрешения. Запазва се тенденцията СРС да се използват най-често за разкриване на престъпления по чл. 321 от НК /организирана престъпна група/, чл. 354а от НК /наркотични вещества/, чл. 234 от НК /акцизни стоки/, чл. 209 от НК /измама/, чл. 195 от НК /кражби/ и чл. 301 от НК /подкуп/. Запазва се относителният дял на заявителите към общия брой инициирани процедури - МВР, Прокуратура, ДАНС и СВП-МО. Информацията, не послужила за изготвяне на веществени доказателствени средства се унищожава в законоустановения срок, а изготвените веществени доказателствени средства са 1714 бр., което увеличение свидетелства за ефективността на прилаганите СРС.

Достъп до данни за трафика съгласно Закона за електронните съобщения. Запазване на данните за трафика на електронни съобщения и осигуряване на пряк достъп до тези данни съгласно Наредба № 40 от 2008 г.

С развиването на технологиите нарасна възможността за използването на данни за електронните съобщения, обменяни чрез мобилните оператори и доставчиците на интернет услуги, за целите на борбата с престъпността. Преди създаването на нарочна нормативна уредба осигуряването на възможност за такъв достъп до базите данни бе включено в изискванията към лицензиите на мобилните оператори. През 2006 г. се прие директива на Европейския парламент и на Съвета за запазването на данни за трафика на електронни съобщения, с която бяха задължени държавите, членки на Европейския съюз (ЕС), да приемат законодателство, чрез което да осигурят запазването на данни за трафика на електронни съобщения за период между 6 и 24 месеца. Целта на хармонизирането на законодателството на държавите, членки на ЕС, бе да се гарантира, че данните са достъпни за разследването, разкриването и преследването на сериозни престъпления, както те са определени в националното право на всяка държава членка.

През януари 2008 г. директивата бе въведена в българското законодателство чрез наредба, издадена съвместно от министъра на вътрешните работи и председателя на Държавната агенция за информационни технологии и съобщения [11]. За разлика от директивата в наредбата е определен много по-широк обхват на престъпленията, за разкриването на които се създава задължението за запазване на данните, свързани с трафика на електронни съобщения, и ред за достъпа до тях. В наредбата се посочва, че запазването и достъпът до данните са просто с цел „разкриване на престъпления", без да се ограничат до категорията „сериозни престъпления", както това е сторено в директивата. Другата цел на запазването и достъпа до данни е формулирана пределно общо – „за нуждите на националната сигурност", като такава цел не е заявена въобще в директивата. С чл. 5 от Наредба № 40/2008 г. бе предвидена възможност органите на досъдебното производство или съда и службите за сигурност да получават достъп при обикновено писмено поискване, без предварително разрешение от съдебен орган. От друга страна, дирекция в МВР придоби възможността да получи неограничен пряк технически достъп до данните за трафика на електронни съобщения чрез компютърен терминал.

Тълкуването на съобразността на Наредба № 40/2008 г. с Конституцията и ЕКПЧ Наредба №40/2008г., приетото от Върховния административен бе оспорена от „Програма достъп до информация" (ПДИ) пред Върховния административен съд с аргументи за противоречие с Конституцията и Европейската конвенция за правата на човека. Тричленният състав на ВАС обяви жалбата за допустима, но я отхвърли по същество като неоснователна. С решение от 11 декември 2008 г., постановено по касационна жалба на ПДИ, петчленен състав на ВАС отмени изцяло чл. 5 от наредбата, отнасящ се до регламентирането на достъпа на държавни органи до запазваните данни за трафика на електронни съобщения [12]. Съдът приема по отношение на разпоредбата, предвиждаща достъп на дирекция в МВР чрез компютърен терминал, че всъщност нормата „не поставя никакви ограничения по отношение данните, до които се разрешава достъпът чрез компютърен терминал, а изразът „за нуждите на оперативно-издирвателната дейност" е много общ и не дава гаранции за спазване на чл. 32, ал. 1 от Конституцията на Република България, че личният живот на гражданите е неприкосновен. Не е установен способ за съблюдаване конституционния принцип по отношение правото на защита срещу незаконна намеса в личния и семейния живот на отделната личност, както и срещу посегателство върху неговата чест, достойнство и добро име". Що се отнася до регламентирана възможност разследващите органи, прокуратурата и съдът да получават достъп до данни за трафика „за нуждите на наказателния процес", а службите за сигурност – „в случай на необходимост, свързана с националната сигурност", след представяне на писмено искане, петчленният състав на ВАС намира, че формулираният текст не поставя условия, препятстващи злоупотреба с възможността да се нарушават конституционно гарантирани права на гражданите, като не е предвидено препращане към специалните закони Наказателнопроцесуален кодекс, Закон за специалните разузнавателни средства, Закон за защита на личните данни, в които са конкретизирани предпоставките за допускане достъп до определени данни, свързани с личния живот и личните данни на отделната личност. Като извод съдът намира, че трите алинеи на чл. 5 от Наредба № 40/2008 г. нарушават чл. 32 и чл. 34 от Конституцията и чл. 8 от ЕКПЧ.

Законова регламентация на запазването и достъпа до данни за трафика на електронни съобщения. След отмяната на чл. 5 от Наредба № 40/2008 г. през януари 2009 г. започна обсъждане в парламента на внесени текстове за изменение и допълнение на Закона за електронните съобщения (ЗЕС). Бе въведен задължителен съдебен контрол, като за всеки индивидуален достъп до данни за трафика следва да се поиска отделно разрешение от окръжния съд. Кръгът на престъпленията, за чието разкриване и разследване се допускаше достъп до трафични данни, бе стеснен до категориите „тежки" и „компютърни" престъпления. Срокът за запазване на данните бе определен на 12 месеца. След парламентарните избори през 2009 г. администрацията на новия министър на вътрешните работи изготви нов проект за изменение и допълнение на ЗЕС, насочен към улесняване на достъпа на органите на Министерството до данни за трафика на електронни съобщения. След обсъждания през 2010 г. бе приет нов вариант на текстовете на ЗЕС, отнасящи се до запазването и достъпа до данни за трафика на електронни съобщения. Той отново не предвиждаше пряк технически достъп до запазените данни. Предвиди се по-широк кръг от органи, имащи възможност да поискат достъп до трафични данни. Бе регламентирано данните за целите на оперативната дейност да се предоставят след разрешение от районния съд, а за целите на разследването на престъпления – по реда на Наказателнопроцесуалния кодекс. Кръгът на престъпленията, за чието разкриване и разследване се допуска достъп до трафични данни, бе отново разширен, като освен категорията „тежки престъпления" бе включена и категорията компютърни престъпления.

Статистика относно достъпа до данни за трафика на електронни съобщения. Според информация от парламента през 2008 г. органите на МВР са получили около 300 000 разпечатки с данни за трафика на електронните съобщения на около 40 000 абоната [13]. С измененията и допълненията в ЗЕС от 2010 г. обаче се позволи по-широк достъп при по-нисък стандарт на защита и гарантиране на правата на хората. Според официалния доклад на компетентната парламентарна подкомисия за периода от 1 януари до 9 май 2010 г., когато действа режимът на достъп, приет с измененията и допълненията на ЗЕС от 2009 г., броят на разрешенията за достъп е 2760, докато за периода от 10 май 2010 г., когато влизат в сила новите изменения и допълнения в ЗЕС, до 31 декември 2010 г. броят им вече е 18 845. Част от измененията в закона създават възможност за заобикаляне на режима за достъп до трафични данни само след съдебно разрешение. Още през 2010 г. прокуратурата приема тълкуване, според което не е необходимо съдебно разрешение, когато достъпът до данни за трафика на електронни съобщения е необходим за целите на разследването на тежки и компютърни престъпления. Действително, с редакцията от 2010 г. по отношение на тези случаи ЗЕС препраща към реда по НПК. Последният оправомощава съда или органите на досъдебното производство да искат от лица да им предадат намиращите се у тях данни, включително „за трафика". Според официалния доклад на компетентната парламентарна подкомисия за 2011 г. в 58 702 случая достъп до данни по ЗЕС е предоставен по реда на НПК (тоест без съдебно разрешение), а след съдебно разрешение по реда на чл. 250б, ал. 1 от ЗЕС е предоставен едва в 15 350 случая. След промените в ЗЕС през 2010 г. броят на разрешенията за достъп до данни по ЗЕС сериозно расте – от общо 20 605 разрешения през 2010 г. числото се увеличава на общо 74 052 през 2011 г., т.е. само за една година броят е нараснал повече от три пъти.

Решения на Съда на Европейския съюз и Конституционния съд. През април 2014 г. Съдът на Европейския съюз обяви Директива 2006/24/ ЕО за невалидна [14]. Според мотивите на съда е налице несъответствие на директивата с разпоредбите на чл. 7, чл. 8 и чл. 52, § 1 от Хартата на основните права на Европейския съюз. През същата година омбудсманът внесе в Конституционния съд на Република България искане за обявяване на разпоредбите в ЗЕС, които въвеждат Директива 2006/24/ЕО, за несъответни на Конституцията. Като заинтересовани страни бяха конституирани държавни органи и неправителствени организации. С решение от март 2015 г. Конституционният съд обяви за противоконституционни всички отнасящи се до запазването на данни за трафика и достъпа до тях разпоредби от ЗЕС [15]. Според Конституционния съд е възможно материята да бъде уредена по начин, който е съвместим с основния закон. Това означава държавната намеса, изразяваща се в задължението за запазване на данни за трафика и възможността за

достъпа до тях, да е уредена със закон, да е в рамките на предвиденото с основния закон изключение, да е подчинена на легитимна/и цел/и от общ интерес. В решението се приема, че запазването на всички данни за трафика на гражданите без оглед евентуалното им участие в престъпна дейност, не е непропорционална мярка, за разлика от срока на запазването. Той е прекомерно дълъг според съда, тъй като натрупването на едногодишна база данни от комуникационен трафик позволява тяхното използване не само за изготвянето на подробен личностен профил (с всички проблеми, които това създава), но и постигане на точна и детайлна диференциация на трайните, обичайни, инцидентни прояви на конкретното лице, неговите контакти, увлечения, интереси, включително с отграничаването на тези, представляващи прецедент в неговото поведение и реакции, а също и систематизиране по различни критерии на местата, които посещава трайно, често, рядко или инцидентно, както и точна идентификация на лицата, с които го прави. Конституционният съд стига до извода, че не са налице необходимите процедурни гаранции за гарантиране на правата на гражданите, като прави съпоставка и с аналогичната уредба на материята, свързана с използването на специални разузнавателни средства. Също така Конституционният съд счита, че оспореното законодателно решение за елиминиране на съдебния контрол в хипотезата на отправено искане за достъп до трафични данни от орган на досъдебното производство (с препратката към реда по НПК) е в противоречие с установените от Конституцията, Европейската харта за правата на човека и КЗПЧОС стандарти. Непосредствено след решението на Конституционния съд бяха приети изменения и допълнения в ЗЕС, които преуредиха материята, свързана със запазването на данни за трафика на електронни съобщения и достъпа до тях [16].

Отказ на достъп до информация по ЗДОИ в случаите на класифицирана информация. Още с приемането на ЗДОИ през 2000 г. бе предвидена възможност за контрол върху законосъобразността на засекретяването на информация. Според приетата регламентация съдът е в правомощието си да изиска съответните доказателства за това, че информацията е законосъобразно засекретена, да ги разгледа в закрито заседание и да се произнася по въпроса. С приемането на Закона за защита на класифицираната информация разпоредбата в ЗДОИ бе съответно редактирана, като контролът се осъществява върху „законосъобразността на маркирането с гриф за сигурност“. В практиката на съдилищата правомощието за изискване на необходимите доказателства се изразява в задължаване на държавната институция ответник да представи по делото съответния класифициран документ [17] Обикновено съдебните състави се фокусират върху процесуалните аспекти на класифицирането на информацията, но не винаги се ограничават само до тях. Следователно разглеждането на основанията за класифициране на документа с оглед въпроса би ли произтекла вреда от широкия достъп до съдържанието му не е изключено от обхвата на съдебния контрол. Изискването на класифициран документ след приключване на устните прения се приема за съществено процесуално нарушение. Следователно възможността на страните да обсъдят констатациите на съда, макар и направени в закрито съдебно заседание, се явява важен елемент от правото на справедлив процес. Непроизнасянето по въпроса дали даден документ, предмет на искане за достъп до информация, е законосъобразно класифициран, след като е бил преглеждан в закрито заседание, е съществено процесуално нарушение [18]

Изводи

От изложеното следва изводът, че законодателството предоставя съществени възможности на гражданите да инициират процедура по преценка на законосъобразността на класифицирането на даден документ като държавна или служебна тайна. Преценката се извършва от независим орган – административен съд, при събиране на необходимите доказателства и спазване на принципа за равенство на страните и състезателност на съдебния процес. Предвидената процедура и практиката по прилагането ú представлява важна гаранция за правата на гражданите и средство за граждански контрол върху законосъобразността на дейността по засекретяване на информация.

References

1. Закон за управление и функциониране на системата за защита на националната сигурност, Обн.ДВ бр.61 от 11 авг.2015 г.
2. Кашъмов, Александър. Съдебен контрол върху сектора за сигурност. В : Границите на секратността. С.,2015 г., с. 56.
3. Решение № 1 от 10 февруари 1998 г. по конституционно дело № 17/1997 г., докладчик конституционният съдия Неделчо Беронов.
4. Решение по делото на „Асоциация за европейска интеграция и права на човека и Екимджиев с/у България”
5. Решение на Софийския градски съд, III-а състав по а.д. № 642/2002 г., оставено в сила от състав на Върховния административен съд, пето отделение, с Решение № 2557/21.03.2005 г. по а.д. № 6362/2004 г.
6. Решение на Софийския градски съд, III-а състав по а.д. № 642/2002 г., оставено в сила от състав на Върховния административен съд, пето отделение, с Решение № 2557/21.03.2005 г. по а.д. № 6362/2004 г.
7. Жалба № 62540/00.
8. Жалба № 22373/2004 и жалба № 27097/2004.Решенията са окончателни от началото на 2013 г
9. Доклад на Националното бюро за контрол на специалните разузнавателни средства за извършената дейност през 2017 г.,, внесен в НС на 31.05.2018 г.
10. Доклад на Националното бюро за контрол на специалните разузнавателни средства за извършената дейност през 2018 г.,, внесен в НС на 30.05.2019 г.
11. Наредба No 40 от 07.01.2008 г. за категориите данни и реда, по който се съхраняват и предоставят от предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги, за нуждите на националната сигурност и за разкриване на престъпления.
12. Решение № 13627 от 11.12.2008 г. по адм. д. № 11799/2008 г. (обн., дв, бр. 108 от 2008 г.)
13. Данните бяха публикувани в пресата с източник тогавашния председател на парламентарната правна комисия
14. Решение от 8.04.2014 г. на Съда на Европейския съюз, разширен състав, по съединени дела C-293/12 и C-594/12.
15. Решение № 2 от 12 март 2015 г. по к.д. № 8/2014 г. (обн. ДВ бр. 23 от 2015 г.).
16. Закона за електронните съобщения, Обн. ДВ бр. 24 от 2015 г.
17. Определение от 27 март от 2003 г. по а.д. № 9898/2002 г. на Върховния административен съд, пето отделение, Определение от 22 декември 2005 г. по а.д.№ 4596/2005 г. на Върховния административен съд, пето отделение.
18. Решение № 3875/28.04.2005 г. по а.д. № 592/2005 г. на Върховния административен съд, петчленен състав.

Stoyan N. Chanev,

THE ARMED FORCES COMMAND AND CONTROL SYSTEM IN HYBRID WARS

Stoyan N. Chanev

National Military University „VasilLevski", Faculty of „Artillery, air defense and CIS", Shumen, Republic of Bulgaria, st.chanev@abv.bg

***Abstract**: The report gives a brief description of the command and control system with its four levels - strategic, operational and tactical. Some specific features of command and control in hybrid threats are discussed. The directions in which the system fall behind in its development are indicated and ways to optimize it are suggested.*

***Keywords**: command and control system, hybrid wars.*

СИСТЕМАТА ЗА КОМАНДВАНЕ И УПРАВЛЕНИЕ НА ВЪОРЪЖЕНИТЕ СИЛИ В УСЛОВИЯТА НА ХИБРИДНИ ВОЙНИ

Стоян Н. Чанев

Национален военен университет „Васил Левски"/факултет „Артилерия, ПВО и КИС" - гр. Шумен,България, st.chanev@abv.bg

Въведение

Системата за командване и управление на Въоръжените сили е специализиран елемент от националната система за сигурност на Република България и има решаващо значение за ефективния им принос към разрешаването на кризи от различен характер и за осигуряване отбраната на страната. Тя позволява на командирите/началниците и техните щабове да изпълняват задачите, произтичащи от мисиите на въоръжените сили.

Функционалната схема на системата за командване и управление на въоръжените сили (Фигура 1) се изгражда в мирно време и се развива в готовност за използване във военно време. Тази система трябва да притежава висока готовност за действие, мобилност, способност за бързо възстановяване, да осигурява непрекъсната връзка между различните управленски звена, надеждност при поставяне на задачите, възможност за централизирано и децентрализирано управление в различни условия, комплексно използване на средствата за управление и комуникация, висока устойчивост и защита.

Фиг. 1. Функционална схема на система за командване и управление на ВС на РБ

Нивата на командване и управление представляват съвкупност от управленски звена, които имат едно и също място в йерархичния строеж на управленската структура.

Обособени са три нива на командване и управление на въоръжените сили: стратегическо, оперативно и тактическо.

Стратегическото ниво на командване и управление включва Президента на републиката, министъра на отбраната и началника на отбраната, подпомагани от щаб на отбраната и обща и специализирана администрация на Министерството на отбраната.

Стратегическото ниво е отговорно за изпълнението на задачите на въоръжените сили, произтичащи от определените мисии.

Оперативното ниво на командване и управление включва командващия на Съвместното командване на силите, командващите/командирите на Сухопътни войски, Военновъздушните сили и Военноморските сили, подпомагани от техните щабове.

То е отговорно за планирането и провеждането на операции на територията на страната и извън нея в определени пространствени, времеви и ресурсни рамки за постигането на стратегическите цели. Това равнище осъществява връзката между тактическото и стратегическото ниво.

Командващият на Съвместното командване на силите осъществява командването на пряко подчинените му военни формирования, както и оперативното командване и управление на придадените му военни формирования от видовете въоръжени сили при провеждането на съвместни операции.

Командващите/командирите на Сухопътните войски, Военновъздушните сили и Военноморските сили осъществяват командването и управлението на подчинените им военни формирования. При провеждане на самостоятелни операции командващите/командирите на видовете въоръжени сили командват и управляват подчинените им тактически формирования. При съвместни операции те формират щабни елементи на сухопътния, военновъздушния и военноморския компонент за управление на участващите в съвместната операция сили и средства.

Тактическото ниво на командване и управление включва командирите (началниците), подпомагани от техните щабове, които осъществяват тактическо командване и управление на подчинените им военни формирования, които са:

- от състава на Съвместното командване на силите;
- от състава на видовете въоръжените сили;
- бригада „Специални сили";
- стационарна КИС;
- от структурите на пряко подчинение на министъра на отбраната.

Тактическото ниво на командване и управление на въоръжените сили е отговорно за провеждането на бойни, поддържащи и осигуряващи действия от подразделенията за изпълнение на поставените им задачи.

Изложение

Все повече се говори за "малки по размер операции". Използването на конвенционалните и специални структури в една операция традиционно е изключително трудно, независимо от техния размер или организация. Като пример за подобно разделение може да се даде Special Operation Joint Task Force (SOJTF) и Щаба на американските сили в Кабул, Афганистан. Ако няма специално разрешение за достъп, никой не се допуска без придружител в Щаба на американските сили, дори и да има съответното ниво на достъп и е от SOJTF.

Хибридни организации и структури, които съчетават управлението при мисия на силите за специални операции и конвенционалните сили трябва постоянно да участват в учения под някаква форма, което развива системата за командване и управление на войските. Един пример за това е необходимостта от разработването на командни структури, които разбират и използват всички културни нюанси на страните, в които се провеждат военни действия, с цел постигане на стратегическите цели.

Изискването за гъвкава и модулна хибридна структура, ръководена съвместно от командири от силите за специални операции и конвенционалните сили ще доведе до комбинация от повишена нужда от информация за ситуацията, умения за разбиране на културните нюанси и въздействието на регионалните събития, преход от конвенционалната война към разширяване на неконвенционални или контра-неконвенционални бойни кампании и необходимост за адаптация към скоростта на промяната.

Основно внимание при изискването за подобряване на командването и управлението на ВС трябва да се обърне към следните фактори:

- Инвестиране в човешкия фактор;
- Оптимизиране на взаимозависимостта между силите за специални операции и конвенционалните сили;
- Разработване на способности на силите за специални операции на оперативно ниво;
- Изграждане на способности за киберотбрана;
- Оптимизиране на логистиката и ресурсното осигуряване.

За оптимизиране на командването и управлението трябва да се предвиди една нова командна структура, притежаваща широк спектър на мащабируеми и способни за развръщане и оцеляване С2-възли, командна структура способна да изпълнява мисия в най-суровите политически среди, с необходимото ниво на експертни знания и опит. Такава архитектура трябва да е в състояние да планира, интегрира и синхронизира всички видове операции и кампании, във всеки ешелон на съвместно командване, в екипна междуведомствена или в партньорска среда, във враждебно обкръжение, независимо от размера на кампанията, включително на стратегически щаб.

Една от най-важните способности на въоръжените сили е да бъдат в състояние да поддържат споделяне на информация през цялата военна система за командване и управление, както и с другите национални участници от невоенния компонент в режим 24/7, а също така и с информационните системи на нашите съюзници. Това изисква пълна съвместимост на мрежово, технологично и софтуерно ниво на информационните системи и платформи.

В настоящия момент по отношение на киберсигурността нашите ВС, пък и Р България са на базово ниво. Проблемът е в това, че нямаме еднопосочност и взаимодействие между всички за-

интересовани страни, между всички играчи, нямаме национална стратегия. Това пряко влияе и на способностите за киберотбрана на системата за командване и управление на ВС. Особеното, обаче е, че киберпространството като пети домейн, в който живеем, е различен от другите четири и изисква други способности и умения, други ангажименти. Големият проблем е, че каквато и защита да използваме на С2-системата тя, все пак е временна. Винаги има средства, които дори да са защитени, криптирани съответните файлове или информация и достъп, винаги има средства, с които това може да бъде заобиколено. Естествено, че групировки - престъпни, политически, недържавни, които упражняват терористична или антидемократична дейност, използват много умело точно тази свобода в киберпространството. В случая свободата се явява наша уязвимост.

Огромно е изоставането в технологично отношение на системата за командване и управление в следните направления:

Системите за управление на високоточни оръжия - Основната цел на умните оръжия е да могат да постигат директни попадения, без да се налага залпов огън или корекция на стрелбата. Поради голямата ефективност те се ползват основно за поразяване на стратегически цели, което ще гарантира изпълнението на мисията. Достатъчно е с помощта на стратегическите ударни (неядрени) сили, които имат на въоръжение високоточно оръжие, да бъде нанесено тежко поражение на противниковите средства за ответен удар, да се унищожат най-важните ключови военни обекти и да се разруши цялата икономика, системата за енергоснабдяване, комуникациите и политическата система на противника ще се разпадне сама.

Система за ранно предупреждение и откриване/разпознаване на хибридните заплахи

Този процес изисква специфични мерки в рамките на системата за командване и управление при кризи от всякакъв характер. Те трябва да бъдат насочени към подобряване на ситуационната осведоменост чрез:

- увеличаване на способностите за разузнаване, наблюдение и оценка на обстановката (ISR), създаване на единно разузнавателно-информационно пространство във въоръжените сили на стратегическо, оперативно и тактическо ниво - събирането, обработката и разпространението на информацията в мирно време и при кризи се извършва централизирано в обединен разузнавателно - информационен център. По отношение на разузнавателно-информационното пространство системата за командване и управление на въоръжените сили трябва да отговаря на няколко основни изисквания:
  1. да създава условия като цяло и по елементи така, че добитата информация да достига до прекия командир и в последствие до всички останали;
  2. отделни нейни елементи да могат да се адаптират с основните командни структури както на национални така и на многонационални военни формирования, а също така да могат да изпълняват задачи в интерес на други ведомствени структури;
  3. да може да работи в рамките на основните мисии на ВС.
- използване на сензори и т.н. тракер системи – нашите въоръжени сили не разполагат с цялостно изградена система от този тип. В придобитите ПИКИС системи има наченки на подобни способности, но те са морално остарели и почти не се използват, а за интегриране на информацията от тях в общата опозната картина на бойното пространство изобщо не може да се говори;
- използване на безпилотни летателни апарати (БЛА) и дронове - съвременните предизвикателства доведоха до все по-масовото използване на БЛС, които са доказали ефективността си от широкоспектърното си приложение от наблюдение и следене на цели и обекти до нанасяне на електронни и огневи удари. Основните им предимства са достатъчния експлоатационен ресурс, многократно по-ниската себестойност спрямо пилотируемите летателни апарати и приложимостта им на всички командни нива. С приноса си към разузнаването от изображения (IMINT) чрез осигуряването на опозната картина на бойното пространство в мащаб на времето близък до реалния, БЛС се превръщат в мощно средство за командирите и планиращите щабове в процеса на вземане на решения, избора на цели и средства за нанасяне на удари по тях.

Система за ефективно вземане на решения

Бързото и ефективно вземане на решения се основава на подобрената ISR-система, ситуационна осведоменост, проста и ясна система за командване и управление, стабилна и сигурна комуникационно-информационна система (КИС) в състояние да продължи да функционира след кибердудара или действия по електронна борба. В известна степен се наблюдава изоставане и в областта на планирането за извънредни ситуации, включително предварителното изграждане на системата за командване и управление и стандартните оперативни процедури за действие при извънредни ситуации. Процеса за вземане на решения изисква достъп на командира до възможно най-пълната информация за бойното пространство, а това може да му бъде осигурено само чрез интегрирането на всички информационни източници, чрез обща платформа.

Образование, обучение и оценяване

Разбирайки значението на образованието, обучението и оценката за провеждането на ефективни операции за борба с хибридните заплахи, военното ръководство предприе някои конкретни стъпки за развитие, адаптация и поддържане на способности за изграждане на устойчива система за командване и управление/система за вземане на решения срещу хибридните заплахи. Началникът на отбраната в "Ръководство за обучение - 2015" е определил дейности за борба с хибридните войни, сценарии и планове за обучение. Въпреки, че тези мерки са продуктивни и изключително необходими, не са всеобхватни и не са залегнали в стратегия за образование и обучение, целяща противодействие на хибридните войни на национално и междуведомствено ниво. Колективното и съвместно обучение и тренировки е от решаващо значение за ефективното противодействие на хибридните войни.

Заключение

Днешната идеология, моделът и принципите за изграждане на системата за командване и управление на ВС дават основание да се направи заключение, че системата е изключително неподготвена за противодействие на хибридните заплахи и предизвикателства. Практиката при формирането на батальонни бойни групи показва, че липсва интегрираност между формированията от сухопътни войски и силите за специални операции. Създаването на единна командна структура между конвенционалните сили и силите за специални операции с общо командване и пълен синхрон между тях е една добра възможност да се противодейства на хибридните заплахи, които ще бъдат предизвикателство за операциите в близкото бъдеще. Необходимо е преструктуриране и изграждане на гъвкава структура на военните формирования, която да е в зависимост от конкретната хибридна заплаха. За да има ефект тази нова за нашите ВС организация е необходимо изучаването на потенциалния противник – вярвания, възгледи, навици и др. както и възможността за бърза адаптация в зависимост от заплахите. Това ще генерира големи предимства на въоръжените силите при участие в хибридна война.

References

1. Иванов В., Същност и диалектика на концепцията за командване и управление на въоръжените сили (С2), София, 2016.
2. Давидов К., Атанасов А., Асиметричните заплахи и участието на формирования от въоръжените сили в хибридни операции, Международна научна конференция «Морската мощ на държавата и борбата с пиратството и тероризма на море» стр.135-139, Варна, 2011, ISSN 1310-9278.
3. Тодорова М., Системата киберсигурност, Сборник доклади на международна научна конференция „Киберсигурността в информационното общество“ на НВУ ”Васил Левски”, Факултет “А, ПВО и КИС”, Шумен, 2017, Издателски комплекс “В. Левски” – Факултет “Артилерия, ПВО и КИС” Шумен, 2017, ISBN 978-954-9681-82-6
4. Стоянова В., Възможности за получаване на конфиденциална информация чрез мобилни устройства, Списание CIO, бр.7, 2017, стр. 82-86, ISSN 1312-5605.

Atanas L. AtanasoV,

AEROSPACE FORCES AS A MEANS OF STRATEGIC DETERRENCE

Atanas L. Atanasov

National Military University „VasilLevski", Faculty of „Artillery, air defense and CIS", Shumen, Republic of Bulgaria, lenkov@gbg.bg

Abstract: The evolution of contemporary views on deterrence shows that the role of means of deterrents is changing, requiring adequate state (union) power, willpower and determination to use force when necessary.

Aerospace forces are an effective means of implementing strategic deterrence resulting from changes in the security environment.

Improvement of aerospace deterrents is evolving in the direction of improving surveillance forces and means, providing information superiority, space strike management, new unmanned aerial vehicles with radar intelligence and special ammunition, stealth technologies, multifunctional missile defense and more.

***Keywords**: aerospace forces, strategic deterrence.*

ВЪЗДУШНО-КОСМИЧЕСКИТЕ СИЛИ КАТО СРЕДСТВО ЗА СТРАТЕГИЧЕСКО ВЪЗПИРАНЕ

Атанас Л. Атанасов

Национален военен университет „Васил Левски"/факултет „Артилерия, ПВО и КИС" - гр. Шумен,България, lenkov@gbg.bg

Въведение

Войните са съпътствали човешката история, като изразяват силови отношения и още по-конкретно - военностратегическите отношения.

Новите военни средства за воюване са наситени с информационни технологии, компютърни и телекомуникационни системи, невидими ударни средства. Все по-широко навлизат нанотехнологиите, изкуствения интелект и психотронните средства. Показателни са и примерите за милитаризиране на космоса. Непрекъснато се увеличават военните разходи на много от държавите по света за усъвършенстване на технологиите, което води до коренни промени в средствата за водене на въоръжена борба. Много от държавите планират мерки за поддържане на стратегическото равновесие или превъзходство. Разработват се планове за операции по суша, въздух, вода, в космоса и в информационната среда за участие в различни въоръжени конфликти.

Новото поколение войни са асиметрични, мрежово-ценрични и многообразни, а изходът от тях е промяна на общественото развитие, не само на победителите и на техните съюзници, но и на победените. Войните и конфликтите в Афганистан, Ирак, Ивицата Газа, Сирия, Либия, Египет, Мали са доказателство за това.

Изложение

Моментната картина на средата за сигурност би била полезна дотолкова, доколкото позволява да се провеждат текущи операции, без да се планират дългосрочни ефекти. Стратегията е изкуството на възможното. За нуждите на стратегическото планиране са необходими достатъчно ясни параметри на бъдещата среда за сигурност. Целесъобразно е да бъде намерен и прилаган такъв инструментариум, за да може тя да бъде прогнозируема в степен, която да съответства на отговорността за вземаните решения. Водещите в информационно отношение страни изразходват огромни средства за поддържане и развиване на анализаторските си служби. Разработват се военни доктрини съответстващи на развитието на военностратегическите отношения, както и различни теории за стратегическото водене на войната и за нейното предотвратяване. Една от тези теории е тази за стратегическото възпиране. Анализът на съществуващата литература показва, че въпросите, свързани с използването на военните средства за възпиране, не са развити в достатъчен обем. Липсват задълбочени изследвания, на базата на които да се очертаят конкретните направления за трансформация на възгледите за стратегическо възпиране с военни средства.

В речника на термините и дефинициите на НАТО AAP-6 е пояснено така: „deterrence/dissuasion (възпиране/разубеждаване) – „Убеждаване на потенциален (опонент) агресор, че последствията от принудително действие или въоръжен конфликт ще надвишат потенциалните ползи. Това изисква поддържането на правдоподобна военна стратегия и сила, основаваща се на ясно политическо желание за действие.”

Така възприетото в НАТО значение за възпиране определя неговата същност, която може да се разглежда като способност на определена държава (съюз, коалиция) да се убеди потенциалния опонент (агресор), че загубите му от противопоставяне и/или иницииране на въоръжен конфликт ще са по-големи от евентуалните му ползи.

На базата на това може да се твърди, че съдържанието на възпирането ще се определя от прилаганите върху потенциалния опонент на различни информационни операции за въздействие, обединени в конкретни форми и способи за възпиране, основаващи се на поддържане на правдоподобна стратегия и военна мощ и на ясно политическо желание за действие.

Стратегическото възпиране може да се разглежда като „система, включваща субекти, обекти и средства за възпиране, обединени за изпълнението на единна цел”[1].

За да се постигне успешно стратегическо възпиране, изхождайки от динамиката и сложността на съвременната среда за сигурност, трябва да се реализират следните три условия: наличие на адекватна държавна (съюзна) мощ, наличие на воля и решимост за използване на сила.

Въздушно-космическото възпиране е възпиране най-вече със средствата на въздушно-космическите военни сили, които страни като Русия, Китай, САЩ и друго държави притежават.

Повече от 130 държави, участващи в дейности в космическото пространство и приложението за военни цели на въздушнокосмическите технологии е също толкова широкомащабно. Военните задачи в космическото пространство включват: наблюдение и разузнаване, откриване и предупреждаване за изстрелване на ракети, поразяване на изстреляни вече ракети, насочване на оръжия, метеорологическо осигуряване, топогеодезическо и картографско осигуряване, изследване на космоса, сателитната комуникация, която вече е с изключителна важност за системата за командване и управление, и други.

Друг важен елемент на въздушно-космическите сили са системите за ПРО, които са с особена важност за постигане на търсения ефект от възпирането относно намеренията за използване на балистични (ядрени и конвенционални) ракети от потенциалния опонент.

Направления за развитие на въздушно-космическите средства за възпиране.

В контекста на предизвикателствата пред съвременната среда за сигурност, не подлежи на съмнение, че космическото пространство и в частност космическите сили и средства имат

решаващо значение за провеждането на редица операции и за изпълнението на задачите от въоръжените сили в мирно и военно време.

Не е случайно създаването на отделен род войски – космическите, в някои от водещите в световен мащаб държави. Способността им да изпълняват широк спектър от задачи като осигуряване на информация, откриване изстрелването на балистични ракети и предупреждение за ракетно нападение, защита на центровете за управление на висшето държавното и военно ръководство, защита на важни държавни и военни обекти от удари с аналогични средства от страна на противник и други, оказва съществена роля за търсения ефект от възпирането върху потенциалните опоненти.

От особена важност за реализиране на възпирането с космически средства е изстрелването на космически апарати за извеждането в орбита на сателитни системи с военно и двойно предназначение.

Като успешен пример за развитието на такива способности, касаещи възпирането, е Съюзната система за наблюдение на земната повърхност (AGS),

Може да се твърди, че развитието на средствата за наблюдение на космически обекти и откриване на заплахите в космоса и от космоса за държавите и съюзите, които ги притежават, е от голяма необходимост. Тези средства могат да се използват при необходимост и за неутрализиране на самите заплахи. Затова трябва да се развиват и усъвършенстват системите за предупреждение от ракетно нападение и осигуряване с информация, които се основават най-вече на космически-базирани сензори и „СТЕЛТ”-технологии, за постигането на глобален контрол на въздушното и космическото пространство.

Увеличаването на обхвата и разнообразието от задачи, които военната авиация трябва да изпълнява, налага необходимостта от усъвършенстване и използване на съвременни типове стратегически бомбардировачи, многоцелеви изтребители, безпилотни летателни апарати (БЛА) и вертолети с възможности за излитане и кацане от необорудвани летища и самолетоносачи.

Водещите във военно отношение държави работят по проекти за увеличаване разстоянието на полета на самолетите, чрез разработки на различни типове двигатели с алтернативно.

Анализирайки изказвания на експерти в свободното пространство, съществува информация, че се разработват хиперзвуковите безпилотен хиперзвуков самолет, който се движи със скорост шест пъти по-голяма от скоростта на звука.

Категорично може да се твърди, че като основна се очертава тенденцията за развитие на военновъздушните сили и средства в направление на безпилотните летателни апарати.

Анализирайки досегашното участие на БЛА в различни военни конфликти, могат да се очертаят някои направления в тяхното развитие. На първо място БЛА ще се използват най-вече за разузнаване и обозначаване на целите. В този случай БЛА ще бъдат основно средство за разузнаване на стратегически обекти, както и на други, с поразяването, на които функционирането на икономиката и отбраната на съответната страна ще се окаже невъзможно. Те ще трябва да се характеризират с възможности за голяма продължителност на полета, да носят на борда радиолокационни средства, инфрачервена апаратура, средства за радиотехническо разузнаване и специални боеприпаси.

Друга насока е към използване на БЛА като бойни средства. САЩ вече са използвали такива за нанасяне на удари по наземни и поразяване на въздушни цели. Не на последно място БЛА могат да се използват като пунктове за управление. Специалистите са на мнение, че оборудването на БЛА с компютърни системи с изкуствен интелект (експертни системи) ще позволи на такива апарати без вмешателство на оператора или при загуба на управлението самостоятелно да извършват опознаване на обектите, да използват средствата за поразяване и да вземат други логически действия.

Заключение

Силите и средствата за противоракетна отбрана на държавите и съюзите са основен компонент за реализиране на стратегическото възпиране с военни средства. Може да се твърди, че те допълват ролята на ядреното оръжие за възпирането, но не могат да го заменят. Това е така, защото ПРО по същество се класифицира като чисто отбранителен потенциал на притежаващите я. Изграждането и усъвършенстването на добре развита ПРО усилва тежестта на възпирането и намалява същевременно зависимостта от притежаване или желание за притежаване на ядрени оръжия.

Системата за ПРО на НАТО определено ще се развива в направления на реализирането й като глобална система на страните-партньори и на постоянно подобряване на материалната й основа (ракетите и пусковите установки).

Най-вероятно новите тенденции в развитието на ПРО ще са към създаване на многофункционални съвременни ударни системи за ПРО от нов тип, в това число основавайки се на използването на кинетично, електромагнитно и лазерно въздействие. Изхождайки от работата на учените по разработване на хиперзвукови самолети и свръхзвукови крилати ракети, ПРО трябва да се развива и в насока за противодействие на такива нови средства.

References

1. Недялков, Н., Трансформация на възгледите за стратегическо възпиране с военни средства, Дисертация, София, Военна академия „Г. С. Раковски”, 2012.

2. Добрев, К., Възпирането като форма за гарантиране на системата за сигурност на държавата, Сборник „Актуални проблеми на сигурността”, София, Военна академия „Г. С. Раковски”, 2009.

3. Стоянова, В., Скриване на информация в изображения, Издателски комплекс на НВУ „Васил Левски” ISBN 978-954-9681-86-4.

4. Чанев, С., Устойчивост на групировка за противовъздушна отбрана, *II International scientific conference CONFSEC 2018, Боровец, 2018, с. 76-78, ISSN PRINT,2603-2945.*

5. Камарашев, Г., Учебно пособие за изучаване на способите за бойно използване на авиацията, ВВОВУ “В. Левски” №03955, В. Търново, 2000.

Anatoly I. Andreev,

ENERGY SECURITY AS AN ELEMENT OF NATIONAL SECURITY

Anatoly I. Andreev

University of Library Science and Information technologies
Institute for Scientific Research and Doctoral Studies

***Abstract**: Energy security is an element of economic security and is a prerequisite for the economic stability of the state. Economic security of the country itself is a foundation of national security and is essential for other types of security - military, political, environmental and technological.*

***Keywords**: security, energy security, economic security, national security*

ЕНЕРГИЙНАТА СИГУРНОСТ КАТО ЕЛЕМЕНТ НА НАЦИОНАЛНАТА СИГУРНОСТ

Анатоли И. Андреев

Университет по библиотекознание и информационни технологии
Институт за научни изследвания и обучение на докторанти
Гр. София, бул."Цариградско шосе"N:119, e-mail:andreevanatoly@gmail.com

***Abstract**: Енергийната сигурност е елемент на икономическата сигурност и е предпоставка за икономическа стабилност на държавата. Икономическата сигурност на държавата, от своя страна е фундамент на националната сигурност и е определяща за другите видове сигурност - военна, политическа, екологична и технологична.*

***Keywords**: сигурност,енергийна сигурност,икономическа сигурност,национална сигурност*

През последните десетилетия разбирането на понятието за сигурност значително се е променило. Това обстоятелство се е наложило поради факт на промяна на потребностите и изискванята на обществото към своята общност, идентичност националност, държава.

Основно място в това ново разбиране заема концепцията за „национална сигурност", която, за разлика от остарялото, тясно разбиране за сигурността има за свой обект не само територията на дадена държава, а най-вече нейните граждани.

Националната сигурност се стреми върху осигуряване на спокоен, стабилен и сигурен живот на гражданите в тяхната страна и извън нея. Характеризира се с тясна свързаност с безопасността и съхранението на самата обществено-политическа система на дадена държава с други страни при осъществяване на националните цели, интереси, като по този начин влиза в междудържавни отношения, които може да способстват или да възпрепятстват изпълнението на целите. Установява се тясна връзка между националната сигурност и икономическата система на държавата. Съществен и неизменен компонент от националната сигурност е икономическата сигурност на държавата. Развитието на националното стопанство се определя като структуроопределящ елемент на икономическата сигурност на държавата. Ако икономическата система не се развива,

то рязко се ограничават възможностите за нейното "оцеляване", а така също и за отпор, съпротива и приспособимост към външните и вътрешните заплахи. Стопанство, в което няма динамика, не е в състояние да генерира икономическа сигурност и не може да се определи като икономически безопасно.

В основата на сигурността винаги са вградени като съставни компоненти признаването на особените национални икономически цели и интереси на всяка държава. Затова въпреки, че е назоваване „икономическа сигурност на държавата" понятието се отличава с многоаспектност по смисъл, съдържание и употреба [1].

Държавата разполага със съвкупност от ресурси – материални, човешки и валутно-финансови. В зависимост от международната обстановка и състоянието на националната икономическа система всяка страна изпитва потребност от задоволяване на недостига в различна степен. Всяка държава се нуждае от привличане на допълнително количество ресурси от други страни.

Необходимо е да се отбележи, че както вътрешните, така и външните измерения на икономическата сигурност на държавата са тясно свързани и зависими от качеството, системността и ефективността на управлението на националния стопански механизъм [2].

Икономическата сигурност на държавата, от своя страна е фундамент на националната сигурност и е определяща за другите видове сигурност - военна, политическа,енергийна, екологична и технологична [3].

Енергийната сигурност е елемент на икономическата сигурност и е предпоставка за икономическа стабилност на държавата.

Енергийната сигурност е една от сферите, които се превърнаха в приоритетни за Република България и Европейският съюз (ЕС) през последните години, особено като се има предвид намаляването на световните запаси на нефт и природен газ [7].

Но понятието енергийна сигурност не обхваща само сигурността на износа и доставките. Понятието на енергийната сигурност се е променило и разширило след първите големи енергийни шокове от 70те и началото на 90те години на XX век. Днес рисковете са различни, а начините за избягването им и разрешаването на проблемите стават все по-сложни. Следователно разбирането, обясняващо съдържанието на понятието енергийна сигурност от 70-те години на миналия век вече не е напълно приложимо. Някои от основните проблеми, даващи смисъл на понятието все още съществуват: регионални и социални напрежения и днес правят нестабилни дадени региони на добив на енергийни суровини [2].

От друга страна обаче глобалният тероризъм е заплаха за цялата система на доставки. През последните години политическите конфликти в Персийския залив, Нигерия и Венецуела също доведоха до проблеми с доставките. Ураганите в Мексиканския залив се отразиха на потребителските цени на бензина и на отоплението в САЩ. Нарасналото потребление в Китай също е на път да изправи страната пред енергийна криза и тя е принудена да преосмисли дефиницията си за енергийна сигурност и да потърси решение, надхвърлящо традиционната ѝ политика на самозадоволяване [4].

Енергийната сигурност не се изчерпва само с въпроса за нефта. Тежките аварии в електрическите мрежи в североизточните части на САЩ, а също така и в Европа и Москва от 2003 г. показаха колко уязвими са тези преносни мрежи. Високите цени на природния газ в САЩ свидетелстват за един зле балансиран пазар на газ, а газовата криза от началото на 2009 г. ясно показа, че потребителите в Европа не могат да се чувстват сигурни, докато газовият пазар е до голяма степен доминиран от една държава – Русия [4].

Терминът „енергийна сигурност" обвързва понятията енергетика, икономически растеж и политическа сила. Перспективата ни за това какво е енергийна сигурност зависи от позицията ни в „енергийната верига". Потребителите и енергоемките индустрии желаят да им се доставя енергия на разумни цени и да не преживяват енергийни шокове. Големите страни-производителки на нефт или газ считат сигурността на доходите и на търсенето за основни теми при всяка дискусия по въпросите на енергийната сигурност. Нефтените и газовите компании, от друга страна, смятат, че достъпът до нови ресурси, стабилните инвестиционни режими и възможността за подобрение

и доразвиване на инфраструктурата са изключително важни аспекти на енергийната сигурност. Електрическите компании се притесняват за целостта и сигурността на цялата мрежа. Политиците се фокусират върху рисковете от преустановяване на доставките и върху сигурността на инфраструктурата, която може да е под заплаха от тероризъм, война или природни бедствия. Те също така трябва да предвидят количеството на стратегическите резерви, размера на излишъците и осигуряването на целостта и функционирането на инфраструктурата. По цялата „енергийна верига" цените и диверсификацията на доставките са два от най-важните елементи на енергийната сигурност [5].

Въпреки тези различни измерения на енергийната сигурност, все пак сърцевината на проблема остава зависимостта на дадена страна от внос на енергийни ресурси. Оттук тръгват всички следващи от това проблеми, свързани с доставките, цените и сигурността на трасетата за пренос. Прекомерната зависимост от един източник на доставки може да направи дадена държава уязвима и да се стигне дотам, че доставките да бъдат използвани като „оръжие" за постигане на политически или икономически цели от страната-производител.

За това енергийната зависимост е един от най-сериозните проблеми, който застрашават сигурността на Европа днес.

Според едно кратко определение за „енергийна сигурност", това е способността да се осигурява енергия с цел задоволяване на търсенето, на цена, която запазва икономическия растеж. Фактът, че всички икономически дейности се нуждаят от енергийни ресурси прави енергийната сигурност важен елемент в енергийната политика на националните правителства. Друга дефиниция определя енергийната сигурност, като способност да се поддържа непрекъснатост на доставките в периоди на свръх търсене или на нарушаване на енергийните потоци и да се осигури задоволяване на бъдещото търсене чрез комбинация от собствени енергийни ресурси и благонадеждни доставки и транзит на вносна енергия.[27]

Традиционните области на заплахи като доставката на енергийни суровини, все по-нарастващото търсене и потребление на енергия, геополитическите парадигми и пазарни условия са в основата на множество дискусии, свързани с това да се намери най-добрият вариант за националните икономики, осигуряващ необходимата им енергия за тяхното нормално функциониране [6].

Енергийната сигурност е съвкупност от взаимосвързани и влияещи си взаимно фактори като: сигурност и диверсификация на доставките, сигурност на инфраструктурата, икономически растеж, цени на енергийните ресурси, достъп до нови източници на ресурси, инвестиционни режими, сигурност на приходите, рискове от война и тероризъм, енергийния сектор като геополитическо оръжие, околна среда, социална политика. Дефинира се като състояние на сигурността на субекти на международното право срещу вътрешни и външни заплахи в енергийния сектор, насочено към осигуряване на ефективно, надеждно, еколого-съобразно енергоснабдяване с цел устойчиво развитие на международната общност.

Енергийната сигурност се поддържа от стратегическо планиране, с цел да се осигури разнообразие на горивата, на доставките от източника и ефективност, и гъвкавост в енергийния сектор. Определянето на заплахите за енергийната сигурност е трудно, защото това е широко понятие, обхващащо много аспекти, включително достъп до горива (на приемливи цени), сигурен транзит и преработка на горивото, както и защита на околната среда и ресурсите. Определянето на енергийната сигурност като понятие се усложнява от факта, че има различни виждани по този въпрос. За някои, това означава защита срещу политически предизвикани прекъсвания на доставките ("изключване на крановете") или технически проблеми, за други това е изправяне пред предизвикателствата на тероризма, за трети - това означава, справяне с проблемите на глобалното затопляне, чрез промяна на консумацията.[28]

[27] Energy Supply Security and Geopolitics: A European Perspective, Energy Policy, 34, 2006; Read, 2006;

[2]Stern Jonathan, The Future of Russian Gas and Gazprom (Oxford, UK: Oxford University Press, 2005). Mitchell, J.V. Renewing Energy Security. London: RIIA, 2002 & Victor, D. G. & N. M. Victor, 'Axis of Oil?' Foreign Affairs, Vol.82. no.2, March/April 2003. Lovins, A.M. et al. Winning the Oil Endgame: Innovations for Profits, Jobs & Security. Snowmass: Rocky Mountain Institute, 2005.; Roberts, J. Energy as a Security Challenge for the EU, Paris: ISS, 2005 Forthcoming;

Терминът „енергийна сигурност" може да бъде разделен на два взаимосвързани аспекта - геоложки и политически.

Първият аспект разглежда енергийната сигурност като дългосрочен практически, геоложки проблем, базиран върху устойчивостта на производството.

Има дебат между геолози и анализатори за бъдещето на световните резерви. В обсъждане на най-високо ниво (главно от геолози и инженери), се твърди, че светът е достигнал максималната продукция, която ще се задържи за известно време и след това ще започне да спада, а подобренията в технологията ще доведат до по-бързо изчерпване на резервоарите. Поради тази причина инвестициите в научно-изследователската и развойна дейност за улесняване на новите технологични скокове за достъп до повече петрол са по-малко.[29]

Според други (особено икономисти), изгледите са по-оптимистични. Те изтъкват факта, че нивото на петрол в земята, макар и ограничено, не е фиксирано. Според тях подобренията в технологията, няма да доведат до по-бързо изчерпване на резервоарите. Доказателство за това е постоянно нарастващата крайна възвръщаема ресурсна база, защото е факт, че потреблението в световен мащаб се е увеличило.

Вторият аспект на енергийната сигурност е ясно рамкиран от самите страни членки на Европейския съюз чрез „Европейска стратегия за енергийна сигурност"[4], съгласно която световните резерви са напълно достатъчни, за да отговорят на търсенето на петрол и природен газ.

ЗАКЛЮЧЕНИЕ: Енергийната сигурност е изключително актуална и популярна през последните години. Причината е – запасите от евтини енергоносители, върху които е базирано функционирането на съвременната икономика ще бъдат изчерпани. Безусловно, тези процеси ще окажат влияние върху живота на всеки от нас.

Европейският съюз, чрез инструментите на своята обща външна политика и политиката си за сигурност и отбрана5, следва да работи целенасочено за осигуряване на политическа стабилност и оттам сигурност на своите енергийни доставки.

Много скоро енергийната сигурност ще бъде синоним на национална и икономическа сигурност.

ЛИТЕРАТУРА

1. Рачев В., Милина В., Бахчеванов Г., Карамфилпов Г., Баев Й., Великова Л., Манев М., Бекярова Н., Воденичарски С., Мичев С. & Семерджиев Ц. (2005). *Национална и международна сигурност*. Сиела, 518 стр.

2. Слатински Н. (2004). *Национална сигурност - аспекти, анализи, алтернативи*. Българска книжарница, София, 248 стр.

3. Стефанов Г. (2005). *Теория на международната сигурност*. Сиела, София, 420 стр.

4. Попов Ю. (2016). Идва ли краят на ерата на петрола? Дневник https://www.dnevnik.bg/analizi/2016/01/22/2688115_idva_li_kraiat_na_erata_na_petrola/

5. Милина В. (2007). Енергийната карта в геополитическата игра. *Военен журнал, 3*.

6. www.europa.eu/rapid/pressReleasesAction.do?reference=IP/08/1696&format=PDF

[29] Deffeyes, K. Hubbert's Peak: The Impending World Oil Shortage. Oxford: Princeton University Press, 2001. www.odac-info.org. 'Oil in Troubled Waters – A Survey of Oil', The Economist, 30th April, 2005; Mitchell; Davies, P. & P. Weston, 'Oil Resources: A Balanced Assessment', The CEPMLP Online Journal, Vol.6, No.15. 2000.;

[4] www.europarl.europa.eu

7. Yergin D. (2006). Ensuring Energy Security. *Foreign Affairs, 85, 2,* 69. [i]

Dilyan K. Markov,

INFLUENCE OF THE INTERVALS BETWEEN THE ARTILLERY SYSTEMS PLACEMENT ON FIRE POSITION

Dilyan K. Markov

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

***Abstract**: This report presents an analysis of national and some international instruments governing the intervals between cannons and the size of the firing position of field artillery. The publication presents variants for positioning the guns on the firing position.*

***Keywords**: field artillery, artillery firing position, guns intervals*

ВЛИЯНИЕ НА ИНТЕРВАЛИТЕ МЕЖДУ ОРЪДИЯТА ПРИ РАЗПОЛОЖЕНИЕТО ИМ НА ОГНЕВАТА ПОЗИЦИЯ

Дилян К. Марков

Въведение

За изпълнение на задачите от артилерията оръдията на батареята (взвода) се разполагат на огневи позиции с определени интервали и отстъпи между тях. В регламентиращите документи тези размери са посочени с определени данни, характерни за всички типове – оръдия, бойни машини и минохвъргачки. Съвременното въоръжение промени способите за водене на огън и изисквания за разполагане на местността. Все повече на преден план стои необходимостта от повишаване на бойните качества на артилерията, нейната мобилност и огнева мощ. Повишаването на мобилността на полевата артилерия чрез въвеждане на образци самоходни артилерийски системи, снабдени с GPS системи, позволява по-бърз маньовър с формированията и скоростно изпълнение на поставените огневи задачи.[5] Способите за разполагане на оръдията на огневите позиции зависят и от редица фактори, оказващи влияние на формата на фигурата образувана от наличните оръдия на огневата позиция.

1. Изисквания на регламентиращите документи

Бойната работа на огневите формирования включва действията на личният състав при оръдията (самоходните оръдия, минохвъргачките, бойните машини), свързани с подготовката и воденето на огън, със заемането и напускането на огневата позиция, с работата с оръдието и бойните припаси на огневата позиция.[3] Елемент от огневата позиция се явяват местата на оръдията, разполагани съгласно регламентиращите документи. В българската артилерия тези документи са два:

- „Ръководство по бойна работа на огневите подразделения от артилерията";
- „Ръководство за използване на полевата артилерия – артилерийски дивизион".

Важно изискване за тези документи е да няма различно тълкуване и противоречия в тях. Анализирайки ги се наблюдават определени различия при определяне на местата на оръдията на огневите позиции. Оръдията се разполагат на определени интервали.

Интервал между оръдията се нарича разстоянието между мерните прибори по фронта между съседни оръдия, измерен по линията, перпендикулярна спрямо основното направление на стрелбата.[3]

Преглеждайки „Ръководство по бойна работа на огневите подразделения от артилерията” се открояват следните противоречия:

- съгласно т.65 оръдията се разставят на следните интервали:
  - за оръдия и минохвъргачки 20-40 м;
  - за бойните машини от реактивната артилерия и оръдията с голяма мощност - 50-60 м;
  - в специални условия (планини, гориста местност и т.н.) и по-други.
- в т.245 се посочва, че закритата огнева позиция трябва да отговаря на определени условия, едно от които е да допуска разполагане на всички оръдия на батареята с интервал 30-50м. между тях. Същите данни фигурират в т. 246 и т. 256.
- в приложение 7 „Мерки за безопасност”, т.1 е записано, че допустимият интервал между стрелящите оръдия е най-малко 30м.

По-голяма разлика е записана в Ръководството за използване на полевата артилерия – артилерийски дивизион, съгласно което разстоянията между оръдията са 50-100 м., поне така се разбира от схемата на приложение 3, а разстоянията между огневите позиции на огневите взводове са 200 – 500 м. В същия документ в приложение 2 се посочва, че разстоянията между огневите позиции на огневите взводове са 500 м.

В т.17 и приложение 8 е посочено, че разстоянията между батареите е до 3 км, а района за бойно използване на дивизиона е до 9 км по фронта и до 3 км в дълбочина.

Допустими ли са тези различия? Отговор на този въпрос могат да ни даде прегледа на част от документите на други държави.

2. Анализ на интервалите между оръдията в други страни с подобно въоръжение

Анализирайки националните документи посочващи какъв е интервалът между оръдията е необходимо да се посочат и тези изисквания за другите армии. За тази цел ще се посочат изискванията в руската артилерия, като страна на произход на артилерийското ни въоръжение, както и на страни членки на НАТО със същото въоръжение.

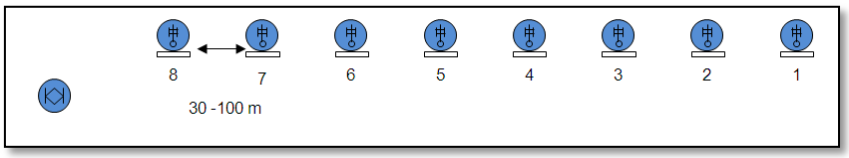
Зависимостта на разстоянията между оръдията в **руската артилерия** е във вида им и се разставят на следните интервали [6]:

- за оръдия и минохвъргачки 20-50 м;
- за бойните машини от реактивната артилерия и оръдията с голяма мощност - 50-100 м;
- за оръдия с навигационна апаратура - 100 м и повече.

В зависимост от организационната принадлежност, далекобойността на артилерийските системи и условията на обстановката, района на огневата позиция в руската артилерия се определя на разстояние 2-6 км или повече от линията на съприкосновение с противника. Размерът на района за бойно използване на дивизиона може да бъде до 2 км по фронта и в дълбочина, а разстоянието между огневите позиции на батареите е най-малко 500 м. В районът за бойно използване на дивизиона се подготвят по 2-3 огневи позиции за всяка батерия.[7]

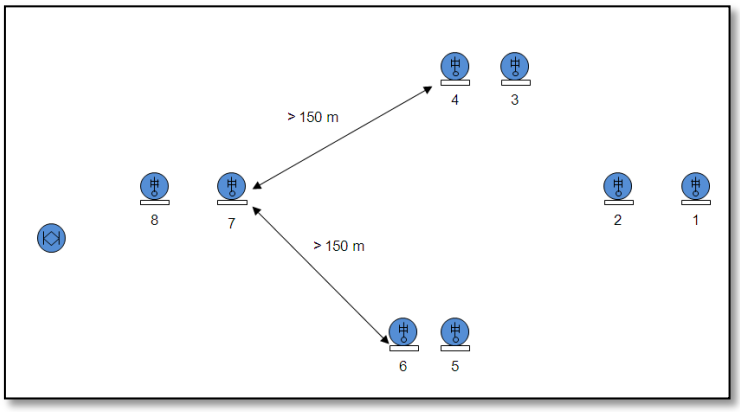
Интервалите между оръдията в **полската артилерия** са от 30 m до 150 m и повече и се определят спрямо конфигурацията на огневата позиция[10]. В зависимост от разположението на оръдията на огнева позиция и разстоянията между тях се използват:

- компактна огнева позиция - разстоянието между оръдията е 30 - 100 m (фиг. 1);



Фиг.1 Компактна огнева позиция

– децентрализирана огнева позиция - разстоянието между участъците е не по-малко от 150 m (фиг. 2).

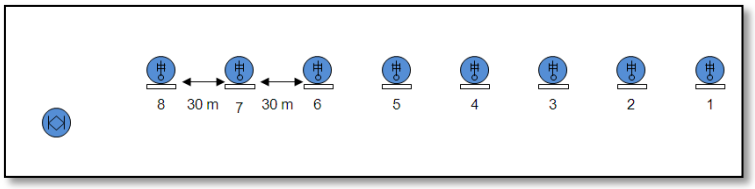


Фиг.2 Децентрализирана огнева позиция

На децентрализирана огнева позиция се определят правоъгълни координати и надморски височини на всички оръдия, а на компактната – най-малко на основното оръдие.

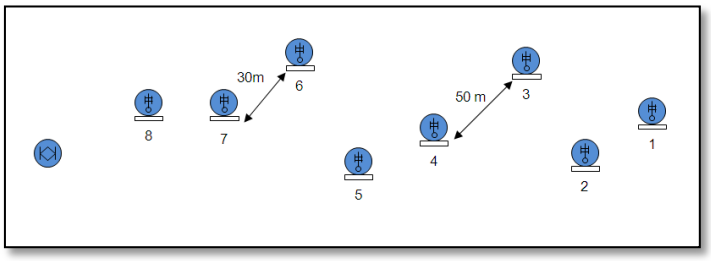
В зависимост от бойния модел на използване на разположение на оръдията огневите позиции могат да бъдат:

- линейни - всички оръдия са разположени на равни интервали в прекъсната линия (фиг. 3);



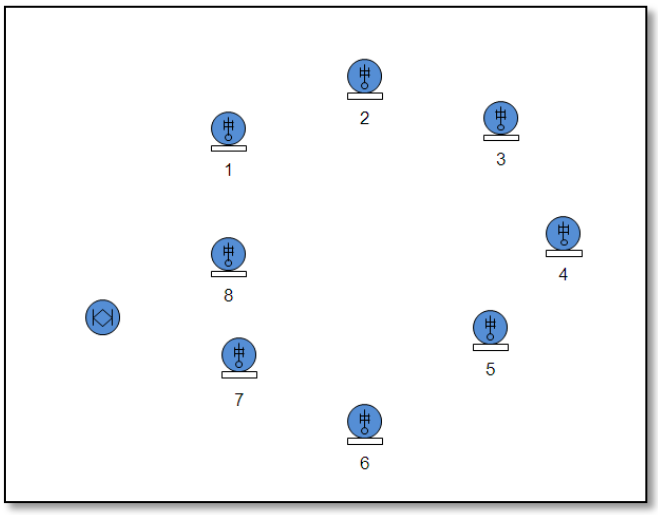
Фиг.3 Линейна огнева позиция

– с градация - оръдията са разположени на различни интервали и отстъпи в прекъсната линия (фиг. 4);



Фиг.4 Огнева позиция с градация на интервалите

– разпръснато – разположението е във вид на геометрични фигури, (окръжност, правоъгълник, трапец) (фиг. 5).



Фиг.5 Разпръснато местоположение

В **чешката артилерия** разстоянието между оръдията може да бъде 30 - 50 m, а между минохвъргачките до 40m. Ако е възможно се използва естествено прикритие, а отделни оръдия (минохвъргачки) се разпръскват в района на огневата позиция. Размерът на огневата позиция на артилерийската батарея е 500-800м по фронта и 300-500м в дълбочина.[9]

Съществуват редица фактори, влияещи на избора на интервали и отстъпи на оръдията на огневите позиции.

3. Фактори, влияещи на избора на конфигурация на огневата позиция

Факторите, влияещи на избора на конфигурация на огневата позиция са поставената задача, настоящия противник, релефа на местността, използваното формирование (оръдие, взвод или батарея) и наличното време за заемане.[8] Основният акцент е върху поставената задача и противника. Като най-голяма заплаха за оръдията на огневата позиция се явяват контрабатарейната борба, авиационните средства, наземния противник и радиоелектронното въздействие върху средствата за комуникация и автоматизация. За да се противопостави на тези заплахи, командирът на огневия взвод (старши офицерът на батареята) трябва да вземе предвид възможните техниките на разполагане на оръдията, способността за бърз маньовър за напускане на огневата позиция и маскировката.

Съгласно т.65 на Ръководството по бойна работа на огневите подразделения от артилерията, оръдията се разполагат по възможност на еднакви интервали и отстъп вляво (вдясно) или в линия. Допускат се и други видове разполагане на оръдията:

- с ъгъл напред (назад);
- с полукръг напред (назад);
- във вид на друга фигура.

Това дава основание за използване на различни техники за конфигурация на огневата позиция, но в т.256 от същия документ е записано, че отстъпите трябва да не са значителни (не повече от 1/3 от интервала между оръдията, което за интервал 20-40 m е 9-15 m). Анализирайки важността на запазване на живучестта на огневите формирования е необходимо да се разгледат възможните форми на разполагане, зависещи от евентуалната заплаха.

При контрабатарейната борба и заплахата от въздушна атака оръдията е необходимо оръдията да се разсъсредоточат върху голяма площ и да се увеличи максимално естественото прикритие на местността. Този тип позициониране на оръдията се нарича разполагане съгласно местността (фиг. 6). Тогава изискването на т. 256 не може да бъде изпълнено, защото ще се получат различия, превишаващи значително изискванията т.256. Най-подходящо е този тип разполагане

да се прилага при огневи позиции с възможност за определяне на координатите на всяко оръдие и наличие на автоматизирана система за управление на огъня.

Фиг. 6 Разполагане на оръдията съгласно местността

Наземните противникови атаки, заплахите от партизански единици и специални сили могат да накарат командира на огневия взвод (старши офицера на батареята) да разположи оръдията в тесен и защитен район. При тези обстоятелства ще е удачно разполагането на оръдията на огневия взвод във вид на диамант или ромб (фиг. 7) или звезда за батарея (фиг. 8). Както при предишния способ, така и при този се получават различия при интервалите и отстъпите спрямо зададените. Този тип разполагане осигуряват отлични възможности за кръгов обстрел 360° (60-00) и отбрана.[8]

Фиг. 7 Разполагане на оръдията на взвода във форма на диамант или ромб

Фиг. 8 Разполагане на оръдията на батареята във форма на звезда

Линейното разполагане (фиг. 9) може най-добре да се използва в ситуации на ограничено време, когато се изисква незабавна огнева поддръжка. При това разполагане формированията

осигуряват групираност на разривите в зоната на целта, а командването и контрола са подобрени. Използва се от всички модификации на въоръжението. Това разполагане е най-добро при неавтоматизиране на управлението на огъня, поради липса на отстъпи и наличие на приблизително равни интервали между оръдията. с изпълнени изискванията от 20-40 m. Като недостатък може да се отбележи лесното разкриване на местоположението на огневата позиция и уязвимостта от въздушни атаки.

Фиг. 9 Линейно разполагане на оръдията

Заключение

Обобщавайки представеното съдържание, трябва да се отбележи, че разположението на артилерийските оръдия на огневата позиция има решаващо влияние за непрекъснатостта на огневата поддръжка и живучестта на формирването. Въпреки многобройните предимства, произтичащи от разнообразното разположение на артилерийските оръдия, не бива да се забравя за недостатъците на вариантите за огневи позиции. Голям проблем е фактът, че голяма част оръдията (отделни гаубици 2С-1 „Гвоздика”, бойните машини БМ-21 „Град”, оръдие-гаубици Д-20 и миновъргачките в българската артилерия) не са оборудвани с GPS приемници, които автоматично биха определили позицията им на местността. Несъмнено липсата им влияе както на времето за готовност за откриване на огън, така и за работата на огневата позиция.

Противоречията в националните документи за различните размери на интервалите между оръдията и посочените отстъпи спрямо тях влияят негативно при практическото изпълнение на поставените задачи при подготовка и заемане на огнева позиция от личния състав от огневите формирования на артилерията. Това довежда до мисълта за прецизен национален анализ за стойността на тези величини за всеки вид оръдие, както и отчитане на наличието на GPS приемници.

Използвана литература:

1. Атанасов А. Действие на артилерията за обща поддръжка в операциите. Военна академия „Г.С.Раковски”. Конференция - 130 г. Артилерия. София. 2009 г. ISBN:978-954-509-491-0 стр.317-326

2. Ръководството за използване на полевата артилерия – артилерийски дивизион. „Военно издателство” ЕООД, 2009г.

3. Ръководството по бойна работа на огневите подразделения от артилерията. Издателство на МО „СВЕТИ ГЕОРГИ ПОБЕДОНОСЕЦ”. София. 1994

4. Сидеров В. Ефективност и ефикасност на подготовката на военнослужещите с моделиране и симулации, Годишник на Факултет командно-щабен, Бр.1/2012 – София, Военна академия „Г.С. Раковски“, с. 71 – 75 ISSN 13122991.

5. Чалъков Р. Полевата артилерия – от черешовото топче до автоматизираните системи за управление на огъня. Международна научна конференция - 105 години знание в интерес на сигурността и отбраната. Сборник доклади от международна научна конференция. Военна академия „Г.С.Раковски”. София. 2018 г. (стр. 195) ISBN 978-619-7478-00-6

6. Руководство по боевой работе огневых подразделений артиллерии, Военное издательство, Москва 2002

7. Савкин С.А., В.Г. Рынгач, А.Д. Лигун, Основы боевого применения артиллерийских подразделений. Учебное пособие. Тольятти. ТГУ, 2008.

8. FIELD MANUAL HEADQUARTERS No. 6-50 DEPARTMENT OF THE ARMY MARINE CORPS WARFIGHTING PUBLICATION UNITED STATES MARINE CORPS No. 3-1.6.23 https://www.myarmypublications.com/images/FM650.pdf

9. KALINA M,K. ŠILINGER, Studijní opora. PROJEKT JE SPOLUFINANCOVÁN EVROPSKÝM SOCIÁLNÍM FONDEM A STÁTNÍM ROZPOČTEM ČESKÉ REPUBLIKY. https://docplayer.cz/42977684-Zpracoval-pplk-gst-ing-milan-kalina-npor-ing-karel-silinger-ph-d.html

10. Szalla A., Struktura organizacyjna oraz ugrupowanie bojowe pododdziałów artylerii, ZESZYTY NAUKOWE WSOWL, Nr 1 (155) 2010, ISSN 1731-8157

Hristo A. Desev,

ENERGY CRITICAL INFRASTRUCTURE RISK ASSESSMENT TECHNOLOGY

Hristo A. Desev

National Military University “V. Levski”, Artillery, “Air Defense and CIS” Faculty
Shumen, “K. Scorpil”str. № 1

***Abstract**: Increasing cyberattack capabilities against critical energy infrastructures qualitatively alters cyberspace and puts security systems at the heart of the challenge. The report proposes consistency technology to detect and assess the risk of cyber threats to infrastructure. The mechanisms for optimal protection of these sites and maintenance of their functioning are disclosed.*

***Keywords:** Energy security, criterion, mhe threat model, threat analysis.*

ТЕХНОЛОГИЯ ЗА ОЦЕНКА НА РИСКА НА КИБЕРБЕЗОПАСНОСТТА НА ЕНЕРГИЙНАТА КРИТИЧНА ИНФРАСТРУКТУРА

Христо А. Десев

Национален военен университет „В.Левски“, Факултет „Артилерия , ПВО и КИС“

Енергийната сигурност е ключов аспект от Националната и глобалната сигурност, а енергийната информационна сигурност е от особено значение за нормалното функциониране на обществото и критичната инфраструктура. Енергийната инфраструктура е била винаги обект на специална защита поради няколко фактора свързани с промените в основните характеристики на енергийната инфраструктура, неопределеността в заплахите, средата за сигурност и преразпределението ролите и отговорностите между държавата и частния сектор. Самото понятие критична инфраструктура се тълкува в широк диапазон на различните обществени сфери, но най-често засяга съвкупността от обекти (физически и виртуални), които могат да доведат до значителни загуби на безопасността на нацията. Изследването на заплахите срещу критичната енергийна инфраструктура има съществено значение за икономика на страната и засяга основно сложните взаимовръзки в общата фактическа инфраструктура. [3]

Установяването на риска от срив на всяка критична инфраструктура е производна на анализа на заплахата и уязвимостта. Повишаването на възможностите за провеждане на кибератаки срещу критичната енергийна инфраструктура качествено променя киберпространството и поставя системите за сигурност пред сериозно предизвикателство.

Рисковете за енергийната критична инфраструктура които са свързани с извън проектни и хипотетични заплахи са най малко изследвани. Отсъствието на статистически данни за инциденти и сложността и обширността на енергийната инфраструктура предполагат прилагане на семантичен подход за моделиране на екстремни ситуации в енергетиката. Основната характеристика на подходите за откриване на аномалии е способността им да откриват нови и нови атаки. Моделът на заплаха определя сценариите за заплаха със свързаните с тях разпределения на риска.[6]

Извънредните ситуации в енергийния сектор са предмет на енергийната безопасност и заплахите се явяват и реализират, като дефицит на ресурсите осигуряващи безпроблемно енергоизточниците. Според ранговката киберзаплахите са от стратегически характер по отношение на безопасността, като тези ситуации се усложняват от липсата на методически ред и регламентация за моделиране на тези заплахи.

Определянето на влиянието на киберзаплахите за възникване на екстремални ситуации може да се реши при спазване на подход за анализ на заплахата, оценка на риска и оценка на поддържащите системи. Подхода следва да включва три методики за работа:

- методика на анализа на киберзаплахите в енергийната критична инфраструктура;
- методика за формулиране на сценарии за развитие на ситуациите след атаката;
- методика за оценка на рисковете на нарушенията на кибербезопасността.

Всяка от методиките решава комплекс от задачи необходим за извличане на изводи за осъществяване на кибербезопасността. В първата се решават следните задачи:

- определяне на ситуацията (същността на проблема, контекста и др.);
- одит на безопасността, който включва:
  - ✓ анкетиране;
  - ✓ определяне на киберуязвимостите в IT сектора;
  - ✓ оценка на активите;
  - ✓ описание на заплахите;
  - ✓ формулиране на типови атаки;
  - ✓ създаване на концептуални сценарии.

Методиката за определяне на сценариите за критични ситуации се основава на системен анализ и изследване на енергийната безопасност при което се включват следните последователности:[5]

- формиране на концептуални сценарии и техните взаимни връзки;
- определяне на вероятните характеристики, критериите и условията на всеки сценарий;
- провеждане на експеримент;
- изработване на частен модел за всеки тип заплаха;
- анализ на алтернативните сценарии.

Методика за оценка на рисковете на нарушенията на кибербезопасността е ориентирана към:

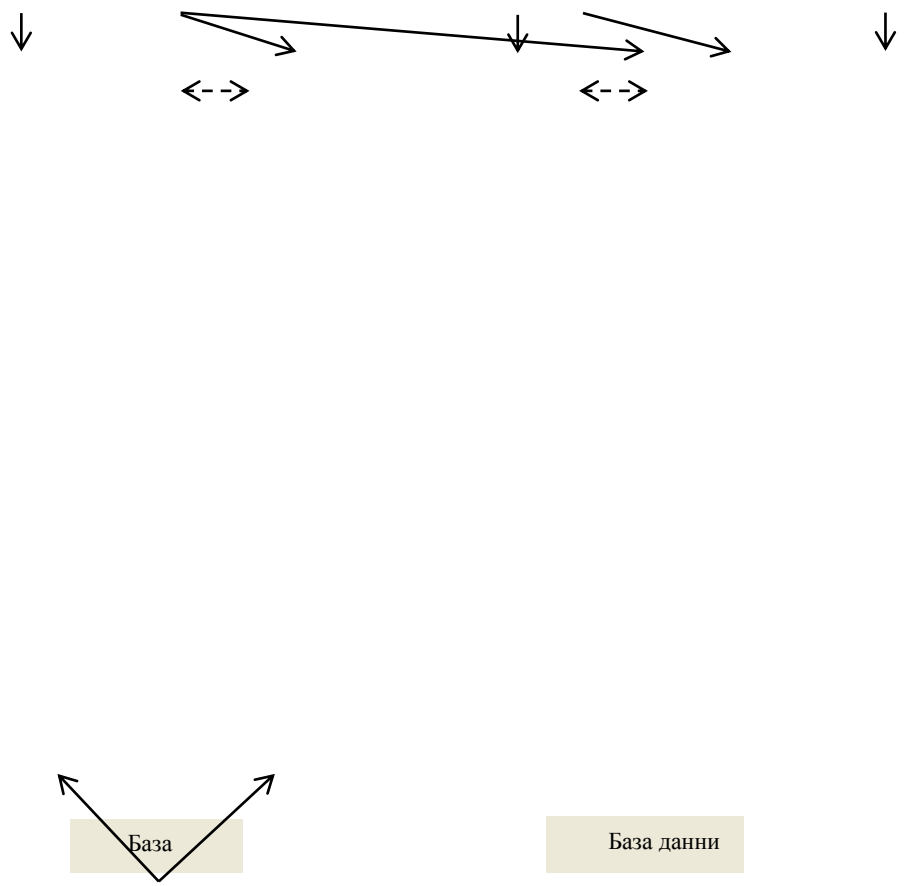
- описание на рисковете;
- качествена и количествена оценка на рисковете;
- ранжиране на обектите по определените критерии;
- оценка на каскадни аварии, безалтернативност на ресурсите и екологични заплахи.

Изложената методология предполага създаване на интелектуална система и технология за разкриване на киберзаплахите фиксира три основни блока: (Архитектура на технологията е представена на фигура 1)

- първи блок – за провеждане на одит за определяне на уязвимостите, актуализиране на заплахите и систематизиране на активите;
- втори блок – за формиране на сценариите, анализ на заплахите и последствията от евентуална реализация на заплахата;
- трети блок – за оценка на риска от настъпване (сбъдване) на екстремалната ситуация.

Технологията на анализа на киберзаплахите и оценката на рисковете от нарушения на кибербезопасността се реализира от алгоритъма за използване на системата. Той преминава през четири основни етапа:

1. Анализ на киберзаплахите:
   - одит на безопасността;
   - определяне на ситуацията;
   - формиране на концепция.



Фигура 1 Архитектура на технологията за разкриване на киберзаплахите

2. Моделиране на сценариите:
   - декомпозиране на заплахите;
   - определяне възможните сценарии на заплахата;
   - определяне на критериите;
   - оценка на вероятността з а проява на заплахата;
   - анализ на оценката;
   - определяне на частни модели на заплахите
3. Оценка на рисковете.
4. Ранжиране на обектите.

Основата на тази технология се опира на добре познатия цикъл на Деминг (PDCA). В детайли отделните етапи преминават през определени последователни стъпки , които позволяват да се разкрие заплахата и вероятните следствия от пробива в киберзащитата.

При анализа на киберзащитата се описват основните характеристики на обекта, описание на активите и обща идентификация на системата. Одитирането на безопасността завършва с определяне на количеството на критични компоненти, които са подложени на уязвимости. Формират се групи от критични активи съответни на заплахата и типовете атаки според зависимостта (1).

$$P = Vi.Tj.Ak.Ra \quad (1)$$

където: P - модел на атаката;
Vi – уязвимост на обекта;
Tj – заплаха за обекта;
Ak – целеви активи;
Ra – възможна големина на атаката.

На етапа на създаване на модел на сценариите те се оценяват по интегрални показатели за възникване на нежелана ситуация. Песимистичните сценарии се свързват с maxколичество загуби. Използва се типов сценарий за реализация на произволна киберзаплаха във вида: (2)

$$S = X^F.X^V.X^T.X^C \quad (2)$$

където:S – структура на сценариите за екстремни ситуации;

X^F - променливи влияещи върху екстремните ситуации;

X^V – променливи обозначаващи активите и техните уязвимости;

X^T – променливи за заплахите;

X^C – променливи отчитащи последствията.

Резултатите от анализа на сценариите са основание за формиране и вземане на решение за достигане на предпочитаното крайно състояние.

При оценката на риска той се интерпретира като съчетание на последствия от нежелани събития и възможности за тяхното възникване. При оценката се комбинират рисковете за информационните технологии и рисковете за аварии и катастрофи на сложни технологични системи. Откриването на уязвимостите позволява да се съчетава списъка с критични активи, които трябва да се осигурят с ресурси за постигане на ниво на безопасност.

Ранжирането на обектите се състои в подреждане на оценените обекти по определени критерии и ниво на риска. Разгледаната технология то се провежда първо по величината на риска за възникване на екстремни ситуации и след това по взаимозависимости с други обекти от инфраструктурата представени като последствия.

В заключение следва да обобщим, че предложената технология е насочена към определени обекти в енергетиката, които потенциално изложени на риска от нарушения в сектора за сигурност. В условията на законова неопределеност и неяснота по защитата на енергийната критична инфраструктура тя позволява да се определят високо рисковите нарушения на киберсигурността, последствията и техните вероятни стойности на загубите и ранжиране на изследваните обекти. Прилагането на предложената технология може да формира подходи за постигане на безопасност от киберпровокации, с които да се поддържа правилно функциониране на обектите.

References

1. Закон за киберсигурност, ДВ 94 от 13.11.2018 г.

2. Наредба за минималните изисквания за мрежова и информационна сигурност, постановление на МС № 186 от 19 юли 2019 г.

3. Dantu R. and Kolan P., 2005, Risk management using behavior based bayesian networks // intelligence and security informatics, стр. 165-184.

4. Gordon A., Hernandez C., Official (ISC)² Guide to the CISSP CBK.

5. Massel L.V. Konvergentsiia issledovanii kriticheskikh infrastruktur kachestva zhizni i bezopasnosti // Trudy VI Mezhdunarodnoi nauchnoi konferentsii ″Informatsionnye tekhnologii i sistemy″. 2017. S. 170-175.

6. Стоянова, В., Интернет на нещата-анализ на сигурността при интелигентни структури, , II International scientific conference confsec, Borovec, 2018, year 2, issue 2(4), ISSN print 2603-2945, ISSN online 2603-2953, http://confsec.eu/sbornik

7. Управление на енергийния сектор и енергийна (не)сигурност в България, С., 2014.,ISBN 978-954-477-216-1

Veliko P. Petrov, Stancho G. Stanchev,

HYBRID WAR, THE MOST MODERN CONCEPT OF MILITARY CONFLICTS

Veliko P. Petrov, Stancho G. Stanchev

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

***Abstract**: This report aims to introduce readers to the "hybrid war", which is the most modern version and form of military conflict that uses all the means and methods of destroying the enemy known to mankind, from the oldest primitive to the latest technology for warfare. The modern understanding of hybrid war is linked to the unclear boundaries between peace and war between state and non-state, between private and public, as well as changes in traditional actors and elements of war. Hybrid war is above all an aggression against the sovereignty and independence of a country.*

***Key words:** hybrid war, military conflict, concept*

ХИБРИДНАТА ВОЙНА – НАЙ-МОДЕРНАТА КОНЦЕПЦИЯ ЗА ВОДЕНЕ НА ВОЕННИ КОНФЛИКТИ

Велико П. Петров, Станчо Г. Станчев

"*Да победиш врага си, без да се биеш, е върхът на военното изкуство*".
Сун Дзъ, IV в. пр.н.е.

В политическия лексикон терминът „хибридна война" стана популярен през пролетта на 2014 г. след началото на военния конфликт в Източна Украйна. В най-общ смисъл, с него се обозначават действия на някоя велика държава, осъществявани зад гърба на иррегулярни бунтовнически формации.

Всъщност „хибридната война" или по-скоро хибридните способи за водене на война не са измислени от сега, а водят началото си далеч назад във времето. Дори бегъл поглед в световната военна история дава основание за твърдението, че повечето известни ни войни са съчетание от различни способи, похвати, форми и тактики за водене на война, прилагани успоредно, последователно или самостоятелно. Може да се спомене използването на неконвенционалните способи, съчетавани с чисто военни от войни като Троянската, войните на Римската империя, двете Световни войни, войната във Виетнам, Студената война, Ливан, Грузия, Украйна, Крим, Либия, Сирия, войната на глобалните терористи и особено на Ислямска държава на няколко фронта.

Възникналите през последните години военни конфликти, които започват с „мирни" антиправителствени акции и завършват с жестоки граждански войни и външна интервенция, могат да се определят като нов тип войни. Те излизат извън рамките на традиционните представи за война, придобивайки комплексен характер, превръщат се в заплетен възел от политически интриги, ожесточена борба за ресурси и финансови потоци, в непримирими цивилизационни сблъсъци. Съдържание на военните действия във войните от нов тип, каквито са хибридните, става не само физическото унищожаване на въоръжените сили на противника, а деморализацията и подчинява-

нето на своята воля на цялото население на държавата.

За създател на „хибридните войни" се смята френският крал Людовик XIV (1643-1715). По време на подготовката на войната за наследството на Пфалц (1688-1697), той стига до извода, че за Версай ще е по-удобно да действа в немските земи не пряко, а с помощта на зависимите от него германски князе. Така, в случай на поражение, Франция ще може, без да навреди на престижа си, да се отрече от тях, а на победа – да си припише заслугите за нея. Оттук следва и основният принцип на френската политика през следващия XVIII век: формирането на регионални силови баланси чрез използването на малки държави (включително, организирайки дворцови преврати в някои от тях) и насъскването им срещу вражеските велики сили[30].

Терминът „хибридна война" е възкресен от британския военен теоретик Базил Лидъл Харт през 1961, в рамките на формиращата се концепция за „гъвкавото реагиране". Разбирането за победата като принуждаване на противника към компромис (в условията, когато воденето на войни с непрекъснат фронт е невъзможно) предполага няколко начина за постигането и. Затова и самата концепия за „гъвкавото реагиране" буквално заимства опита на европейските войни през XVII-XVIII век и предполага следното:

– създаването на приятелски режими в малките държави на границата на противника или на собствената граница;

– войната за изтощаване на противника;

– нанасяне на локално поражение на противника, което да го убеди, че е безсмислено да продължи войната;

– обезценяване на ресурсите на противника.

Всички тези стратегии за постигане на победа възкръснаха в рамките на възприета през 1961 г. американска стратегия за „гъвкаво реагиране", която и до днес си остава фундамента на военно-политическата стратегия на САЩ. В основата на тази стратегия са заложени три компонента:

– *сдържане* (т.е. убеждаване на противника, че евентуални агресивни действия от негова страна са безмислени заради заплахата да му бъдат нанесени неприемливи загуби);

– *ескалираща доминация* (убеждаване на противника в превъзходството на САЩ в случай, че започне война);

– *принуждаване* (локално използване на сила с цел нанасяне поражение на противника на определен театър на военни действия).

Когато през 2014 г. беше зает Крим от така наречените „зелени човечета", светът за пръв път се сблъска с една привидно нова форма на война, а именно „хибридната война". Предприетите от Русия комплексни действия срещу Украйна на практика демонстрират, че правилно планираният и реализиран общ стратегически подход гарантира постигането на необходимия ефект на объркване и неяснота. Умелото избягване на директен военен сблъсък, базиран на цялостна стратегия, осигури на Москва необходимата свобода на действията и спомогна за изпълнението на поставените задачи.

Приложеният в Украйна руски модел е представен в началото на 2013 г. от армейски генерал Валерий Герасимов в доклад за развитието на формите и способите на използване на въоръжените сили. В него се отчита, че правилата за водене на съвременната война съществено са променени, като е нараснала ролята на невоенните способи за постигане на стратегическите цели. Акцентира се на прилагането на политически, икономически, информационни и други невоенни мерки с използване на потенциала на местното население. Фронталният сблъсък на крупни групировки от войски на стратегическо и оперативно ниво се очаква постепенно да отпадне, а широко приложение да получат асиметричните действия, които включват сили за специални операции, провеждане на пропагандна кампания и подкрепа на опозицията в страната.

Днес „хибридната война" е най-модерната версия и форма на военен конфликт в който се използват всички познати на човечеството средствата и методи за унищожаване на противника,

30 Алексей Фененко, Войните на бъдещето, списание „Геополитика", януари 2018 г., стр. 4.

от най-старите примитивни до най-новите технологии за водене на война. Съвременното разбиране за хибридната война се свързва с неясните граници между мира и войната между държавното и недържавното, между частно и публичното, както и промените в традиционните участници и елементи на войните. Хибридната война е преди всичко агресия срещу суверенитета и независимостта на една държава.

Терминът „хибридна война" няма ясна и единна дефиниция, а обобщава в себе си няколко значения – „комплексно и нетрадиционно водене на война", а също и „аморфно" водене на война. За някои военни стратези понятието отразява своеобразна еволюция на войната, която се състои в това, че към класическите действия се включват нетипични и асиметрични стратегии и тактики, които целят да ерозират националния суверенитет и да попречат на намеренията на дадена страна, заключаващи се в независими решения и проекти.

„Хибридна война" е всякакво умишлено и целенасочено въздействие, от всякакъв характер, в условията на противоборство между страните, обхващащ една, няколко или всички области на въздействие, с цел постигането на планирана междинна или крайна цел.

Възможните определения за „хибридна война" (хибридния характер на войните): неконвенционална война; модерна война, обединяваща конвенционалната с „гореща"; високотехнологична война; етап от конвенционалната война; война от ново поколение; съчетание от различни способи, форми и тактики за водене на война или тотална война.

Тя не е ново откритие на военните, а естествена еволюция на войната. В противовес на съсредоточаването на сили, огън и маньовър от конвенционалната война, по-слабите икономически страни изобретиха асиметричния начин за водене на бойни действия. В отговор на това беше създадена концепцията за изпреварващ, превантивен удар за борба с тероризма и всеобхватния подход на НАТО към операциите. При тази концепция се обхващат всички аспекти при управлението конфликти и е от ключово значение синхронизирането на действията на въоръжените сили с всички правителствени и неправителствени структури в рамките на единна стратегия и план.

В Русия хибридната война е описана през 50-те години в монографията на полк. Евгений Едуардович Меснер[31] „Метежна война (бунтовническа война)". Евгений Меснер обръща внимание на процеса на размиване на различието между състоянието на мир и състоянието на война, посочва как се заличават границите между редовните военни подразделения и паравоенните формирования, включително и между недържавните, специални въоръжени социални групи, например престъпните, въоръжени формирования на търговски компании, партийните бойни подразделения и обществено-политическите организации. През последните години характерните черти на практическото използване на концепцията за метежните (хибридни) войни, обогатени с нови технологични разработки (които Меснер предсказва още през 60-те години на XX век, когато пише, че по време на война ще се използват „електронен мозък" и съвременни технологии), можеха да се видят не само в Украйна, но и по време на войната в Сирия.

През 1999 г. китайската армия също създаде асиметрична стратегия наречена „Неограничена война" (или „война без граници"), която включва бойни действия във всички съвременни пространства на бойното поле. Други специализирани източници определят хибридната война, като разновидност на дифузната война (разпръсната война), която е модерна версия на въоръжената битка и дава възможност да се прави всичко, което е забранено при традиционните военни действия.

Първата научна разработка (изследване) се появява през 2008 г. в Американски държавен военен колеж за Ливанската война от 2006 г. В това изследване „Хизбула" е оценена като посилна и ефективна от всяка друга арабска армия. Експертите използват формулировките „*хибридно водене на война*" от Хизбула, или „*комплексно иррегулярно водене на война*", което е нараства заплаха за израелските и американски въоръжени сили. Бунтовническата организация съчета-

31 Евгений Едуардович Меснер (1891–1974) е офицер-артилерист от Руската императорска армия и е един от крупните военни теоретици на 20-ти век. Започва да се занимава с научна работа от 20-те години на миналия век. През 50-те създава в Аржентина Институт за изследване на проблемите на войната и мира.

ва стари тактики с конвенционални военни тактики и модерни оръжейни системи. В изводите се посочват, че „недържавни актьори" могат да водят конвенционална война и да я съчетават с други средства, а американските въоръжени сили трябва да се готвят едновременно както за конвенционална, така и за асиметрична война.

Днес „Хибридната война" е най-модерната версия и форма на военен конфликт в който се използват всички познати на човечеството средствата и методи за унищожаване на противника с използването на най-новите технологии за водене на война. В света винаги има война, а въоръжената борба е само една от формите (фазите) на войната. Нейната същност е война на недържавни военни формации срещу държавата и без официалното участие на правителствени въоръжените сили по метода на въоръжено нашествие. Военните експерти описват новия начин на водене на война с термина „война на управлявания хаос".

Технологията на „управлявания хаос" без оглед на конкретния регион, в който се прилага, обикновено залага на следните елементи: информационните войни, кибератаките и шпионажа, корупционното управление, разпалването на националните и религиозни конфликти, стимулирането на различните форми на сектантство, прокарването на фалшиви ценности и ерозията на националните и културни основи на съответната общност. Целта на тази „мека" агресия е преформатирането на неудобните държави, трансформацията на масовото съзнание, понижаване съпротивителния потенциал на обществото и неговата способност да се самоорганизира и лишаването му от историческа памет.

Във второто десетилетие на XXI-ви век ролята и значението на *концепцията за хибридната война* придоби особена популярност. Хибридната война си поставя за цел не унищожаване на противника, а силово завземане на властта в страната за преразпределение на ресурсите и ролите в обществото от новото правителство в интерес на друга страна. В съвременната война основната печалба не са ресурсите, територията или властта на победената нация, а новите промени в националния и манталитет. Победителят в тази война печели бъдеще за своята цивилизационна култура.

Целите на хибридната война са междинни и крайна. Междинните цели на хибридната война са създаване на неблагоприятна среда за сигурност, нанасяне на вреди или поражения, постигане на срив или неблагополучия в обекта на въздействие, а крайната цел на хибридната война е постигане на превъзходство над опонентна държава или група държави и налагане на собствената ценностна система. След постигането на крайната цел има ново преразпределение на сферите на влияние, на пазарите, суровините, енергийните източници, морското, въздушното и космическото пространство, териториите, населението и съюзите.

Хибридни войни, се водят между високо технологично развити противници, използващи асиметрични средства и методи за водене на въоръжена борба. В същността си хибридната война представлява различен тип нетрадиционна война, в която се използва уникална комбинация от заплахи за въздействие върху уязвимите места на противника.

Действията на Русия в и около Украйна показаха прилагането на сложен модел на държавно ръководена хибридна война, адресирана към отслабване на всички лостове на легитимната власт чрез синхронизирано продължително прилагане на натиск с използване слабостите за причинявайки разстройство на основните държавните институции.

Страните на въздействие се явяват противници и чрез осъществяваните въздействия и контра въздействия се намират в противоборство. Страните на въздействие в хибридната война са следните:

– *страна субект на въздействието* – приносителя (осъществителя) на въздействието;

– *страна обект на въздействието* – потърпевшия, засегнатия от въздействието.

Може да се очертаят от събитията в Украйна и Сирия няколко основни методи на хибридната война:

– въоръжено нашествие и традиционен сблъсък със смъртоносни оръжия;

– конфронтация в областта на дипломацията;

– провеждане на информационни операции;

– провеждане на психологически операции;
– финансовата и икономическа война;
– масово използване на кибератаки;
– жестоко технологично противоборство;
– идеологически сблъсък на културно и религиозно ниво;
– поведенческа война – целенасочено въздействие върху поведението на големи групи и структури в противостоящата страна, които са потенциални източници на заплаха;
– местни граждански конфликти съпроводени с терористични атентати, масови кланета, грабежи и страх. Тотална въоръжена борба срещу всички несъгласни, под лозунга на борба със съществуващия недемократичен режим или лидер.

Възможностите на войската се използват за бързо и ефективно внедряване и поддържане на контрол върху дадена територия на различни места и региони. Военните сили са необходими и за да гарантират новото национално статукво. В даден момент елемента военна сила може да включи и да допълни въздействието на невоенните инструменти, активирани преди това.

Възможните способи за водене на „хибридната война" са:
– разузнаване, контраразузнаване;
– оперативно проникване;
– информационни, дезинформационни, контрадезинформационни;
– идеологически;
– пропагандни;
– психологическо въздействие;
– демонстрационно-показни;
– преднамерено насочване на мигрантски потоци;
– някои видове тероризъм (технологичен, религиозно мотивиран, децентрализиран, енергиен, самоубийствен).

ХВ може да се прояви в следните области на въздействие:
– политика;
– икономика;
– институции и държавност;
– енергетика;
– финансова система;
– военна област;
– ресурси;
– екология;
– международни отношения;
– вътрешни работи;
– отношенията между социалните групи в рамките на държавата;
– духовните, религиозни и общообразователни устои;
– и много други;

Базови условия за успех в хибридната война:
- слабо правителство;
- международна изолация;
- разделение в обществото;
- икономика в упадък;
- слаби и деморализирани структури за сигурност;
- приятелски опозиционни сили;
- наличие на етническо или религиозно малцинство

Типични фази на хибридната война:
– *подготвителна* (продължава до няколко години) – изграждане на идеологическата, политическата и военна база за предстоящата агресия;
– *активна* (продължителност до 1 година) – осъществяване на скрита агресия;

– *заключителна* (неограничена продължителност) – консолидиране позициите на агресора.

За хибридната война може да се посочат следните основни характеристики:

- ***цивилизационна*** – това е сблъсък на културно ниво за правото на съществуване на определен социум;
- ***глобална*** – води се навсякъде по света. Заявява се, че бъдещите войни трудно ще намерят непознат противник и непознато място за провеждане на бойните действия. Войната в условията на протичащата глобализация се води за правото на съществуване на отделните цивилизационни групи и се използват всички конвенционални и неконвенционални методи навсякъде по света до пълно унищожаване на противостоящата страна;
- ***универсална*** – налице е постоянно увеличаване на интензитета на всички фронтове и театри на войната, където противниците използват традиционни, нетрадиционни и хибридни стратегии, за да заплашват жизнените интереси на противостоящите сили. Армията е необходимо да бъде в постоянна готовност за всякакво развитие на ситуацията, навсякъде по света, с всякаква възможна структура на военни съюзи и формати;
- ***хибридна*** – използват се всички познати до сега средства и методи за водене на война;
- ***дифузна*** – взаимно проникване на организационна, технологична и информационна основа, т.е. това е пътят на война цивилизована, инстинктивна, от държавни организирани форми на въоръжена борба, регламентирани с военни закони и военна етика, до общ геноцид на хора на територията на противника;
- ***всеобхватна*** – наличие и на вътрешен враг;
- ***инвазията*** е от типа на мрежова война без контролен център;
- ***недържавните сили*** са срещу държавата и нейните институции;
- ***прилагат се масово информационните и психологическите операции***;
- ***масово използване на всички видове тероризъм*** като част от общата стратегия за постигане на целите.

Хибридната война е военно-политическо явление. Тя включва пропагандни действия, разузнавателни действия и шпионаж, организиране на масови безредици в страната. Този вид война прави и „неконвенционален" политически и икономически натиск върху държавата в международната политическа арена. Хибридната война е все още неясно и трудно разграничимо понятие. Въпреки това е налице тенденция за все по-голям фокус върху тази концепция както в публичното пространство, така и в експертните изследвания. Свидетели сме на прехвърляне на взаимни обвинения между водещите глобални сили за това коя от тях използва хибридната война и по какъв начин. Опитите за обяснение на почти всяко вътрешни проблеми (обикновен социален протест, изборни изненади, обществени разногласия, икономически проблеми и др.) биват прехвърляни върху евентуалния външен враг и използваните от него хибридни средства. Хибридната война се явява лесно обяснение и става отговор за причините за тези проблеми, което води до усещане за несигурност и постоянен конфликт.

Измеренията на „хибридната война " са от местно към регионално и глобално ниво, а действията могат да бъдат насочени към постигане на цели от тактически до стратегически мащаб, които да променят (модифицират) политическа ситуация в държави или региони, вкл. чрез създаване на условия за повлияване на развитието на обществени, политически и/или икономически процеси.

ИЗПОЛЗВАНА ЛИТЕРАТУРА:

1. Алексей Фененко, Войните на бъдещето, списание „Геополитика“, януари 2018 г.

2. Нурышев Г.Н., Доктрины „управляемого хаоса“ в современной глобальной геополитике, Научный журнал НИУ ИТМО, Серия: „Экономика и экологический менеджмент“, 2014. № 1.

3. Петко Димов, Основни характеристики на оперативната среда и алгоритъм на хибридната война, списание „Военен журнал“, бр. 1, 2016 г.

4. Любомир Монов, Руският модел за хибридната война, списание „Военен журнал“, бр. 3, 2015 г.

5. Христов Н., Хибридните заплахи – новото предизвикателство пред сектора сигурност – Военен журнал, 2014, № 4, с. 102.;

6. Атанас Ст. Атанасов, Един вариант за динамично обучение на слушателите във Военна академия, ВА „Г.С.Раковски“, годишна конференция на факултет „Командно-щабен“, 2016 г., ISSN 1312-2991 с. 115 .

7. Илиан Алипиев ,Измененията в средата за сигурност и прилаганите нови форми, методи и средства за противоборство. Хибридна война, Проблеми на сигурността и реформа в сектора за сигурност, бр. 30, София 2015, ISSN 1314-5754.

8. Калоян Илиев, Станчо Станчев, Specifics of contemporary armed conflicts, International Scientific Conference факултет “А, ПВО и КИС октомври 2015, ISSN 2367-7902

9. Боян Хаджиев, Хибридната война – същност, предпоставки и противодействие, списание Икономически и социални алтернативи, бр. 2 2019 г., https://www.unwe.bg/uploads/Alternatives/Xadjiev11_Alternativi_BG_br_2_2019.pdf

Stancho G. Stanchev, Veliko P. Petrov,

FORMATION OF CREATIVE PERSONALITIES IN THE SYSTEM OF PROFESSIONAL QUALIFICATION OF ARTILLERY SPECIALISTS

Stancho G. Stanchev, Veliko P. Petrov

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

***Abstract**: The focus of the report is the work on improving the quality of training, which is achieved through a balance and interconnection between the motivation of teachers, cadets and the introduction of innovative teaching methods.*

***Key words:** education, organization of the learning process, teaching.*

ФОРМИРАНЕ НА ТВОРЧЕСКИ ЛИЧНОСТИ В СИСТЕМАТА ЗА ПРОФЕСИОНАЛНА КВАЛИФИКАЦИЯ НА АРТИЛЕРИЙСКИТЕ СПЕЦИАЛИСТИ

Станчо Г. Станчев, Велико П. Петров

Променящите се основни параметри на международната и националната сигурност определят нови по характер и съдържание изисквания към Въоръжените сили и военния професионализъм. Като сложен комплекс от качества, професионализмът зависи от редица фактори и условия, изисква значителни усилия, време, талант, упоритост и организираност. Неговата основа се залага в системата на обучение и възпитание във военния университет, проверява се и се утвърждава във военната практика и дава своите резултати на един по-късен етап от развитието на офицерската професия.

Комплексното изучаване на реализацията на випускниците от специализация полева артилерия във военните формирования, оценката и реакцията на съответните командири поставя проблема с професионалната квалификация на артилерийските специалисти и по-специално практическите навици и умения, организационните способности и качества за ръководство и управление на подчинените подразделения. Ето защо е необходимо привеждането на образователната дейност в съответствие с тези изисквания и потребности на военните формирования. Това поставя на преден план въпросите за непрекъснатото усъвършенстване и актуализация на учебното съдържание на учебните програми.

При анализа на заложените в програмите цели и задачи за постигане, е видно, че на всяка учебна дисциплина са поставени две цели. Първата е да се дадат на обучаемите определени пълни и задълбочени познания по учебния материал, а втората е те да придобият навици и умения за извършване на определени практически действия. За осъществяването на тези две цели от обучаемите се изиска решаване на две важни основни задачи: да знаят и да умеят. Първата се постига чрез изучаване на теоретичен материал по основното съдържание на учебната дисциплина. Вто-

рата задача се постига чрез създаване на умения за поставяне на задачи на подчинените подразделения и тяхното управление в хода на операциите. Отделна задача е за създаването на умения за работа в екип. Смята се, че по този начин обучаемите ще придобият необходимите умения за качество в своята по-нататъшна работа, наречено майсторство. Ако се направи анализ на целите и задачите, залегнали в учебните програми, ще се види, че обучаемите на изхода от обучението си в НВУ ще бъдат добри изпълнители на задълженията си на първите длъжности във формированията. Това може да бъде много добро равнище за завършващите курсанти и тяхната реализация в малките тактически формирования - взвод и батарея, но дали е достатъчно?

Възниква въпросът придобитото майсторство при изпълнение на служебните задължения достатъчно ли е за качествена и ефективна работа в различните звена от йерархичната структура в армията. Отговор може да се получи, ако се анализира цялостната дейност в работата на артилерийските специалисти - особено при тяхното обучение в НВУ. Изводите са, че „компетентностите на обучаемите се получават като съвкупност от способности, качества и свойства, необходими за работа във военните формирования".

Обучението за творческо прилагане на съвременни методи за изпълнение на поставените задачи следва да стане основна и най-важна част от целия образователен процес. Това може да се постигне само ако обучаемите се учат да бъдат творчески личности и всяка задача се решава с прилагане на творчество, без да се повтарят стари постулати.

Творческото мислене във военното дело е насочено към разработване и внедряване на нови способи и форми на въоръжената борба, усъвършенстване на обучението и възпитанието на личния състав, към ефективно използване на въоръжението и техниката, поддържане на висока бойна готовност на формированията за изпълняване на задачите и др.

Творческата активност на военнослужещите е една от важните задачи при тяхното обучение и в практическата им дейност. Ето защо в постигането на творческо мислене от обучаемите в НВУ възникват много въпроси, които следва да се решават в процеса на тяхното обучение и формирането им като лидери и творчески личности. В творческия процес се определят няколко важни етапа: възникване на проблем; търсене на идеи за неговото решаване, доказателства и разработване на идеите за конкретизиране на проблема; реализиране на идеите и формулиране на препоръки за бъдещи действия. При решаването на даден проблем възникват противоречия между желаното и действителното, наличното и исканото, целта и ограничените средства за постигането й и др. Много често обучаемите следва да използват своята интуиция и да правят аналогии с други дейности. В хода на обучението трябва да се учат да издигат своите идеи, първоначално като хипотези, които са нужни за доказателства и потвърждаване на идеите.

Формирането на творчески личности и сложността в обучението предполага редица особености в цялостната дейност за тяхното създаване.

Първо, творчеството се характеризира с много сложна дейност, съставена от няколко елемента: научно творчество (познаване на закономерностите на въоръжената борба, бойната обстановка и тяхното влияние върху морално-психическото състояние на личния състав на своите подразделения и на противника); педагогическо творчество (умение да се оказва въздействие върху хората при подготовката и воденето на операциите); организаторско творчество (умение за сплотяване, за работа в екип, насочване на усилията към важните задачи и способност да се поема отговорност за взетите решения).

Второ, творчеството на военния ръководител се характеризира със силно ограничено време за решения и за тяхното изпълнение.

Трето, творчеството е свързано с висока отговорност за живота на много хора.

Четвърто, творчеството е свързано и с постоянно изменящата се обстановка в операцията, а това обуславя появата на нов проблем, който следва да се решава в дефицит от време и ресурси.

В хода на обучението трябва да се търси развитие на всички видове и равнища на творческо мислене. Това следва да се извършва в класните и извънкласните занятия. Възпитанието на обучаемите на творчество зависи не толкова от получените знания, колкото от способите за това и проявената степен на активност в този процес от обучаемите и преподавателите.

Това налага в хода на обучението да се прилагат все повече активните форми, които способстват в максимална степен за формиране на творческо мислене у обучаемите. Те не трябва да бъдат водени за ръка в детайлите на военната наука, а да се ръководи и развива творческото начало в тях. Защото самото натрупване на знания не означава, че могат самостоятелно и творчески да се прилагат. Ето защо обучението следва да е насочено към въпроси от страна на обучаемите, а и да се научат сами да търсят отговори на тях. Обучението може да се раздели на „индивидуално и колективно, което да отчита необходимостта от подготовката на лидери и да подготвя екипи за съвместна работа”. Само тогава ще се открие новото и ще се развие творческо мислене от бъдещите артилеристи.

За да се обучават на творческо мислене, на обучаемите следва да се поставят задачи за достигане на качество в дейността им, което да преминава през няколко стъпки на познавателната дейност: да знаят, да разбират, да използват, да анализират, да систематизират и да оценяват – приложение № 5. Следвайки тези стъпки, обучаемите в края на обучението ще се превърнат в творчески личности.

Майсторството и творчеството следва да се определят като главни критерии за ефективност в обучението на военните специалисти. Очевидно е, че за постигане на необходими умения за качество в работата „майсторството” има две важни стъпки: да се знае и да се умее, а за постигане на критериите за ефективност на обучението „творчество” е необходимо:

- изработване на определен стил на мислене, който позволява да се анализират проблемите и да се намери най-точното и икономично решение; обучаване на изкуството да се използват знанията; реализация на методите за организиране на мисленето и развитие на качества, създаващи от обучаемите творчески личности;
- обучаемите да умеят да ползват придобитите знания за решаване на проблеми, да са усвоили частните закони на различните науки и да ги привеждат в изпълнение в областта на военната наука;
- обучаемите да знаят, да разбират, да използват, да анализират, да систематизират, да проявяват творчество за постигане на определените цели.

Задачите, които трябва да осигурят достигането на този критерий, могат да бъдат: изработване на стил на мислене, позволяващ определяне на проблема и намиране на най-точното и икономично решение; обучаване на изкуство да се използват знанията; пълно реализиране методите на организаторско мислене и развитие на обучаемите като творчески личности. Това може да стане, ако вместо репродуктивно предаване на информация в хода на учебния процес се организират групови изследователски дейности за придобиване на нови знания. В такъв случай обучаемите ще бъдат ориентирани не към получаване на правилния отговор, а към разбиране по какъв начин е получен.

Този начин на мислене е основа, която осигурява не толкова получаване на определени знания, но и тяхното умело прилагане в практическата работа с цел осигуряване постигането на необходимите способности за изпълнение на поставените цели.

В програмите за обучение следва да намират място дисциплини, модули и теми, осигуряващи високо качество в теоретичната и практическата подготовка, обучение в създаване на способности за реализиране на новости, извършване на научноизследователска работа, които да осигурят постигане на критерия „творчество”. Справедливо е да се посочи, че в последно време „теоретиците на военната наука все по-често поставят въпроса, че е необходим принципно нов подход към конструирането и развитието на военната наука”. Това може да се реализира чрез нова образователна политика и тя да бъде една от приоритетните задачи за цялата система за професионална квалификация.

Основните стълбове за усъвършенстване на обучението на артилерийските специалисти се изразяват в:

- повишаването на мотивацията на преподавателите и обучаемите;
- повишаването на равнището на подготовка на преподавателите;
- внедряването на иновационни методи на обучение;

- информатизация на процеса на образователната дейност.

Повишаването на мотивацията на преподавателите и обучаемите е най-важното направление в дейността на занимаващите се с ръководство на системата за придобиване на професионална квалификация на артилерийските специалисти както и на научно-преподавателския състав. Да накараш някого да учи и мисли е невъзможно. Може да се принуди всеки да изпълнява формални дейности за обучаване и преподаване: да се идва навреме и да се присъства на занятия; да се напуска работното място след края на работното време; да се полагат предвидените по учебните програми изпити; да се разработват формални, без научна стойност курсови проекти, есета и др. Това обаче в никакъв случай не означава, че са постигнати целите на обучението, най-вече формирането на творческо мислене. Затова се изисква определена мотивация от участниците в образователния процес.

Нивото на мотивацията на преподавателите и обучаемите се определя от взаимосвързани и неразделни фактори:

- убеждението, че само висшето военно образование е това средство, което позволява успешно да се изпълняват целите на операциите;

- обучаемите трябва да разберат, че кариерното им развитие е резултат от техния труд, а не от наличие на диплома за завършено висше военно образование. Трябва да знаят, че то не дава право от само себе си да се заемат ръководни длъжности, ако не се стремят да се доказват непрекъснато, да се научат да анализират, да могат да вземат правилни решения в условия на неопределеност, прилагайки най-новите постижения на военната и другите науки, на поуките от практиката.

Интересът към обучението възниква в хода на правилната организирания и творчески насочен образователен процес, който зависи най-вече от начина на преподаване; непрекъснатото представяне на новости в теорията и практиката; вида, качеството и формите на учебните занятия по всички дисциплини; съотношението на активните и пасивните форми на занятията; предоставените възможности за самостоятелна работа и др.

Повишаването на равнището на подготовка на преподавателите определя тяхната мотивация и способности за овладяване и преподаване на необходимите знания на обучаемите, самостоятелност в разсъжденията, увереност в себе си, бърза и правилна ориентация в сложна и неопределена обстановка и способност да направят от себе си творчески личности. Само ако са такива, могат да създават от обучаемите творци, способни да вземат решения при възникване на кризисни ситуации и управляване на различни формирования при висока неопределеност на обстановката. От психологията е известно, че само личност може да създаде нова личност и само талант може да създаде и издигне нов талант.

Оттук възниква и една от главните задачи в системата за придобиване на професионална квалификация на артилерийските специалисти, чието изпълнение може да доведе до повишаване на ефективността в учебния процес - подготовката на преподаватели творци, а не търсещи репродуктивно мислене от обучаемите. Това изисква и непрекъснато повишаване знанията и уменията на преподавателите чрез самостоятелна работа и изпращане на курсове за повишаване на квалификацията у нас и в чуждестранни военноучебни заведения, ротация за работа в оперативните, включително в международни структури, които трябва да залегнат в перспективните планове за развитие на преподавателския състав на НВУ.

Внедряването на иновационни методи на обучение цели преминаване от майсторство към творчество. По този начин може да се постигне по-лесно и по-бързо овладяване на знанията и усъвършенстване на уменията, формиране на творчески светоглед, развиване на способностите да се вземат най-ефективни и икономични решения и да се работи в екип при ръководене на формированията.

Използването на различни методи на обучение трябва да е насочено към развиване познавателната дейност на обучаемите, под умелото ръководство на преподавателя. Все по-нарастващият обем от знания трябва да е съпроводен с увеличаване на изучаваните литературни източници, бързо ориентиране в научната информация в тях и творческото й извличане като изводи, препо-

ръки за доразвиване и начини на използване в практическата дейност.

Посредством прилаганите методи в обучението преподавателите трябва да се стремят да анализират и оценяват хода и резултатите от учебния процес, да правят необходимите корекции в учебните програми и учебното съдържание и непрекъснато да търсят новостите в преподавания материал. Те следва непрекъснато да създават проблемни ситуации и да организират подготовката на обучаемите за правилното и точното им изучаване, да осигуряват оптимално съчетаване на използването на готови изводи и препоръки и търсенето на научност при решаване на определени учебни задачи и прилагане на творчество в цялостната дейност.

Репродуктивният метод се реализира чрез непрекъснато даване на указания и провеждане на инструктажи за подготовка на всяко занятие и предполага непрекъснато ръководене на обучаемите от преподавателите в процеса на ученето. Най-често се съчетава с използване на обяснително-илюстрования метод, при който преподавателят обяснява учебното съдържание с онагледяване със схеми, графици, презентации и др. Репродуктивният метод обогатява знанията, уменията и навиците на обучаемите и поставя основите на формиране у тях на мисловни процеси, но не гарантира творческото им развитие.

Проблемният метод на обучение е съвременен и е насочен към формиране на самостоятелност, развиване на логическо, рационално, критично и творческо мислене и на познавателни способности. Този метод способства за развитие на интелекта на обучаемите, тяхната емоционална сфера, а на тази основа - за формиране на нов вид мислене. В това се заключава и главната разлика на проблемния метод от традиционния обяснително-илюстрован метод на обучение, който в момента е основен. При това проблемният метод на обучение предполага не само усвояване на резултатите от научното познание, но и на пътищата за постигане на познанието, с което се развива и творческата дейност на обучаемите.

За преподавателите от НВУ реализирането на проблемния метод на обучение следва да е приоритетна задача. Защото намаленото време за обучение и съотношението на лекции към други форми на обучение (30 % към 70 %) все повече затрудняват прилагането на обяснително-илюстрования метод и ефективността от него в бъдеще ще бъде много ниска.

Евристичният метод на обучение е специален и сравнително нов, който се използва за решаване на творчески задачи в процеса на откриване на новото. Той може да се прилага при провеждане на групови упражнения и решаване на тактически летучки, но е най-ефективен при военни игри и разработване на курсови проекти.

Изследователският метод на обучение е съвременен и предполага организация при провеждане на обучението, при която обучаемите са в положение на изследователи: самостоятелно определят и поставят проблема, търсят и намират методи за неговото решаване, изхождайки от известните данни, правят се изводи и обобщения, формулират се нови идеи, постигат се определени научни резултати, а не се търси готовият им вид. В зависимост от степента на сложност и подготовката на обучаемите се използват няколко нива на този вид обучение.

На първо ниво преподавателят поставя проблема и набелязва методи за неговото решаване, а обучаемите използвайки определени методи, се явяват само изпълнители.

На второ ниво преподавателят поставя проблема, а обучаемите сами търсят и намират методи за неговото решаване.

На трето ниво обучаемите самостоятелно формулират проблема, предлагат методи за неговото решаване и постигат резултат.

Този метод на обучение може да се прилага при разработване на курсови проекти, реферати, есета, при провеждане на изследователски учения, при участие в научни конференции и др.

Внедряването на иновационни методи на обучение зависи от степента на прилагане на информационните технологии в обучението. За целта е необходимо да се създаде единно информационно пространство в НВУ. Основни елементи могат да бъдат електронни учебници, електронни библиотеки и библиографски каталози и справочници, информационна и справочна система за всички новости в областта на военната наука, методически занятия за обмяна на опит в преподаването на различни учебни дисциплини, събиране и обобщаване на факти от практиката и офор-

мянето им като поуки за практическата работа, тестов контрол на обучението и др. При тези процеси повишаването на ефективността следва да се търси не чрез предаване на определени знания, а чрез тяхното придобиване след указания от преподавателите за нивото на изучаване на проблемните въпроси. Електронните учебници притежават редица предимства пред останалите източници. Те могат да се актуализират в съответствие с настъпили промени в учебното съдържание или в резултат на нови постижения на военната теория и практика, значително по-евтини са и са достъпни за всички обучаеми.

От това може да се заключи, че при организацията на учебния процес в конкретната ситуация е важно да се подходи креативно към избора на педагогическа концепция, за да се реализират принципите на творческо обучение. При това е необходимо да се вземат предвид целите и задачите на специфичното обучение на конкретните артилерийски специалисти, съдържанието на изучавания материал, нивото на усвояване, категорията на обучаемите и техния период на обучение, с други думи, в програмите за подготовка и обучение следва да намират място дисциплини, модули и теми, осигуряващи високо качество в теоретичната и практическата подготовка, обучение в създаване на способности за реализиране на новости, които да осигурят постигане на критерия „творчество”. Това може да се реализира чрез нова образователна политика и тя да бъде една от приоритетните задачи за цялата система за придобиване на професионална квалификация на военнослужещите.

ИЗПОЛЗВАНА ЛИТЕРАТУРА:

1. Атанасов А., Управление на знанието в системата на военното образование, 2010, стр. 129-131 СУБ Секция „Сигурност” ISBN: 978-954-9348-27-9.

2. Военна педагогика, ВИК „Св. Георги Победоносец”, София 1993.

3. Илиев, К., Подходи за обучение на бъдещи офицери в някои от водещите армии на НАТО. International Scientific Conference, Collection of papers, 2017, стр 453-459, ISSN 2367-7902.

4. Кацев, И., Проблеми на обучението, подготовката и сертифицирането на специалисти по информационна сигурност. *MATTEX 2018*, т 2, ч 1, стр. 164-169, ISSN: 1314-3921.

5. Ненов, Н., Традиции в обучението на артилерийските кадри. Артилерийска научна конференция, 2007.

6. Rogers, C. Freedom to Learn. Columbus. Ohio: Merrill, 1990.

Kaloyan A. Iliev,

AUTHORITIES FOR PLANNING AND MANAGING JOINT EFFECTS IN NATIONAL JOINT FORCE OPERATIONS

Kaloyan A. Iliev

*Faculty of Artillery, Air Defense and Communication and Information Systems,
National Military University, Shumen, Bulgaria, kacho_78@abv.bg*

***ABSTRACT**: Joint fire support planning and effects is a supportive process of the operational planning process and is directly relevant to the order and manner of conducting joint fire support and the order of impact on the objectives at the various stages and phases of the operation. The achievement of the required effects is directly related to the planning, coordination and execution of the tasks in the joint fire support, taking into account the expected and acceptable accompanying losses.*

***KEY WORDS**: Fire support, Effects, Planning process, Joint fire support.*

ОРГАНИ ЗА ПЛАНИРАНЕ И УПРАВЛЕНИЕ НА СЪВМЕСТНИТЕ ЕФЕКТИ В ОПЕРАЦИИТЕ НА НАЦИОНАЛНИ СЪВМЕСТНИ СИЛИ

Калоян А. Илиев

Въведение

Планирането на съвместната огневата поддръжка и ефектите се явява поддържащ процес на процеса на оперативно планиране и има пряко отношение към реда и начина за провеждане на съвместната огнева поддръжка и реда за въздействие върху целите в различните етапи и фази на операцията.

Ефектите играят решаваща роля в операциите на националните съвместни сили. Те определят фокуса на действията и допринасят за постигане на целите и желаното крайно състояние. Действията имат за цел създаване на ефекти, които да водят както до промени в способностите, поведението или вариантите за действие на участниците в рамките на оперативната среда, така и в стратегическата среда.

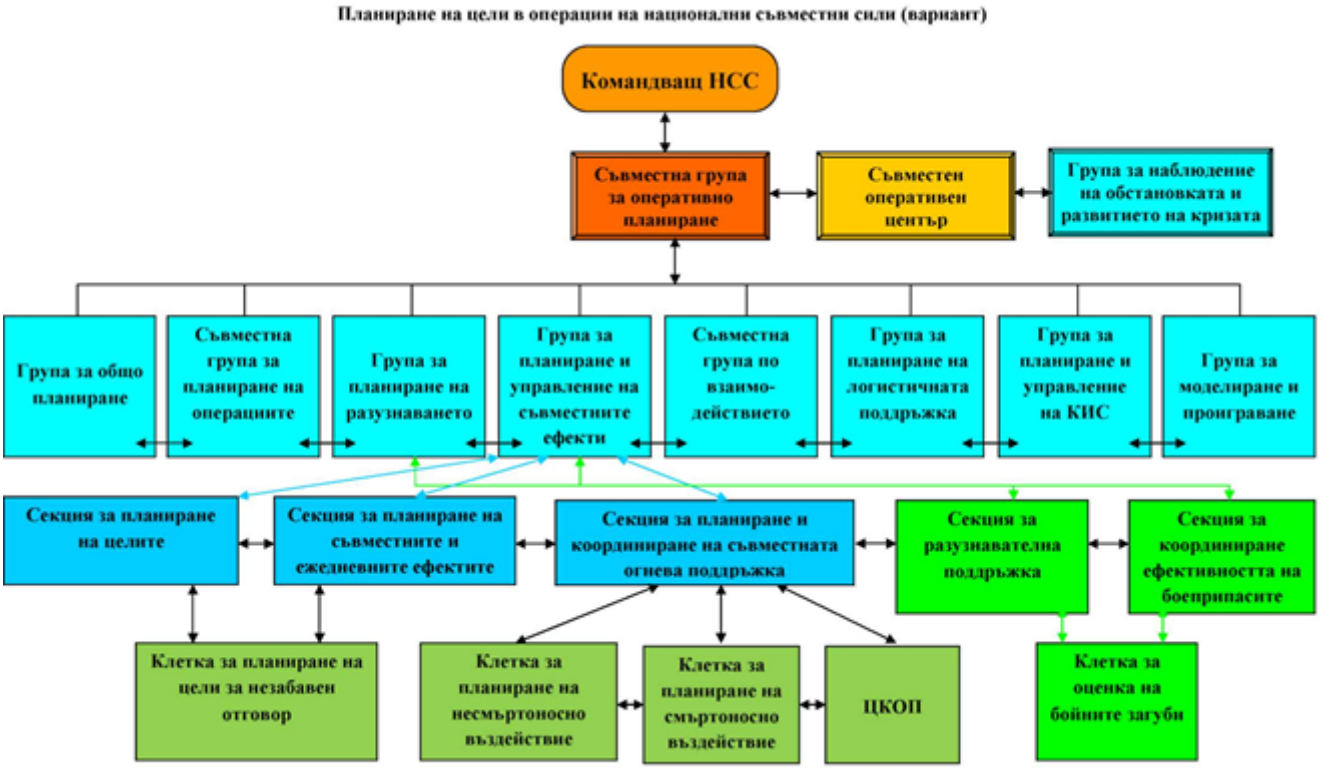
Постигането на исканите ефекти е пряко обвързано с планирането, координирането и изпълнението на задачите в съвместната огнева поддръжка, при което задължително се отчитат очакваните и допустими загуби.

За планиране и поразяване на целите е целесъобразно създаването на **функционални групи, подгрупи и секции** в различните формирования от състава на националните съвместни сили, които на различните етапи могат да имат определени отговорности по отношение на процеса на планирането на целите. Тези групи, подгрупи и секции могат да бъдат различни по състав и с различни функционални отговорности в зависимост от целта на създаването им и степента на интензивност на военния конфликт.

Основен работен орган на процесите на планиране в щаба на националните съвместни сили е съвместната група за оперативно планиране, която е основният планиращ орган по отношение на

всички аспекти на бъдещата операция. Вариант за органите за планиране и управление на процеса за планиране на цели е посочен в Схема № 1.

Схема № 1



Съвместната група за оперативно планиране се развръща на основата на отдел „Планиране, развитие и бюджетиране”, с привличане на специалисти от всички функционални области в щаба на националните съвместни сили и представители на компонентните командвания, а по заповед на командващия и на офицери от подчинени формирования и взаимодействащи щабове.

В зависимост от типа на операцията и с искане до националния кризисен щаб или по разпореждане, в групата могат да бъдат включени представители на органи от държавната администрация, и органи на местното самоуправление и местната администрация.

Основната функция на съвместната група за оперативно планиране е разработване на оперативния план и съпътстващите го документи. Групата съгласува дейностите и направлява процеса за разработване на плановете. Своевременно изисква от останалите групи необходимата информация за планирането. Групата извършва дългосрочен анализ на изпълнението на оперативния план и разработва други документи в интерес на успешното провеждане на операцията от националните съвместни сили.

Планирането на съвместната огневата поддръжка и ефектите може да се извърши в мирно време или в застрашаващия период (в операции с различна степен на интензивност), до началото или в хода на сухопътната операция.

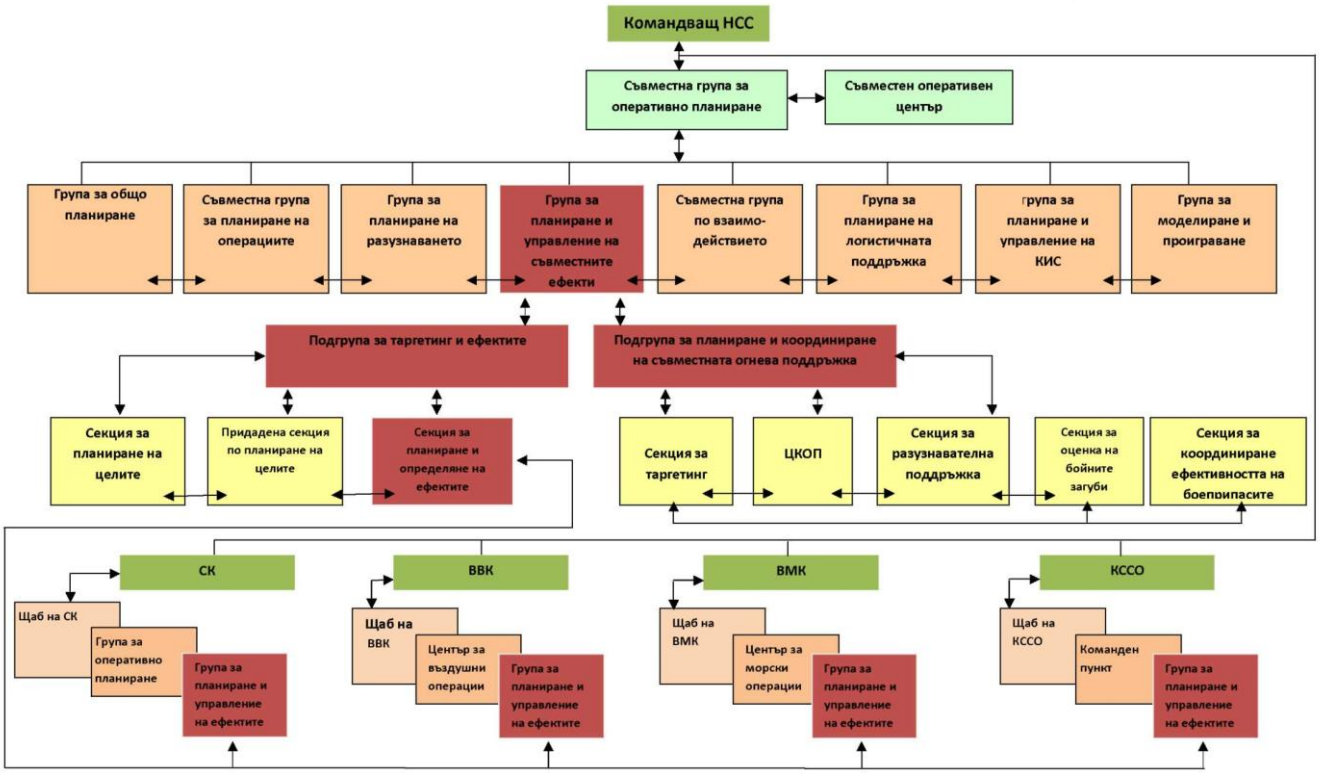
В националните съвместни сили планирането и управлението на процеса за оценка на бойните и съпътстващите загуби се извършва от „групата за планиране и управление на съвместните ефекти”, която се формира на функционален признак и е елемент от съвместната група за планиране на операциите.

В компонентите планирането и управлението на таргетинг процеса се извършва от групата за планиране и управление на ефектите.

Вариант на органите за планиране и управление на ефектите в съвместните сили и компонентите е посочен в Схема № 2.

Схема № 2.

Органи за планиране и управление на ефектите на ниво съвместни сили и компонент (вариант)



Група за планиране и управление на съвместните ефекти се развръща и се ръководи от отдел „Операции”. Групата за планиране и управление на съвместните ефекти гарантира, че военните ефекти са в съответствие с политическите, икономическите и гражданските усилия в рамките на всеобхватния подход. Тя осигурява координация на усилията, чрез сътрудничество на военните и невоенните организации, както и стратегически комуникации за изпълнение на стратегическите военни цели и изгражда необходимите условия за постигане на желаното крайно състояние. Групата за планиране и управление на съвместните ефекти гарантира, че оперативния модел и поддържащите го ефекти, не само могат да бъдат оценени, но са пряко свързани с постигането на оперативните цели определени от командващия.

От състава на групата за планиране и управление на съвместните ефекти се формират:

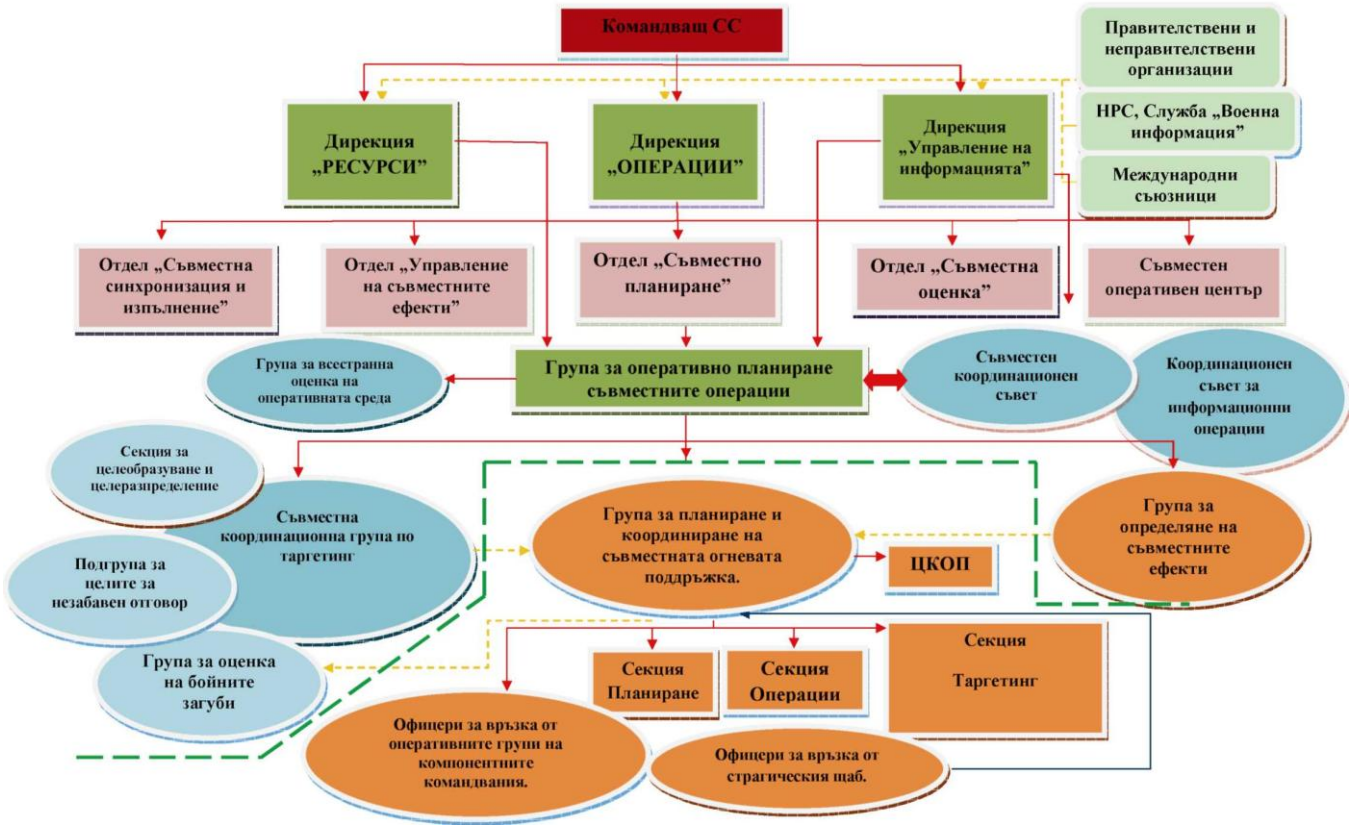
- Секция за планиране на целите;
- Секция за определяне на съвместните и ежедневните ефекти;
- Секция за планиране и координиране на съвместната огнева поддръжка;
- Секция разузнавателна поддръжка.
- Секция за координиране ефективността на боеприпасите.

За водене на операцията се развръща **съвместен оперативен център**. Той се явява основен орган на командващия на националните съвместни сили за водене на операцията.

Като правило цялата текуща информация по отношение развитието на обстановката трябва да постъпва в съвместния оперативен център при информационния мениджър, който от своя страна я разпределя до изпълнителите. Съвместния оперативен център е органа, който контролира изцяло управлението на текущата операция по решаване на кризата (конфликта) в рамките на 72 часа (3 денонощия).

Прилагането на всеобхватен подход за планиране на операциите на стратегическо, оперативно и тактическо ниво се извършва от постоянни или сформиращи се органи, центрове и групи за планиране на съвместните операции в щаба на националните съвместни сили, така и в процеса на планиране на операцията. Вариант на органите за планиране на съвместните операции в щаба на национални съвместни сили е посочен в Схема № 3.

Схема № 3.



На оперативно ниво се създават три основни дирекции:

- Дирекция „Операции” – обединява основно отделите „Съвместни операции” и „Съвместно планиране на операциите” и е основното ядро при планирането и управлението на съвместните операции в щаба на националните съвместни сили, в която се извършва всестранен анализ, планиране, синхронизация, изпълнение и оценка на операциите и задачите изпълнявани от съвместните сили;
- Дирекция „Управление на информацията” – обединява отделите - „Разузнаване” и „Подготовка”, и включва представители и експерти от Национални разузнавателни служби, служба „Военна информация”, министерства, правителствени и неправителствени организации, международни съюзници имащи отношение към конфликта или кризата;
- Дирекция „Ресурси” – създава се на основата на отдел „Логистично осигуряване” и обединява отделите – „Управление на човешките ресурси” и „Комуникационни информационни системи”, включва представители на невоенни организации осигуряващи ресурс и участващи в логистичното осигуряване на националните съвместни сили.

Основен работен орган за извършване на процеса на планиране в щаба на националните съвместни сили и щабовете на компонентните командвания е **групата за оперативно планиране на съвместните операции**, която се развръща на основата на отдел „Съвместно планиране” и е основният планиращ орган на текущата операция. Групата за оперативно планиране на съвместните операции подпомага командващия на националните съвместни сили при поставянето на задачи и управление на подчинените, извършва непосредствено планиране на операцията.

Групата има следния състав:

- Съвместна координационна група по таргетинг;
- Група за планиране и координиране на съвместната огнева поддръжка;
- Група за определяне на съвместните ефекти.

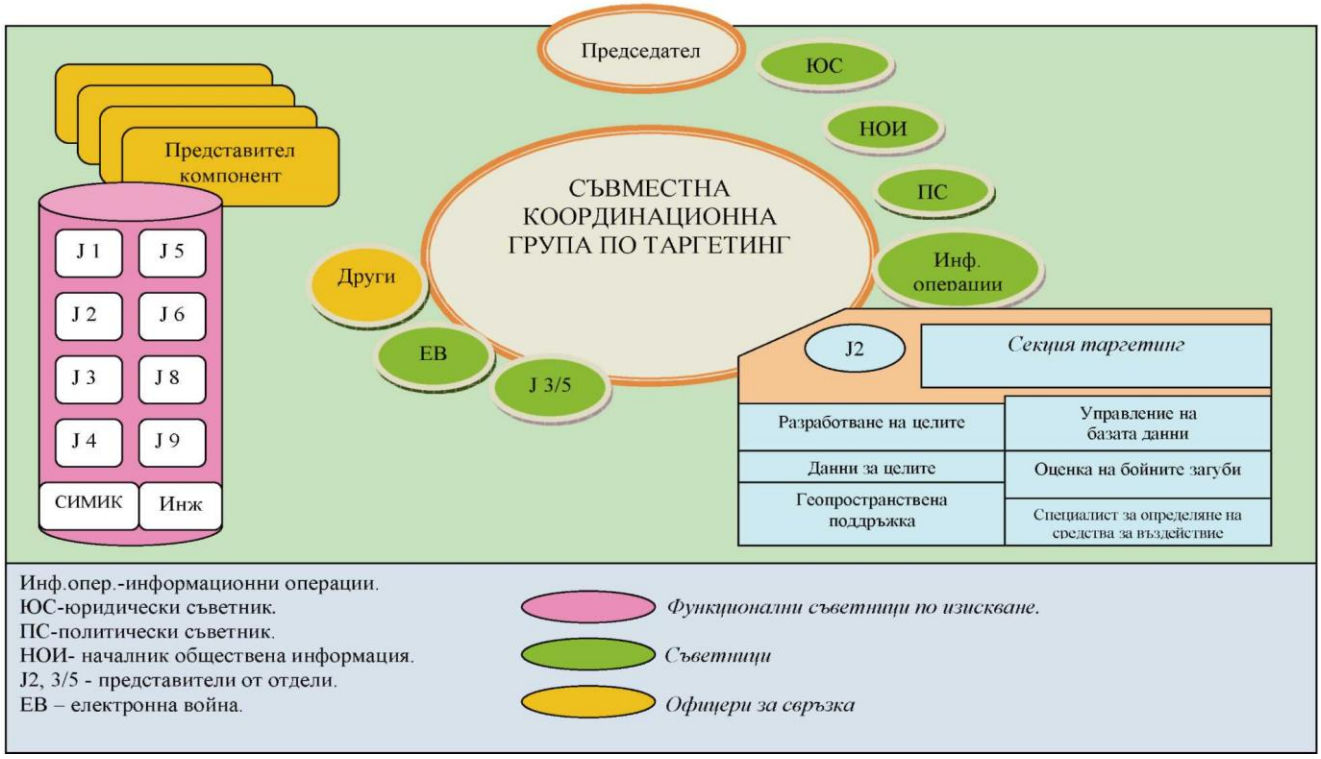
Съвместната координационна група по таргетинг отговаря за изпълнението, отговорностите, приоритетите и синхронизацията на всички аспекти от използването на средствата с несмър-

тоносен и смъртоносен ефект. Групата гарантира, че информационните операции и усилията на таргетинг процеса са координирани и съсредоточени върху постигане на определените оперативни цели от командващия многонационалните съвместни сили. Групата е отговорна за постигането на общите цели от отделните компонентни командвания, за уточняване на поддържано или поддържащо компонентно командване и взаимовръзките между тях. Съвместна координационна група по таргетинг анализира избора на цели, приоритетите, ограниченията и разпределението им при въздействието.

Вариант на съвместната координационна група за таргетинг е посочен в Схема № 4.

Схема № 4

Съвместна координационна група за таргетинг (вариант)

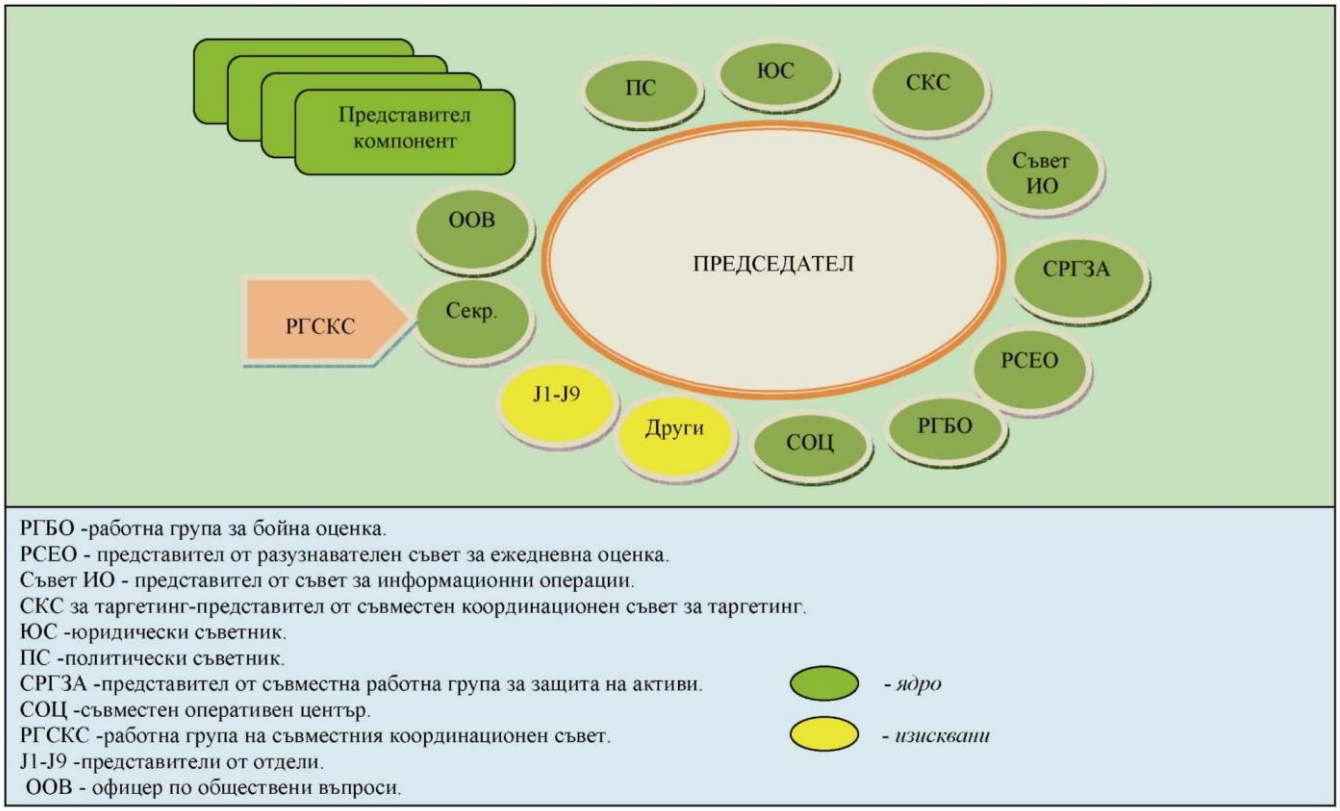


Съвместната координационна група се подкрепя от секцията за таргетинг за незабавен отговор, която е от състава на групата. Офицерите за връзка, които представляват различните компоненти са информирани за изискванията, намеренията, целите, плановете, средствата и възможностите на техните командири. Различните представители подпомагат функционирането на съвместната координационна група за таргетинг. Офицерите за връзка имат право да вземат решения от името на своите командири на компоненти.

Съвместния координационен съвет има определен състав, като членовете му са изпълнителен орган, интегриран в рамките на щаба на националните съвместни сили и включва представители на всички функционални области в рамките на щаба и елементите за връзка от компонентите. Представителите в съвместния координационен съвет имат опит, знания и правомощия да вземат решения от името на своите командири. Този съвет ръководи макро аспектите от дейността на съвместните сили и синхронизира резултатите от тези действия, като издаване на приоритети и указания на командващия националните съвместни сили до командирите на компоненти за разрешаване на потенциални конфликтни зони. Чрез заповедта на командващия, съвместния координационен съвет възлага изпълнението на отговорности, дава приоритет, разрешава конфликти и синхронизира всички аспекти на употребата на средства с несмъртоносен и смъртоносен ефект. Вариант на Съвместния координационен съвет е даден в Схема № 5.

Схема № 5

Съвместен координационен съвет (вариант)



Като краен резултат от работата на съвместния координационен съвет се явява съвместната координационна заповед. Тя предвижда, в един документ, общата оперативна насоченост на операцията, показва общият размер на взаимодействие на всички сили и възможности, използването на несмъртоносни и смъртоносни средства за въздействие. В своята дейност съвместния координационен съвет взаимодейства с координационния съвет за информационни операции за съгласуване използването на несмъртоносни въздействия в зоната на операцията.

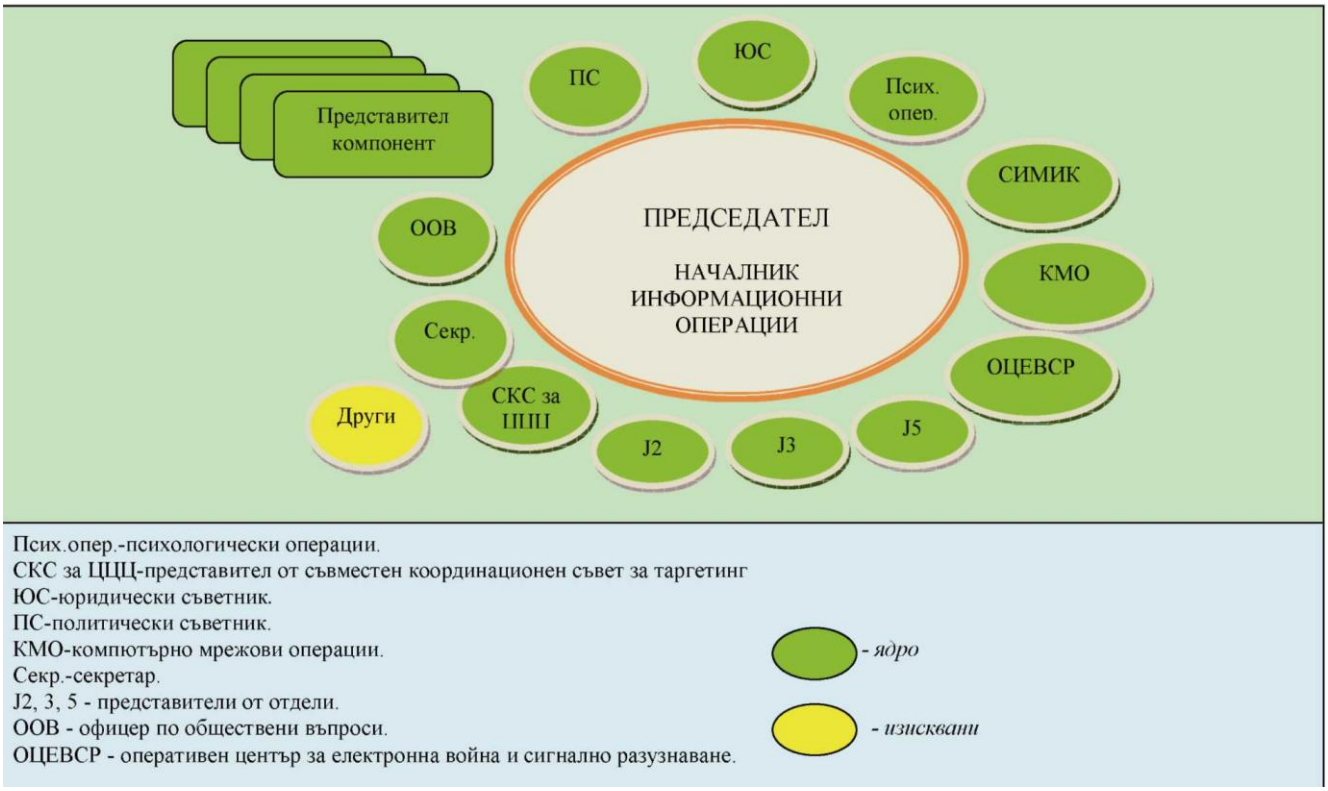
Информационните операции са интегрираща функция, насочена към информационната среда, а не толкова към способностите. Информационните цели са степен от планираното координиране и съгласуване на всички военни възможности, инструменти и техники, засягащи информацията или информационните системи. Употребата на сила може да допринесе за постигане на желания ефект в информационната среда. Всички планове и дейности следва да бъдат координирани и синхронизирани, с разрешени противоречия, за да не се правят компромиси с една дейност, което да доведе до отхвърляне или намаляване на желания ефект от друга. Тази координация е отговорност на органите провеждащи информационните операции и се синхронизира в **координационния съвет за информационни операции.**

Координационен съвет за информационни операции е подчинени на съвместния координационен съвет и е неразделна част от него, като в следствие на неговата дейност изготвя анекс по информационните операции като приложение към съвместната координационна заповед. Вариант на състава на координационния съвет за информационни операции е посочен в Схема № 6.

Съвместния координационния съвет за информационни операции допринася за реализирането на таргетинг процеса чрез номиниране на цели, които могат да повлияят чрез своите действия на провеждането на информационните операции. Съвместния координационния съвет за информационни операции съветва за последващо появяване на нежелани ефекти в информационната среда и координира военните информационни дейности с цел избягване на нежелани ефекти.

Схема № 6

Координационен съвет за информационни операции (вариант)



Заключение

Резултатите от направеното изследване позволяват да се направят следните **изводи**:

1. Анализът на схема №1 показва, че съвместната група за оперативно планиране е основна по отношение на планирането, същата подпомага командващия при определяне на концепцията, поставянето на задачи на подчинените и извършва предварително планиране на операцията;

2. Анализът на схема №2 показва, че в маневрените формирования планирането и управлението на огневата поддръжка и ефектите от нанасяните удари се извършва в подгрупата за планиране и координиране на огневата поддръжка, в центровете за координиране на огневата поддръжка и в елементите за огнева поддръжка;

3. Анализът на схема №3 показва, че тази организационна структура осигурява интегрирането на функционални експертизи за планиране и управление на основните процеси на оперативно ниво. Дирекциите, отделите, подгрупите и секциите в щаба на националните съвместни сили си сътрудничат, взаимодействат и координират през време на всички фази и линии на операцията;

4. Анализът на схема №4 показва, че тази група отговаря за таргетинг процеса, неговото изпълнение, протичане и контролиране. Съвместната координационна група за таргетинг е основната група за синхронизация и управление на съвместния процес на планиране на целите. Тя подготвя за одобрение списъци с целите и матрица на целите за незабавен отговор за одобрение и участие в цикъла на съвместната координационна заповед касаеща всички въпроси, свързани с процеса на таргетинг.

5. Анализът на схема №5 показва, че този координационен съвет работи с командващия на националните съвместни сили, а членовете му са изпълнителен орган, интегриран в рамките на щаба на националните съвместни сили.

6. Анализът на схема №6 показва, че съществува определена зависимост между информационни операции и съвместния таргетинг процес.

References

1. Атанасов, А. Органите за планиране на съвместната огнева поддръжка във всеобхватният подход при планиране на операциите. *Сборник научни трудове* на НВУ "В.Левски", факултет "Артилерия, ПВО и КИС", 2011, стр. 28-37, ISSN 1313-7433.
2. Гюргаков, И. Нов поглед към системата за поразяване на противника в операциите на съвместни оперативни сили. *Военен журнал*, книжка 5, 2009.
3. Гюргаков, И. Огнева поддръжка и ефекти в съвременните сухопътни операции. *Военен журнал*, 2/2008.
4. Гюргаков, И. Проблеми при планирането на огневата поддръжка при поразяването на първостепенни обекти и цели в операцията. *Учебно пособие*, С, ВА, 2006.
5. Димитров, Р. Всеобхватен подход или подход, базиран на ефектите при планиране на военните операции. Военна академия „Г. С. Раковски”, 2011, стр.111-114, *Стратегия за образование и наука в системата за сигурност и отбрана*, ISBN 978-954-9348-28-6.
6. Пехливанов, Г. и колектив. Подход към операциите, базиращ се на търсения ефект. *Военен журнал*, 2009.
7. Ташков, Д. и колектив. Щабни процедури при участие на съвместни оперативни сили в многонационални операции, *Учебно пособие*, В. А. 2008.
8. Точилов, В. Подход за планиране на съвместните операции, базиран на ефектите. *Монография*, В.А. 2010.
9. Доктрина на съвместните операции. ГЩ на БА 2001.
10. Доктрина на съвместните операции на съюзническите войски (AJP – 01 (A). 2001.
11. Katsev, I. Evaluation method of the Artillery's effectiveness against unitary target. *International scientific conference “CONFSEC 2018”*, vol 2, pp 208-210, ISSN: 2603-2945.
12. Joint Publication 5-0, Joint Operation Planning, 11 August 2011.
13. Joint Publication 3-31, Command and Control for Joint, Land Operations, 29 June 2010.

Kaloyan A. Iliev,

PROCEDURE FOR THE OPERATION OF JOINT EFFECTS PLANNING AND MANAGEMENT BODIES IN THE OPERATIONS OF NATIONAL JOINT FORCES

Kaloyan A. Iliev

*Faculty of Artillery, Air Defense and Communication and Information Systems,
National Military University, Shumen, Bulgaria, kacho_78@abv.bg*

***Abstract**: Component commands are closely linked to the joint operational planning process. At the operational level, this information is obtained in the form of an operational order or concept for the operation, which includes a mission, desired end state, goals, effects and tasks for the subordinates. For specific planning areas, such as fire support and targeting, additional information is provided, such as guidance on planning the targeting process, as well as general priorities for the process itself.*

***Keywords**: Fire support, Targeting, Effects, Planning process, Joint fire support.*

РЕД ЗА РАБОТА НА ОРГАНИТЕ ЗА ПЛАНИРАНЕ И УПРАВЛЕНИЕ НА СЪВМЕСТНИТЕ ЕФЕКТИ В ОПЕРАЦИИТЕ НА НАЦИОНАЛНИ СЪВМЕСТНИ СИЛИ

Калоян А. Илиев

Въведение

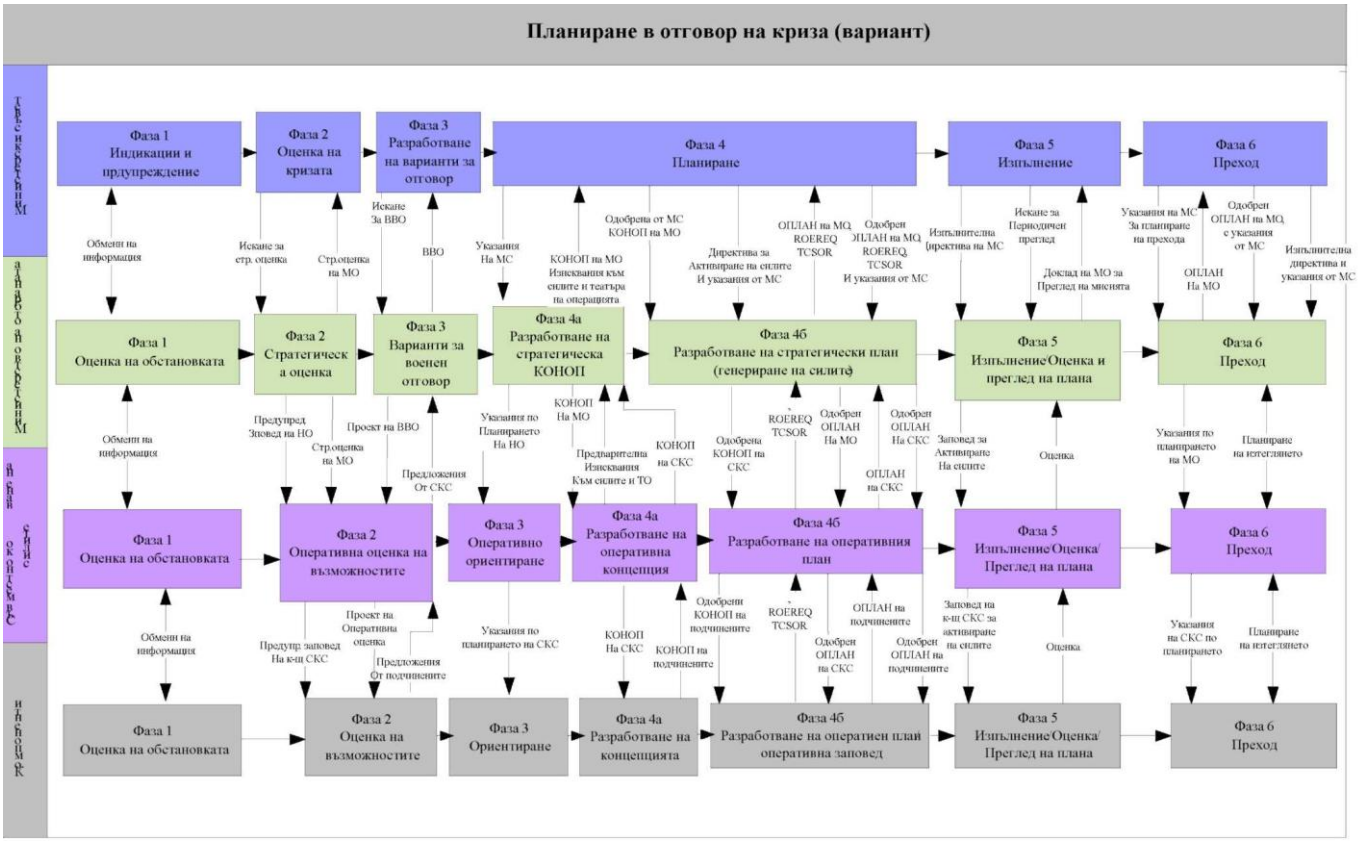
Компонентните командвания са тясно свързани със съвместния процес на оперативно планиране. На оперативно ниво, тази информация се получава под формата на оперативна заповед или концепция за провеждане на операцията, която включва мисия, желано крайно състояние, цели, ефекти и задачи за подчинените. За специфични области на планиране, като огнева поддръжка и таргетинга се предоставя допълнителна информация, като указания по планиране на таргетинг процеса, както и общи приоритети за самия процес.

Планирането на процеса изисква детайлна координация и синхронизация. В операции на национални съвместни сили едновременно могат да се използват конвенционални сили и такива за специални операции на цялата широчина и дълбочина на съвместната зона за операцията в линейно и нелинейно построение. Директните и индиректните атаки срещу противниковия център на тежестта, трябва да бъдат насочени към постигане на необходимите оперативни цели съгласно концепцията на операцията, като същевременно ограничават потенциалните нежелани ефекти в следващите фази от операцията. Интегрирането и синхронизирането на възпиращите действия и маньовъра подпомага командирите за максималното постигане на целите на оперативно ниво. В рамките на своите зони за провеждане на операциите, сухопътния, военновъздушния и военноморския компоненти могат да бъдат определени за поддържащи или поддържани командири с цел интеграция и синхронизация на маньовъра, съвместната огневата поддръжка и възпиращите действия. При това те определят и планират цели, приоритети, ефекти и график за въздействие. Командира на компонент определен като поддържан в съвместната зона на операцията въздейства по цели в цялата в цялата зона на операцията и има отговорности да планира и управлява про-

цеса на планиране на цели в съответствие с приоритетите определени от командващия на многонационалните съвместни сили. Тези дейности следва да са съгласувани със съответните командири на компонентни командвания. В случай, че тези въздействия имат неблагоприятно влияние върху другите операции проблема се разрешава от командващия.

Планирането включва анализиране и разбиране на взаимодействието и свързаността на множество системи на оперативно ниво (политически, икономически, социални, информационни и други), с цел определяне на следствията от действията на националните съвместни сили. Планирането на операции на съвместните сили се състои от шест фази, посочени в Схема № 1.

Схема № 1



Основните процеси на планирането на целите, определянето на реда за въздействие по тях и очакваните ефекти се извършва при разработването на плана за операцията, като началото се поставя в фаза 1 а края с разработването на оперативния план и неговото утвърждаване от стратегическия командващ.

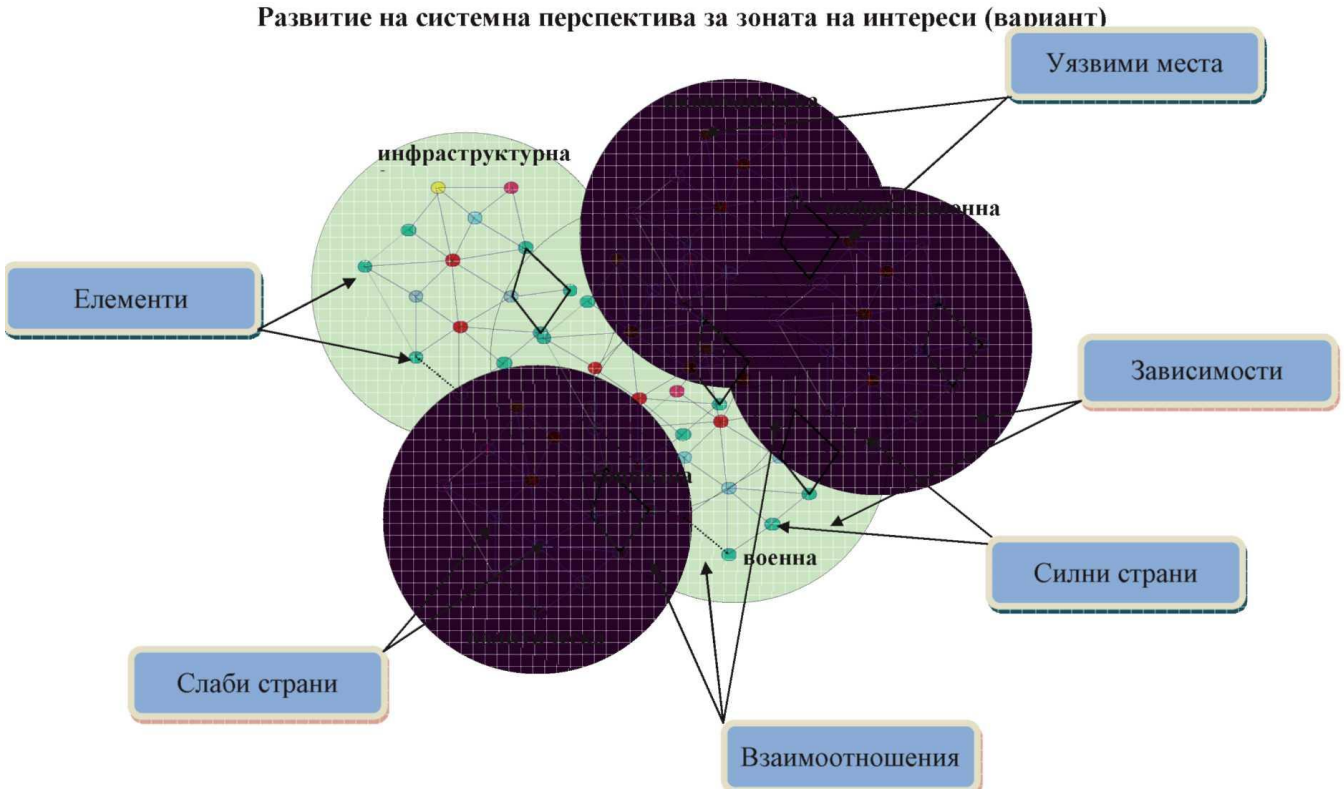
- Фаза 1 – „Оценка на обстановката";
- Фаза 2 – „Оперативна оценка на вариантите за военен отговор.";
- Фаза 3 – „Оперативно ориентиране";
- Фаза 4А – „Разработване на оперативната концепция на операцията";
- Фаза 4В – „Разработване на оперативния план";
- Фаза 5 – „Изпълнение /оценка и преглед на плана";
- Фаза 6 – „Преход"[32].

Фаза 1 – „Оценка на обстановката" се провежда с основна цел да се развие и поддържа определено ниво на осведоменост на оперативната обстановка, за да се осигури извършване на оперативни оценки, разчети и представяне на оперативни становища на стратегическия командващ.

[32] Ръководство за планиране на операциите, МО на РБ, 2011

През тази фаза се разработва системна перспектива за определената зона на операцията посочена в Схема № 2.

Схема № 2



През тази фаза в зависимост от планираната операция се определя вида, състава и времето за развръщане на различните групи и центрове от отделите от щаба на съвместните сили и взаимоотношенията между тях. Желаните резултати от тази фаза на планиране в отговор на криза са определяне на необходимостта от развръщане на оперативен екип за връзка и разузнаване, поемане на отговорност в зоната на интереси и оценка същността на заплахите и рисковете.

Фаза 2 – „Оперативна оценка на възможностите” - започва на основа на получаването на предупредителна заповед от стратегическия командващ или негови указания за иницииране на предварително планиране, проект на стратегическа оценка или проект на варианти за военен отговор. През тази фаза се активира групата за оперативно планиране на съвместните операции, отдава се предупредителна заповед до подчинените компоненти. Групата за оперативно планиране на съвместните операции извършва анализ на задачата за изпълнение, наличното време, политическите цели, желаното крайно състояние, потенциалните военни и невоенни фактори, необходимостта от външна координация и от допълнителни указания. През тази фаза се развръща групата за всестранна оценка на оперативната среда. Резултатите от анализите и дейността през тази фаза могат да бъдат следните:

- Разработване и отдаване на предупредителна заповед до компоненти;
- Извършване на анализ на мисията, базиран на оценката на командващия на съвместните сили;
- Изготвяне на предложения за военен вариант за отговор от съвместните сили след получаването на предложения от командирите на компоненти и изпращането им до стратегическия командващ.

Фаза 3 – „Оперативно ориентиране” Фазата стартира при получаване на стратегическата оценка на кризата, военните варианти за отговор или указанията по планирането на стратегическия командващ. През тази фаза по решение на началника на групата за оперативно планиране на съвместните операции се развръщат съвместната координационна група за таргетинг, групата за

определяне на ефектите и групата за планиране и координиране на съвместната огнева поддръжка. Предложените групи и взаимоотношенията между тях следва да осигуряват планомерна работа на всяка група, доколкото тя зависи от дейността на друга група.

Желани резултати от фазата на оперативно ориентиране могат да бъдат:

- Изяснени са желаното крайно състояние и стратегически цели;
- Определена е мисията, задачите и целите;
- Анализирани са ключовите фактори;
- Определени са оперативните центрове на тежестта на основните субекти и са анализирани техните критични способности, критични изисквания, критични уязвими места;
- Определени са оперативните цели, ефекти, линиите на операцията и критични точки и е разработен оперативен дизайн;
- Определени са първоначални изисквания на командващия за критична информация;
- Издадени са указанията на командващия по планирането;

В стратегическия щаб могат да бъдат изпратени:

- Искане за допълнителна информация;
- Искане за правила за поведение и употреба на сила;

Резултатите от тази фаза могат да бъдат:

- Всеобхватна оценка на оперативната обстановка;
- Оперативен дизайн;
- Указания на командващия по планирането до щаба и командирите на компоненти;
- Искания за правила за поведение и употреба на сила.

Фаза 4А – „Разработване на оперативната концепция" Процесът на планиране на съвместните операции се провежда с цел да се определи как най-добре да се проведе операцията за осигуряване на ефективно изпълнение на мисията в съответствие с намерението на командващия на съвместните сили. Необходими условия за стартиране на тази фаза от процеса на планиране на съвместните операции е получаване на концепцията на операцията от стратегическото ниво. Командващият на съвместните сили към този момент следва да е утвърдил: анализа на мисията, оперативния дизайн и указанията по планирането включващи неговото намерение и указания за разработване и избор на варианти за действие.

Желаните резултати от тази фаза на оперативното планиране могат да бъдат:

- Съвместните действия на силите и средствата за съвместна огнева поддръжка да бъдат синхронизирани във времето и пространството, така че да осигурят създаване на оперативни ефекти, които водят до постигане на последователно въздействие по определени критични точки;
- Последователността от операции по определените линии, постигат критични точки, които осигуряват свобода на действие и водят до изпълнение на оперативните цели;
- Способностите необходими за поддържане и осигуряване на съвместните действия по отношение на съвместната поддръжка са идентифицирани и синхронизиране с времето и мястото, в които да бъдат осигурени;
- Оперативните аспекти на факторите време, пространство, сили и информация са балансирани до степен на приемлив риск.

Крайните продукти на тази фаза на планиране могат да бъдат следните:

- Концепция на операцията;
- Искания за необходимите съвместни способности;
- Искания за необходимите способности в театъра на операцията;
- Изисквания за комплектуване на щабовете с личен състав;

Фаза 4В „Разработване на оперативния план" се провежда с цел съгласуване и уточняване на необходимите дейности от концепцията на операцията. През тази фаза на предварителното планиране се детайлизира провеждането на операцията, осигуряват се условия на подчинените формирования за планиране и се извършва адаптация на оперативния план в отговор на изменящата се оперативна обстановка.

Необходимите изходни данни за стартиране на тази фаза от процеса на оперативно планиране могат да бъдат:

- Утвърдена концепция на операцията на съвместните сили от стратегическия командващ;
- Списък на силите и средствата на съвместните сили;
- Проект на необходимите способности в зоната на операцията;
- Получени отговори на исканията на командващия на съвместните сили, относно правилата за поведение и използване на сила.

Разработването на плана преминава през следните стъпки:

- Иницииране разработването на плана;
- Разработване план за използване на съвместните сили;
- Разработване на план за командване и управление;
- Разработване на план за подготовка и поддръжка на силите;
- Разработване на план за развръщане на силите;
- Разработване на план за защита на силите;
- Разработване на план за прекратяване на конфликта;
- Разработване и изпращане на координиращ оперативен план за провежданата операция от съвместните сили към стратегическия командващ за утвърждаване.

При предварителното планиране през тази фаза следва да бъдат постигнати следните резултати:

- Общ план за действие при непредвидими ситуации;
- Постоянен план за отбрана;

Взаимоотношенията, ролите и отговорностите органите и групите в щаба на съвместните сили през тази фаза трябва да осигурят изготвянето на оперативния план за действие на националните съвместни сили.

Фаза 5 „Изпълнение, оценка на операцията и преглед на оперативния план провежда се с цел проверка изпълнимостта на плана изискващ командване и управление на силите и взаимодействие с другите невоенни средства за планиране, координиране и синхронизиране на действия, с които се създадат желаните оперативни ефекти. Преглед на оперативния план може да се наложи при рязка промяна на оперативната среда или съвместната зона на операцията. Командващия на съвместните сили и неговия щаб извършват периодична оценка за определяне ефективността на действията на съвместните сили в създаването на желаните ефекти.

През тази фаза се извършва управление на процеса на планиране на целите за постигане на желаните ефекти и достигане на желаното крайно състояние.

През тази фаза се извършва управление на съвместния таргетинг процес при което процеса протича с в следната последователност:

- **Цели на командващия и желано крайно състояние.**
- **Определяне и приоритизиране на целите.**
- **Разработване на списъци и матрици с цели.**
- **Анализ на възможностите.**
- **Вземане на решение от командващия и определяне на изпълнителите.**
- **Планиране и изпълнение.**
- **Оценка.**

Фаза 6 „Преход" Процеса на предварителното планиране се провежда с цел да се разработи и координира оперативен план за изтегляне. Когато се планира изтеглянето на силите от кризисния район се цели създаването на положителни резултати за достигане на целите и желаното крайно състояние. Основните дейности при планиране изтеглянето на силите могат да бъдат следните:

- Намаляване на риска и неблагоприятните последствия от изтеглянето на съвместните сили от зоната на операцията;
- Осигуряване на координация по време на изтеглянето, предаване на контрола на зоната за отговорност на местните сили за сигурност;

- Осигуряване на контрол и управление на процеса по планиране на изтеглянето на оперативно ниво;
- Засилване на сътрудничеството и координацията между стратегическото, оперативното и тактическо ниво;
- Планиране на сили и средства, които ще осигуряват продължаване на обучението на силите за сигурност след изтеглянето на основната част от коалиционните сили;
- Оценка на резултатите на процеса по планиране на изтеглянето.

Процеса за планиране на изтеглянето представлява периодичния процес за оценка развитието на операцията и позволява разработването на препоръки за коригиране на оперативния план, възприемането на нови подходи и преразглеждане на използваните сили и способности.

Съвместният таргетинг процес е този процес, който се ръководи от командващия на националните съвместни сили. Съвместният таргетинг процес и процеса на съвместна огнева поддръжка подкрепя единството на усилията и те трябва да са постоянно във взаимодействие един с друг. Взаимоотношенията между двете системи могат да бъдат следните:

- Съвместимост с целите, указанията и намеренията на командващия на националните съвместни сили;
- Съсредоточаване върху противниковия център на тежестта и критичните му точки;
- Координацията, интеграцията, синхронизиране и разрешаване на конфликти на действията;
- Общ поглед върху усилия за провеждане на съвместна огнева поддръжка и съвместния таргетинг в подкрепа на командващия;
- Бърз отговор в условия на ситуации за провеждане на динамичен процес, които представя ограничени възможности за действие;
- Намаляване на дублирането на усилия;
- Бърза оценка на планираните и изпълнените операции;
- Пълното интегриране на всички налични възможности;
- Намаляване на риска от собствен огън и странични щети.

По време на планирането, съвместния таргетинг процес започва със съществуващата информация. Дейности по събиране на информация, таргетинг процесите, планиране на мисията, изпълнение на огневата поддръжка, както и формата за оценка са гъвкави, повтарящи се процеси, като се развива информацията за целите през цялата операция.

Планирането и управлението изискват дефиниране на ясна визия за това какво трябва да се осъществи в рамките на таргетинг процеса. Тази визия синхронизира и съчетава изкуството и науката на всяка бойна операционна система и допринася за фокусиране на усилията и спечелване на предимство в зоната на операцията.

Заключение

Резултатите от направеното изследване позволяват да се направят следните **изводи:**

1. Анализът на схема №1 показва, че планирането на цели в операциите на съвместните сили се извършва в общия процес на планирането на операциите и следва неговите фази. Основните процеси на планирането на целите, определянето на реда за въздействие по тях и очакваните ефекти се извършва при разработването на плана за операцията, като началото се поставя в фаза 1 а края с разработването на оперативния план и неговото утвърждаване от стратегическия командващ;

2. Анализът на схема №2 показва, че основна отговорност през тази фаза носи групата за оперативно планиране на съвместните операции като определя състава и времето за подготовка на групата за оперативно планиране на съвместните операции, която се поддържа от всички отдели в щаба на съвместните сили, представители на министерства, правителствени, неправителствени организации;

3. Планирането на ефектите, в операциите на съвместните сили се явява поддържащ процес на процеса на оперативно планиране и има пряко отношение към реда и начина за провеж-

дане на съвместната огнева поддръжка и реда за въздействие върху целите, в различните етапи и фази на операцията.

4. Планирането на целите се извършва във фаза 5 на операцията на съвместните сили, като се спазва определена последователност, като началото на процеса започва с вземане на решение от командващия за поразяване на дадена цел и завършва с оценка на резултатите от въздействието и предложение на следващи решения. При управлението на процеса командващия на съвместните сили по-често взема решение за въздействие по планирани цели, а командирите на компоненти и формирования използват динамичния процес.

5. Планирането на ефектите се извършва във всеки етап от планиране на операциите, с което се подпомага командващия на съвместните сили, командирите на компонентите и командирите на тактически формирования да вземат целесъобразни и точни решения при спазване на всички правила за употреба на сила и международното хуманитарно право при поразяване на различни по характер цели в зоната на операцията.

Литература:

1. Атанасов, А. Марков, Д. Условия за единно управление чрез интегриране на системите за огнева поддръжка при участие в многонационални операции, 2016, стр. 104-115, ВА "Г.С.Раковски". *Годишна конференция* на факултет "Командно-щабен", ISSN 1312-2991.
2. Чалъков. Р. Марков, Д. Фактори, влияещи на огневата поддръжка в операциите, 2018, стр. 130-135, *International Scientific Conference*, Collection of papers Shumen, ISSN 2367-7902.
3. Гюргаков, И. Нов поглед към системата за поразяване на противника в операциите на съвместни оперативни сили. Военен журнал, книжка 5, 2009.
4. Гюргаков, И. Огнева поддръжка и ефекти в съвременните сухопътни операции. Военен журнал, 2/2008.
5. Гюргаков, И. Проблеми при планирането на огневата поддръжка при поразяването на първостепенни обекти и цели в операцията. Учебно пособие, С, ВА, 2006.
6. Димитров, Р. Всеобхватен подход или подход, базиран на ефектите при планиране на военните операции. Военна академия „Г. С. Раковски”, 2011, стр.111-114, Стратегия за образование и наука в системата за сигурност и отбрана, ISBN 978-954-9348-28-6.
7. Пехливанов, Г. и колектив. Подход към операциите, базиращ се на търсения ефект. Военен журнал, 2009.
8. Ташков, Д. и колектив. Щабни процедури при участие на съвместни оперативни сили в многонационални операции, Учебно пособие, В. А. 2008.
9. Точилов, В. Подход за планиране на съвместните операции, базиран на ефектите. Монография, В.А. 2010.
10. Доктрина на съвместните операции. ГЩ на БА 2001г.
11. Доктрина на съвместните операции на съюзническите войски (AJP – 01 (A). 2001.
12. Joint Publication 5-0, Joint Operation Planning, 11 August 2011.
13. Joint Publication 3-31, Command and Control for Joint, Land Operations, 29 June 2010.

Kaloyan A. Iliev,

"INFORMATION WAR" FACTOR IN MODERN MILITARY CONFLICTS

Kaloyan A. Iliev

*Faculty of Artillery, Air Defense and Communication and Information Systems,
National Military University, Shumen, Bulgaria, kacho_78@abv.bg*

***ABSTRACT**: The coming war is one of the paradigms that are the subject of many futuristic analyzes and forecasts. Predicting its features and character is a difficult but not impossible process. Each of the modern armies is trying to change in order to adapt to future challenges. To this end, military specialists and experts are constantly working hard to develop new concepts, doctrines, and concrete programs.*

***KEY WORDS**: Information War, Doctrines, Future challenges, Information Impact.*

„ИНФОРМАЦИОННАТА ВОЙНА“ - ФАКТОР В СЪВРЕМЕННИТЕ ВОЕННИ КОНФЛИКТИ

Калоян А. Илиев

Въведение

“Този, който умее да води война, покорява чуждата армия без да се сражава, превзема чуждите крепости без обсада и разрушава чуждата държава без да държи дълго войската си. Той запазва всичко и така си оспорва властта в Поднебесната.”.
Сун Цзи

Бъдещата война е една от парадигмите, които са обект на много футуристични анализи и прогнози. Предсказването на нейните особености и характер е труден, но не невъзможен процес. Всяка от съвременните армии се старае да се променя така, че да се адаптира към бъдещите предизвикателства. За тази цел военните специалисти и експерти непрекъснато полагат огромни усилия в разработването на нови концепции, доктрини и конкретни програми.

Според военните специалисти войната търпи развитие в няколко епохи: праисторическа, антична, средновековна, ранно модерна, индустриална и модерна. По своята структура тя се подразделя на отделни кампании, операции, сражения, боеве и удари, провеждани на театъра на войната, на отделни оперативни направления и райони. Целта на всяко едно военно ръководство е приключване на военният конфликт във възможно най-кратки срокове, посредством провеждане на успешни действия от различен мащаб и с различна цел. През последните години особена популярност доби концепцията за информационна война. Тя се основава на твърдението че информацията и информационните технологии са стратегически ресурс, от жизненоважно значение за националната сигурност и за военните действия.

Информацията играе съществена роля във военното (а и всяко друго) противоборство от най-древни времена. Счита се обаче, че именно в края на XX-ти век информацията и знанието придобиха решаващо значение за военния успех.

Информационната война ще измести на заден план конвенционалните форми за водене на бойни действия. Информацията е била и ще бъде все по важна за воденето на войната на всички нива, тя се очертава като четвъртия фактор, заедно с трите традиционни оперативни фактора - пространство, време и сили. Най-новите възгледи за бъдещата война бяха отразени в последното издание на „Наставлението за провеждане на операции на сухопътните сили на САЩ“. В него се предвижда, че бъдещите бойни действия ще се развиват в три макросфери: физическа, информационна и морална.

Информационното въздействие е преднамерено или непреднамерено въздействие на върху човека, чрез предаване на информация (сигнали, съобщения, сведения, образи). Основният обект на информационно въздействие е съзнанието на човека, групата, или общественото съзнание. С помощта на такова въздействие може преднамерено или непреднамерено да се изкриви картината на обективната реалност. Целите на това изкривяване могат да бъдат различни: от модификация на поведението на личността и управление на колективното (обществено) съзнание, до патологично нарушаване на психическите и физиологични процеси в човека.

Съвременните възгледи за въоръжена борба в информационната макросфера предвиждат те да протекат под формата на стратегически информационни операции. Основната им цел е да се постигне информационно превъзходство над противника на театъра на бойните действие и да се осигури ефективно командване и управление в хаоса на сраженията. Едновременно информационните операции ще пречат на противника да направи същото, създавайки "възпиращо триене" в когнитивните цикли на неговата командно-управленска система. Днес концепцията за информационната война заема важно място в общата парадигма за бъдещата война. Тя е важен инструмент за гарантиране на националната сигурност на всички нива - тактическо, оперативно и стратегическо.

Възгледите за въоръжена борба в моралната макросфера са тясно свързани с информационната и с основание се интерпретират като един от видовете информационна война. Тя се реализира като последователност от психологически операции, както в подготвителния период, така и по време на размяната на огневите удари. Целта е да се постигне морално превъзходство над противника, като се ослабят неговите съпротивителни сили и воля за победа. В последните години се забелязва трайно намаляване на желанието да се използват традиционни методи за война, като използването на физическо насилие, особено ако информационните операциите са успешни. Известно е, че днес може да не се обявява официално война срещу нечии врагове, като се използва военна сила и стандартните методи на огнево поразяване. По-ефективно е да се води скрита информационна война, която е значително по-лесно приложима. Независимо от това дали си даваме сметка или не, психологическите информационни операции са всекидневна реалност. Победите и загубите в тях формират бъдещия световен ред и етиката на човешкото общество. Медийните форми на психологически информационни операции бяха широко прилагани от всички участници във войната в Косово от 1999 г. (Операция Съюзна сила), войната в Афганистан през 2001-2002 г. (операция "Трайна свобода") и от войната срещу Ирак през 2003 г. Поведението на медиите през тази войни показа, че те са станали част от инструментариума на военните стратези и се третират като важно средство за въоръжена борба. С огромната си тиражност, глобален обхват и неограничена памет съвременните глобални информационни системи превръщат медийните психологически операции в стратегическо оръжие за въздействие върху човешката цивилизация.

В публикуваната литература се формулират и обсъждат 7 вида на тази офанзивно-агресивна форма на Информационната война:

- Радиоелектронна;
- Психологическа;
- Културна;
- Хакерска;
- Икономическа;
- Кибер-война;
- Война на Гибсън.

Радиоелектронната борба е една от най-добре осветените в литературата у нас. Основния обект на атаката са системите ISR и C4I на противника. Класифицирани по обектна ориентация, основните методи за борба са:

- Антирадиолокационни;
- Антикомуникационни;
- Криптографски.

Психологическата война е основана на използването на глобалното разпространение на информация по масмедиите (радио, телевизия). Тази форма води до обработка на общественото мнение в глобален мащаб, в необходимата посока. Ефектът от такава операция е твърде значим. Въздействието обикновено е пряко срещу личния състав и срещу командването. Наличието на полеви мултимедийни компютърни студия и компютърни TV - приемници, осигурява предаването на информация в реално време с цел - въздействие на противника. Въздействието върху командването е главно насочено към дезориентация, объркване и емоционално разстройване. Съществена е възможността за внасяне на невярна информация по отношение на намеренията на атакуващата страна и нейните възможности. Добавянето на агентурите информационни канали в тази посока дава значителен резултат.

Културната война се реализира в такива битово-обществени явления като Бързата закуска, Холивуд, Мадона, рисуваните филми, сините джинси и т. н., които според редица автори са проява на нова форма на културна агресия. Експанзията на чужда култура формира ново информационно-културно пространство, подменящо коренните национални традиции и ценности, възпитаващо космополитизъм и мултинационалност. Културната война е и политика. Емигрантската вълна, изтичането на мозъци на запад, както и импортът на културни продукти от запад са основните проявления на тази тиха и невидима война.

Хакерската война като правило се формулира като атаки срещу компютърните мрежи на противника. Използват се известни "дупки" в хардуера или софтуера. Въздействията могат да бъдат: тотална парализа на мрежите, междинни спирания, въвеждане на случайни грешки в потока данни, кражба на информация, кражба на услуги, незаконен мониторинг на системата и събиране на разузнавателна информация, въвеждане на фалшив трафик на съобщения, модификация на наличните данни с цел - въвеждане в заблуждение. Обикновено се атакуват цивилни цели (компютърни мрежи). Военните такива са обект на "командно -управленска война". Естествено физическото разделяне на двата вида системи прави военните по-защитени и недостъпни. И тук могат да се разграничат дефанзивна и офанзивна стратегии. Атаките срещу компютърните мрежи могат да са на физическо, синтактично и семантично равнища. Проблемите за военните системи на физическо равнище са сравнително малко. Със синтактичните атаки днес се постига най-значителен ефект. Семантичните атаки са предмет на отделен вид - "Кибер-война". Дефанзивните форми на хакерска война са насочени към защитата на компютърните мрежи и са дискутируеми като отделни форми, поради мощните защити на комерсиалния софтуер. В някои случаи се предлага атаката като най-добра форма на защита. Офанзивните форми са абсолютно нови форми и са в процес на синтезиране, анализиране и експериментиране. Основен въпрос е тяхната реална приложимост. Интернет, Електронната поща, предаването на данни и мултимедийните реализации, интегрирани в кабелно-разпределителните среди, осигуряват великолепни условия за подобни форми на разрушаване на инфраструктурите на стопанския живот на противника.

Затягането на многослойните системи за хардуерна и софтуерна защита се противопоставя на изобретяването на нови хитроумни способи за тяхното преодоляване. Особено важно е да се осигури защитата на компютърните системи за управление на енергийни, противопожарни, медицински, транспортни, телефонни, охранителни и др. подобни технологични компютърни системи. Отделен раздел на този вид война е компютърната вирусология, която е добре известна у нас. Терористичният характерна този вид война е особено опасен. Естествено редица природни бедствия носят по-разрушителен характер, но този вид въздействие е по-трудно доказуем и оценим като упражнения.

Икономическата информационна война се третира като информационна блокада и информационен империализъм. Блокадата по своята същност е прекъсване на потока от информация, както сега се прекъсва потока от стоки и материални ресурси. На практика се отнема печалбата от международния информационен обмен. Инфо-блокадата включва и физическата блокада на информационните носители. Прекъсва се достъпа в реално време до спътници, ретранслатори, GPS & GSM сателитни системи, картографски информационни системи и др. За подобна блокада е необходимо да се притежава контролът върху световните информационни ресурси във вид на глобално присъствие като международен оператор. Това за сега е възможно само в рамките на консорциум на най-развитите в икономическо отношение страни. С по-нататъшното разпространение на информационните връзки и тяхното интензифициране в глобален мащаб, все по-трудно ще става информационното блокиране на отделни държави или групи лица. Информационният империализъм може да се третира като разновидност на икономическият империализъм, поради тясната зависимост между стопанската дейност и информационното и осигуряване. Като цяло, тази форма може да се разглежда като продължение на търговската конкуренция с други средства. Аналогията с културната война е очевидна.

"Кибер-войната" включва: информационен тероризъм, семантични атаки и стимулационни войни. Информационния тероризъм е атака на персоналните файлове, на отделната личност. Те са в личния компютър и в обществени и квази-обществени бази данни, в областите на обучението, здравеопазването, административните услуги, търговията и финансовото обслужване и др. Семантични атаки водят до резултат, който е в вид на работеща система, даваща периодични груби грешки в информационно-обработващия процес. Смисловата същност на сензорната информация, или съдържанието на базите данни се подменя, с което се обезсмисля процесът на вземане на решения. Този вид атаки ще е особено болезнен в гражданските системи за обработка на информация (здравеопазване, финанси, материално-техническо снабдяване и др.). Стимулационната война е чисто и безболезнено провеждане на война на базата на добро симулиране, подобряващо непрестанно своята достоверност. Резултатът е една точна оценка на изходът от конфликта. Така противникът се убеждава, че ще загуби и взема съответните решения.

Ефектът от притежаването на по-добри бойни средства, в съчетание с тяхното умело използване, може да се демонстрира чрез симулации, без да се употребяват върху жива сила. Основният ефект от тази форма на борба е възможността операторът да моделира и прогнозира състоянието на бойното поле. Така по методът на "пробите и грешките" може да се оптимизира поведението в конфликта. На практика по-добрата техника за симулация, ще даде по-добро поведение. В този смисъл стимулационната война е война за по-пълни, по-достоверни, по-точни и по-надеждни модели на военните системи. По добрата система ще даде по-добри планове за действие. Автоматичното управление на сензорната мрежа и оръжията, на базата на вградените модели, прави войната по-между им стимулационно -моделна.

Войната на Гибсон (Виртуална реалност) е основно - борба на виртуалните реалности. Тя е тясно обвързана с бъдещето на Интернет и глобалните информационни мрежи, в частта "мултимедийни симулации". Войната на Гибсон третира аудио-визуалното присъствие на "воинът" в информационното и кибернетичното пространства. Стимулационните и Гибсон- войните са очевидни бъдещи модели, които ще се напълнят с практическо съдържание, при по нататъшното технологично развитие на глобалните информационни системи. Очевидно, този момент не е далече.

Като всички останали, войната с информационно-базирани оръжия предполага превъзходство, победа и загуба. Едновременно тя е нож с две остриета. Тази форма на информационна война е в неразривна връзка с останалите форми на противоборство, като отбранителните форми са явно по-ефективни и ясни.

Съгласно теорията на древния китайски владетел и пълководец Сун-Цзи, опознаването на културата на противника е основна задача на воюващият. Ролята на информацията в този процес е огромна. Неприятелските бази данни, алгоритми за обработка, комуникационни топологии, сензорни възможности и използвани знания за моделиране и управление са от първостепенна важност.

Разпространението на глобалните информационни инфраструктури и внедряването на висшите информационни технологии във военното дело радикално промениха съотношението между огневата мощ и информационното осигуряване, което продължава да се променя с високи темпове, в полза на информационното осигуряване. Тази тенденция наложи да се преразгледат фундаменталните приоритети в структурата на въоръжените сили, тяхната екипировка, въпросите на командването и управлението, бойната подготовка и персоналният тренинг. На практика, превръщайки се в основен способ за радикално решаване на възникналите кризи и конфликти, информационните операции се превърнаха в една от основните стратегически заплахи за националната сигурност. В края на столетието Интернет, сателитните телевизионни системи, оптичните кабелно-разпределителни мрежи и мултимедийните технологии са монопол на малка част от човечеството, която предопределя тяхното развитие и начин на използване. Публичността на информационните канали и носители дава възможност за достъп до тях на всеки. Но този достъп днес е поставен под контрол и е собственост на малка група държави, корпорации и частни лица, които получават едно ново стратегическо превъзходство.

Днес оперативният командир може надеждно и когато е необходимо, непрекъснато да комуникира с все по-разсредоточени сили в зоната на операцията. Информацията може да бъде предадена и получена в световен мащаб, в рамките не само дадена зона, но също и на стотици и хиляди километри извън границите, в които са разположени приятелските и вражеските сили. Новините за военните действия се излъчва в реално или в почти реално време. Глобалната информационна среда вече има дълбоко въздействие върху геополитиката, икономиката, военните дейности като цяло и операциите. Колкото повече една страна използва информация, толкова е по-уязвима нейната икономика и общество от нарушаване или дори парализа от действията на враждебни правителства или групи, проявяващи прикрита или явна враждебност. В информационната война географското местоположение и разстояние оказват съществено влияние върху използването на интернет.

Логично възниква въпросът за мястото на въоръжените сили в борбата за господство в световното информационно пространство. Създаването на възможности за тотален контрол и управление на информационните канали на въоръжените сили, позволява на реализиралия го:

- да концентрира и подчини човешките знания и култура на военната практика, като ги използва в реално време в боя;
- да създаде нова концепция за организацията и управлението на въоръжените сили, базираща се на превъзходство (доминиране) със знания на бойното поле.

Новите информационни техники и технологии позволяват на оперативните командири и техните екипи да имат много по-подробна и точна информация отколкото са имали в миналото за всички аспекти на физическо пространство. Това е критичен елемент в оценката на оперативният командир за ситуацията при планиране и провеждане на кампании или операции.

На практика който успее да усвои новите информационни техники и технологии в процеса на управление на войските, ще си осигури максимално превъзходство над този, който е закъснял да направи това.

Информацията играе съществена роля в командването и управлението на силите. Веднъж започнали военните действия, командира трябва да бъде в състояние да коригира плановете си с цел намаляване на уязвимостта. Началото на това, което се нарича обща оперативна картина за командирите на всички нива на командване се превръща в реалност. Подбираната или непълна информация се заменя със стандартизирани комплекти съобщение, които предлагат по-малко възможности за объркване или двусмислие.

Погледнато през призмата на Въоръжените сили провеждането на информационни операции, представляват един елемент от глобалното информационно противоборство. Ето защо информационната политика и стратегия трябва да са постоянно действащи, а не да се формират за конкретна операция. Този пропуск може да се избегне чрез приемане на постоянно действащи документи в тази област, които трябва да са в съответствие с действащите съюзнически документи. Само тогава ще можем да говорим за равностойно участие на въоръжените ни сили в информационни операции в многонационална среда. В НАТО е приета директива за стратегическите ко-

муникации ACO Directive (AD) 95-2, ACO Strategic communications, 18 April 2012 и политика за информационните операции Military decision on MC 0422/4, NATO Military policy on information operations, 20 July 2012, които са двата основни регламентиращи документа на съюза в областта на информационните операции, прилагането на които е предпоставка за съвместимост между националните и съюзните способности в тази област, както и възможност за постигане на информационно превъзходство при провеждането на съвместните операции.

Информационните операции са интегрираща функция, насочена към информационната среда, а не толкова към способностите. Информационните цели са степен от планираното координиране и съгласуване на всички военни възможности, инструменти и техники, засягащи информацията или информационните системи. Употребата на сила може да допринесе за постигане на желания ефект в информационната среда. Всички планове и дейности следва да бъдат координирани и синхронизирани, с разрешени противоречия, за да не се правят компромиси с една дейност, което да доведе до отхвърляне или намаляване на желания ефект от друга. В многонационалните съвместни сили тази координация е отговорност на органите провеждащи информационните операции и се синхронизира в **Координационния съвет за информационни операции**. Той е подчинени на съвместния координационен съвет и е неразделна част от него, като в следствие на неговата дейност се изготвя анекс по информационните операции, като приложение към съвместната координационна заповед. Вариант на състава на координационния съвет за информационни операции е посочен в фигура № 1.

Фигура № 1

Координационен съвет за информационни операции (вариант)

Псих.опер.-психологически операции.
СКС за ЦЦЦ-представител от съвместен координационен съвет за таргетинг
ЮС-юридически съветник.
ПС-политически съветник.
КМО-компютърно мрежови операции.
Секр.-секретар.
J2, 3, 5 - представители от отдели.
ООВ - офицер по обществени въпроси.
ОЦЕВСР - оперативен център за електронна война и сигнално разузнаване.

- *ядро*
- *изисквани*

Съвместният координационния съвет за информационни операции допринася за реализирането на таргетинг процеса чрез номиниране на цели, които могат да повлияят чрез своите действия на провеждането на информационните операции. Съвместния координационния съвет за информационни операции съветва за последяващо появяване на нежелани ефекти в информационната среда и координира военните информационни дейности с цел избягване на нежелани ефекти.

Друг аспект на информацията е сътрудничество с медиите. Военните лидери на всички нива трябва да са наясно, че в ерата на информацията всички военни събития и действия се представят чрез медиите и това може значително да повлияе на общественото мнение, както и на ангажираността на силите.

Информацията включва не само познания и разузнавателни сведения, но и разнообразна информация от страна на медиите, която засягат морала, дисциплината, единството и мотивацията за борба. Информацията също оказва влияние върху морала на населението а оттам и на волята на страната да се бори. Това пряко или косвено влияе върху политическото ръководство и оперативния командир. По този начин информацията е едно от най-важните съображения при вземането на стратегически и оперативни решения.

Информацията все по-често засяга всичките три традиционни оперативни фактора. Нейният ефект върху фактора на пространството нараства, особено в невоенни аспекти на ситуацията. Това вече има някои съществени последици върху използването на военни сили за изпълнение на оперативните и стратегическите цели, което я определя като основен оперативен фактор. Стойността на информацията не трябва да се подценява, но също така не трябва и да се преувеличава. Информацията трябва правилно да се разглежда като помощ за оперативният командир и неговия щаб. Самата сложност и количеството на информацията се увеличават и ще имат решаващо влияние върху бъдещите резултати на кампаниите или операциите.

Заключение

Резултатите от направеното изследване позволяват да се направят следните **изводи**:

1. Войните в края на изминалия век нагледно показаха, че превъзходството ще е на страната на онези военни организации, които имат по-голяма информационна мощ, т.е. по-добра обработка на информация в инфраструктурните си подсистеми;

2. Бъдещата война ще е изцяло организационно явление, в което всяка от страните ще използва своята държавна мощ за унищожаване на противника. В началото на XXI век ще сме свидетели на невиждан синергизъм в концентрацията на тази мощ, постигнат чрез тотално използване на информационните технологии;

3. Като отчитаме тенденцията на насищане на съвременните информационни инфраструктури с качествено нови средства и технологии и особено автоматизацията на управлението на страните в мирно и военно време, можем да направим извода, че опасността от несанкциониран достъп в тях и провеждане на информационни операции нараства. Това е причината за предприемане на решителни мерки от редица държави по изграждане на информационна отбрана и защита на населението от информационна агресия и опазване на националните интереси в информационното пространство.

4. Характерът на бъдещите информационни конфликти, в повечето случаи ще се формулира като "не военни операции". Малко ще са нациите, които ще имат възможността да водят стратегическа информационна война във всичките и форми. По-скоро тези войни ще са локални, краткотрайни и едностранни по форма и вид.

5. Информационната война е концепция за постигане на решителните (крайни) военни и политическите цели чрез използване на нови нетрадиционни средства и форми на въоръжена борба за въздействие върху обществените информационни инфраструктури на противника с цел - нарушаване (или разрушаване) на организационния интегритет и командно-управленската свързаност на обществото и постигане по този начин на решителните (крайните) военни и политически цели на военната кампания.

6. Анализът на фигура №1 показва, че съществува определена зависимост между информационните операции и съвместния таргетинг процес.

Литература:

1. Желев, Ж. Отговорности при планирането на информационните операции. *Сборник научни трудове – част I*, 2014, стр. 78-85, ISSN 1313-7433.
2. Доктрина на Въоръжените сили на Република България, С., 2011, НП-3,
3. Доктрина за провеждане на операциите, С., 2012.
4. Национална отбранителна стратегия, С., 2011.

5. Стратегия за национална сигурност, С., 2011.
6. Alexandrov, B. Petrov, V. ISIS/ISIL into the “Internet” – Political and Military Weapon. *Годишник на Национален военен университет* „Васил Левски“. Велико Търново: НВУ „Васил Левски“, 2017, стр. 274-283. ISSN 1312-6148.
7. AJP-3.1, Allied joint doctrine, for Information operations, 2009.

Ivelin G. Katsev,

METHOD FOR EVALUATION OF THE ARTILLERY FIRE EFFECTIVENESS AGAISNT AREA TARGET

Ivelin G. Katsev

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

***ABSTRACT**: Artillery’s effectiveness heavily depends on how accurate and powerful will be weapon delivery, which is a function of dependent and independent errors, effective weapon radii, salvo coverage and target resilience, all of those are related to weapon-target interaction.*

***KEY WORDS**: Damage probability, damage function, multiple weapons with dependant error.*

МЕТОД ЗА ОЦЕНКА НА ЕФЕКТИВНОСТТА НА АРТИЛЕРИЙСКИЯ ОГЪН ПО ГРУПОВА ЦЕЛ

Ивелин Г. Кацев

Въведение

Артилерията е основно огнево средство на сухопътния компонент за поразяване на различни цели и обекти на противника разположени в зоната на операцията. Главното съдържание на бойното използване на артилерийските формирования е огневата поддръжка. Огневата поддръжка е една от основните бойни функции и представлява прилагане на огнева мощ, чрез използване на огъня на огневите системи в състава на артилерийските формирования. Основна задача на артилерията е максимално да се намали бойния потенциал на групировката на противника и да се ограничат неговите възможности за водене на бойни действия. Успеха на операцията зависи от ефективността на огневата поддръжка, която от своя страна зависи от ефективността на войските и силите участващи в поддръжката. Като основно средство на сухопътния компонент, участващо в огневата поддръжка, артилерията има основна роля за постигане и удържане на огнево превъзходство в операцията.

Артилерийските формирования поразяват различни по характер цели и обекти на противника. Целите и обектите в състава на противниковата групировка в операциите могат да бъдат най-общо разделени на отделни и групови. За да изпълним целта на това изследване ще се съсредоточим върху огневото въздействие по групови цели и метода за определяне на ефективността на огъня на артилерията по тях.

Ефективността на огъня на артилерията по групова цел зависи от вероятността за поразяване на елементарните цели в състава на груповата цел. Тази вероятност зависи от:

- отклонението, в разстоянието и направление на точката на попадение от центъра на целта(точката на мерене);
- разположението на елементарните цели спрямо точката на мерене,
- поразяващото действие на един снаряд;
- накриването на целта от огневото въздействие;
- устойчивостта и подвижността на груповата цел.

Отклоненията в разстояние и направление са породени от множество случайни грешки свързани със спецификата на работата на артилерийските формирования по подготовка на данните за стрелба. Случайните грешки обикновено се делят на два вида: повтарящи се за всички изстрели свързани с неточности в насочването вследствие на грешки в пресмятането на координатите на ОП, НП и целта, грешки в насочването на огневите системи, грешки при определяне на метеорологичните и балистичните условия на стрелбата и други. Втория вид случайни грешки са неповтарящите се грешки свързани с балистично разсейване на снарядите причинени от отклонения във формата на боеприпасите, ъгъла на изхвърляне на снаряда, количеството на барута използвано в гилзите и други.

Елементарните цели в състава на груповата се приемат за равномерно разпределени и стрелбата на артилерийските формирования се характеризира с нормално разпределение.

Поразяващото действие на снарядите в зависимост от вида на снаряда, взривателя и съответното накриване на целта от проекцията на огневото поразяване на артилерийските формирования показват количествената стойност на ефективността на поразяването.

1. Метода за оценка на ефективността на огневото въздействие на артилерийските формирования по групова цел

Метода за определяне на ефективността на стрелба за поразяване на артилерийските системи по групова цел може да бъде разгледан в следния алгоритъм:

1. Определят се средно-квадратичните отклонения на грешките от разсейването и грешките в подготовката на данни за стрелба по формулите:

$$(1)\ \sigma_{mpi_x} = \frac{E_{x_s}}{0.6745}$$

$$(2)\ \sigma_{mpi_y} = \frac{E_{y_s}}{0.6745}$$

$$(3)\ \sigma_{d_x} = \frac{E_{d_x}}{0.6745}$$

$$(4)\ \sigma_{d_y} = \frac{E_{d_y}}{0.6745}$$

$$(5)\ \sigma_x = \sqrt{{\sigma_{mpi_x}}^2 + {\sigma_{d_x}}^2}$$

$$(6)\ \sigma_y = \sqrt{{\sigma_{mpi_y}}^2 + {\sigma_{d_y}}^2}$$

където:

σ_{MPI_x} и σ_{MPI_y} – стандартни отклонения в разстояние и направление на срединните грешки от подготовката;

σ_{PE_x} и σ_{PE_y} – стандартни отклонение на балистическото разсейване;

E_{d_x} и E_{d_y} – случайни грешки от балистическото разсейване на снаряда, който се изчисляват в зависимост от количеството и вида на артилерийски системи участващи в огневото въздействие, по формулите:

$$(7)\quad E_{d_x} = \sum_{i=1}^{n} E_{d_{x_i}}$$

$$(8)\quad E_{d_y} = \sum_{i=1}^{n} E_{d_{y_i}}$$

E_{x_s} и E_{y_s} – сумарни грешки в подготовката на данните за стрелба, който се изчисляват в зависимост от количеството и вида артилерийски системи участващи в огневото въздействие, по формулите:

$$(9)\quad E_{x_s} = \sqrt{E_{x_1} + \cdots + E_{x_j}}$$

$$(10)\quad E_{y_s} = \sqrt{E_{y_1} + \cdots + E_{y_j}}$$

$$(11)\quad E_{x_j} = \sum_{i=1}^{n} E_{x_i}$$

$$(12) \quad E_{y_j} = \sum_{i=1}^{n} E_{y_i}$$

, където:

$E_{d_{x_i}}$ и $E_{d_{y_i}}$ – случайни грешки от балистическото разсейване на снарядите за артилерийските системи участващи в огневото въздействие;

E_{x_i} и E_{y_i} – срединни грешки в разстояние и направление от подготовката на данните за стрелба на i-тия елемент за огневото формирование;

E_{x_j} и E_{y_j} – срединна грешка в разстояние и направление в подготовката на данните за стрелба за огневото формирование;

i – брой на елементите влизащи в подготовката на данните за стрелба;

j – брой на огневите формирования участващи в поразяването на груповата цел.

2. Определяне на поразяващото действие на снарядите и ефективната зона за поразяване на целта

Поразяване с ударна вълна от разрива на снаряда:

$$(13) \quad S_r = \overline{Al}$$

$$(14) \quad S_d = S_r$$

Поразяване с осколките от разрива на снаряда:

$$(15) \quad S_r = \overline{Al * \alpha}$$

$$(16) \quad S_d = \frac{S_r}{\alpha}$$

където:

S_r – размери на ефективната зона за поразяване на един снаряд в разстояние;

S_d – размери на ефективната зона за поразяване на един снаряд в направление;

Al – размери на приведената площ за поразяване на целта;

α – коефициент отчитащ ъгъла на падане.

3. Изчисление на увеличената зона за поразяване на всяка огнева система, със стойността на балистическото разсейване и намиране на условната вероятност за поразяване:

$$(17) \quad S_r^k = S_r + k * E_{d_x}$$

$$(18) \quad S_d^k = S_d + k * E_{d_y}$$

$$(19) \quad P_{CD1} = \frac{S_r * S_d}{S_r^k * S_d^k}$$

където:

k – коефициент на статистически анализ на грешките в следствие разсейването на снаряда;

S_r^k – увеличена зона за поразяване с отчитане на балистическото разсейване в разстояние;

S_d^k – увеличена зона за поразяване с отчитане на балистическото разсейване в направление;

P_{CD1} – условна вероятност за поразяване.

4. Определяне на проекцията на огневото въздействие и зоната на целта накрита от стрелбата:

$$(20) \quad L_c = (N_m - 1) * \frac{L_a}{N_m}$$

$$(21) \quad W_c = (N_w * N_u - 1) * \frac{W_a}{N_w * N_u}$$

$$(22) \quad L_{vp} = L_c + S_r^k$$

$$(23) \quad W_{vp} = W_c + S_d^k$$

където:

N_m и N_w – броя на точките на насочване на огневите системи в разстояние и направление;

L_c и W_c– коефициенти отчитащи размерите на целта и броя на точките за насочване на огневите системи;

L_{vp} и W_{vp}– размери на проекцията на залпа на огневите системи с отчитане размерите на целта.

5. Определяне на застъпването на зоните за поразяване на снарядите на отделните артилерийски системи.

$$(24) \quad n_{od} = N_w * N_u * \frac{S_d^k}{W_{vp}}$$

В зависимост от стойността на n_{od} дали е по голяма или по-малка от единица се изчислява условната вероятност за поразяване в направление $P_{CD\backslash d}$ с използване на различен математически апарат:

$$(25) \quad n_{od} < 1 \rightarrow P_{CD\backslash d} = N_w * N_u * P_{CD1} * \frac{S_d^k}{W_{vp}}$$

$$(26) \quad n_{od} \geq 1 \rightarrow P_{CD\backslash d} = 1 - \left(1 - P_{CD1}\right)^{n_{od}}$$

Изчисляването на застъпването на зоните за поразяване на оръдията в разстояние n_{or} се определя с помоща на формулите:

$$(27) \quad n_{or} = N_m * \frac{S_r^k}{L_{vp}}$$

$$(28) \quad n_{or} < 1 \rightarrow P_{CD\backslash s} = N_m * P_{CD\backslash d} * \frac{S_r^k}{L_{vp}}$$

$$(29) \quad n_{or} \geq 1 \rightarrow P_{CD\backslash s} = 1 - \left(1 - P_{CD\backslash d}\right)^{n_{or}}$$

6. Определяме ефективността на стрелбата на артилерията по груповата цел.

Определя се увеличената зона за поразяване в разстояние и направление:

$$(30) \quad LEP = max\left(L_{vp}, L_a\right)$$

$$(31) \quad WEP = max\left(W_{vp}, W_a\right)$$

където:

LEP – увеличена зона за поразяване в разстояние;

WEP – увеличена зона за поразяване в направление.

Пресмятане на границите на интервалите с помощта, на които ще може да бъде определена очакваната зона, която накрива модела на поразяваната площ от огневите системи. В разстояние формулите имат следния вид:

$$(32) \quad S_{range} = \frac{LEP + L_a}{2}$$

$$(33) \quad T_{range} = \frac{LEP - L_a}{2}$$

$$(34) \quad a_{range} = \frac{S_{range}}{\sigma_{x^*}\sqrt{2}}$$

$$(35) \quad b_{range} = \frac{T_{range}}{\sigma_{x^*}\sqrt{2}}$$

В направление формулите са идентични:

$$(36) \quad S_{deflection} = \frac{WEP + W_a}{2}$$

$$(37) \quad T_{deflection} = \frac{WEP - W_a}{2}$$

$$(38) \quad a_{deflection} = \frac{S_{deflection}}{\sigma_{y^*}\sqrt{2}}$$

$$(39) \quad b_{deflection} = \frac{T_{deflection}}{\sigma_{y^*}\sqrt{2}}$$

След това се пресмятат интервалите в разстояние:

$$(40) \quad I_{r_1} = normcdf\left(T_{range}, 0, \sigma_x\right) - normcdf\left(-T_{range}, 0, \sigma_x\right)$$

$$(41) \quad I_{r_2} = \frac{LEP + L_a}{2 * L_a}\, normcdf\left(T_{range}, 0, \sigma_x\right) - normcdf\left(-S_{range}, 0, \sigma_x\right)$$

$$(42) \quad I_{r_3} = \frac{LEP + L_a}{2 * L_a} normcdf\left(S_{range}, 0, \sigma_x\right) - normcdf\left(T_{range}, 0, \sigma_x\right)$$

$$(43) \quad I_{r_4} - I_{r_5} = \frac{2\sigma_x}{L_a\sqrt{2\pi}}\left(e^{-a_{range}^2} - e^{-b_{range}^2}\right)$$

Аналогично се постъпва за направлението.

Сумират се получените стойности и резултата е очакваното накриване на целта от поразяваната площ от огневите средства $E\ F_c$ в разстояние и направление:

$$(44) \quad E\ F_r = I_{r_1} + I_{r_2} + I_{r_3} + I_{r_4} - I_{r_5}$$

$$(45) \quad E\ F_d\ = I_{d_1} + I_{d_2} + I_{d_3} + I_{d_4} - I_{d_5}$$

$$(46) \quad E\ F_c\ = E\ F_r\ * E\ F_d$$

За изчисляване на очакваната поразена площ от целта (Expected Fractional Damage $E\ D$) използваме очакваното накриване на целта от поразяваната площ от огневите средства $E\ F_c$, надежността на въоръжението R и условната вероятност за поразяване $P_{CD\backslash s}$ съгласно следната формула:

$$(47) \quad E\ D\ = E\ F_c\ * \ 1 - \ 1 - R * P_{CD\backslash s}\ ^{n_v}$$

където:

n_v – броя на залповете на артилерийските системи.

Пример: Стрелба по групова цел с размери по фронта 300м., в дълбочина 200м., разстояние на стрелбата 12км, сумарна грешка от подготовката в разстояние $E_{x_s} = 75$м, сумарна грешка от подготовката в направление $E_{y_s} = 44$м, случайна грешка от разсейването в разстояние $E_{d_x} = 46$м, случайна грешка от разсейването в направление $E_{d_y} = 23$м; брой артилерийски системи участващи в огневото въздействие $N_w = 8$; брой на мерници $N_m = 3$; разхода на снаряди по норма $N = 108$.

Таблица 1 Стойности на параметрите от метода за оценка на ефективността на стрелбата на артилерията по групови цели определени чрез използване на софтуер за обработка „Excel" и програмен пакет „Data analysis".

Параметър	Стойност	Параметър	Стойност	Параметър	Стойност
E_{x_s}	75	S_r	24,9	S_{range}	248,1
E_{y_s}	44	S_d	28,4	T_{range}	48,1
E_{d_x}	46	S_d^k	194,5	a_{range}	2,57
E_{d_y}	23	S_r^k	100,5	b_{range}	0,99
N_w	8	P_{CD1}	0,036	$S_{deflection}$	329,9
N_m	3	L_c	133,3	$T_{deflection}$	29,9
N	108	W_c	262,5	$a_{deflection}$	3,17
σ_{mpi_x}	111,2	L_{vp}	296,2	$b_{deflection}$	0,28
σ_{mpi_y}	65,2	W_{vp}	259,9	$E\ F_r$	1,27
σ_{d_x}	68,2	n_{od}	2,16	$E\ F_d$	1,24
σ_{d_y}	34,1	$P_{CD\backslash d}$	0,077	$E\ F_c$	1,56
σ_x	130,4	n_{or}	1,65	$E\ D$	0,362
σ_y	73,6	$P_{CD\backslash s}$	0,123	36,2% МО на процента поразени елементарни цели	

Заключение

Резултатите от направеното изследване позволяват да се направят следните **изводи**:

1. Таблица 1 показва математическото очакване на процента поразени елементарни цели в състава на груповата цел по входните данни от примера по реда на предложения метод за оценка на ефективността на стрелбата за поразяване по групови цели;
2. Условната вероятност за поразяване на коя да е елементарна цел в състава на груповата цел е 3,6%;
3. Застъпването на зоната за поразяване в направление е $n_{od} = 2{,}16$, в разстояние е $n_{or} = 1{,}65$, което повишава условната вероятност за поразяване $P_{CD\backslash s} = 12{,}3\%$;

4. Вероятността за поразяване на груповата цел при така зададените стойности е 36,2%, което отговаря на степента за поразяване унищожение;
5. Модела за оценка на ефективността на поразяване на артилерийските формирования по групова цел обхваща всички аспекти на огневото въздействие и позволява моделирането на стрелбата по груповата цел с задача да разкрие най-благоприятните условия при което ще бъде изпълнена задачата за поразяване на целта;
6. Оценката на ефективността на стрелбата на артилерийските системи е основен елемент при определяне съотношението на сили и средства в операцията.

Литература:

1. Атанасов, А. Проблеми на определяне на степените за поразяване на войскова групировка в операциите. Сборник научни трудове, научна сесия НВУ "В.Левски", факултет "Артилерия, ПВО и КИС", 2010, стр. 69-78, ISSN 1313-7433.
2. Марков, Д. Повишаване на способностите на артилерийските системи за изпълнение на задачи в системата за артилерийска поддръжка на сухопътен компонент. *Сборник доклади от Годишна университетска научна конференция, електронна издание, издателски комплекс на НВУ „Васил Левски”*, 2019, с. 842-851, ISSN 2367-7481.
3. Anderson, C. Generalized weapon effectiveness modeling. *Master’s Thesis, Naval post graduate school*, 2004, p 113.
4. Explosive weapon effects. *Report, GICHD, Geneva*, 2017 ISBN: 978-2-940369-61-4.
5. Eckler, A., Burr, S. Mathematical models of target coverage and a missile allocation. *Military operations research*, 1972, p 254.
6. Wang, H., et al, Average damage caused by multiple weapons against an area target of normally distributed elements. *American journal of operations research*, 2017,vol 7, pp289-206, ISSN: 2160-8830.
7. Washburn, A. Diffuse-Gaussian multiple-shot pattern. *Military operations research*, 2003, v8, n 3, pp 59-64.

Ivelin G. Katsev,

REGRESSION AND CORRELATION ANALYSIS OF FACTORS INFLUENCING ARTILLERY FIRE

Ivelin G. Katsev

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

***ABSTRACT**: Major elements in the effectiveness of artillery are the factors affecting artillery fire, they needs to be analyzed and evaluated for their possible functional dependencies and relationship to firing efficiency, by means of regression and correlation analysis it can be determined functional relationship and correlation between random errors in preparation and artillery fire effectiveness.*

***KEY WORDS**: Correlation analysis, Regression analysis, Factors influencing artillery fire.*

РЕГРЕСИОНЕН И КОРЕЛАЦИОНЕН АНАЛИЗ НА ФАКТОРИТЕ, ВЛИЯЕЩИ НА СТРЕЛБАТА НА АРТИЛЕРИЯТА

Ивелин Г. Кацев

Въведение

Артилерията е основно огнево средство на сухопътния компонент, участващо в огневата поддръжка в операциите. Основна задача на артилерията е максимално да се намали бойния потенциал на групировката на противника и да се ограничат неговите възможности за водене на бойни действия. Успеха на операцията зависи от ефективността на огневата поддръжка, която от своя страна зависи значително от ефективността на използване на артилерийските формирования. Значителна част от ефективното използване на артилерийските формирования се заключава в ефективността на огневото въздействие по целите на противника.

Ефективността на стрелбата за поразяване на артилерията зависи от следните фактори:

- характера, вида, размерите и устойчивостта на целта;
- подвижността на целта;
- точността в определяне на данните за стрелба на артилерията;
- характеристика на техническото разсейване и надежноста на въоръжението;
- поразяващото действие на снарядите;
- количеството артилерийските системи за стрелба от закрита огнева позиция и средства за стрелба с право мерене, привличани за поразяването на противника;
- разхода на снаряди при неконтролируемо поразяване на целта;
- способа за обстрел на целта (броя на мерниците и ъгломерите, скока по мерника и скока по взривателя и интервала на веера за батареята, разпределението на снарядите по мерници, ъгломери и оръдия);
- реда и темпа за водене на огъня от артилерията;

- точността в определянето и въвеждането на корекция през време на стрелбата на артилерията и средствата за стрелба с право мерене;
- противодействието от страна на противника.

Факторите влияещи на ефективността на стрелбата могат да бъдат разгледани като сума от срединни грешки и срединни отклонения, които характеризират елементите влизащи в състава на всеки фактор, например грешките при определяне на данните за стрелба, техническото разсейване, поразяващото действие на боеприпасите във всяка конкретна стрелба се проявяват случайно и за тях предварително чрез теоретични изследвания и практически анализ се определят съответстващите характеристики, които след това се използват при оценка на бойната ефективност. Други фактори,като количеството артилерия привличана за стрелба, способът за обстрел на целта могат да бъдат избирани в зависимост от характера на целта и задачата.

Като се изхожда от съдържанието и реда за подготовка на данни за стрелба и поради закръгляванията, които се правят в данните за мерника и ъгломера, може да се отделят следните независими групи източници на грешки:

- топогеодезическата подготовка $-X_{\text{тг}}$ и $Z_{\text{тг}}$;
- положението на целта $-X_{\text{ц}}$ и $Z_{\text{ц}}$;
- метеорологичната подготовка $-X_{\text{м}}$ и $Z_{\text{м}}$;
- балистичната подготовка $-X_{\text{б}}$;
- таблиците за стрелба - $X_{\text{тс}}$ и $Z_{\text{тс}}$;
- закръгляванията на данните за мерните прибори - $X_{\text{зак}}$ и $Z_{\text{зак}}$;
- техническата подготовка - $X_{\text{тех}}$ и $Z_{\text{тех}}$.

Източниците на грешки могат да бъдат разделени, както следва:

- Оръдейни източници на грешки:
  a. заради износване на канала на тялото;
  b. в техническата подготовка;
  c. в следствие на разсейването;
- Батарейни източници на грешки:
  a. при определяне положението на огневата позиция;
  b. при определяне на температурата на заряда;
  c. при определяне на балистичните характеристики на барута;
  d. при ориентиране на оръдията;
- Дивизионни източници на грешки:
  a. при определяне положението на целта;
  b. при определяне положението на огневата позиция;
  c. в метеорологичната подготовка;
  d. поради разликите във физико-химичните свойства на партидата заряди;
  e. заради грешки(закръглявания) в таблиците за стрелба.

От разгледаните източници на грешки се установява, че случайните грешки при подготовката на данните в разстояние $X_{\text{п}}$ и в направление $Z_{\text{п}}$ могат да се представят като сума от независими случайни грешки по формулите:

$$1. \qquad X_{\text{п}} = X_{\text{ц}} + X_{\text{м}} + X_{\text{б}} + X_{\text{тс}} + X_{\text{зак}} + X_{\text{тех}}$$

$$2. \qquad Z_{\text{п}} = Z_{\text{ц}} + Z_{\text{м}} + Z_{\text{тс}} + Z_{\text{зак}} + Z_{\text{тех}}$$

Съвкупността от грешките в подготовката и грешките в разсейването се нарича система от грешки съпровождаща стрелбата за поразяване. Системата от грешки по повторяемост зависи от количеството огневи средства, изпълняващи огневата задача, организационно-щатната структура на артилерийските формирования и организацията на подготовката на данните за стрелба и управление на огъня. Следователно могат да се идентифицират групите грешки въз основа на количеството артилерия, което изпълнява огневата задача.

1. Грешки при стрелба с дивизион:

- случайни грешки, които се повтарят за всички батареи от дивизиона – Δд;
- случайни грешки, които се повтарят за всички оръдия на i-тата батарея, но не и за останалите батареи – Δб;
- случайни грешки, които се повтарят за всички изстрели на j-тото оръдие от i-тата батарея – Δор;

грешки в разсейването на k-тия изстрел на j-тото оръдие от i-тата батарея – Δр.

2. Грешки при стрелба с батарея:

- случайни грешки, които се повтарят за всички оръдия на батареята – Δб;
- случайни грешки, които се повтарят за всички изстрели на j-тото оръдие от батареята – Δор;
- грешки в разсейването на k-тия изстрел на j-тото оръдие от батареята – Δр.

3. Грешки при стрелба с оръдие:

- случайни грешки на изстрела на оръдието – Δор;
- грешки в разсейването на k-тия изстрел на оръдието – Δр.

Количеството на грешките, съставящи системата от грешки зависи от назначения разход на снаряди за изпълнение на огневата задача. При допускане, за конкретна стрелба да бъдат изразходвани N снаряда, то системата от грешки ще се състои от N вектор-грешки.

Свеждане на системата от няколко групи грешки (стрелбата с батарея, дивизион, група артилерия се съпровожда съответно с три, четири и пет групи грешки) към еквивалентна система от две групи грешки, се състои в:

- изчисляване на приведените повтарящи се срединни грешки (грешки в подготовката на данните) в разстояние Ep_o и направление En_o при стрелба с батарея, дивизион, група артилерия.

- изчисляване на приведените неповтарящи се срединни отклонения (грешки в разсейването) в разстояние $\text{Вд}_\text{о}$ и направление $\text{Вс}_\text{о}$ при стрелба с батарея, дивизион, група артилерия.

Като основен елемент за ефективността на артилерията в операциите, факторите влияещи на стрелбата за поразяване е необходимо да бъдат анализирани и оценени техните възможни функционални зависимости и тяхната свързаност с ефективността на стрелбата. За целта, чрез регресионен и корелационен анализ определяме функционалните взаимовръзки и свързаността между случайните грешки в подготовката и ефективността на стрелбата.

Определяне на функционалните зависимости между случайните грешки в подготовката на данните за стрелба на артилерийска батарея въоръжена с оръдия-гаубици Д-20, на разстояния на стрелбата от 4км. до 16км., по цел с размери по фронта 300м., в дълбочина 200м., при разход на снаряди 48сн. резултатите са представени в таблица 1.

Таблица 1

км	Epo	Eno	Вдо	Всо	% пор
4	42	33	33	17	23,5
5	42,5	33,5	36	17,5	28,9
6	43	34	39	18	27,5
7	51	34,5	38,5	18,5	27,4
8	59	35	38	19	27,4
9	61	36,5	43	20	25,2
10	63	38	48	21	23,4
11	70	40	54	22,5	21,3
12	77	42	70	24	17,9
13	82,5	44,5	72	25	17,3
14	88	47	74,5	26	16,7
15	93,5	49,5	77	27	16,1
16	99	52	79	28	15,6

След определяне на ефективността на стрелбата за различните разстояния се извършва корелационен анализ с помощта на софтуер за статистическа обработка „Microsoft Excel" и програмния пакет за статистическа обработка „Data analysis".

Таблица 2

	км	*Ерo*	*Ено*	Вдо	Вco	% пор
км	1					
Ерo	0,992025	1				
Ено	0,966937	0,978558	1			
Вдо	0,960484	0,964669	0,969881	1		
Вco	0,988203	0,991297	0,989448	0,986318	1	
% пор	−0,89878	−0,92152	−0,92884	−0,95303	−0,94116	1

Определяне на функционалните зависимости между случайните грешки от подготовката и ефективността на стрелбата за поразяване. Данните от регресионния анализ са показани в таблици 3,4 и 5.

Таблица 3

SUMMARY OUTPUT	
Regression Statistics	
Multiple R	0,97779
R Square	0,956073
Adjusted R Square	0,924696
Standard Error	1,362699
Observations	13

Таблица 4

ANOVA TABLE					
	df	*SS*	*MS*	*F*	*Significance F*
Regression	5	282,9135077	56,58270154	30,47079717	0,000130869
Residual	7	12,9986396	1,856948515		
Total	12	295,9121473			

Таблица 5

	Coefficients	*Standard Error*	*t Stat*	*P-value*	*Lower 95%*	*Upper 95%*
Intercept	87,79636577	24,6774023	3,557763686	0,009247081	29,44358183	146,1491497
км	3,663441008	1,337264915	2,739502822	0,028938935	0,50131196	6,825570055
Ерo	−0,175211018	0,208789702	−0,83917462	0,429095173	−0,668920211	0,318498175
Ено	1,302308072	0,701913672	1,855367867	0,105929309	−0,357454019	2,962070164
Вдо	0,176680238	0,249252322	0,708840892	0,501341457	−0,412707847	0,766068323
Вco	−6,974938291	3,468718466	−2,0108113	0,08426486	−15,1771541	1,227277514

Заключение

Резултатите от направеното изследване позволяват да се направят следните **изводи**:

1. Данните в таблица 1 показват вероятността за поразяване на групова цел по данните от примера, от нея може да бъде наблюдавана промяната на вероятността за поразяване с промяна на разстоянието на стрелбата;

2. Корелационния анализ на данните от таблица 1 показва силна негативна корелация между разстоянието на стрелбата, срединните грешки от подготовката на данни за стрел-

ба(Epo,Eno), случайните грешки от разсейването(Вдо,Всо) и вероятността за поразяване на груповата цел, което показва, че статистическата (теоретична) зависимост и логическата (емпирична) зависимост се съвпадат, с увеличаване на стойността на грешките се намалява вероятността за поразяване на целта;

3. Корелационния коефициент на Пирсън (Multiple R) и коефициента на детерминация(R Square) показват каква част от вариацията на вероятността за поразяване се обяснява с промяна на срединните грешки от подготовката на данни за стрелба(Epo,Eno) и случайните грешки от разсейването(Вдо,Всо) (таблица 3);

4. Дисперсионния анализ включва две отделни таблици (таблица 4 и 5), като таблица 4 се използва за проверка на адекватността на регресионния модел, като отновен елемент тук е F-критерият на Фишер (*Significance F*).В случая *Significance* F = 0,000130869< 0,05, което означава, че зависимостта е статистически значима за избраното ниво на значимост 0,05. Таблица 5 съдържат данни за коефициентите на регресионното уравнение и тяхната статистическа значимост.

Литература:

1. Атанасов, А. Фактори влияещи на системата за индиректна огнева поддръжка. *Сборник научни трудове.* научна сесия НВУ "В.Левски", факултет "Артилерия, ПВО и КИС", 2014, стр141-146, ISBN-978-954-9681-60-4.
2. Илиев, К. Метод за определяне на бойният потенциал на войскови формирования. *International Scientific Conference, 2017, Collection of papers Shumen, Bulgaria*, с. 93-97, ISSN 2367-7902.
3. Cowan, G. Statistical data analysis, *Oxford University Press*, 1998.
4. Fann, Ch. Development of an artillery accuracy model. *Master’s Thesis, Naval Postgraduate School, 2006.*
5. Smith, M. Statistical analysis handbook. *The Winchelsea Press*, 2018, ISBN-978-1-912556-06-9.
6. Šilinger, K. et al, Artillery Firing Data Correction Calculation by Using Computers, *International journal of systems applications, engineering & development*, 2016, v10, pp 309-314 ISSN: 2074-1308.

Ivelin G. Katsev,

METHOD FOR CLASSIFICATION AND PRIORITIZATION OF THE TARGETS ENGAGED BY ARTILLERY

Ivelin G. Katsev

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

***ABSTRACT**: In modern armed conflicts, combat operations are characterized by great complexity, dynamism, unpredictability and short-termism, which creates the need for a more detailed definition of the targets in the opposing force, dynamic prioritization and timely updating of the prioritized list of targets and analysis of the number of target factors that affect the reconnaissance – target designation – target selection – target distribution process.*

***KEY WORDS**: target characteristics, target classification, target prioritization criteria.*

МЕТОД ЗА КЛАСИФИКАЦИЯ И ПРИОРИТИЗИРАНЕ НА ЦЕЛИТЕ, ПОРАЗЯВАНИ ОТ АРТИЛЕРИЯТА

Ивелин Г. Кацев

Въведение

Определяне на целите в зоната на операцията е основен елемент при планиране на огневата поддръжка в операциите и се извършва на базата на предварително уточнени и съгласувани методи с определени критерии за избор на цели. В различните операции, критериите за избор на цели са различни. Те се определят в зависимост от желания краен резултат. В бойни операции критериите за избор на цели са насочени към военни формирования и техните сили и средства. В операциите по поддържане на мира и други небойни операции критериите са насочени към лидерите на различните формирования, оказващи неблагоприятно влияние по време на възстановяване или опазване на мира. В зоната на операцията първоначално се определят обекти за разузнаване. След назначаване на въздействие по разузнатите обекти, те стават цели за поразяване. Целите се определят след задълбочен анализ на всеки обект от зоната на операцията, който може да бъде цел. За всяка цел се извършва анализ на ефективността при огневото въздействие, какви ще бъдат положителните и отрицателните ефекти от поразяването и как те влияят на групировките участващи в операцията, ефектите се анализират в икономическата, социалната, военната, информационната, инфраструктурата и политическа области. Този анализ се извършва за всяка цел и се явява основа за това, коя цел какъв приоритет ще има и къде ще попадне в приоритизирания списък с целите в зоната на операцията. Разпределянето на целите по етапи и фази на операцията, както и разпределяне на средства за въздействие по тях е основна задача на органите за планиране на огнева поддръжка на оперативно ниво извършвана с цел да се използва максимално ударите и огъня на ударните и огневите формирования на компонентите по целите на противника.

1. Същност, характеристики и видове цели

Целта е обект (лице, място или нещо), планиран за поразяване или въздействие за променя или неутрализиране на функцията, която изпълнява за противника. Оперативното значение на целта е характеризирано чрез извършване на оценка за определяне дали поразяването й е съвместимо с планираната операция, постигането на цел (целите) на командира и желаното крайното състояние.

Всяка цел има различни присъщи или придобити характеристики, които формират основата за откриване, определяне на местоположението, идентификация, класификация за текущо и бъдещо наблюдение, анализ, поразяване и оценка. Физическите, функционалните, когнитивните и други са категориите, които помагат да се определят общите характеристики на дадена цел.

Физически характеристики. Тези характеристики или функции помагат да се опише целта. Тези общи физически характеристики обикновено се различават от сетивата или чрез сензорно получени сигнатури и могат да оформят или влияят върху избора на вида и броя на оръжия, оръжейните системи и методите или тактиките, използвани срещу целта. Физическите характеристики най-често включват:

- Местоположение;
- Форма;
- Размер или заета площ;
- Външен вид (външна форма и характеристики, включително цвят);
- Брой и характер на елементите, съставляващи целта като цяло;
- Дисперсия или концентрация на елементи;
- Рефлексивност (към топлина, светлина, звук, радарна енергия и др.);
- Структурен състав;
- Степен на защитеност;
- Електромагнитен отпечатък (например радарни и радиопредавания).
- Характеристики на мобилността:
    - Стационарни (не могат да се движат);
    - Буксирни (работят от фиксирани позиции, но могат да бъдат преместени);
    - Мобилни (работят в движение или с много кратко време за заемане на позиция).

Функционални характеристики. Тези характеристики описват каква е и как се извършва бойната дейност на целта. Те характеризират функцията на целта в по-голяма система от цели, как целта или системата от цели функционира като общ елемент, нивото на активност, състоянието на нейната функционалност и някои случаи, функционалното значение. Функционалните характеристики често са трудни за различаване, като изисква внимателен преглед на известни факти и използването на дедуктивни и индуктивни разсъждения. Функционалните характеристики обикновено включват:

- Нормална или докладвана активност на целта;
- Състояние на целта (състояние или състояние в даден момент от време [напр. изпълняващ бойни задачи, не въведен в бой]).
- Степен, пропорция или процент на функционалност (напр. функционира на 50 процента, поразена);
- Материали, които целта изисква, за да изпълнява функциите си;
- Възможност за възстановяване на целта или нейната функция;
- Възможност за самозащита;
- Целево значение в рамките на оперативната структура;
- Необходими взаимоотношения (ако целта е отделна или групова, какви други елементи или формирования са необходими, за да може да функционира);
- Физически уязвимости (разкриване на потенциални точки за насочване по уязвимите части от целта).

Когнитивни характеристики. Тези характеристики описват как целите извършват бойни, информационни, контролни или управленски функции. Когнитивните характеристики са особено

важни при правилната оценка на критичните възли в система от цели на противника, тъй като всяка система има централен елемент с контролна или управленска функция. Неутрализиране на контролиращите или управленските функции може да има решаващо значение за постигане на желания краен резултат в операцията.

Както при функционалните характеристики, познавателни характеристики могат да бъдат трудни за идентифициране. Когнитивни характеристики може да се отнася до:

- Как целта извършват бойни, информационни, контролни или управленски функции;
- Как работи цикълът на вземане на решение на системата от цели на противника (ако е приложимо);
- Разкриване на необходимите елементи доставящи разузнавателна информация, които целта изисква за да изпълнява функциите си;
- Разкриване на когнитивни уязвимости на целта.

Характеристики на околната среда. Тези характеристики описват ефекта на среда за провеждане на операцията върху целта. Те могат също да повлияят на методите използвани за въздействие, разузнаване и наблюдение.

- Атмосферни условия(температура, видимост и т.н.);
- Характеристики на терена (форма на земята, растителност, почва и др.);
- Възможности за укриване и маскировка;
- Физически взаимоотношения (като близост с цивилни, приятелски сили и др.);
- Зависимости (суровини, персонал, енергия, вода и др.).

Времеви характеристики. Времето, като характеристика на целта, описва уязвимостта на целта за разкриване, поразяване или друг вид въздействие във връзка с времето на разположение. Всички потенциални цели и всички цели, планирани за поразяване, непрекъснато променя приоритета си поради динамичния характер на развиващата се оперативна среда. Тази характеристика може да помогне за определяне кога и как да се разкрие или порази дадена цел. Сравнявайки времевата характеристика с инертността на информационния поток и познаването на възможностите на собствените формирования, могат да бъдат определени по-добри препоръки към командира по отношение на възможни действия в определена ситуация. Факторите допринасящи за това включват:

- Време на появяване(въвеждане в бой). Очакваното време, за което целта ще се появи в определена оперативна зона;
- Време за престой. Очаква се продължителността на времето, през което дадена цел ще остане на едно място (може да бъде пряко свързано с физическата характеристика – мобилност). Целта е по-трудна за разкриване или поразяване, когато е в движение;
- Време за изпълнение на бойната си задача. Времето, необходимо за целта да започне да функционира, да изпълни задачата си и да се укрие;
- Идентифицируемо време. Времето, през което дадена цел може да бъде идентифицирана като заплаха.

Артилерийските формирования поразяват различни по характер цели на бойното поле, които най-основно могат да се разделят на отделни и групови.

Отделни цели са такива цели за поразяване, които не могат да се разделят на други елементарни цели или да се разчленяват на части, без да се наруши тяхната физическа цялост. Такива цели на бойното поле са: отделен танк; бойна машина на пехотата; бронетранспортьор; радиолокационна станция; установка противотанков ракетен комплекс; противотанково оръдие; минохвъргачка; оръдие; гаубица; бойна машина; командно-наблюдателен пункт на батальон и рота; център за управление на огъня на дивизион, команден пункт на батарея и други.

Групови цели са такива цели, които се състоят от еднородни или разнородни елементарни цели, разположени на определена площ. Към тях се отнасят: пунктовете за управление; батареи и взводове реактивни системи за залпов огън и полева артилерия; батареи и взводове за противовъздушна отбрана; пехотни, мотопехотни и танкови взводове и роти на отбранителна позиция;

пехотни, мотопехотни и танкови взводове и роти в райони за съсредоточаване, при извършване на марш, развърнати в боен ред при настъпление, в райони за съсредоточаване и други.

Освен основното разделение на целите, могат да бъдат разгледат и други разпределения на целите по-важните от които са:

- Маневрени и стационарни;
- Бронирани и небронирани;
- Еднородни и разнородни.

Група цели са целите, обединени в групи по важност, еднородни признаци и характер на използване на бойното поле, по които е необходимо да се води огън едновременно. Такива цели могат да бъдат: средствата за противовъздушна отбрана; артилерията; маневрените формирования; авиацията; корабите; пунктове за командване и управление и др.

Система от цели е съвкупност от всички функционално свързани цели разположени в определен географски район и се определя, като група цели, свързани по такъв начин, че с поразяването им се постига определен ефект, необходим на атакуващия (отбраняващия се).

Групировката на войските е съвкупност от отделните и груповите цели на бойното поле, обединени от общо управление и действащи по единни намерения и план. Тя може да бъде групировка на войските в Театъра на операцията (зоната на операцията), в зоната на сухопътната операция и полосите за действия на маневрените формирования, на направленията на ударите, на тактическите направления, на участъка за съсредоточаване на усилията и т. н.

2. Класификация на целите

Целите, поразявани от артилерията от закрити огневи позиции могат да се класифицират и характеризират според планираните или възможни въздействия по тях и се разделят на:

- Планови цели (по график) са тези,за които се знае, че съществуват в зоната на операцията и по тях е планирано въздействие в определен момент;
- Целите по извикване са планови цели, по които не е планирано времето за въздействие. Огневото въздействие по тези цели е планирано посредством плановия процес на целеобразуване, целеразпределение и целеуказване, но изпълнението обикновено се извършвана базата на динамичния процес на целеобразуване, целеразпределение и целеуказване;
- Непланови цели са тези, за които се знае, че съществуват в зоната на операции, но те не са открити или локализирани и по тях не е планирано въздействие в определен момент;
- Неочаквани цели са тези, които са неизвестни или неочаквани в зоната на операцията, но когато се открият или локализират, изискват незабавна преценка и решение как те ще влияят върху хода на операцията и какво въздействие да се планира по тях;
- Чувствителни цели са тези цели, на които много внимателно са преценени допустимите физическите загуби и нежелани ефекти настъпили случайно в резултат на военни операции върху цивилни граждани, собственост и околната среда надхвърлящи установените национални прагове на чувствителност. В тях се включват и такива цели, за които е преценено че въпреки големите нежелани ефекти, които ще се получат в резултат на тяхното поразяване, ще допринесат директно за постигане на стратегическа или политическа цел;
- Цели за незабавен отговор са тези, които изискват незабавно поразяване след разкриването им, защото излагат (или скоро ще изложат) на опасност собствените сили (ще ни поразят непосредствено) или са с висок боен потенциал в групировката на противника. Тези цели не се задържат продължително на бойна позиция, след като са се появили или са разузнати, като при това за тях съществува благоприятна възможност да бъдат разузнати и поразени възможно най-бързо и употребата на сила по тях е с достатъчно висок приоритет, за да има основание за незабавно поразяване в ред поддържащ целите на операцията.

Поразяването на която и да е от изброените видове цели допринася за изпълнение на определена задача на огнева поддръжка.

В зависимост от нивото на определянето на целите за поразяване те могат да бъдат класифицирани като: стратегически, оперативни и тактически.

- Стратегически цели са тези, които имат важно значение за стратегическата устойчивост на противника и при чието поразяване се нарушават възможностите му за водене на операцията за дълъг период от време, значително снижават нивото на бойния му потенциал или застрашават изпълнението на мисията на операцията като цяло. Такива могат да бъдат: стратегическите системи за командване и управление; стратегически ядрени средства; средства за масово поразяване; крупни войскови обекти; авиация; флот; военнопромишлени, административно-политически и икономически центрове; големи пристанища; бази; енергийни комуникационни системи; икономическата инфраструктура или цели, чието поразяване може да окаже последващо въздействие върху гражданското население. Оценяването на една цел като стратегическа не винаги е обосновано от нейната големина и мощност на средствата в нея. При промени във военнополитическата обстановка такива цели могат да променят тежестта си в общата система.
- Оперативни цели, са такива цели, които влияят върху военните способности на противника. Такива цели са системите за противовъздушна отбрана; складове за боеприпаси; пунктове за командване и управление на съединенията и важните елементи от пунктовете за командване и управление на обединенията; комуникации; огневите взводове на оперативни и тактически ракети; батареите реактивни системи за залпов огън и далекобойна артилерия; пунктове и центрове за управление на огъня; зенитно ракетни батареи (дивизиони); елементи от разузнавателно-ударни и огневи комплекси и системи; съединенията и частите от всички родове войски (особено маневрените формирования); армейските складове за материални средства от различни класове; формированията за електронна война; близките авиобази, летища и основните им елементи; авиоескадрилите на летищата; подводните и надводни кораби с, близките военноморски бази и най-важните им елементи; комуникационни възли; елементи от инфраструктурата намиращи се в зоната за съвместни операции.
- Тактическите цели, са такива цели, които имат потенциал да окажат въздействие върху действията в тактическото бойно пространство и се определят като малки по пространствени характеристики, но важни по местоположение и значение елементи с овладяването (поразяването), на които се изпълнява основната задача от собствените формирования или се нарушават ефективните действия на формированията на противника в рамките на текущите операции. Такива цели са командните пунктове на подразделенията и частите; командните пунктове и наземни елементи на разузнавателно-ударните и разузнавателно-огневите комплекси и системи; огневите взводове на тактическите ракети; артилерийските батареи стрелящи със специални боеприпаси; полевите пунктове за съхраняване и снабдяване с боеприпаси; зенитно-ракетните батареи със средна и малка далекобойност; площадките (летищата) на армейската авиация и групите самолети и вертолети базирани на тях; отделните кораби, катери и транспортни съдове; участъци с минновзривни и други заграждения; отделни мостове, преправи, проходи, превали, райони с разрушения или пожари; войскови комуникационни възли; елементи от тила на формированията на противника и други.

3. Характеризиране и приоритизиране на целите за поразяване от артилерията

Определянето на целите за поразяване от артилерията се извършва на два етапа:

- При планиране на операцията – по очакван брой цели;
- При започване на операцията – по реално разкрити цели в зоната на операцията.

И в двата случая целите се обединяват в групи по степен на важност, разпределят се по етапи и фази на операцията, по дни на операцията и по периоди на огневата поддръжка. Обединяването на целите в групи при планиране на огнева поддръжка е необходимо за първоначален анализ и предварителни разчети за определяне на целите и тяхното разпределение между средствата за огнево поразяване.

При планиране на огневата поддръжка, разпределянето на целите по етапи и фази на операцията, както и разпределяне на средства за въздействие по тях е основна задача на органите за пла-

ниране на огнева поддръжка на оперативно ниво, за да се използва максимално ударите и огъня на ударните и огневите формирования на компонентите по приоритизирани цели, при което се извършва:

- Съставяне на списък с приоритетните цели;
- Съставяне на списък с целите с голяма важност;
- Събиране и анализиране на разузнавателните данни (карти, известни местоположения на противника и на приятелските сили, зони забранени за стрелба и т.н.) в зоната на операцията;
- Непрекъснато събиране и анализиране на данните за времето;
- Събиране и анализиране на информация за бойна идентификация;
- Поддържане на база данни за състоянието на оръжията на всички компоненти;
- Определяне на правилата за употреба на сила и поведение;
- Непрекъснато изучаване намеренията на командващия за изпълнение на мисията;
- Събиране на информация за оперативни сили и състоянието на компонентите.

За определяне на приоритета за поразяване на целите е необходимо да се присвоят тежестни коефициенти на всеки от критериите. След определяне на всички цели за операцията в зависимост от конкретната обстановка, те се подреждат във възходящ ред на приоритет и така се оформя списъците на приоритизираните цели.

На базата на приоритизацията, целите се групират по сходни характеристики. Приоритизацията на целите може да се променя постоянно, с цел отразяване на промяната на оперативната обстановка в зоната за провеждане на операцията. Ако промяната на приоритизацията на целите води до съществена промяна в групирането им, тази промяна се докладва по команден ред и се актуализират списъците с данните за целите.

В зависимост от целите, задачите, желания краен резултат, ресурсите, силите и средствата за въздействие по целите се извършва разпределение на целите по етапи и фази на операцията. Разпределението на целите може да се извършва и по използваните средства за въздействие и по исканите ефекти след въздействието по тях, също така може да направи разпределение на целите в зоната за провеждане на операцията, поразявани от различните компоненти .

Предложените в доклада критерии за приоритизирането на целите са следните:

- **Критичност** - качествен критерий, отразяващ значението на всяка цел от групировката на противника, каква опасност представлява за собствените войски и до каква степен нейното унищожаване или повреждане оказва значително влияние върху постигането на желания краен резултат;
- **Достъпност** – целта е достъпна, когато оперативен елемент (формирование) може да достигне целта или целта може да бъде поразена от огневите формирования. Тази оценка включва идентифициране и изучаване на критични пътища, които оперативните елемент трябва да предприеме, за да постигне целите си и отчита досегаемостта на артилерията;
- **Възвръщаемост** – на целта се измерва във време, тоест колко време ще отнеме подмяната, ремонта и възстановяването на целта от нанесеното унищожаване или увреждане. Възвръщаемостта варира в зависимост от източниците и вида на съставните компоненти на целта и наличието на резервни части;
- **Уязвимост** – количествен критерий, който характеризира възможностите на огневите формирования успешно да въздействат на целта. При определяне на уязвимостта на дадена цел е необходимо да се сравни характера на уязвимите компоненти от целта със способността на атакуващия елемент да го унищожи или повреди;
- **Ефектност** - количествен критерий, характеризиращ възможни военни, политически, икономически, психологически и социологически въздействия на целта и извън нея. Това е тясно свързано с оценката за критичност на целта. Типът и стойността на желаните ефекти подпомагат планиращите в избора на отделни и групови цели за въздействие;
- **Въвеждане на целта в бой** (огнева дейност) - качествен критерий, отразяващ важността на дадена цел в определено време. Тук се анализира и прогнозира в кои момент противника ще използва своите огневи средства. Ако дадена цел се намира в район за съсредоточаване, в марш

тя може само да се проследява нейната дейност, а в същото време да се въздейства по други по важни към момента цели;

- **Разпознаваемост** - Разпознаваемостта на целта е степента, в която тя може да бъде разпозната от разузнавателните органи при различни условия. Времето има очевидно и значително влияние върху видимостта. Дъжд, сняг, мъгла и други атмосферни условия могат да попречат на разузнаването и наблюдението.

Критериите с най-голяма тежест са **критичност, достъпност и ефектност**. Критерии с по-ниска тежест са **уязвимост, разпознаваемост и възвръщаемост**. Критерият критичност може да бъде характеризиран като основен критерий, въз основа на който се определят приоритетите за поразяване на целите с отчитане на коефициентите на останалите критерии.

Заключение

В съвременните въоръжени конфликти бойните действия се характеризират с голямата сложност, динамичност, непредвидимост и скоротечност, което поражда необходимостта от по-детайлно дефиниране на целите от състава на противостоящата групировка, динамично приоритизиране и своевременно актуализиране на приоритизирания списък на целите и анализиране на голям брой фактори, които влияят върху процеса на разузнаване – целеуказване – целеобразуване – целеразпределение. За постигане на целите на планирането на огневата поддръжка в операциите в зависимост от различните критерии за избор на цели за постигане на желания краен резултат, следва целите да се определят след задълбочен анализ на всеки обект от зоната на операцията, който може да бъде цел. За постигане на тази цел е необходимо да се определи какви ще бъдат положителните и отрицателните ефекти от поразяването и как те влияят на групировките участващи в операцията, ефектите се анализират в икономическата, социалната, военната, информационната, инфраструктурата и политическа области.

References

1. Илиев, К., Чалъков, Б. „Съвместна огнева поддръжка" – фактор в съвременните операции. *Сборник доклади от международна научна конференция, НВУ, Факултет „Артилерия, ПВО и КИС"*, с. 120-127, Издателски комплекс на факултет „Артилерия, ПВО и КИС", Шумен, 2017, ISSN 2367-7902.
2. Марков, Д. Поразяване на цели при съвместна огнева поддръжка в зоната за координиране на въздушното пространство. *Сборник доклади от международна научна конференция, НВУ, Факултет „Артилерия, ПВО и КИС"*, с. 154-160, Издателски комплекс на факултет „Артилерия, ПВО и КИС", Шумен, 2017, ISSN 2367-7902.
3. AJP 3.9 Allied doctrine for joint targeting, 2016.
4. Joint targeting JP 3-60, 2013.
5. Joint targeting student guide, Joint targeting School, Virginia, 2007.

ARMS, TECHNOLOGIES, LOGISTICS

Florin-Marian Dîrloman, Traian Rotariu, Tudor-Viorel Ţigănescu,
Mihai Ionuţ Ungureanu,

ECO–FRIENDLY OXIDIZERS: MINIREVIEW

**Florin-Marian Dîrloman*), Traian Rotariu*),
Tudor-Viorel Ţigănescu**), Mihai Ionuţ Ungureanu*)**

*) *Military Technical Academy "Ferdinand I" 39-49 Av. George Cosbuc, Bucharest, Romania*
florin.dirloman@mta.ro, traian.rotariu@mta.ro
**) *Military Equipment and Technologies Research Agency , Ilfov, Romania*
viorel.tiganescu@mta.ro

***Abstract**: In order to protect the environment, today's legislation encourages the development of materials, substances and so on, which can lead to a minimum harmful effect. As a result, the concept of eco-friendly makes its appearance and begins to occupy a leading place on the working boards of engineers from different fields of aerospace engineering as well as in the field of mechanical engineering (such as fertilizers, building materials, energy generation, and so on).This paper aims to go through the existing literature up to the present moment regarding the stage of development of environmentally friendly oxidants, which can be found in the specific structure of a solid propellant.*

***Keywords**: Propellant, Eco-friendly oxidizers, Ammonium perchlorate, Ammonium nitrate, Ammonium dinitramide, Hydrazinium nitroformate.*

Introduction

Analyzing the environment, more precisely, the level of pollution that is achieved by using excessively and improperly the materials that favor its growth, we can conclude only one sure aspect, the concept of eco-friendly must become an imperative one.

Starting from the typical structure of a solid propellant for rocket engines: fuel, oxidant and binder, all these elements put together must meet the three requirements that a product must present: safety, performance and financial part. When it comes to environmentally friendly propellants we refer to those constituents that are used in their manufacture, which, during the combustion develop products that have a minimal harmful effect on the ecosystem, but at the same time confer at least equal performances with those that exist on the market at the moment, preferably even to exceed them.Reduced performance would lower payloads and increase propellant consumption, and thereby have a negative impact on the environmen. From the point of view of the mass proportions of a solid rocket fuel, the oxidant is the vital element, it is the center of the mixture and the others gravitate around it to fulfill the requirements specified above. Usually this is the basis of the eco-friendly character.

The development of eco-friendly propellants represents at moment the most coveted aspect that aerospace engineers want to achieve, by identifying new oxidants capable of successfully replacing non-environmentally friendly oxidants, such as ammonium perchlorate. Good candidate compounds for green high performance propulsion are amonium nitrate (AN), hydrazinium nitroformate (HNF), and ammonium dinitramide (ADN). They are being studied as eco-friendly oxidizers for future solid propellants with improved properties.[1-6, 21]

1. Non-environmentally friendly versus environmentally friendly

Combustion products are an important issue that we must take into account when it comes to environmental protection. Usually, gaseous products and solid residues are to be determinated.

Regarding the non-evironmentally friendly oxidants, the bigest candidate it is represented by ammonium perchlorate (AP). Its structure is shown in Figure 1.

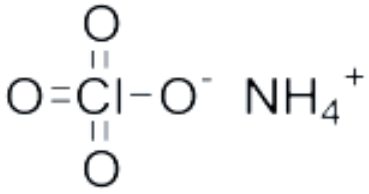


Figure 1: Structure of ammonium perchlorate[7]

Despite its non-ecofriendly character, history and specialized studies[8-12] have shown us that ammonium perchlorate is the most effective oxidant in terms of aerospace performance. Its efficiency is related to the burning rate. However, it does possess a series of major disadvantages that bring him a leading position on the black board of non-environmentally friendly oxidants. Figure 2 describes its decomposition reaction, where it can be easily observed among the reaction products (nitrogen, oxygen, and water), the appearance of hydrogen chloride, which in contact with water leads to the formation of hydrochloric acid. This type of acid produces smoke and is highly toxic, in addition to the corrosion of the launch pad. Also, the reaction products have a negative effect on the ozone layer which increases the global warning.

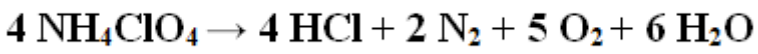
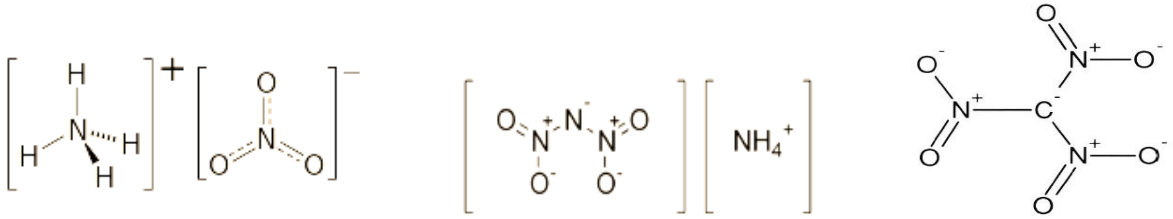


Figure 2: Decomposition reaction of ammonium perchlorate [13,14]

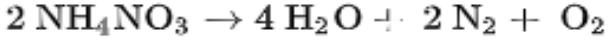
In order to overcome these environmental problems, specialists in the field have begun to identify new compounds capable of successfully replacing ammonium perchlorate but to present at least the same characteristics in terms of thermodynamic / energetic, kinetic, and physico-chemical properties. Among these oxidants are ammonium nitrate, ammonium dinitramide and hydrazinium nitroformate (Figure 3), which are currently studied extensively.



a **b** **c**

Figure 3: Structure of AN (a), ADN (b), HNF (c)

The eco-friendly character that these three posess results from the decomposition reactions shown in Figure 4.



$$NH_4N(NO_2)_2 \rightarrow (2NH_2NO_2) \rightarrow 2N_2O + 2H_2O$$

$$HNF \longrightarrow 2\,NO + CO_2 + 2\,H_2O + 3/2\,N_2 + 1/2H_2$$

Figure 4: Decomposition of AN, ADN and HNF

Although, ammonium nitrate is a conventional oxidant without non-eco products, this one has drawbacks of hygroscopic nature and multiple transition phases in the temperature range of practical importance and comparatively lower energy. Therefore, related studies on ammonium dinitramide (ADN) and hydrazinium nitroformate (HNF) as potent candidates regarding eco-friendly oxidants are developed all over the globe. Related to the last two, HNF has certain advautages over ADN, such as its simple method of synthesis, non-hygroscopic nature, higher density and melting point[18].

Considering the structure of a solid rocket propellants in addition to the oxidant, there are also other elements such as the binding agent. The main purpose of this kind of agent is to hold together in a matrix the mixture. The necessity of development of solid rocket propellants based on ammonium nitrate, ammonium dinitramide and hydrazinium nitroformate more energetic led to the emergence energetic binders, such as glycidyl azide polymer (GAP), polyglycidyl nitrate (PGN), polynitromethyloxetane (PLN) and 3,3-bis(azydomethyl)oxetane (BAMO).

A theoretical study regarding the energetic was conducted by G. Gadiot et al[20]. In this study, a series of combinations eco-friendly oxidants and energy binders were made. The mass percentages used were 80% for oxidants and 20% for binder. The Table 1 lists the theoretical maximum perfomance for selected smokelles solid propellants obtained in this study.

Oxidizer (% by weight)	Fuel (% in weight)	Maximum I_{vac} (m/s)	Gain in I_{vac}† (%)	Flame temperature, T_f (K)	Increase in T_f (%)
80% AP*	20% HTPB	2713	—	2266	—
80% AN	20% HTPB	2412	−11.1	1420	−37
80% AN	20% GAP	2717	+0.2	2353	+4
80% ADN	20% GAP	3150	+16.1	3132	+38
80% HNF	20% GAP	3278	+20.8	3275	+45
80% ADN	20% PGN	2938	+8.3	2900	+28
80% HNF	20% PGN	3282	+21.0	3318	+46
80% ADN	20% PLN	3111	+14.7	3018	+33
80% HNF	20% PLN	3306	+21.9	3321	+47
80% ADN	20% BAMO	3175	+17.0	3139	+39
80% HNF	20% BAMO	3255	+20.0	3381	+49

*Reference propellant.
†Gain with respect to reference propellant.

Table 1: The theoretical maximum perfomance for 80% oxidiant and 20 % binder

Propellants are designed to produce high temperatures and pressures in a closed chamber to accelerate projectiles, rockets, or missiles by means of the resulting propulsive force of the gas produced by its decomposition (burn). As it can be seen, the green oxidants can give good results using them in different combinations with another material.

Even if the energetic problem is overcome, the majority of oxidants present other problems too.

For instance ammonium nitrate, besides the low energetics, this one is also very hygroscopic, undergoes a room temperature phase transformation (see Table 2), involving a significant volume change and burns very slowly.These adverse properties make it even less attractive as an alternative oxidizer. From here the concept of phase stabilized ammonium nitrate (PSAN) becomes known.

Phase transition	Temperature (°C)	State	Volume variation (%)
-	>169.6	liquid	-
I	169.6 to 125.2	cubic	+2.1
II	125.2 to 84.2	tetragonal	-1.3
III	84.2 to 32.3	α-rhombic	+3.6
IV	32.3 to −16.8	β-rhombic	−2.9
V	−16.8	tetragonal	-

Table 2: Ammonium nitrate phase transition [21]

2. Phase trasition. Experimental study regarding ammonium nitrate

2.1 Materials

To obtain the desired phased stabilized ammonium nitrate desired, the following materials were used: ammonium nitrate (NH_4NO_3), potassium nitrate (KNO_3) and distillated water as a solvent.

2.2 Co-crystallization process

It was made a mixture of ammonium nitrate and potassium nitrate (PN), using distillated water as a solvent agent. The quantities used in the experiment were: 47,5 grame ammonium nitrate, 2,5 grame potassium nitrate and 100 ml distillated water (DW). After weighing and measuring using an analytical balance and a graduated cylinder the mixture was placed in a 600 ml Berselius glass placed on a magnetic agitator. The dissolving process of the two salts in the 100 ml of distilled water took 3 hours, with a rotational speed of the magnetic agitator of 500 rpm. After the total dissolving the obtained mixture was placed in a plastic vessel to be subsequently introduced into a ventilation drying stove. The mixture was dried at a temperature of 50-80° C for water evaporation. The total duration of the process was 72 hours, and the obtained compound consisted in a salt of ammonium nitrate and potassium nitrate (see Figure 4). The co-crystallization reaction was successfully performed. All the stages regarding the completion of the co-crystallization reaction are presented in the Figure 5.

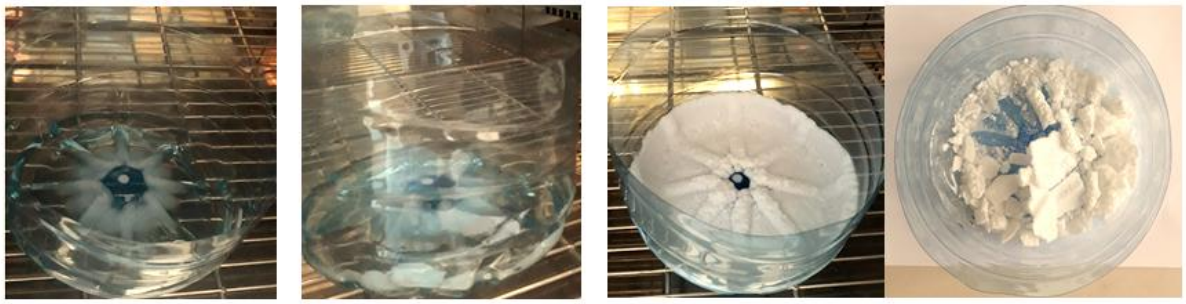


Figure 5: Ammonium nitrate-potassium nitrate salt

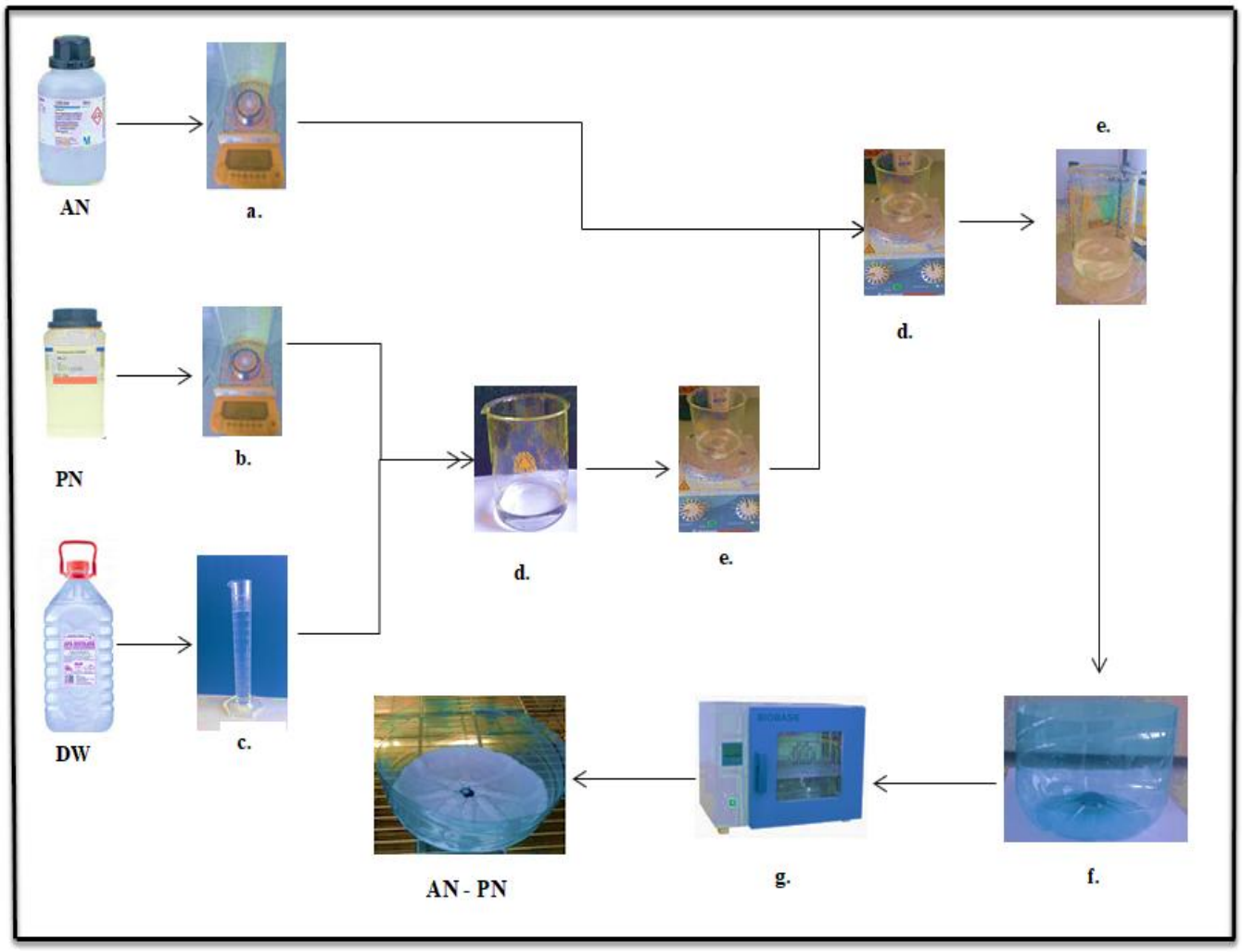


Figure 6: Process of co-crystallization ammonium nitrate-potassium nitrate
(a,b- weighing; c- measuring; d- mixture; e- dissolving; f-sampling; g-drying)

For proper storage the salt obtained was disposed in a vacuum desiccator during the laboratory tests.

2.3 Characterisation

After the salt is obtained, the next step is to check the stability of the ammonium nitrate by a differential thermal analysis to see if it is PSAN. The tests of the samples were carried out using a DTA 551-Ex model, by employing a heating rate of 5° C. The sample size used was about 30 mg.

The reported transition temperatures for various phases of AN are shown in Table 2. Since the transition depends on the purity of the sample, AN used was characterized using the same experimental conditions, as the same for the PSAN used in the present study. Figure 7 shows all the transitions phase from the room temperature upwards as expected from an untreated sample. The IV-III transition occurs 42° C instead of 32° C, wich is not unusual since this transition is known to take place anywhere between 32 and 80° C depending on the source of the sample. After this transition, the sample has three more transitions before decomposing endothermically above 300 ^{o} C.

At a close look to the PSAN phase transitions it can be observed that the transition which normally occurs at 42° C, in case of AN, had vanished by using potassium nitrate in the process of co-crystallization. The co-crystalization is believed to cause formation of solid solution of K^{+} salts in AN[19].

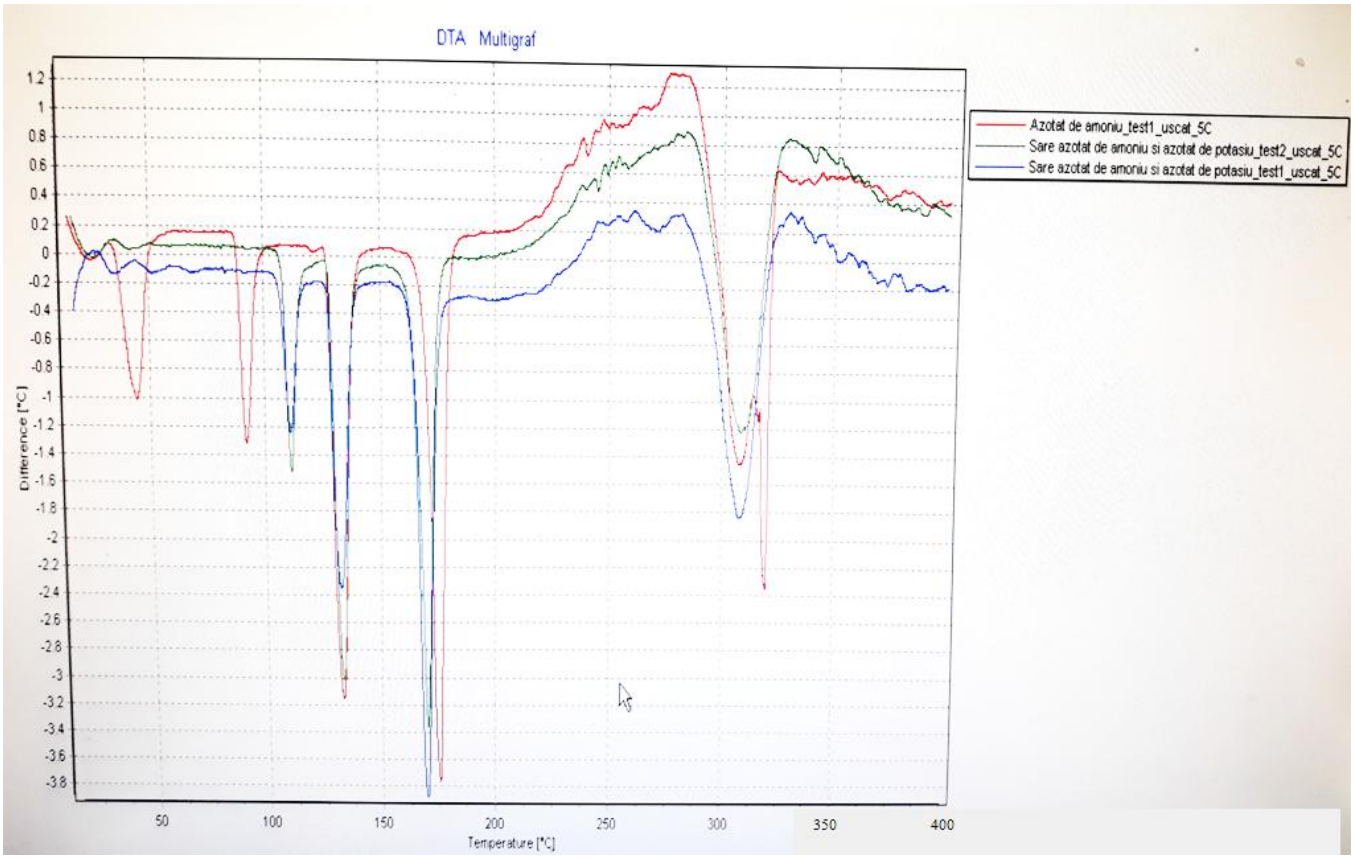


Figure 7: DTA traces on AN and PSAN

3. Conclusions

In conclusion, composite solid propellants based on oxidants such as ammonium nitrate or ammonium dinitramide and hydrazinium nitroformate possess good characteristics regarding eco-friendly character. However, these oxidants have a low response when it comes to performance and most of the time they have to be used with other components, such as energetic binders to improve their characteristics. Taking into consideration all the factors, the eco-friendly oxidants are the next step wich can be used as an alternative to AP composite solid propellants.

Acknowledgments

This study has been supported by a grant of Romanian Ministry of Education and Scientific Research – UEFISCDI, under Complex Projects Realized in Consortium Program, project no. 70PCCDI/2018.

References

1. Jisna Jos & Suresh Mathew (2017) *Ammonium Nitrate as an Eco–Friendly Oxidizer for Composite Solid Propellants: Promises and Challenges*, Critical Reviews in Solid State and Materials Sciences, 42:6, 470-498, DOI: 10.1080/10408436.2016.1244642
2. Shalini Chaturvedi & Pragnesh N. Dave (2013) *Review on Thermal Decomposition of Ammonium Nitrate, Journal of Energetic Materials*, 31:1, 1-26, DOI: 10.1080/07370652.2011.573523
3. G. da Silva, S. C. Rufino, and K. Iha (2013). *Green propellants oxidizers*, J. Aerosp. Technol. Manag. 5, 139

4. P. Ding, H. Wang, L. Wen, G. Cheng, C. Lu, and H. Yang, (2014). *Studies on synthetic technology and reduced sensitivity technology of hydrazinium nitroformate*, Ind. Eng. Chem. Res. 53, 13851
5. M. J. Tummers, A. E. D. M. van der Heijden, and E. H. van Veen, (2012). *Selection of burning rate modifiers for hydrazinium nitroformate*, Combust. Flame 159, 882
6. E. Landsem, T. L. Jensen, F. K. Hansen, E. Unneberg, and T. E. Kristensen (2012).*Mechanical properties of smokeless composite rocket propellants based on prilled ammonium dinitramide*, Propellants Explos. Pyrotech. 37, 691
7. https://en.wikipedia.org/wiki/Ammonium_perchlorate
8. YU, Z., CHEN, L., LU, L., YANG, X., & WANG, X. (2009). DSC/TG-MS *Study on in Situ Catalytic Thermal Decomposition of Ammonium Perchlorate over CoC2O4*. Chinese Journal of Catalysis, 30(1), 19–23. doi:10.1016/s1872-2067(08)60087-x
9. Fong, C. W., & Smith, R. F. (1987). *The relationship between plateau burning behavior and ammonium perchlorate particle size in HTPB-AP composite propellants. Combustion and Flame*, 67(3), 235–247. doi:10.1016/0010-2180(87)90099-x
10. Al-Harthi, A., & Williams, A. (1998). *Effect of fuel binder and oxidiser particle diameter on the combustion of ammonium perchlorate based propellants. Fuel*, 77(13), 1451–1468. doi:10.1016/s0016-2361(98)00059-3
11. Oommen, C. and S. R. Jain. 1999. *Journal of Hazardous Materials*, 67: 253–281.
12. Kohga, M. and Y. Hagihara. 1998. *Propellants, Explosives, Pyrotechnics*, 23: 182–187.
13. Boldyrev, V. V. (2006). *Thermal decomposition of ammonium perchlorate. Thermochimica* Acta, 443(1), 1–36. doi:10.1016/j.tca.2005.11.038
14. Jacobs, P. W. M., & Whitehead, H. M. (1969). *Decomposition and combustion of ammonium perchlorate. Chemical Reviews*, 69(4), 551–590. doi:10.1021/cr60260a005
15. Venkatachalam, S., Santhosh, G., & Ninan Ninan, K. (2004). *An Overview on the Synthetic Routes and Properties of Ammonium Dinitramide (ADN) and other Dinitramide Salts*. Propellants, Explosives, Pyrotechnics, 29(3), 178–187. doi:10.1002/prep.200400043
16. Kumar, P. (2018). *An overview on properties, thermal decomposition, and combustion behavior of ADN and ADN based solid propellants*. Defence Technology. doi:10.1016/j.dt.2018.03.009
17. Dendage, P. S., Sarwade, D. B., Asthana, S. N., & Singh, H. (2001). *Hydrazinium nitroformate (HNF) and HNF based propellants: A review.* Journal of Energetic Materials, 19(1), 41–78.
18. H.F.R. Schoyer, A.J. Schnorhk, P.A.O.G. Korting, P.J.Van Lit, J.M. Mul,G.M.H.J.L. Gadiot, and J. J. Meulenbrugge. (1995). *J. Propul. Power*, 11(4) 856
19. Oommen, C., & Jain, S. R. (1999). *Journal of Thermal Analysis and Calorimetry*, 55(3), 903–918. doi:10.1023/a:1010146203523
20. Gadiot, G. M. H. J. L., Mul, J. M., Meulenbrugge, J. J., Korting, P. A. O. G., Schnorkh, A. J., & Schöyer, H. F. R. (1993). *New solid propellants based on energetic binders and HNF*. *Acta Astronautica*, 29(10-11), 771–779. doi:10.1016/0094-5765(93)90158
21. Kalev, K.G., Thermodynamic and gas dynamics processes in engineering practice, Shumen, 2017 г., ISBN 978-954-9681-78-9
22. https://ro.wikipedia.org/wiki/Azotat_de_amoniu

Cristian-Emil Moldoveanu, Alin-Constantin Sava, Pamfil Somoiag,

THE INTERNATIONALIZATION PROCESS IN THE TECHNICAL MILITARY HIGHER EDUCATION INSTITUTIONS

Cristian-Emil Moldoveanu, Alin-Constantin Sava, Pamfil Somoiag

***Abstract*:** *The most important universities have as objectives the increasing of the internationalization of higher education and the development of student, teaching staff and researchers' mobility, as well as the international compatibility of bachelor's, master and PhD study programs. Although the functioning of the technical military higher education institutions is subject to further limitations imposed by the rigors of the military system, its connection to the quality requirements of the European system is a necessity as well as a reality. While for the students of civil universities Erasmus mobility represents an opportunity to increase their employability chances, for military students Erasmus mobility represents the chance to gain international experience which, along with the new skills and knowledge acquired, provide them a better adaptation to fit into a new, international and multicultural environment.*

1. Introduction

Military Technical Academy "Ferdinand I", Bucharest (MTA Bucharest) is a polytechnic higher education military institution having as mission the training of engineer officers for the Ministry of National Defense and for other beneficiaries from the national system of defense, public order and national security [1]. MTA Bucharest conducts higher education study programs organized in undergraduate, master and doctoral studies in its accredited fields and specializations: Armament, Ammunition and Missiles Engineering, Aerospace Engineering, Automotive Engineering, Military Engineering, Civil Engineering, Geomatics, Electronic Engineering, Telecommunication and Information Technology, Computers and Information Technology, System Engineering etc. Regarding international relations, MTA Bucharest conducts outgoing and incoming student mobilities in collaboration with military and civilian universities. Student mobilities target undergraduate and master exchange study programs, the development of bachelor's, master and PhD projects and theses, the development of strong collaborations and, specific for military institutions, training sessions including military activities.

2. Erasmus+ KA1 Higher Education Student and Staff Mobility Projects

Military Technical Academy "Ferdinand I" Bucharest has been taking part in mobility programs such Erasmus since 1998. . Every year, MTA Bucharest sends about 70 students abroad (50 undergraduate students, 15 master students and 5 PhD students) in Erasmus mobilities (SMP or SMS) and receives about 20 foreign students. At the same time, about 30 staff mobilities are realized yearly (10 for teaching and 20 for training). About 10 foreign teachers take part in mobility exchanges in MTA Bucharest every year. In general, the MTA Erasmus student and teaching staff mobilities are conducted in military and civilian universities, and sometimes in research civilian institutions with technical concerns [3].

3. Erasmus+ KA2 Strategic Partnership Greener and Safer Energetic and Ballistic Systems (GSEBS)

Greener and Safer Energetic and Ballistic Systems (GSEBS) (2014-2016) was a Strategic Partnerships for higher education program, funded by Erasmus+ programme, Key Action 2 - Cooperation for innovation and the exchange of good practices. The project was run by Military Technical Academy "Ferdinand I"(RO), University of Coimbra (PT), ENSTA Bretagne (FR) and Imperial College London (UK). The aim of the project was to provide an Intensive Study Programme (IP) for MA and PhD students coming from four prestigious HEIs across Europe. This includes a wide range of multi and interdisciplinary lectures delivered by distinguished professors and researchers from the participating HEI with renowned expertise in their field of interest. Theoretical information is experienced in practice by the students through case studies and demonstrations using the most advanced ICT modeling tools and laboratories. The course teaching activities are followed by conferences, workshops and other multiplier events which ensure a wide dissemination and debate of the topics in academia, research areas, industry and governmental organizations.

4. International Semester "Defence and Security Technical Systems"

The project of an international semester on military technical education was set up by the Military Technical Academy "Ferdinand I" of Bucharest in 2018 and implemented for the first time in 2019. The teaching objective of the semester is to prepare the participants for the acquisition of professional and transversal competencies that will allow them to develop projects in the field of technical defence and security systems in international, multidisciplinary and intercultural teams. The semester consists of 3 parts: core curriculum, scientific project and military training.

The core curriculum addresses all the students enrolled in the international semester. This part contains common subjects useful for all the engineering braches (Project Management, Methods and Tools of Modeling and Simulation of Technical Systems, Sensors, Acquisition and Data Processing Systems, Intercultural and Professional Communication etc). The military training part comprises subjects related to the military science such as Armament Systems, Electronic Warfare, Cyber Security Elements, Sport and Physical Training, etc. This part addresses all the military students enrolled in the international semester.

The scientific project is the most important part of the international semester. In this part a project is developed by a multi-national and multi-disciplinary team of 3 to 6 students. At the beginning of the semester, the available projects are presented after which the students are given the opportunity to choose their preferences for the project they want to participate in. The main objective of the project is to train students from different countries and different engineering branches to work together in intercultural and multi-disciplinary groups. The students work together to complete an integrated engineering project, focusing on the development of personal competences, especially the ability to work and communicate within cross-cultural groups in combining several disciplines like mechanical, electrical engineering, information technology, aerospace engineering, armament engineering etc Every week they have a plenary meeting during which the teams present the progress of their work and receive assistance and guidance. At the end of the semester there should be a written final report from each team. In the final presentation all the team-members are expected to participate on equal terms.

In the first spring international semester organized in the Military Technical Academy "Ferdinand I" were enrolled 15 students from Military University of Technology, Warsaw, Poland (5 cadets), "Vasil Levski" Military National University, Bulgaria (1 cadet) and Military Technical Academy "Ferdinand I" of Bucharest, Romania (3 cadets) and 6 civilian students from IUT "Paul Sabatier" Toulouse, France. They were divided in 3 teams: weapon systems, aerospace engineering and military engineering.

5. Conclusions

Although the majority of bachelor's, master or PhD projects could be developed in MTA Bucharest, it appears that by taking part in international mobilities, students will improve considerably their knowledge and professional skills by having the chance to observe, during their international mobility, a new approach to the professional project content. International mobility is a first test for students to see whether the knowledge and skills gained while studying in MTA Bucharest are effective or not.

At the same time students will have the chance to learn the design, structure and mode of operation of new or similar equipment, which is a challenge. This is an advantage for students who carry out activities abroad. Basically, by means of Erasmus mobility, students will have a very large number of specialized technical equipment and laboratories in which to develop their projects, improving their knowledge and skills gained in MTA Bucharest. Another aspect that should not be overlooked is the fact that during mobilities, students accumulate knowledge and skills complementary to those ensured by the educational program of MTA Bucharest, which leads to an increase of their professional level.

The experience MTA Bucharest gained from the implementation of Erasmus mobility projects and of GSEBS Erasmus+ KA2 project was used to organize a pilot international semester for technical field. Other military academies such as Military University of Technology Warsaw, Poland, "Vasil Levski" Military National University, Bulgaria, Italian Air Force Academy, Pozzuoli, Italy, Portuguese Air Force Academy, Lisbon, Portugal and Hellenic Air Force Academy, Athens, Greece are interested in a long-term collaboration with MTA Bucharest in order to develop the international semester in the technical field in the frame of Erasmus+ KA2 Strategic Partnership project and create a new LoD in the frame of Military Erasmus Initiative [2]. The organizing of the international semester for technical field will increase student and staff teaching exchanges between technical military higher education institutions.

References

[1] **Jane Knight**, *Internationalization: Key Concepts and Elements*, University of Toronto, Canada, 2004;

[2] **Harald Gell, Sylvain Paile-Calvo, Symeon Zambas,** *European Education and Training for Young Officers. European Initiative for the Exchange of Young Officers , Inspired by Erasmus*, 2nd Edition, Austria, 2018;

[3] **Moldoveanu Cristian-Emil.**, **Edu Ioana Raluca, Rotariu Traian, Andruseac Gabriela,** *The Impact of Erasmus Mobility on Military Technical Higher Education*, Proceedings of the 9th International Technology, Education and Development Conference, INTED 2015, pp. 4233-4238, ISSN 2340-1079, ISBN: 978-84-606-5763-7, Madrid, Spain, 2-4 March 2015.

Cristian Ene, Cristian-George Constantinescu,

INCREASING THE AIR DEFENSE CAPACITY BASED ON THE IMPLEMENTATION OF THE MODERN AIR DEFENSE MISSILES

Cristian Ene, Cristian-George Constantinescu

Department of Surveillance and Air Defense, "Henri Coandă" Air Force Academy, Brașov, Romania,
bvcristiene@yahoo.com.com, ccg_cristi@yahoo.com

***Abstract**: The main objective of all air defense systems is to ensure the protection of the national territory, by carrying out its research having in the foreground the following goals:*

- air threats detection;
- identification and tracking of air targets;
- destruction of air targets.

The present case study focuses on the possibility of improving the air defense capabilities by implementing modern anti-aircraft missile systems and by adapting contemporary combat tactics. The obtained results are sustained by their Matlab simulations.

***Keywords**: air defense systems, air threats detection, air defense capabilities, Matlab simulations.*

Introduction

Due to the necessity to respect the conditions characteristic of the interarm operations corresponding to the alliances under whose directives we act, the authors decided to present in this case study the improvement of the air defense capability by implementing the Patriot PAC-3 system and by adapting to it the specific combat tactics.

In order to highlight the difference in defense capability depending on the system used to fight the targets and the combat tactics adopted, we organized operating groups of two anti-aircraft missile systems, each group acting according to a predetermined scenario.

The CA-94 antiaircraft missile complex is included in the composition of each task force to ensure the immediate defense of the target in the event of a surprise attack or at very low heights. The second component of each operating group is one of the "OSA-AKM", "KUB" or "Patriot" systems.

To project the appropriate scenario for each task force, we used the MatLab program, through which we performed the mathematical simulation of the missile trajectories and the target route. We think that comparing the results of the operating groups shows both the strengths of the complexes and their operational deficiencies, which are particularly important in the process of highlighting the improvement of the air defense capability.

In order to be able to perform the simulation itself, we have developed an algorithm, through which the continuous calculation of the target and missile coordinates is performed in order to choose the appropriate launch time and to follow the evolution of the target flight, the approach of the target missile and the meeting.

All of these will be detailed in the paper sections, being sustained by their corresponding Matlab simulations.The advantages of using the modern anti-aircraft missile systems will be clearly highlighted in this way.

The air defense system including CA-94 and OSA-AKM systems

To achieve the first scenario we assumed the following situation: There is information that the objective "Nest" (the reference point of the system) of coordinates $\boldsymbol{x = 0\,; y = 0}$ is to be attacked. The enemy aircraft that is to execute the air attack is the "Sea Harrie" fighter aircraft with a maximum evolution speed of 550 m/s.
The first task force chosen for the action to combat the air threat is formed by the CA-94 and OSA-AKM systems. The result of the scenario scrutiny reflects the level of effectiveness of the task force. The data used in this simulation represent the maximum capacities or which are close to the maximum.
The input information is as follows:

- Maximum target discovery distance: 20000 m;
- The maximum distance at which the target can be fought: 10500 m;
- Maximum missile flight speed: 400 m/s;
- Initial target flight speed: 200m/s;
- Maximum missile flight time: 28 s.

Considering that through the process of illuminating the target, the position and intention of the operating group were revealed and that the altitude and speed of the target are variable, we have performed the following simulation:

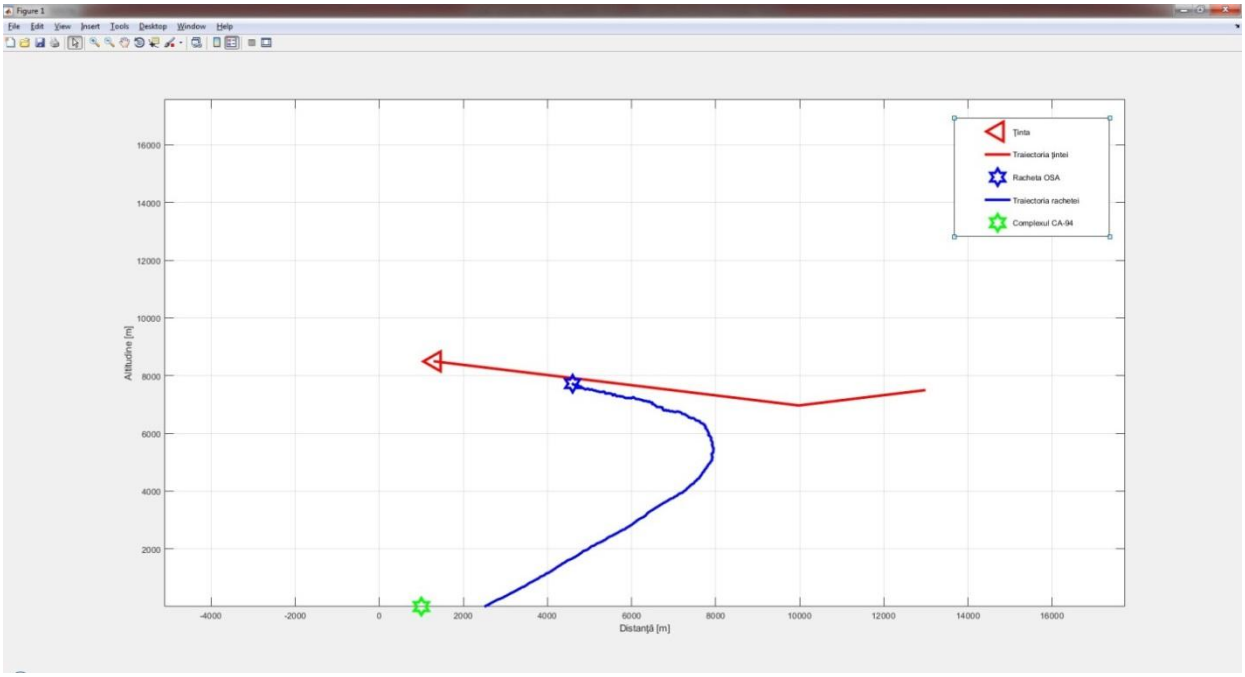


Fig. 1: OSA-AKM_CA-94 Task Force Result

The missile trajectory launched by the OSA-AKM system is represented in blue, the position of the CA-94 complex is represented in green, and the red trace is the trajectory of the target aircraft.
The above graph simulates a tactical situation with the role of testing the effectiveness of the CA-94 and OSA-AKM systems. As we specified, the illumination process led to a rapid discovery of the operating group, at which point the target executed an element of maneuver and suddenly changed its direction and speed. The fact that the capture of the enemy was inefficient, led to the loss of the target and thus to the diminution of the air defense capability.

The air defense system including CA-94 and KUB systems

The second operating group that we chose to submit to the script using the MatLab software, consists of the CA-94 and KUB systems. For the second simulation, the maximum and initial data are different from those used for the previous simulation.
The input information is as follows:

- Maximum target discovery distance: 40,000 m;
- The maximum distance at which the target can be fought: 20,000 m;
- Maximum speed of the KUB missile: 750 m/s;
- Maximum flight speed of the A-94 missile: 250 m/s;
- Initial target flight speed: 200 m/s;
- The maximum flight time of the KUB missile: 24 s.
- The maximum flight time of the missile A-94: 14 s.

On the same principle as in the previous case, we consider that through the process of illuminating the target, the position and intention of the operating group were revealed.

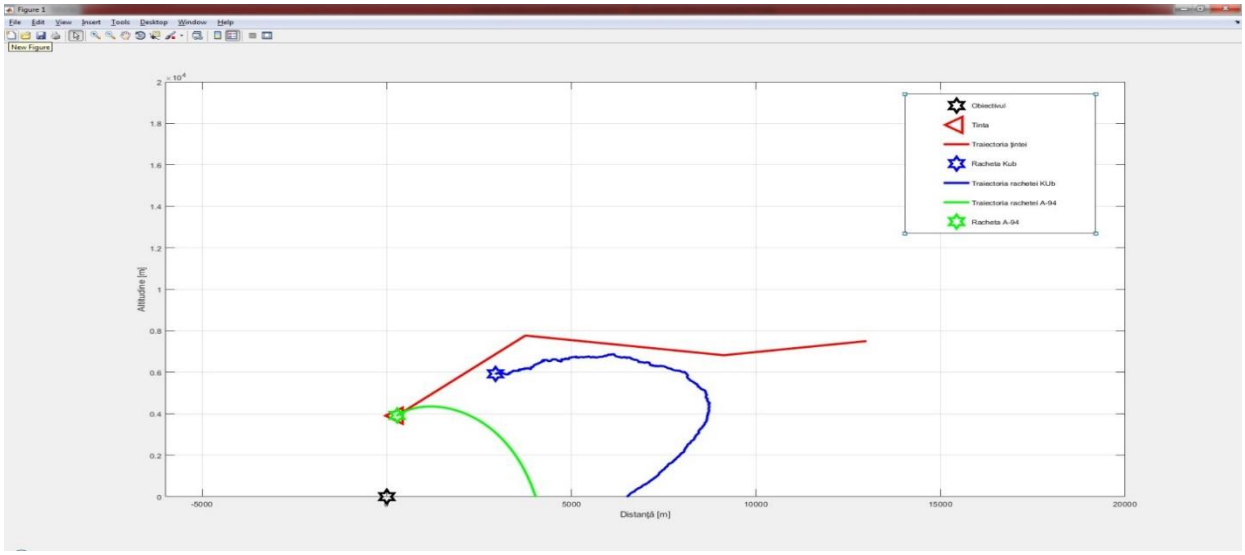


Fig. 2: The result of the operating group KUB_CA-94

The missile trajectory launched by the KUB system is represented by the blue trace, the missile trajectory launched by the CA-94 system is represented by the green curve, the position of the main objective is the black point and the trajectory of the aerial target is represented in red color.
As in the previous case, following the target illumination, the position of the operating group was discovered, following a series of maneuvers carried out by the target (figure 2) in order to avoid being intercepted and to fulfill its mission. The difference is that this time, in an attempt to reach the target, the target was destroyed by CA-94 complex. In the first phase, the target flies at a speed of 200 m/s until the operating group is discovered, when it suddenly changes direction and increases its speed. The missile launched by the KUB complex could not intercept the target due to the sudden change of parameters. In the second phase, in order to be able to execute the maneuvers necessary to hit the target, the aircraft reduces the flight speed and tries to get as close to the target as possible for a more precise destroying effect. Once entered into the area of CA-94 complex action, the plane is taken to accompany and fought.

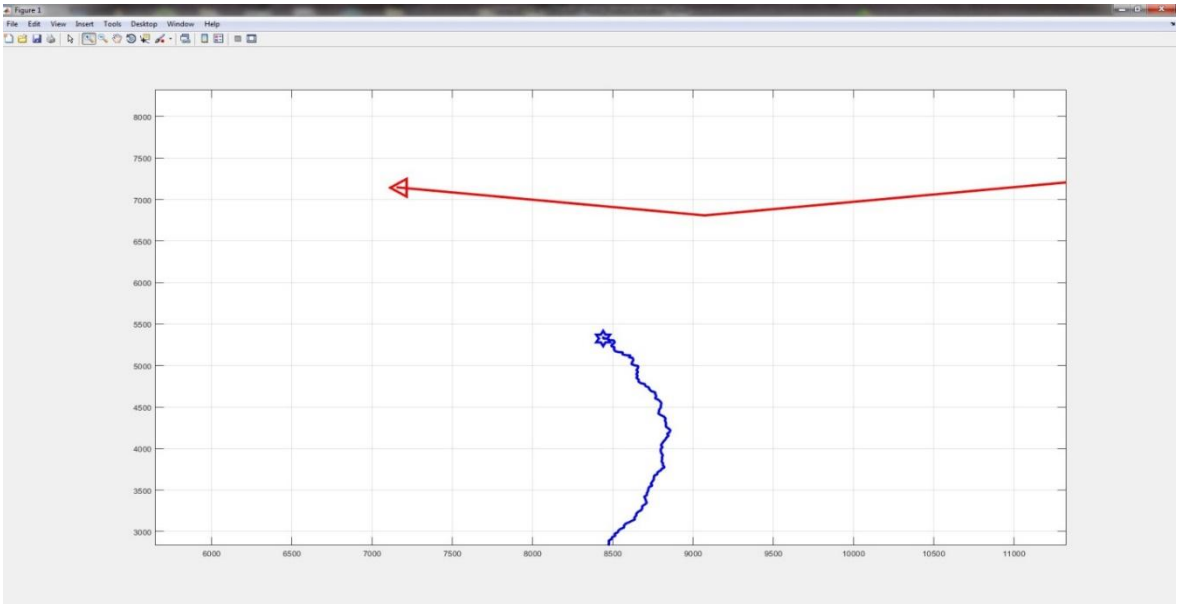


Fig. 3: Destabilization of the missile path

The graph above shows the effects after the target maneuvered in altitude and speed. One can easily see the destabilization of the missile on the trajectory.

The air defense system including CA-94 and Patriot systems

As opposed to the two previous cases, the third operating group has one of the most modern anti-aircraft defense systems, namely the Patriot system. In the next simulation we will be able to observe the degree of improvement of the air defense capability by implementing modern anti-aircraft missile systems.
The input information is as follows:

- Maximum target discovery distance: 60 km;
- The maximum distance at which the target can be fought: 40km;
- Maximum flight speed of the PAC-3 rocket: 1200m/s;
- Maximum flight speed of the A-94 rocket: 250 m/s;
- Initial target flight speed: 200m/s;
- The maximum flight time of the missile A-94: 14 s.

Fig. 4: The result of the Patriot_CA-94 Task Force

The path of the missile launched by the Patriot system is represented by the blue color, the trajectory of the missile launched by the CA-94 system is represented in green, the position of the objective is the black point, the trajectory of the aerial target is represented by the red curve and the purple represents the explosive charge with the infrared fingerprint.

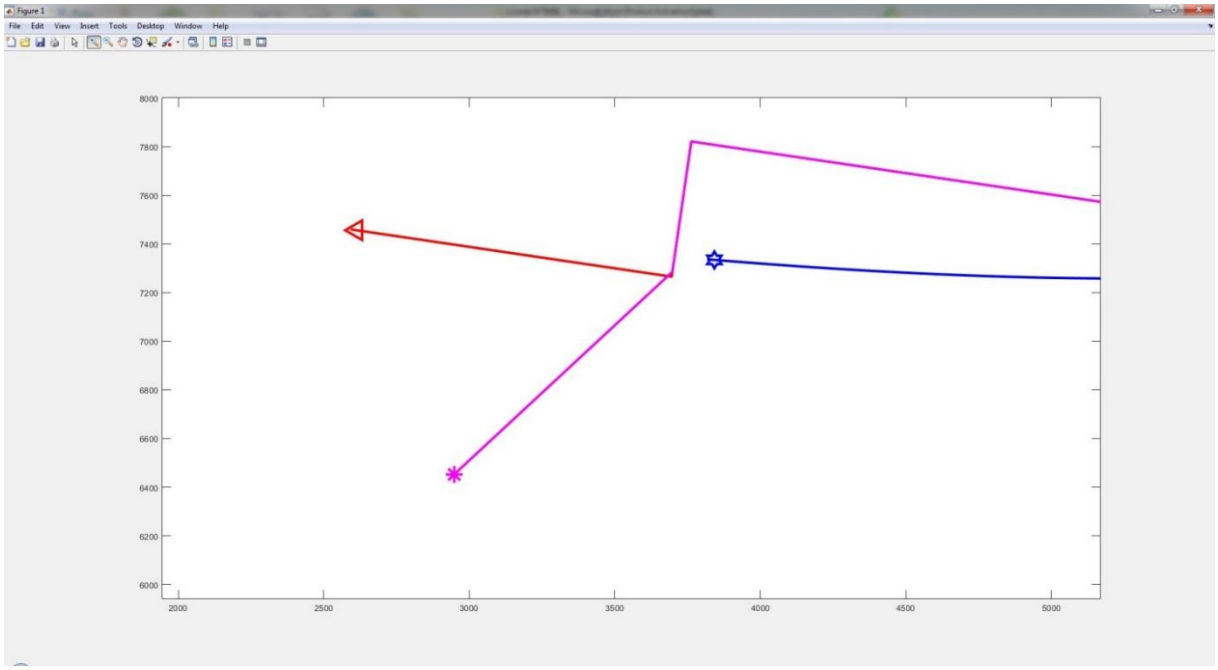


Fig. 5: Launch of the explosive charge

The above graph shows the clear difference in efficiency between the last operating group, the main component of which being the Patriot complex and the other two. In this case, the Patriot complex keeps pace with the sudden change of the target parameters (figure 4) and manages to fight it, but not before the target launches an explosive charge with an infrared fingerprint (figure 5). Even so, the defended target is not jeopardized because the A-94 missile launched by the CA-94 complex intercepts this load and destroys it.

Although the target is changing direction, the Patriot missile does not undergo trajectory destabilization, so it continues to track the target till intercepting it, as shown in figure 6.
According to this chart, the Patriot missile maintains its stable trajectory (blue color) during the maneuvers of launching the explosive charge.

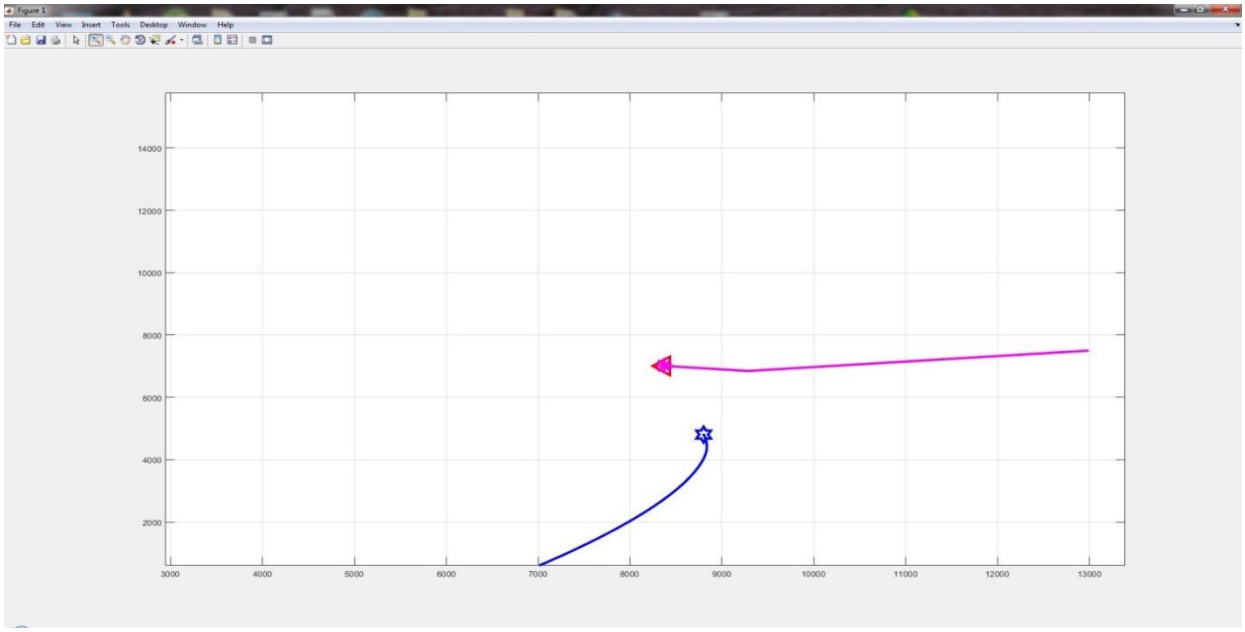


Fig. 6: Maintaining the stability of the Patriot missile trajectory

Conclusions

The following comparative analysis completes this study and highlights the anti-aircraft defense capability characteristic of modern systems.

First of all, the modernization of anti-aircraft defense systems oscillates around the electronic warfare field, so the Patriot system is able to withstand a variety of active and passive jams, while older systems like KUB or OSA-AKM systems are vulnerable to jam resistance.

Secondly, the range of air threats that a complex can combat can play a particularly important role in assessing air defense capabilities. In this case, the Patriot complex is again above the other systems, being able to combat both supersonic targets and ballistic missiles.

References

1. Cristian ENE, Catalin CIOACA (2014). *Rachete antiaeriene autodirijate, vol.I*, Brasov, Romania: Editura Academiei Fortelor Aeriene
2. Eugene FLEEMAN (2012). *Missile Design and System Engineering*, Lilburn, Georgia, Lulu inc.
3. Jeffrey STRICKLAND (2010). *Missile Flight Simulation - Surface to Air Missiles*, Colorado Springs, USA, American Institute For Aeronautics And Astronautics inc.

Marius Alexandru Rizescu,George Bucăța,

ORGANIZATIONAL CHANGE STRATEGIES AND METHODS OF EVALUATION

Marius Alexandru Rizescu*,George Bucăța,**

***"Nicolae Bălcescu" Land Forces Academy, Sibiu, Romania
****"Lucian Blaga" University, Sibiu, Romania
mariusrizescu@yahoo.com
george.bucata@yahoo.ro

Abstract: *Change management can be considered a process, part in the evolution of a company and takes place when the level of performance drops. In order to be conclusive, it must be proper planned and understood by everyone in the company, shared by all employees.*

Keywords: organizational change, change management, organizational strategies.

Introduction

Organizational change can be classified in many ways. The most comprehensive of this is the one that presents the change in the function of three major dimensions: origin, outcome and process of change. The origin of the change has to do with the manner in which the change occurs in an organization, from the environment in which the organization operates or at the latter's initiative. Thus one can speak of unintended changes, which happens simply, and intentional or deliberate changes, actions taken by the organization. Of course, in real life the difference is not so clearly drawn, even deliberate changes can be influenced by an event outside of the organization. Another classification can be made depending on how changing the link to key events in the external reactive changes (changes initiated in response to an event or series of events) and expected changes (as evidenced by its name, initiated in anticipation of events).

The classification practice in terms of management can be done as the level of change, the extent to which the organization is affected by the change. An example of a change to low level would be reorganizing the structure of workstations, whilst a change throughout organisations would be restructuring its complete structure. Some authors continue this idea, giving clear examples of interventions at every level:

- Macro-intervention affecting the entire organization, strategic analysis, the existence of a vision or a mission, strategic development, restructuring and reorganization of the labor process at the level of the organization.
- Major intervention affecting a production unit-a unit formation, planning or strategic positioning, continuous improvement programs, recruitment of new leadership.
- European intervention training strategies for the restructuring of the European teams, teams work and work process reorganization.
- Intervention at the level of the staff-staff development, professional growth, leadership development and reorganisation of workstations.

The process of change is the third dimension according to which one can classify organizational change and relates to the modalities and the progression of events in the changing organization. The

process of change may rank according to its duration or the resources (human and material) to be used in implementing the change. Change unit may be a single entity-an individual or an organization-or interaction between people or relationships within an organization. The manner of change, on the other hand, describe what exactly determines the sequence of events (deterministic or stochastic laws) or if it is built by changing entity as the process evolves.

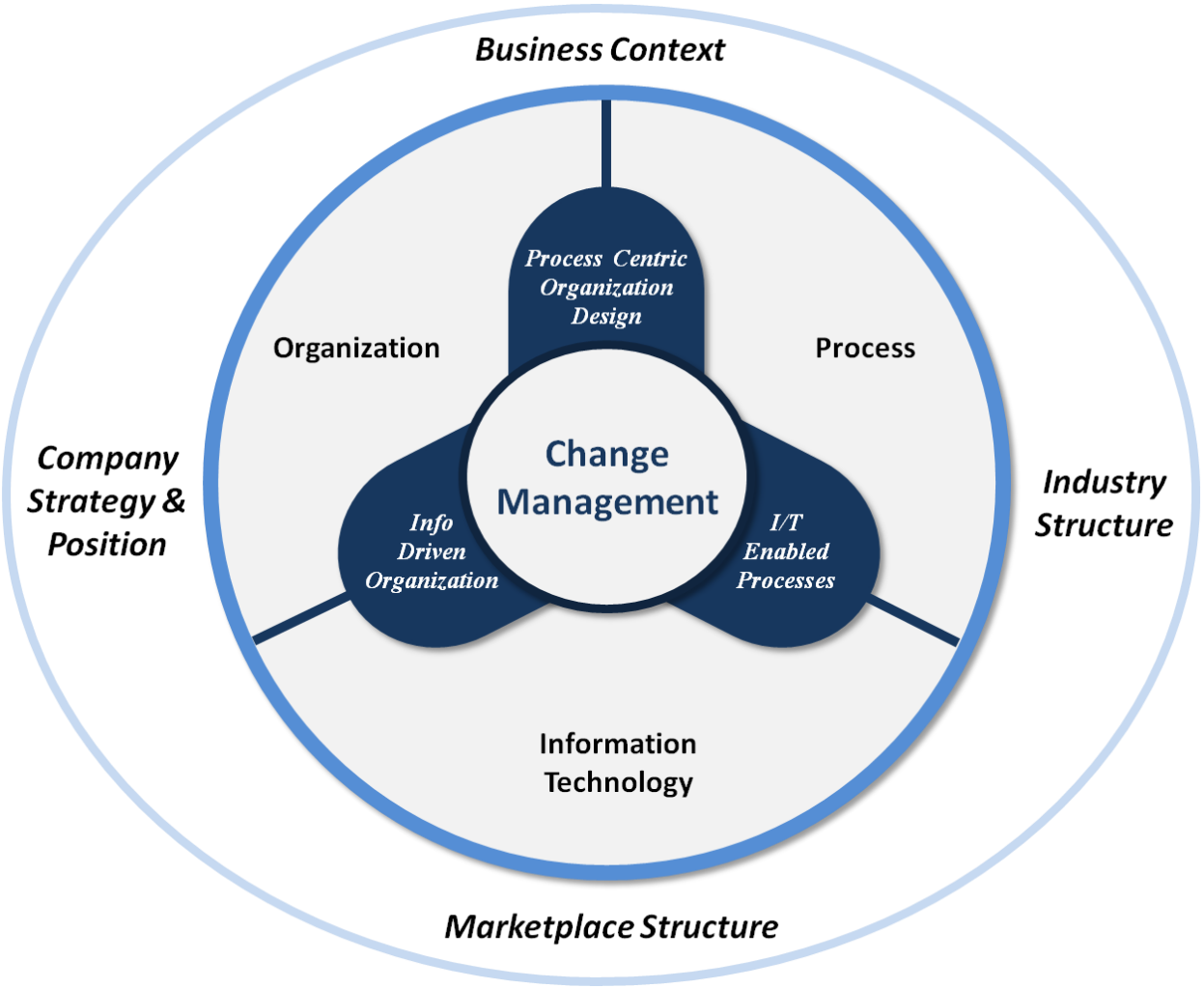


Fig. 1. General overview of the change management process

Organizational change corresponds generally to a new orientation, a radical and fundamental orientations concerning the manner in which an institution can operate and with direct implications on the members. Change management in the organization refers to the totality of activities carried out by a manager so as to orient employees in the implementation of change to accomplish the mission and achieve the proposed goals. Changes that can be planned or re-planned are difficult to manage because they occur randomly and their effects are difficult to predict.

Planned changes can be successfully implemented in the case of compliance with the following steps:

- problem identification and setting goals of change;
- gathering information on the matter;
- synthesis and analysis of information;

- framing of the issue in the light of the information obtained;
- implementation of the plan of action for the implementation of change;
- implementation of the plan or actual deployment of action for change;
- evaluation of the implemented action.

Fig. 2. Management of change in the continuous improvement process

Change is a phenomenona present in developments but always looked with fear and skepticism in its early stages. Within organizations, the changes may generate resistance on the part of employees that is materialized in a delayed implementation or even impossible for organizational improvements. Thus, the managerial ability to create and maintain a climate that minimizes resistance behaviors and encourage participation, acceptance and support becomes essential to any effort to change.

In organizations, resistance to change is any attitude or behavior that indicates opposition to make or support a change. Agents of change see often any kind of resistance as something which must be exceeded in order for the process of change to succeed. It is necessary to change resistance as the feedback which can be used by the agent of change in order to achieve the objectives of the change. The essence of this constructive approach is to understand that when people oppose the change, they defend something important to them.

Depending on the style of management but also by the context in which change is initiated, there is a possibility of pro-active adaptation, in which case the changes are benefiting from a greater implementation and have a lower risk due to settlement through feedback loops. The alternative variant is reactive approach in which the organisation will be strongly shaken by the change. In practice, the

change must be adaptable enough to react to events during the period of transition. A successful transition will include both proactive decisions and reactive.

Systems that form the present organisation are complex: each of them had their own formal and informal targets that, when managed effectively, is the primary objective. The change applied to any of the systems, or in its relationship with other systems, may therefore have an impact on the overall structure and ultimately on the organizational performance. The manager initiates a change that employees need to understand very clearly what are the components affected by that change and what will be the impact of a change in the organization. Thus, a successful strategy will require increasingly more, information about events and conditions outside the institution to increase adaptability to changing organization. In these circumstances, it becomes extremely important for competitiveness, it will express how well will they understand the organization's environment and how well it will be adapted.

Even if it comes to the adoption of a new technology (computer system, production equipment, production process, etc.) there are three major directions for the implementation of change:

- processing mode of enterprise management (Leadership)
- processing enterprise processes (Workflows)
- organizational transformation of culture (Cultural Change).

Stages of implementation of a change are well known by most managers: establishment of an urgent character, creating a guiding coalition, developing the vision and strategy for this change, communicating the change vision and strategic plan, delegating employees, generating benefits in the short term for building credibility, reinforcing the gains and making several changes, anchoring new changes in the culture of the organization. And these constraints are known as: limited resources, insufficient time and especially resistance to change to those involved. The difference between those who succeed and those who fail is given by the level of understanding of the external environment and internal organisation.

Organizational change efforts will fail if this organizational culture remains fundamentally unchanged. The effectiveness of organizational change requires integrating strategies for improvement in a change of organizational culture. Procedural changes remain superficial and cannot be maintained in the long term unless fundamental changes occur, values, ways of thinking and approaches relating to problem-solving. The forces that oppose resistance will enhance its efforts to restore the old status quo. It is possible, in some cases, organizations lose more than if changes were not adopted and would be no strategy in change. Change requires those involved to get out of the comfort zone, considering that all those involved will seek personal comfort, resulting in the current situation that will prevail. Without changing the organizational culture, there is little hope that improving the performance of the organization will be enduring.

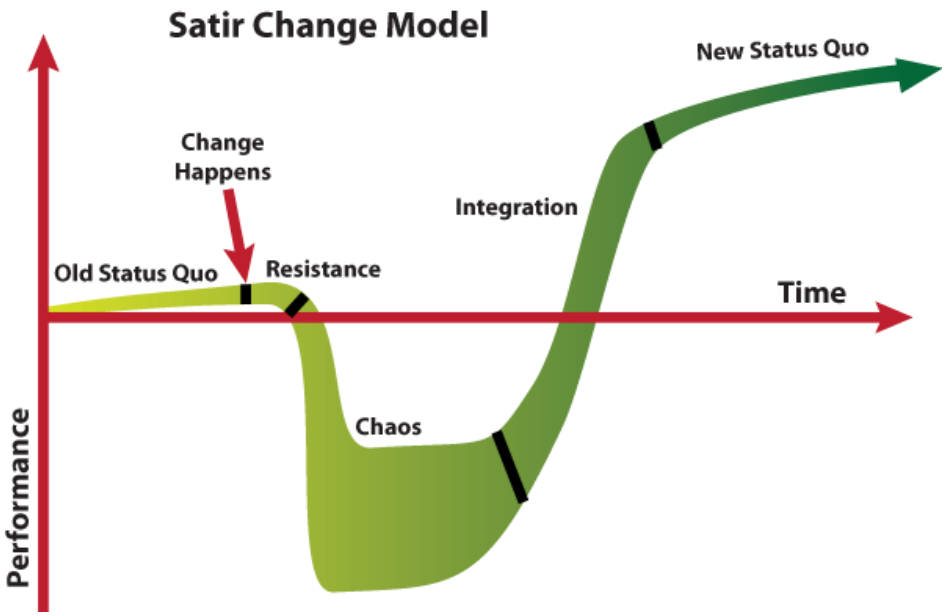


Fig. 3. Satir change model (performance vs time)

Change is constructed on a basis of a new company, slowly transferring employees from the old company to the new company. Most of all, it is recommended that the range of a project management of change should be limited. Following this, a company can achieve success in a short period of time.

Fig. 4. Organizational development strategies model

Successful management of change is more a matter of leadership ability than managerial skills. It's pretty much the same as managing any disorderly, tangled or chaotic. Building a team. Managing change requires a smart team and a great team leader.

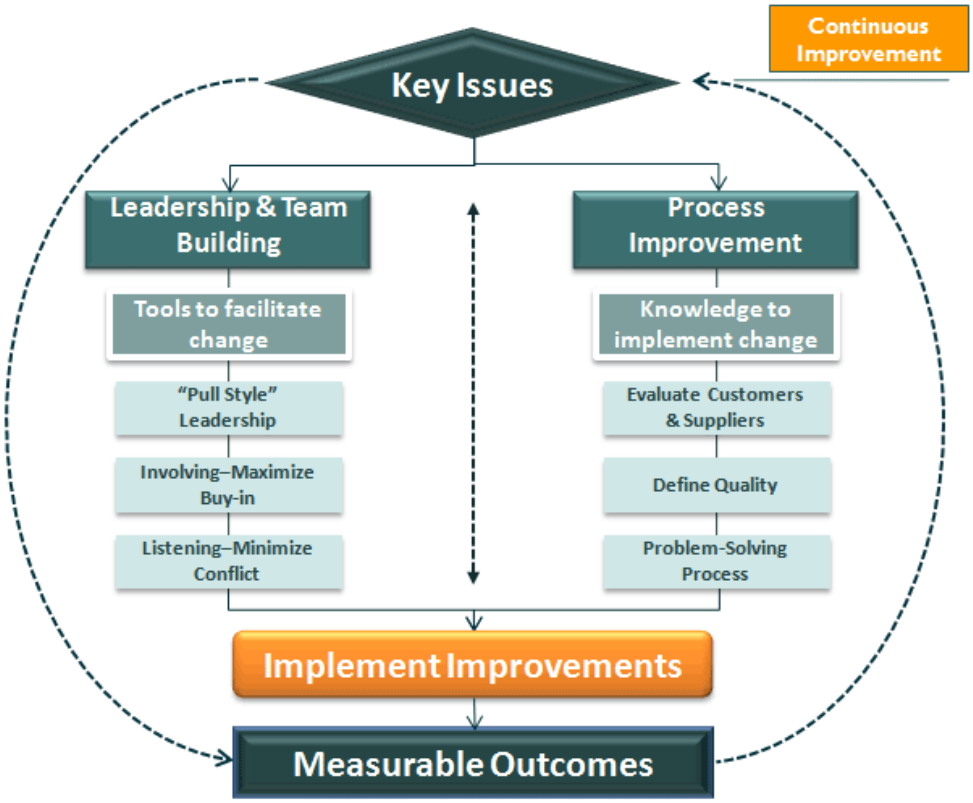


Fig. 5. Performance management, change management strategy

Given that change is inevitable, there are several benefits of applying management of change in organizations, among which are:

- Effective monitoring of the process of change: change process is planned and managed, the desired results are clearly defined and the organization knows that it is the direction of evolution, as well as attaining the stage. People involved in the process have at their disposal a set of procedures, tools and key performance indicators which will guide specific activity related to the process of change. In addition, you can assess the impact of change on the Organization and people, both during implementation and after completion thereof.

- Proper management of human resources through the effective management of change is encouraged, the management of human resources, during and after the process of change, while minimizing resistance to change and maximizing people's commitment involved in or affected by the change (stakeholders, clients, suppliers, employees, managers, etc.), both towards the desired change and the face of the organization.

- Control and minimize the negative impact on the current activity: managing the process of change, as a distinct approach enables its adaptation according to the operational requirements of

the organization, so that the impact on current activity is minimal. Also, the necessary resources are estimated and provided separately towards current operations.

- Acquisition best practice: implementing a process of change is a valuable exercise for the organization and allows for the development of new skills, new knowledge accumulation, development teams and organizational leadership, improve communication, etc., all of them becoming new practices beneficial to the organization and integrated into the current activity.

Organizational development is a continuous and planned effort to change organizations to become more effective and more human. The fact that organizational development is planned a different from routine or accidental efforts taking place in all organizations. Continuous efforts to DO in at least two senses: they stretch over a long period of time and become elements of organizational culture. The following specific strategies of organizational development (OD) can be identified:

- Team training aimed at increasing the effectiveness of work teams by improving interpersonal processes, clarify objectives and roles. The objective of this phase is to build a picture of the strengths and weaknesses of the team, and the ideal result is a list of changes required to improve the functioning of the team. The following meetings are usually are usually decided to aim. Along training, change agent can glean confidential information from members, acting as a catalyst and a resource provider.

- Reengineering of organizational processes to achieve major improvements in terms of cost, time and service. Essentially, a large portion of reengineering is geared towards one or both goals listed below:

    - reduction of intermediate steps to streamline the process:
    - strengthening cooperation between those involved in the process.
    - reengineering typically includes certain practices, posts are usually redesigned and enriched;
    - a strong emphasis is placed on teamwork;

This strategy is extended in areas where it has been installed a bureaucracy, large gains are possible through advanced technology and deregulation of hot competition. Such fields are insurance, banks, brokerage, or telecommunications.

- downsizing (downsizing) consists of a set of activities centred on the management of the organization in order to improve efficiency, productivity and/or competitiveness. The adoption of this strategy affects both the number of persons working in the organization, and the processes of work. Four characteristics of this strategy are considered essential to distinguish phenomena such as organizational decline or even dismissal.

First, the downsizing involves a set of actions undertaken intentionally. Secondly, although the strategy involves downsizing, it boils down to this. There are a number of strategies associated with this in mind, such as transfers, assistance to persons in order to find a new job, etc. The third characteristic is that downsizing is centered on increasing the efficiency of the organization. Finally, the strategy for reducing the size of affect and work processes, whether intentionally or unintentionally. If the size of the

reduction strategy has been appreciated and adopted as a solution for increasing performance and competitiveness, it is important to know what line exists between the initial expectations and achievements. It seems that the effects are not far from the expected ones. When the strategy was used, with no previous training, it has produced serious organizational dysfunction, especially prominent in the impossibility of introducing any form of improvement of activity and even in increasing organizational inefficiencies.

Conclusion

Across all industries change rate increases very quickly and the time of changes is reduced significantly. Change management in organizations becomes increasingly more difficult and more important. The mission of changing an organization is an extremely challenging, dynamic environment and resistance to change is acting against the person who is trying to achieve change. Any attempt to put in place an organizational change will constitute a threat to some groups or coalitions. Organizational changes are often accompanied by conflicting interests, ethics and behaviors outside of emotional turmoil. Leaders responsible for the change must learn to navigate through these dangerous waters. Top management has to assume responsibility for the elaboration of a strategic plan which has to be well developed. Even though the existing methods of innovative enhancement, focuses on the employee involvement in the strategic planning process, the ultimate responsibility belongs to the top management.

References:

1. Altindis, S. (2011). Job motivation and organizational commitment among the health professionals: A questionnaire survey. African Journal of Business Management Vol. 5(21) , 8601- 8609.

2. Frontiera, J. (2010). Leadership and organizational culture transformation in professional sport. Journal of Leadership & Organizational Studies, 17(1), 71–86.

3. Grieves, J. (2010) Organizational Change. London: Oxford University Press

4. Hayes, J. (2010) The theory and practice of change management. New York: Palgrave McMillan

5. Küng, L. (2013). Innovation, technology and organisational change. Legacy media's big challenges. An introduction. In T. Storsul&Krumsvik Arne H. (Eds.), Media innovations. A multidisciplinary study of change (pp. 9–12). Gothenborg: Nordicom.

6. Kelloway, E. K., Turner, N., Barling, J., & Loughlin, C. (2012). Transformational leadership and employee psychological wellbeing: The mediating role of employee trust in leadership. Work & Stress, 26(1), 39–55.

7. Lunenburg, F. (2010). Approaches to Managing Organizational Change. INTERNATIONAL JOURNAL OF SCHOLARLY ACADEMIC INTELLECTUAL DIVERSITY VOLUME 12, NUMBER 1, 2010 , 1-10.

8. Luecke, R. (2013) Managing Change and Transition. Boston, MA: Harvard Business School Press.

9. Pettigrew, &Whipp. (2013). Value Based Management. Retrieved january 26, 2013, from valuebasedmanagement.net:

10. Whelan-Berry, K. S., & Somerville, K. A. (2010). Linking Change Drivers and the Organizational Change Process: A Review and Synthesis. Journal of Change Management , 175-193.

Svetozar B. Botev,

SHAPED CHARGE WITH DIFFERENT LINER MATERIALS

Svetozar B. Botev

Joint force command, Bulgaria, Sofia, sitenaz@abv.bg

***Abstract**: The existing shaped charge mostly adopts a metal shaped jet. Using a low-density material as the liner for shaped jets: floatglass, Lucite, Plexiglas and copper. Measure jet tip velocity, density,length,diameter and mass. The results show that the three kinds of low-density shaped jets compared with cooper linear..*

***Keywords**: shaped charge, liner, low-density materials*

КУМУЛАТИВНИ ЗАРЯДИ С ОБЛИЦОВКА ОТ НИСКО ПЛЪТНИ МАТЕРИАЛИ

Светозар Б. Ботев

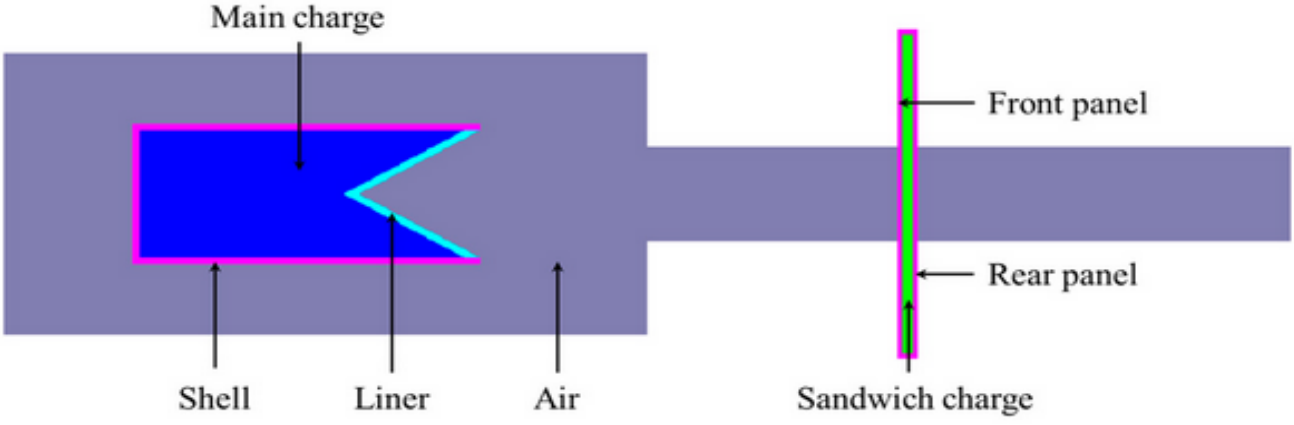
Експериментални данни за кумулативни заряди КЗ с различни материали за облицовка [3].

Shell Length	Shell Thickness	Shell Diameter	Cone Bottom Diameter	Liner Thickness	Front Panel Thickness	Sandwich Charge Thickness	Rear Panel Thickness
135 mm	3 mm	60 mm	54 mm	3 mm	2 mm	4 mm	2 mm

Фигура 1:Параметри на КЗ

Material	A (Mbar)	B (Mbar)	C (Mbar)	R_1	R_2	ω	ρ_0 (g/cm^3)	P_{CJ} (Gpa)	D (m/s)
CompB	5.242	0.07678	0.01082	4.20	1.10	0.34	1.717	29.5	7980

Фигура 2:Взривно вещество на КЗ и активната броня

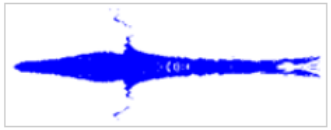


Фигура 3:Обстановка на тестване

Облицовка на кумулативната кухина на заряда от различни материали влияе върху плътността, скоростта, формата и стабилността на образуваната кумулативна струя КС.[1]

Температурата на стопяване на материала влияе пряко върху формирането на кумулативната струя.

Точка на топене на мед 1083 °C, стъкло – 720°C, а на термопластична акрилна смола и плексиглас около 110°C. Колкото температурата на топене е по ниска формирането на КС протича в течно състояние на материалите, което води до увеличаване на дължината и скоростта и.

Material	Shaped Jet Configuration	Jet Tip Velocity (m/s)	Jet Tail Velocity (m/s)	Jet Length (mm)	Pestle Length (mm)
Copper		6088	138	84	56
Floatglass		7421	953	98	58
Lucite		9715	667	137	77
Plexiglas		9871	632	141	78

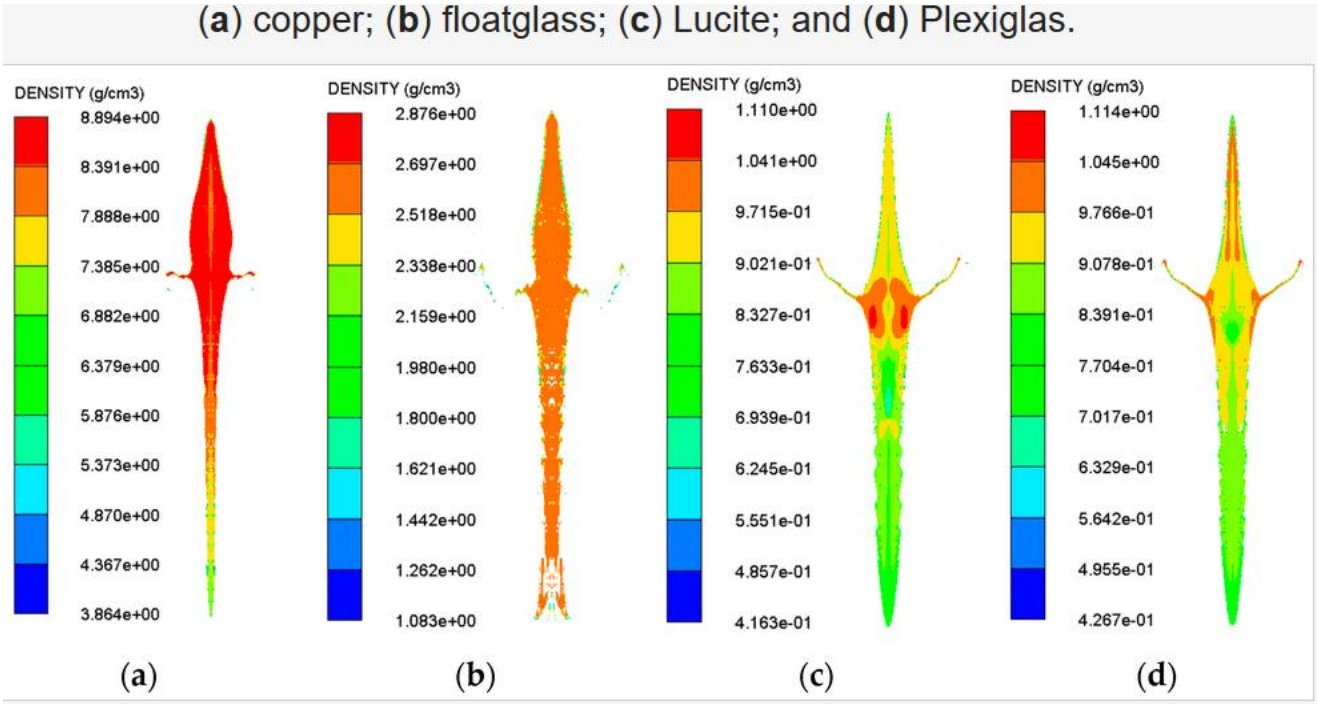
Фигура 4:Формиране на КС при различни материали на облицовката

От горния анализ, основан на точката на топене и точката на омекване, е очевидно, че пластичността на три аморфни материала с ниска плътност под действието на оформения заряд е по-добра от тази на медта.Превърнатата маса кумулативна облицовка в струя е ηPlexiglas ≈ ηLucite > ηfloatglass > ηcopper най висока при облицовка от плексиглас.Скоростта на КС VPlexiglas ≈ VLucite > Vfloatglass > Vcopper, като най-високата скорост на КС е при облицовка от плексиглас.

	Material	Jet Tip Velocity v_t (m/s)	Jet Tip Diameter d_t (mm)	Density ρ (g/cm^3)
a)	Copper	6042	2.6	7.02
b)	Floatglass	7464	5.2	2.53
c)	Lucite	9785	6.0	0.763
d)	Plexiglas	9849	6.0	0.776

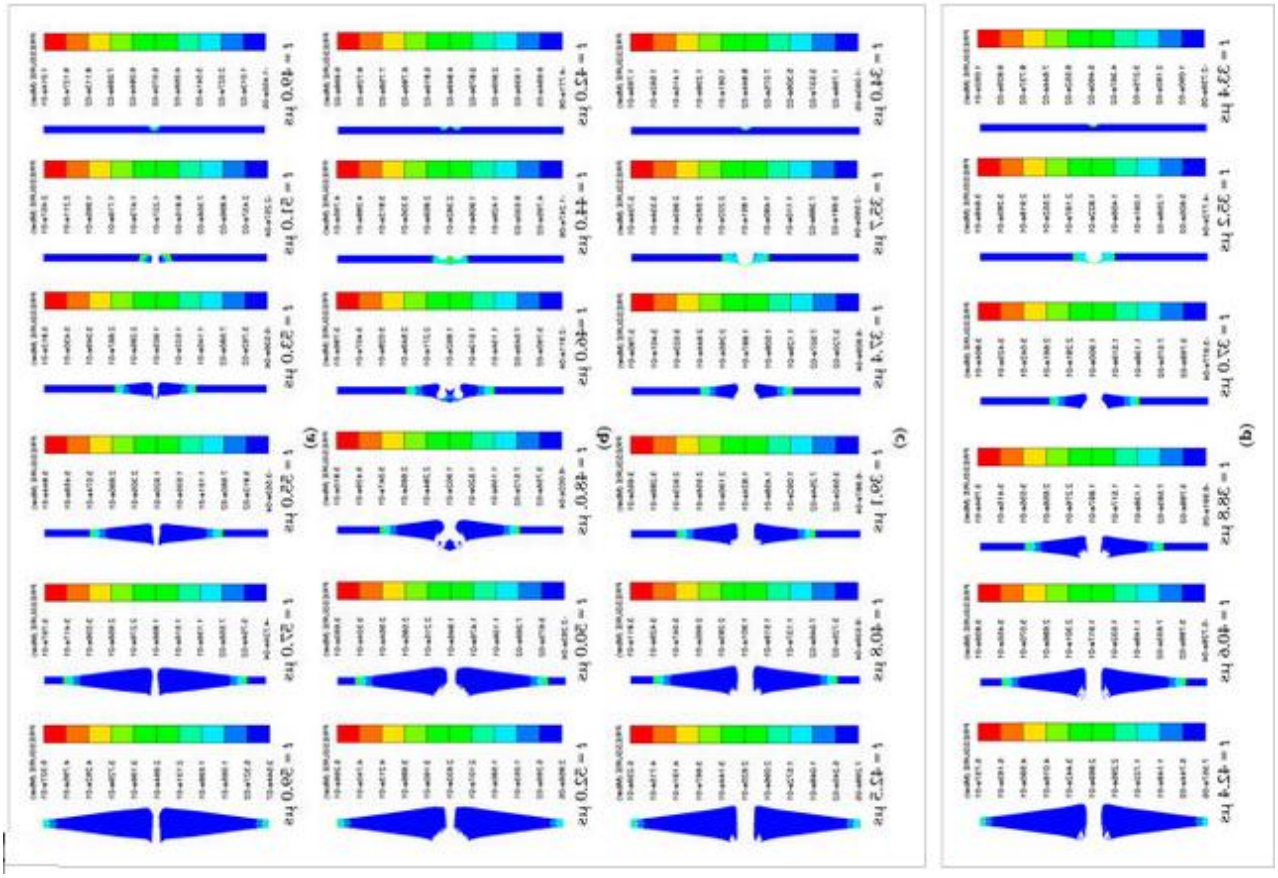
Фигура 5: Характеристики на материалите за облицовката на КЗ

Плътността на образуваната КС от различните материали е показана на фигура. Най-плътна струя се образува от медта следвана от стъклото и накрая на материала с ниска плътност.От Фигура 6 се виждат различията на формираните КС с облицовка от стъкло, термопластична акрилна смола, плексиглас и мед. Образуваната КС от медната облицовка е изострена и с най малък диаметър. Скоростта на струята е най-ниска, а плътността и е най-висока и пробивната и част е най-къса видно от фигура 4 и 5. С най дълга пробивна част на КС е формирана от облицовката от стъкло. Най високата скорост на образуваната КС е от плексиглас.[4]



Фигура 6:Формирана КС с различни ниско плътни материали сравнени с медна

Кумулативната струя избива при излизане от бронята нещо подобно на тапа поради специфичната чашовидна форма фигура 6*b* на образуваната челна част на струята. Струята от плексиглас пробива най-голям диаметър в бронята. [2]



Фигура 7:Пробива на активната бронявъв различни времеви интервали

От фигура 6 и 7е видно, че използваните материали с висока пластичност и скорост образуват КС по-бързо от медта. Видно е как КС от стъкло избива при излизане от бронята нещо подобно на тапа поради специфичната чашовидна форма на образуваната челна част на струята.

Диаметърът на пробоините респективно върха на струи от мед, стъкло, луцит и плексиглас е 2,6 mm, 5,2 mm, 6,0 mm и 6,0 mm, което съответства на скорости на върха 6042 m / s, 7464 m / s, съответно 9785 m / s и 9849 m / s, скоростта на КС с ниска плътност са по-големи от медта. Дължината на струята от мед, стъкло, луцит и плексиглас е 84 mm, 98 mm, 137 mm и 141 mm при време t = 35 μs, Формирането на КС с нископлътни материали се формира по рано в сравнение с медта комутативна облицовка.

References

1. Held, M. (1999). Effectiveness factors for explosive reactive armour systems. Propellants Explos
2. Held, M. (2004). Dynamic plate thickness of ERA sandwiches against shaped charge jets. Propellants Explos
3. Mayseless, M. (1999). Jet plate interaction: The precursor. In Proceedings of the 18th International Symposium on Ballistics
4. Koch, A. Häller, F. (2001). Sensitivity of era-boxes initiated by shaped charge jets. In Proceedings of the 19th International Symposium on Ballistics
5. Zeng, F.J. Ma, X.Q. Liang, X.Q. (1996). Initiation mechanism and the measurment of criterion value for jets on double reactive armor. Trans. Beijing Inst.

Svetozar B. Botev, Valya M. Simeonova,

DEVELOPMENT BULGARIAN ARMY FULL INTEGRATED LOGISTIC SYSTEM

Svetozar B. Botev, Valya M. Simeonova

Joint force command, Bulgaria, Sofia, sitenaz@abv.bg
valiasimeonova_sweet@abv.bg

Abstract: *The existingBulgarian army military full integrated interoperabilitylogisticsystem gives management tool to analyzed and minimize charge for defense. Synchronized logistic and account record in all military units. Learning, development, invent, data base exchange, cooperate logistic and account records in one Enterprise resource planning ERP system, compare account recordsbetweenBulgarian information system BILS and used local account system used inmilitary units.*

Keywords *Interoperability,development, account system, logistic system, Bulgarian army, military management*

Информационна система „Логистика на Българската армия"/ИС ЛБА/ съществува в Доктрината за логистика на Българската армия, която е в приоритетите за развитие на всички управленски нива в министерството на отбраната/МО/ и БА и е ориентирана изцяло към потребителите. [1] и[5]

Информационна система **ИС ЛБА** е съвкупност от взаимосвързани модули попълвани от специалистите във всички военни формирования и анализирани от управлението в МО.

Успехът при внедряването на ИС ЛБА може да има само тогава, когато в съвременното информационно общество, потребителите и управлението изграждат еднакви електронни бизнес модели за обобщаване на финансова и логистична информация. Естествена цел на ръководството на МО и България като член на НАТО е да развива ИС ЛБА за по-високо ниво на ефективност в управлението и създаване на оперативна съвместимост на МО и НАТО в многонационална среда по всички декларирани мисии на БА. В този смисъл ИС ЛБА е проект без алтернатива за всеобхватно повишаване на оперативната съвместимост и ефективността при управление на логистичните и финансови информационни потоци в БА и МО. [2]

Тенденцията в развитието на електронното управление като цяло в МО следва международния тренд за активно използване на цифрови данни във всички сфери на НАТО и ЕС.[4]Зависимостите при въвеждане на електронни системи в България, и в частност в МО, имат едни и същи проблемни въпроси: само наличието на техника не може да даде желаните електронни услуги; провеждането на обучение на персонал неможе да задвижи в желаната бързина данните намиращи се в други разпръснати системи и не на последно място необмислени и недетайлно описани алгоритми за миграция на данните от използваните към новите информационни системи.

Проектът ИС ЛБА стартира през 2003 г. и преминава през различни фази на технологично развитие до 2013 г. Със заповед на началника на отбраната 134/30.06.2014 г.е въведена в реална експлоатация.

В МО напредъкът в развитието на ИС ЛБА се свързва основно с развитие и надграждане на елементи от инфраструктурата и основните информационни и комуникационни системи и техника и мащабни обучения на служители в ИТ умения за работа със ИС "Логистика на БА".

Първите стъпки по внедряване на ИС ЛБА във военните формирования стартират през 2013 година от дирекция „Логистика".

В подкрепа на горните думи са фактите, че по тогавашния пилотен проект ИС ЛБА е получено комуникационно оборудване за **сто** работни места в цяла България и е осигурено разработване на основните бизнес процеси случващи се в логистиката на БА.

От 2003 г. до 2012 г. след няколко фази от развитието на проекта са проектирани, разработени и тествани основните бизнес процеси използвани в логистичното и финансово осигуряване на БА.

От 2012 г. до 2014 г. са обучени над 750 служители от логистичните и финансови звена в цялата БА, а въведеното формирование е само едно. Обучен разнороден личен състав от БА за работа с ИС ЛБА от 2014 г. до начало на 2019 г. 765 човека;

Обучен разнороден личен състав от БА за подготовка и мигриране на данните в ИС ЛБА от 2017 г. до начало на 2019 г. - 846 човека;

От 2013 г. до 2016 г. е въведено **едно военно формирование** с 2200 номенклатури. За една година от създаването на Сектор "Информационна система „Логистика на Българската армия"при **Съвместно командване на силите /СКС/** е въведено едно военно формирование с 2500 номенклатури, без поддръжка от фирма „Рила солюшънс". Със заповед на началника на отбраната 12.2016 г. се създава нов сектор ИС ЛБА от отдел „Логистика" при Съвместното командване на силите. Няколко месеца след създаването си е въведено в експлоатация още едно военно формирование с около 3200 записа.

През началото на 2019 г.,след близо две години,са въведени 2 военни формирования с 31500 номенклатури.Въвеждането на реални данни в ИС ЛБА има реален успех след създаване на изпълнителско звено в СКС. Наред с проблемите по скоростта за въвеждането с норми от 2 дни за формирование, технически несъвършено разработената система създава редица взаимосвързани проблеми при експлоатацията на реализираните модели в ИС "Логистика на БА". Всички технически несъвършенства се проявяват при реалната експлоатация на ИС ЛБА. Модификациите за системата започнаха и продължават да валят, въпреки приетата на въоръжение ИС "Логистика на БА".

Състоянието при използване на ИС ЛБА може да са анализира от резултатите на всички участници, ползващи активно ресурсите й. На този етап работят от 2014 г. - 24510 – София(със заповед на командира 48960 София от 05.07.2019г. работи само с ИС ЛБА), от 2017 г. - 42700 Сливен, от 2019 г. - 24350 Кочово, 24480 Ловеч, 48960 София и 42610 Козарско.

В бързината за изпълнение на утвърдените от началника на отбраната графици се омаловажават логистичните детайли, въвеждани в ИС ЛБА. Детайлите за логистиката са не по- малко важни от събраните през 2006 г. с МЗ и ПМС за въвеждане на двустранното счетоводно записване във военните формирования на БА. Практиката при въвеждането и трансформирането на данните от използваните до момента счетоводни продукти във военните формирования на БА ясно показва, че има съществени различия между изпращаните по команден ред логистични и счетоводни отчети и данните в ползваните продукти. Постигане на оперативна съвместимост между различни военни формирования без единна кодификационна система е невъзможно.Данните й на този етап от развитието на ИС го доказват за пореден път. Един и същи артикул е заведен с различни номера, дори и в едно и също военно формирование, така също и между формированията. Създадената оперативна съвместимост с използването на ЕМК за сега не се е изгубила само при автоматизирана подсистема НИКЕ.

Полагането на усилия за максимално синхронизиране на работата на ИС ЛБА и прилагане на „Служебното начало" при въвеждане на данни за различни взаимосвързани операции ще доведе до намаляване на субективни грешки. ИС ЛБА предостави ефективно решение за осъществяване на принципа на „Служебното начало", състоящ се в еднократно събиране и многократно

използване на информацията в цялата йерархия на БА и МО. На този етап в развитието на ИС ЛБА „Служебното начало" е частично залегнало и се налага въвеждане на една и съща информация многократно, което води до възможност за субективни грешки.

Оперативна съвместимост

Съществува съществен проблем с постигане на оперативна съвместимост в работата на сега използваните счетоводни продукти помежду си в обща йерархична цифрова среда и често е невъзможно постигане на интегритет на получени отделни проектни резултати и постигане на висока ефективност в управлението на БА и МО. Това се дължи до голяма степен на липсата на системен подход при провеждане на процеса по въвеждане на данни в ИС „Логистика на БА", което да позволи централизирано налагане на стандартите за оперативна съвместимост, както и координиране дейността на оперативно отговорните звена в управлението на БА и МО. Неадекватното оперативно състояние на ИС ЛБА е не само вътрешен проблем за МО, но и за поетите ни ангажименти за оперативна съвместимост с електронни системи в NATO (NSPA ползващ NSN). Използване на ЕМК като справочна информация и преминаването към NSN с МЗ- ОХ 1082/13.12.2001 г. доведе до информационен вакуум при кодифицирането на наличните и до момента изделия без NSN номер. Има добри примери за частична оперативна съвместимост на финансовите данни обобщавани в щаба на ВВС по електронен път от счетоводен продукт Алгос (ежемесечен отчет по сметки/параграфи). На този етап в единен номенклатурен списък ЕНС брой номенклатури с NSN – е около 0,01%.

Предоставяне на електронни услуги

Процесите с електронна идентичност и електронният подпис не са развити и усъвършенствани в ИС ЛБА, което изключително много затруднява хората при използването на всички налични електронни услуги в МО. Липсата на универсална електронна идентичност е от съществено значение за цифровизацията като цяло. Електронният подпис не се използва от ИС ЛБА и на този етап от развитието си.

Съгласно МЗ 137/06.03.2012 г.: чл. 7 ал.1 Първичния счетоводен документ е хартиен или магнитен носител и ал.5 замяна на подписи в първичните счетоводни документи с електронни по смисъла на Закон за електронния документ и електронни подпис ДВ бр. 34, чл. 25 ал. 3 Ценните образци първични счетоводни документи могат да се съставят и като електронни, като се спазват изискванията на Закон за счетоводството и Закон за електронен документ и електронен подпис.[5]

Единствения документ позволен за електронна обработка е книга за отчитане на материалните средства ПФСР 101.[5]

Все още не е постигнато пълно интегриране на данните във военните формирования от БА, използващи различни счетоводни системи и ИС ЛБА. Осигурена е свързаност с КИС ЩИТ на БА с малка част военните формирования, като се планира бъдещо инфраструктурно изграждане.

Факт е, че срочните отчетни донесения се обогатяват със специфично търсена информация (липсваща в ИС ЛБА) по административни указания и оригиналния подписан документ е носителят и за йерархията, което е сред основните причини, поради които структурите и потребителите в тях да не използват активно, предлаганите електронни данни въведени вИС ЛБА.

Проблемни въпроси:

- Липса на съответно популяризиране на предлаганите услуги от ИС ЛБА и произтичащата от това слаба информираност на служителите използващи въведената логистична и финансова информация.
- Липса на йерархичен оперативен отчет по различни класове материални средства в ИС ЛБА;
- Слаба заинтересованост на всички нива на управление от данните в йерархичната структура;

- Липса на техническа информация за стандартни номенклатури от NSN.

Положителни страни

- Концентриране на финансово материалната информация на едно място.
- Възможност за обобщаване на огромен обем от информация.
- Анализиране и управление на логистичните и финансовите потоци.

Разработване на модификации обслужващи най-тежките звена, периодично обобщаващи движението както на финансови, така и на материални ресурси.

References

1. Доктрина за Логистиката в БА – МО, 2013 г.
2. Михайлов, Ж.Логистичната ИС на БА – проект без алтернати-
ва.https://cio.bg/digitalizacia/2014/07/23/3440488_logistichnata_is_na_ba_proekt_bez_alternativa/
3. Националната отбранителна стратегия
4. Стратегия за развитие на електронното управление в Република България 2014–2020 г.
5. Счетоводен документооборот МЗ 137/06.03.2012 г.

Maxim M. Alashki,

DOCUMENT REGULATING THE LIFE CYCLE MANAGEMENT OF DEFENSE PRODUCTS IN THE MINISTRY OF DEFENCE

Maxim M. Alashki

Address: 3, Dyakon Ignatii Str., 1092 Sofia, Ministry of Defence, Defence Acquisition Directorate

***ABSTRACT**: Brief information is provided on the life cycle of defence products and the document that should regulate it within the Ministry of Defence, its development over the years, and the current situation around its lack. The author proposes an alternative version of the document.*

***KEY WORDS**: Life Cycle, Life Cycle Process, Defense Product, Defense Acquisition System, Regulation, Alternative version.*

ДОКУМЕНТ, РЕГЛАМЕНТИРАЩ УПРАВЛЕНИЕТО НА ЖИЗНЕНИЯ ЦИКЪЛ НА ОТБРАНИТЕЛНИТЕ ПРОДУКТИ В МИНИСТЕРСТВОТО НА ОТБРАНАТА

Максим М. Алашки

Адрес за кореспонденция: 1092 гр. София, ул. Дякон Игнатии № 3, Министерство на отбраната, дирекция „Отбранителна аквизиция".

***АНОТАЦИЯ**: Дадена е кратка информация относно процеса на жизнения цикъл на отбранителните продукти и документа, който следва да го регулира в рамките на Министерството на отбраната, неговото развитие през годините и настоящата ситуация около неговата липса. Авторът предлага свой алтернативен вариант на въпросния документ.*

***КЛЮЧОВИ ДУМИ**: Жизнен цикъл, процес на жизнения цикъл, отбранителен продукт, Система за отбранителна аквизиция, Наредба, алтернативен вариант.*

Процесът за управление на жизнения цикъл на отбранителните продукти е насочен към поддържане на постоянно и високо ниво на надеждност и експлоатационна годност на отбранителните продукти в интерес на потребностите на Въоръжените сили (ВС) с цел изпълнение на техните мисии, цели и задачи. Той е най-основният (фундаментален) процес на Системата за отбранителна аквизиция (СОА), който обединява всички останали процеси на системата и от чиято ефективност зависи в значителна степен ефективността на цялата система. С понятието „жизнен цикъл на отбранителните продукти" се представя по-тясното разбиране на понятието „отбранителна аквизиция".

През всичките години от деветдесетте години на миналия век считано до 2013 г. винаги е съществувал документ в Министерството на отбраната (МО), който да регламентира управлението на жизнения цикъл на въоръжението и техниката. Последният такъв се наричаше Правилник за управление на жизнения цикъл на отбранителните продукти (ПУЖЦОП или П-7), обнародван в ДВ, бр. 70, от 09.09.2011 г. [1]. Същият е отменен с Правилник за отмяна на правилника за управление на жизнения цикъл (П-5) от 15.07.2013 г. [2] по предимно субективни причини, без да се осмислят напълно последствията на отсъствието на такъв документ.

С този правилник се определят условията и редът за осъществяване на управлението на жизнения цикъл на отбранителните продукти в МО, структурите на пряко подчинение на министъра на отбраната (СППМО) и Българската армия (БА), както и фазите му. С него се дава правна уредба на процесите от жизнения цикъл на отбранителните продукти: планиране на жизнения цикъл на отбранителни продукти във ВС, придобиване на отбранителни продукти за нуждите на МО, структурите на пряко подчинение на министъра на отбраната и БА, управление изпълнението на инвестиционни проекти за модернизиране на въоръжение и техника и тяхната категоризация, провеждане на изпитвания на отбранителни продукти в интерес на отбраната, изготвяне на ведомствени и осигуряването на международни стандартизационни документи и контрола по спазването им, осигуряване и управление на качеството на отбранителните продукти, извършване на кодификация на отбранителните продукти, изменение на срока на експлоатация на отбранителните продукти, приемане на и снемането от въоръжение, приемане на и снемане от употреба (въоръжение и експлоатация), разкомплектоване, бракуване и унищожаване, придобиване и/или използване на отбранителни продукти по междуправителствени споразумения, ратифицирани от НС, и високотехнологични проекти по Програмата на НАТО за инвестиции в сигурността. Правилникът регламентира участниците в управлението на жизнения цикъл на отбранителните продукти - ръководството на МО и БА (видовете въоръжени сили и Съвместното командване на силите), подпомагано от щатни и нещатни органи и техните функционални задължения [3].

Според ПУЖЦОП жизненият цикъл на отбранителните продукти включва следните 5 фази: концепция; разработване, с 4 етапа: проучване, идеен проект, работен проект и опитен образец; придобиване; експлоатация и поддръжка; снемане от употреба (експлоатация или въоръжение).

Както бе посочено, този основен за функционирането на СОА е отменен и липсата му създава огромна празнота във функционално и чисто практическо и процесуално отношение. Този нормативен вакуум към момента, повече от шест години след отмяната, не е запълнен, за което са правени множество опити – многократно създаване на работно групи, които да предложат как да бъде разрешен получилият се неприятен казус и свързаните с него проблеми, варианти на проекти на нов документ, които така или иначе не биват одобрени, отдадени са заповеди и вътрешни указания за работа по някои от направленията (процесите), които регулира правилника, търси се регулация в други нормативни и подзаконови документи т.н.

От 2016 г. има промяна в Закона за отбраната и ВС (ЗОВС, чл. 26, т. 11а. – нова/ДВ, бр. 98 от 2016 г.) [4], с която на министърът на отбраната се вменява да ръководи политиката по управление на жизнения цикъл на отбранителни продукти и да издава наредба за условията и реда за осъществяване на тази дейност в МО, СППМО и БА (липсата на което до сега, според юристите в МО, е било пречка за наличието на подобен документ). В резултат на това с министерска заповед № МЗ Р-101/03.04.2018 г. е създадена работна група за изготвяне на проект на нов такъв документ. След много перипетии и варианти, от месец ноември 2018 г. има изготвен проект от работната група, който по ред причини от обективно и субективно естество (които не са предмет на настоящия доклад) не е приет все още.

Анализирайки въпросния проект на работната група, обаче, се откриват множество неточности, непълноти и несъответствия, както от техническо естество, така и от принципно и идеологическо такова. Поради необходимост от ускоряване на работата по документа, предвид сроковете, ангажиментите, отговорностите и практическата му необходимост, и възможност за представяне на лични (алтернативни) мнения по темата, от друга страна, авторът е разработил и предоставил на обсъждане свой собствен вариант, базиран на многогодишния му опит, изследователска

и анализаторска дейност и експертиза в предметната област, както и използвайки чуждата подобна практика. Този вариант на документ/наредба има следните общи положения и идеология:

- 4 фази (+ 1 опционална - Разработване):
  1. Заявяване (Concept),
  2. Придобиване, приемане на въоръжение и въвеждане в експлоатация (Acquisition),
  3. Експлоатация и поддръжка (ILS),
  4. Извеждане от експлоатация и снемане от въоръжение (Disposal).
- Модел за всяка фаза: цел; с какво започва; с какво завършва; преминаване от една фаза в друга само при осигурено финансиране и утвърден документ; Съветът по въоръженията на входа и на изхода (и със старшинство спрямо други съвети); ясно изписване на процедурите и действията.
- Препратки към други нормативни документи.
- Пределна краткост и яснота.

Авторският проект е следния:

НАРЕДБА
ЗА УСЛОВИЯТА И РЕДА ЗА УПРАВЛЕНИЕ НА ЖИЗНЕНИЯ ЦИКЪЛ НА ОТБРАНИТЕЛНИТЕ ПРОДУКТИ В МО, СППМО И БА

Чл. 1. (1) С Наредбата се определят условията и реда за осъществяване на управлението на жизнения цикъл на отбранителните продукти в Министерството на отбраната (МО), структурите на пряко подчинение на министъра на отбраната (СППМО) и Българската армия (БА), както и фазите, процесите и процедурите на жизнения им цикъл.

(2) Управлението на жизнения цикъл на отбранителните продукти включва:

1. планиране на жизнения цикъл;
2. управление на фазите на жизнения цикъл;
3. всички дейности по придобиване на отбранителни продукти;
4. приемане на въоръжение, снемане от въоръжение, въвеждане в експлоатация, експлоатация и поддръжка, и извеждане от експлоатация на отбранителни продукти;
5. управление на изпълнението на инвестиционни проекти в МО;
6. провеждане на изпитвания на отбранителни продукти;
7. осигуряване и управление на стандартизацията, качеството и кодификацията на отбранителни продукти;
8. управление на риска през жизнения цикъл;
9. научноизследователската и развойната дейност (НИРД) свързана с отбранителните продукти;
10. индустриалното сътрудничество в МО.

(3) НИРД свързана с отбранителните продукти и индустриалното сътрудничество в МО, както и други неуредени с настоящата наредба дейности се регламентират с отделни актове на министъра на отбраната.

Чл. 2. Жизненият цикъл на отбранителни продукти включва следните фази:

1. Заявяване;
2. Придобиване, приемане на въоръжение и въвеждане в експлоатация;
3. Експлоатация и поддръжка;
4. Извеждане от експлоатация и снемане от въоръжение.

Чл. 3. Опционално (сравнително по-рядко, за отделни отбранителни продукти) към жизнения цикъл се включва (добавя след фаза „Заявяване“) и фаза „Разработване“, която се изпълнява при:

1. разработване и производство на нов, специфичен, отбранителен продукт, какъвто не

може да бъде доставен от търговската мрежа;

2. производство по лиценз на отбранителен продукт;

3. модернизация на съществуващ отбранителен продукт.

Чл. 4. Преминаването от една фаза в друга, спирането или връщане към предхождаща фаза се извършва с акт на министъра на отбраната или определено от него длъжностно лице, след решение на Съвета по въоръжения и осигурено необходимо финансиране.

Заявяване

Чл. 5. Целта на фазата е да се инициират дейностите по реализиране на определена необходима отбранителна способност чрез придобиването на отбранителен продукт.

Чл. 6. (1) Фазата започва с изготвянето на Доклад за отбранителна способност (ДОС). ДОС се изготвя от отговорната структура от МО, СППМО и БА при възникнала необходимост от изграждането на определена отбранителна способност. Съдържанието и оформянето на ДОС се определя съгласно (отделно) *Приложение (1)*.

(2) ДОС се изпраща по команден ред до дирекция „Стратегическо планиране" за внасяне в Съвета по отбранителни способности (СОС).

(3) След разглеждане и приемане от СОС, ДОС се утвърждава от министъра на отбраната или определено от него длъжностно лице.

Чл. 7. (1) След утвърждаването на ДОС, работна група, назначена от министъра на отбраната или определено от него длъжностно лице, по предложение на дирекция „Отбранителна аквизиция", изготвя Концепция за изграждане на отбранителна способност (КИОС), съгласно (отделно) *Приложение (2)*.

(2) Концепцията съдържа не по-малко от два варианта за изграждане на отбранителната способност, които могат да бъдат:

1. придобиване чрез закупуване на нов отбранителен продукт или такъв втора употреба;

2. наемане, дарение, предоставяне за безвъзмездно ползване на отбранителен продукт;

3. придобиване чрез участие в международни проекти и проекти на НАТО и ЕС;

4. придобиване по силата на междуправителствено споразумение;

5. разработване и производство на нов, специфичен, отбранителен продукт или производство по лиценз;

6. модернизация на съществуващ отбранителен продукт;

7. друг или комбинация от изброените в т. 1-6.

При представяне на само един вариант се прави подробно аргументиране защо не може да има алтернативен такъв.

Чл. 8. (1) Ръководителят на работната група по чл. 7, ал. 1 представя в дирекция „Отбранителна аквизиция" за разглеждане в Съвета по въоръжения КИОС с различните варианти и оценка на риска по отношение на възможностите за тяхното изпълнение. Съветът по въоръжения разглежда и приема КИОС.

(2) Приетата КИОС е основание за извършване на дейностите по иницииране на проект/проекти съгласно Ръководство за проектно управление в МО, СППМО и БА (РПУ). Борда за управление на портфолио от проекти (П2Б) включва съответния проект в портфолиото от проекти на МО, което се утвърждава от министъра на отбраната.

(3) За всеки проект П2Б предлага на министъра на отбраната или определено от него длъжностно лице за назначаване на Борд за управление на проекта (БУП) и ръководител на проекта (РП) с обема от права и отговорности, съгласно РПУ.

(4) Ръководителят на проекта изготвя План за реализация на инвестиционен проект, съгласно РПУ и други документи свързани с изпълнението на проекта. Планът се приема от БУП и се утвърждава от министъра на отбраната или определено от него длъжностно лице.

(5) Ръководителят на проекта подготвя необходимите документи за внасяне в Министерски съвет (МС) и Народно събрание (НС) за решение, съгласно чл. 16, т. 7а и чл. 22 ал. 2, т.

11а от ЗОВС на Р. България.

Чл. 9. Фазата завършва с наличието на утвърдени от министъра на отбраната или определено от него длъжностно лице КИОС, План за реализация на инвестиционен проект и назначени органи съгласно РПУ (БУП, ръководител на проекта, работен екип, група за техническа и административна поддръжка).

Придобиване, приемане на въоръжение и въвеждане в експлоатация

Чл. 10. Целта на фазата е да се осигури доставка на готови отбранителни продукти, производство или модернизация на отбранителни продукти в съответствие с изискванията установени в опционалната фаза „Разработване" (чл. 32-37), приемането им на въоръжение и/или въвеждане в експлоатация, както и изпълнението на всички дейности осигуряващи тяхната готовността за експлоатация и поддръжка.

Чл. 11. (1) Фазата започва с наличие на основания за придобиване на отбранителен продукт за изграждане/задоволяване на определена отбранителна способност.

(2) Дирекция „Отбранителна аквизиция" организира придобиването на отбранителни продукти на основание на утвърдени Вътрешни правила относно реда за планиране и организация на провеждането на процедурите за възлагане на обществени поръчки и за контрол на изпълнението на сключените договори и Дългосрочна инвестиционна програма на МО или друг стратегически документ свързан с модернизацията и/или превъоръжаването на БА.

Чл. 12. (1) Приемането на въоръжение на отбранителни продукти се извършва със съответна заповед на министъра на отбраната след разглеждане в Съвета по въоръжения.

(2) Въвеждането в експлоатация на отбранителни продукти в МО се извършва със съответна заповед на определено от министъра длъжностно лице след разглеждане в Съвета по въоръжения.

(3) Въвеждането в експлоатация на отбранителни продукти в БА се извършва със съответна заповед на началника на отбраната след разглеждане в Съвета по въоръжения.

(4) Въвеждането в експлоатация на отбранителни продукти в СППМО се извършва със съответна заповед на определено от министъра длъжностно лице или на съответните им командири и началници след разглеждане в Съвета по въоръжения.

(5) Въвеждането в експлоатация на отбранителните продукти, предоставени на български контингенти извън страната по програми за международна помощ, включително и такива за временно ползване, се извършва със съответна заповед на началника на отбраната след разглеждане в Съвета по въоръжения, по предложение на потребителя им и при положение, че са приети на въоръжение в страни-членки на НАТО и ЕС.

(6) Заповедите се изготвят от дирекция „Отбранителна аквизиция" и след подписване се изпращат на всички касаещи ги структури.

Чл. 13. Фазата се счита за завършена с изготвяне от дирекция „Отбранителна политика" на протокол за съответствие на съответния отбранителен продукт с предварително зададени изисквания, утвърден от министъра на отбраната или определено от него длъжностно лице и заповед за приемане на въоръжение или въвеждане в експлоатация на отбранителния продукт, след решение на Съвета по въоръжения.

Чл. 14. (1) Приетите на въоръжение отбранителни продукти се кодифицират в дирекция „Отбранителна аквизиция".

(2) Дирекция „Отбранителна аквизиция" поддържа Регистър на приетите на въоръжение и снетите от въоръжение отбранителни продукти в МО, СППМО и БА.

(3) Дирекция „Логистика" поддържа Регистър на въведените в експлоатация и изведените от експлоатация отбранителни продукти в МО, СППМО и БА.

Чл. 15. (1) Отбранителни продукти, които са променили съществено основните си тактико-технически характеристики се приемат на въоръжение като новопридобити.

(2) Решението, относно това дали промяната на тактико-технически характеристики по ал. 1 е съществена или не, се приема от Съвета по въоръжения.

Чл. 16. Условията и реда за придобиване на отбранителни продукти по линия на международни проекти и програми, междуправителствени споразумения, дарение, наемане, за временно ползване и др. се регламентират с отделни актове на МС или министъра на отбраната.

Чл. 17. Редът за осигуряване и управление на качеството при разработване и придобиване на отбранителни продукти, както и за провеждането на техните изпитвания, сертифициране и кодификация се регламентират с отделни актове на министъра на отбраната.

Експлоатация и поддръжка

Чл. 18. Целта на фазата е създаване на организация и условия за правилната експлоатация и поддръжка на придобитите отбранителни продукти, според тяхното предназначение, в рамките на утвърдените норми за разход на материални и финансови средства, при спазване на установените правила от производителя и изискванията за безопасност.

Чл. 19. Фазата започва след доставката на отбранителния продукт в мястото за експлоатация и поддръжка и включва: регистрация, отчет, използване, техническо обслужване, ремонт, съхранение, усъвършенстване, модернизация, удължаване на срока за експлоатация и евентуално предявяване на рекламации към качеството на отбранителните продукти.

Чл. 20. (1) Експлоатацията и поддръжката на отбранителните продукти се организира от командирите/началниците на структурите от МО, СППМО и БА.

(2) Обучението и подготовката на личния състав, който ще експлоатира и поддържа съответния отбранителен продукт се организира от лицата по ал. 1 и се извършва чрез Системата за управление на човешките ресурси в МО.

Чл. 21. Експлоатацията и поддръжката на отбранителните продукти се организира според изискванията на ръководствата, инструкциите и другите регламентиращи документира за експлоатация и поддръжка, а когато такива липсват, редът и начинът за тяхната експлоатация и поддръжка се определят от началника на отбраната и/или определено от министъра на отбраната длъжностно лице.

Чл. 22. (1) В хода на експлоатацията и поддръжката на отбранителните продукти потребителите им могат да предлагат тяхното усъвършенстване, модернизация и изменение на срока на експлоатация.

(2) Усъвършенстване на отбранителен продукт е повишаване на технико-икономическите показатели на продукта без да се изменят съществено основните му тактико-технически характеристики.

(3) Модернизация на отбранителен продукт е повишаване на технико-икономическите показатели на продукта чрез изменение на основните му тактико-технически характеристики.

(4) Изменение на срока на експлоатация на отбранителен продукт е промяна на ресурса и/или възможността за неговата употреба, определени в техническата му документация, които имат два компонента: 1. определената работа в часове, брой цикли или изминати километри; 2. календарен срок на експлоатация. Отбранителният продукт се извежда от експлоатация при изчерпване на поне единия от посочените два компонента. Процедурата на изменение на срока на експлоатация се регламентира с акт на министъра на отбраната или определено от него длъжностно лице.

Чл. 23. Необходимите материални и финансови средства за експлоатация и поддръжка на отбранителните продукти се планират от ръководителите на (основните) бюджетни програми на основата на Указания за програмиране в МО, като се отчитат и наличностите от отбранителни продукти в логистичните складове и бази.

Чл. 24. (1) Лицата, които извършват експлоатацията и поддръжката, както и началниците и командирите от всички степени, осъществяват непрекъснато наблюдение, контрол и анализ на състоянието на отбранителните продукти и изготвят оценки на резултатите от тяхното използване.

(2) Оценките по ал. 1 се изпращат по команден ред в дирекция „Логистика", която ежегодно до 15 януари на текущата година изготвя и изпраща обобщена информация в Съвета по

въоръжения за отбранителните продукти, чиито срок на експлоатация изтича през следващата календарна година, и информация по всяко време на годината, когато се констатират отклонения от нормалното състояние на продуктите.

Чл. 25. Фазата се счита за завършена с настъпването на основания за извеждане от експлоатация или снемане от въоръжение на отбранителни продукти и изготвянето от дирекция „Отбранителна аквизиция" на заповед на министъра на отбраната или определено от него длъжностно лице за извеждане от експлоатация или снемане от въоръжение, след решение на Съвета по въоръжения.

Извеждане от експлоатация и снемане от въоръжение

Чл. 26. Целта на фазата е извеждане от експлоатация или снемане от въоръжение на даден отбранителен продукт по съобразно най-ефективен, ефикасен, безопасен и екологичен начин, съответстващ на националното законодателство и вътрешните нормативни документи на МО.

Чл. 27. Извеждане от експлоатация или снемане от въоръжение на отбранителни продукти се извършва при наличието на:

1. количества, надхвърлящи щатните потребности;
2. изчерпване на техническия и експлоатационен ресурс;
3. негодност за употреба, вследствие на природни бедствия, инциденти или авария, или опасност за съхранение;
4. съществени отклонения от изискванията на техническата документация, които не позволяват нормалната експлоатация и не подлежат на ремонт;
5. спряно производство и невъзможност за осигуряване с резервни части;
6. отпадане на потребността от определена отбранителна способност;
7. техническа невъзможност за постигане на съответната отбранителна способност;
8. разпоредби на международни договори или други нормативни актове;
9. друга аргументирана причина.

Чл. 28. (1) Фазата започва с изготвянето на Доклад за отпадане на потребността от отбранителния продукт (ДОПОП) при възникнала необходимост от извеждане от експлоатация или снемане от въоръжение на отбранителни продукти.

(2) ДОПОП се изготвя от отговорната структура от МО, СППМО и БА и съдържа подробни мотиви и обосновка на обстоятелствата, довели до необходимостта за извеждане от експлоатация или снемане от въоръжение, както и начините как отбранителния продукт следва да се утилизира (разкомплектова, бракува и унищожи) подходящо, подписва се от съответния началник/командир и се представя в дирекция „Отбранителна аквизиция", която го внася за разглеждане в Съвета по въоръженията.

Чл. 29. (1) Снемането от въоръжение на отбранителни продукти се извършва със съответна заповед на министъра на отбраната след разглеждане в Съвета по въоръжения.

(2) Извеждането от експлоатация на отбранителни продукти в МО се извършва със съответна заповед на определено от министъра длъжностно лице след разглеждане в Съвета по въоръжения.

(3) Извеждането от експлоатация на отбранителни продукти в БА се извършва със съответна заповед на началника на отбраната след разглеждане в Съвета по въоръжения.

(4) Извеждането от експлоатация на отбранителни продукти в СППМО се извършва със съответна заповед на определено от министъра длъжностно лице или на съответните им командири и началници след разглеждане в Съвета по въоръжения.

(5) Извеждането от експлоатация на отбранителните продукти, предоставени на български контингенти извън страната по програми за международна помощ, включително и такива за временно ползване, се извършва със съответна заповед на началника на отбраната след разглеждане в Съвета по въоръжения.

(6) Заповедите се изготвят от дирекция „Отбранителна аквизиция" и съдържат подроб-

ни мотиви относно причините (обстоятелствата) по чл. 27. След подписване се изпращат на всички касаещи ги структури.

Чл. 30. Отбранителни продукти, представляващи оръжия, боеприпаси, взривни вещества и пиротехнически изделия (ОБВВПИ) се извеждат от експлоатация или снемат от въоръжение при настъпване на някое от условията, посочени в чл. 82, ал. 1 от Наредбата за условията и реда за осъществяване на дейностите, свързани с оръжията, боеприпасите, взривните вещества и пиротехническите изделия и контрола над тях във и от въоръжените сили на Република България, приета с ПМС № 278 от 2010 г., обн., ДВ, бр. 96 от 2010 г.

Чл. 31. Фазата се счита за завършена с наличието на заповед за извеждане от експлоатация или снемане от въоръжение на даден отбранителния продукт и неговата утилизация (разкомплектоване, бракуване и унищожаване) или реализация по друг начин, съответстващи на националното законодателство и вътрешните нормативни документи на МО.

Разработване

Чл. 32. Опционалната фаза „Разработване" се изпълнява при необходимост от разработване и производство на нов, специфичен, отбранителен продукт, производство по лиценз или модернизация на съществуващ отбранителен продукт и включва етапите: 1. „Проучване", 2. „Идеен проект", 3. „Работен проект" и 4. „Опитен образец".

Чл. 33. (1) Фазата започва с решение на Съвета по въоръжения на база одобрения КИОС с предложение на възможност съгл. чл. 31.

(2) Ръководителят на проекта представя изходно задание (ИЗ), съгласно (отделно) *Приложение (3)*. ИЗ се утвърждава от ръководителя на основната (бюджетна) програма и се изпраща в дирекция „Отбранителна аквизиция", където се включва в Регистър на утвърдените ИЗ и се изпраща писмо-заявка до директора на Института по отбрана „Проф. Цветан Лазаров" (ИО) за извършване на етап „Проучване". В случай, че ИО не разполага със съответната експертиза за извършването на етап „Проучване", той може да бъде възложен на друг изпълнител.

Чл. 34. (1) Изпълнителят на проучването изготвя технико-икономически доклад (ТИД) и го изпраща в дирекция „Отбранителна аквизиция".

(2) Дирекция „Отбранителна аквизиция" внася ТИД за разглеждане в Съвета по въоръженията. След приемането на ТИД от Съвета по въоръженията и избор на вариант за разработване на тактико-техническо задание (ТТЗ)/техническа спецификация (ТС), ТИД се предлага на П2Б за разглеждане и утвърждаване, съгласно разпоредбите на РПУ.

(3) На база утвърдения вариант в ТИД, изпълнителят на проучването изготвя ТТЗ/ТС, съгласно (отделни) *Приложения (4/5)* и го изпраща в дирекция „Отбранителна аквизиция" за внасяне в Съвета по въоръженията и П2Б, съгласно разпоредбите на РПУ.

(4) След утвърждаването на ТТЗ/ТС, дирекция „Отбранителна аквизиция" ги завежда в Регистър на ТТЗ/ТС като им присвоява уникален номер.

Чл. 35. Утвърденото ТТЗ/ТС е едно от условията за откриване на позиция в ЕФП за МТО на МО и БА.

Чл. 36. Организирането на процедура за възлагане на обществена поръчка за изпълнение на разработването се осъществява съгласно Вътрешни правила относно реда за планиране и организацията на провеждането на процедурите за възлагане на обществени поръчки и за контрол на изпълнението на сключените договори и другите регламентиращи документи.

Чл. 37. (1) Изпълнението на етапи „Идеен проект", „Работен проект" и „Опитен образец" се реализира съгласно РПУ и другите регламентиращи документи.

(2) Ръководителят на проекта внася доклад за резултатите от фаза „Разработване" за разглеждане в П2Б и след неговото приемане в Съвета по въоръженията.

Чл. 38. Фаза „Разработване" се счита за изпълнена след като Съветът по въоръжения приеме доклада за резултатите от фазата и съпътстващата документация, и след заповед на министъра на отбраната или определено от него длъжностно лице, която се изготвя от дирекция „Отбранителна аквизиция".

Управление на риска

Чл. 39. Управлението на риска при управление на жизнения цикъл на отбранителните продукти се извършва с цел оценка и справяне с бъдещи неблагоприятни събития, които биха попречили на успешното осъществяване на жизнения цикъл на отбранителните продукти във всичките му фази.

Чл. 40. Управлението на риска при управление на жизнения цикъл на отбранителните продукти включва неговото дефиниране, анализиране, планиране и управление.

Чл. 41. Ръководителят на проекта изготвя доклад за управление на риска, съгласно нормативната уредба в МО.

Термини и дефиниции

1. „Управление на жизнения цикъл“ е съвкупност от координирани действия на ръководене, планиране, организиране, контрол и други съпътстващи мероприятия по реализиране на дейностите във фазите на жизнения цикъл.

2. „Жизнен цикъл“ (ЗОВС, Допълн. разпоредби, § 1, т. 25., нова - ДВ, бр. 98 от 2016 г.) са фазите по заявяване, придобиване, приемане на въоръжение, въвеждане в експлоатация, експлоатация и поддръжка, извеждане от експлоатация и снемане от въоръжение, през които преминават отбранителните продукти.

3. „Отбранителни продукти“ (ЗОВС, Допълн. разпоредби, § 1, т. 26., нова - ДВ, бр. 98 от 2016 г.) са продукти, осигуряващи създаването и поддържането на отбранителни способности на Въоръжените сили (ВС) на Р. България:

а) оръжия, боеприпаси, взривни вещества и пиротехнически изделия по смисъла на Закона за оръжията, боеприпасите, взривните вещества и пиротехническите изделия;

б) продукти, свързани с отбраната, и изделия и технологии с двойна употреба по смисъла на Закона за експортния контрол на продукти, свързани с отбраната, и на изделия и технологии с двойна употреба;

в) оборудване, специално проектирано или адаптирано за военни цели и предназначено за използване, като оръжие, боеприпаси или материал с военно предназначение.

4. „Отбранителна способност“ е способността, необходима за успешното изпълнение на отбранителна задача или мисия;

5. „Инвестиционен проект“ е дефиниран процес за управление на дейностите по придобиване или модернизация на продукти в МО, СППМО и БА, съобразен с определени финансови средства и времеви граници**.**

6. „Приемане на въоръжение“ (ЗОВС, Допълн. разпоредби, § 1, т. 27., нова - ДВ, бр. 98 от 2016 г.) е акт на министъра на отбраната, с който се декларира, че отбранителен продукт, придобиван за първи път, ще се използва от ВС на Р. България.

7. „Снемане от въоръжение“ (ЗОВС, Допълн. разпоредби, § 1, т. 28., нова - ДВ, бр. 98 от 2016 г.) е акт на министъра на отбраната, с който се декларира прекратяване на използването на приет на въоръжение отбранителен продукт от ВС на Р. България.

8. „Въвеждане в експлоатация“ (ЗОВС, Допълн. разпоредби, § 1, т. 29., нова - ДВ, бр. 98 от 2016 г.) е акт за разрешаване използването на приет на въоръжение отбранителен продукт от ВС на Р. България, който се издава от определено от министъра на отбраната длъжностно лице.

9. „Извеждане от експлоатация“ (ЗОВС, Допълн. разпоредби, § 1, т. 30., нова - ДВ, бр. 98 от 2016 г.) е акт за забрана на използването на приет на въоръжение отбранителен продукт от ВС на Р. България, който се издава от определено от министъра на отбраната длъжностно лице.

ПРЕХОДНИ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. С тази наредба се отменят:
1. …….
2. …….
3. …….

§ 2. Наредбата се издава на основание ……. от ЗОВС.

§ 3. Наредбата влиза в сила от ..... 20__ г.

МИНИСТЪР НА ОТБРАНАТА (п)
……

References:

1. Правилник за управление на жизнения цикъл на отбранителните продукти (П-7) от 09.09.2011 г.;
2. Правилник за отмяна на правилника за управление на жизнения цикъл (П-5) от 15.07.2013 г. г.;
3. „Система за отбранителна аквизиция на Република България - възможности за усъвършенстване", Максим Алашки, монография, МО, 2016 г.;
4. Закон за отбраната и Въоръжените сили - ДВ, бр. 98 от 2016 г.

Ivaylo I. Ralev,

IMPROVING THE SUPPLY OF THE AIR FORCE UNITS DURING OPERATIONS

Ivaylo I. Ralev

Logistics Department, National Defence College "G. S. Rakovski", Sofia, Bulgaria, e-mail: ralev_mil@abv.bg

***Abstract**: The paper considers the importane of the supply process for the Air Force units during expeditionary operations. Next, the paper describes the options for improving the supply process of the Air Force units and the main factors from which they depends.*

***Key words**: military aviation, supply, forward operating base, needs of material resources*

ВЪЗМОЖНОСТИ ЗА УСЪВЪРШЕНСТВАНЕ СНАБДЯВАНЕТО НА АВИАЦИОННИТЕ ФОРМИРОВАНИЯ В ОПЕРАЦИИ

Ивайло И. Ралев

Катедра „Логистика", Военна академия „Г. С. Раковски", София, България, е-мейл: ralev_mil@abv.bg

***Резюме:** В разработката се разглежда значението на снабдяването с материални ресурси за авиационните формирования при участието им в експедиционни операции . След това са описани възможностите за усъвършенстване на снабдяването на авиационните формирования и факторите,от които зависи тяхното реализиране.*

***Ключови думи**: военна авиация, снабдяване, предна оперативна база, потребност от материални ресурси*

Съвременната среда за сигурност налага използването на силите на НАТО както за колективни отбранителни действия, така и в операции в отговор на кризи извън територията на НАТО (експедиционни операции извън чл. 5 на Вашингтонския договор) за постигане на различни политически и военни цели. В много случаи, за участие в експедиционни операции авиационните формирования на НАТО се развръщат в предни оперативни бази (летища за развръщане) извън територията на собствената им държава със слаба или без никаква поддръжка от страната домакин [6]. В тези случаи националните логистични системи трябва да снабдяват авиационните формирования със значително количество материални ресурси на далечни разстояния от постоянните им пунктове за базиране. Това превръща процеса на снабдяването в един от основните проблеми на логистичното осигуряване на авиационните формирования при участието им в експедиционни операции [8].

Опита на Военновъздушните сили (ВВС) на САЩ по време на войната в Персийския залив през 1991 г. показва, че за пребазирането на една изтребителна ескадрила на необорудвано летище и изпълнение на задачи в продължение на 3 седмици са били необходими 72 бр. обслужваща техника, 1 347 тона боеприпаси, почти 5 млн. литра авиационно гориво и над 400 тона други товари [5].

Този и други примери показват, че за успешното изпълнение на задачи от необорудвани или частично оборудвани летища логистичните системи на авиационните формирования трябва да притежават способности за своевременно снабдяване на големи количества материални ресурси на далечни разстояния.

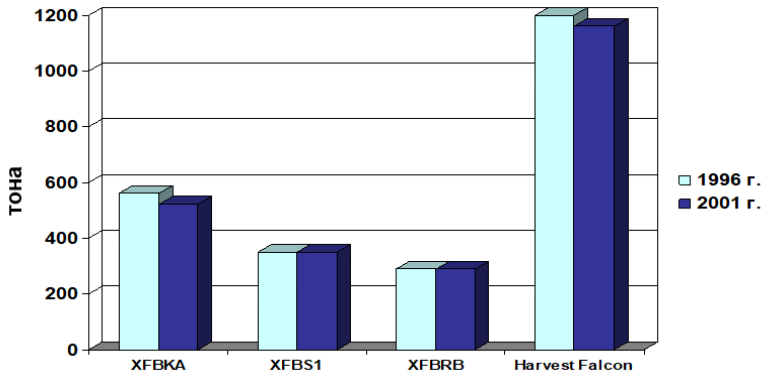
За усъвършенстване снабдяването на авиационните формирования в летища за разгръщане са проведени редица изследвания в рамките на НАТО. Резултатите от тях показват, че един от основните фактори за повишаване на ефективността на снабдяването е редуцирането на потребностите от материални ресурси за операцията. В тази връзка са изследвани различни възможности за физическо редуциране на потребностите чрез намаляване на броя, теглото и/или размерите на необходимите материални ресурси. Например във ВВС на САЩ са предприети мерки за физическо редуциране на потребностите чрез проектиране, разработване и внедряване на:

- Оборудване за тестване и ремонт на авионика и двигатели на самолети F-15 и F-16 с по-малки тегло и размери;
- Съоръжения за настаняване и обслужване на личен състав при полеви условия от по-лек тип (контейнери, палатки, електрически агрегати и други);
- Екипировка за личен състав с по-малко тегло и размери. [3]

Пример за положителен резултат в това направление е намаляването на общото тегло на логистичния модул "Harvest Falcon" на ВВС на САЩ. Модулът служи за настаняване и битово осигуряване на личния състав на една изтребителна ескадрила (около 1 100 души) при разгръщане на необорудвано летище. Този логистичен модул се състои три комплекта, както следва [3]:

- Комплект "XFBKA" – съоръжения и техника за настаняване на личен състав (палатки с климатични инсталации) и битово осигуряване (приготвяне и раздаване на храна, добиване и пречистване на вода, поддържане на личната и колективната хигиена, осветление, електрически агрегати и други);
- Комплект "XFBS1" – хангари и оборудване за извършване на първо ниво на поддръжка и ремонт на авиационната техника на една ескадрила;
- Комплект "XFBRB" – хангари и оборудване за извършване на поддръжка и ремонт на наземна техника.

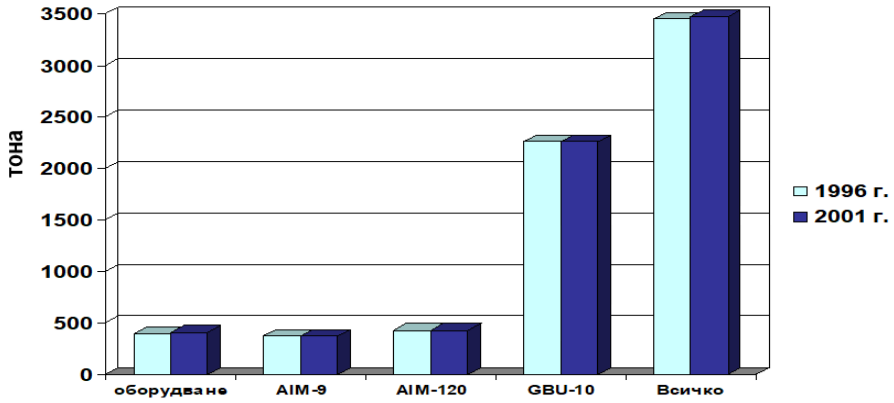
От Фиг. 1 е видно, че през 1996 г. общото тегло на логистичния модул "Harvest Falcon" е около 1 200 т. През 2001 г. теглото му е намалено с около 40 т в резултат на разработването и внедряването на ново оборудване от по-лек тип. Промените са основно в модула "XFBKA" за настаняване и битово осигуряване. След промените модулът е наречен "E-Falcon".



Фиг. 1. Тегло на логистичния модул "Harvest Falcon" на ВВС на САЩ

Друга област, в която е постигнато физическо редуциране на потребностите от материални ресурси е медицинското осигуряване. В началото за експедиционни операции ВВС на САЩ използват въздушнопреносими полеви болници от типа “ATHs”. За медицинското осигуряване на една авиационна ескадрила е била необходима една такава полева болница с капацитет от 25 легла. Нейното общо тегло е около 120 т. За нейното транспортиране по въздуха са били необходими 3 бр. транспортни самолета С-17. В резултат на промени в организацията на медицинското осигуряване при експедиционни операции и въвеждането на ново оборудване от по-лек тип е постигнато редуциране на теглото на полевите болници на ВВС на САЩ с около 60 %. Оборудването на новото полево медицинско формирование “EMEDS” тежи около 50 т и за транспортирането му са необходими 1,3 бр. самолети С-17. Част от редуцираното тегло на “EMEDS”, обаче, е за сметка на снети електрически агрегати от списъка с оборудване, които осигуряват електрическата автономност на формированието. Предвидено е необходимата електрическа енергия да се осигурява от логистичния модул за настаняване и битово осигуряване “E-Falcon”. Това налага увеличаване на електрическите агрегати в този модул, а от там и на неговото тегло. Ето защо, физическото редуциране на потребностите в една област не трябва да е за сметка на увеличаването им в други функционални области на логистичното осигуряване. [3]

В други функционални области намаляването на теглото и размерите на материалните ресурси изисква значителни инвестиционни разходи и продължителен период за развитие на нови технологии. Например, такива са авиационните боеприпаси, които заедно с оборудването за тяхното транспортиране, съхранение и обслужване, заемат един от най-големите дялове в снабдяването на авиационните формирования в операции. На Фиг. 2 е показано сравнение на потребностите от авиационни боеприпаси на една ескадрила с 18 бр. изтребители F-15 за изпълнение на мисия по непосредствена авиационна поддръжка в продължение на 7 денонощия.



Фиг. 2. Потребности от оборудване и авиационни боеприпаси за непосредствена авиационна поддръжка на ескадрила със самолети F-15

За изпълнение на посочената мисия през разглеждания период се използват авиационни бомби с лазерно насочване от типа “GBU10E/B” и ракети „Въздух-Въздух” от типа “AIM-9 Sidewinder” и “AIM-120”. От фигурата е видно, че през периода е настъпило незначително увеличение на теглото на необходимото наземно оборудване (около 20 т), а теглото на авиационните боеприпаси се запазва – приблизително 190 т на самолет за 7 денонощия. След този период е постигнато по-голямо намаление на теглото на боеприпасите за посочената мисия чрез разработването и въвеждането на нови високоточни боеприпаси от типа “Small Diameter Bombs”. Те са с по-малки размери и тегло, но за целта са вложени значителни инвестиционни разходи за тяхното проектиране, разработване и внедряване [3].

В други функционални области, като например военноинженерното осигуряване, е

установено, че физическото редуциране на потребностите е почти неизпълнимо. Затова са потърсени алтернативни възможности за редуциране на потребностите от материални ресурси за операции. Такава възможност е централизирането на способностите за снабдяване в зоната на операцията. За целта са направени редица изследвания за възможностите за обединяване на способности за снабдяване и ремонт в общи логистични бази, които да обслужват всички летища за развръщане в зоната на операцията. При определени условия това направление повишава ефективността на снабдяването чрез намаляване или премахване на необходимостта от развръщане на допълнително оборудване и екипировка за авиационните формирования. Също така, централизирането може да намали и броя на необходимите транспортни средства за операцията и така да оптимизира процесите по снабдяване и ремонт на техниката. В повечето случаи централизирането на способностите за снабдяване се постига чрез прилагане на многонационални подходи.

Друга алтернативна възможност за редуциране на потребностите от материални ресурси е формулирана от американската компания за изследвания и развитие в областта на сигурността и отбраната "RAND" (Research and Development Corporation). В нейно изследване се посочва, че освен чрез физическо редуциране, ефективността на снабдяването на авиационните формирования може да се повиши и чрез конфигуриране (разпределяне) на потребностите от материални ресурси във времето и пространството. Това донякъде разширява традиционното разбиране за потребност от материални ресурси – необходими количества ресурси, които трябва да се развърнат в зоната на операцията. Според "RAND" потребностите от материалните ресурси трябва допълнително се разпределят по фази на операцията и по място на доставка. В концепцията се предлага методология за определяне на потребностите, алгоритъм за разработване на различни варианти за разпределяне на потребностите и показатели за оценка на вариантите. Всичко това осигурява на органите по планиране на логистичното осигуряване рамка за анализ на потребностите от материални ресурси за операцията в процеса на непосредствено планиране на снабдяването. [1]

Изложеното до тук дава основание да се открояят две основни възможности за редуциране на потребностите от материални ресурси на авиационните формирования в операции, както следва:

- Физическо редуциране;
- Усъвършенстване на процеса по планиране на снабдяването.

Както стана ясно физическото редуциране е насочено към намаляване на броя, теглото и размерите на материалните ресурси, необходими за операции. Може да се каже, че неговото реализиране зависи три основни аспекта – военен, финансов и икономически (Фиг. 3).

Фиг. 3. Аспекти на физическото редуциране на потребностите от материални ресурси

Военният аспект е свързан с инициирането на изследвания за физическо редуциране и предоставяне на военна експертиза в тази област. Финансовият аспект е свързан с осигуряването на необходимите капиталови разходи от военните бюджети за изследване, проектиране,

разработване, придобиване и усвояване на нови образци въоръжение, техника, оборудване и екипировка от по-лек тип за нуждите на авиационните формирования. Икономическият аспект е свързан с капацитета и възможностите на военната и гражданската промишленост за проектиране и разработване на нови образци материални ресурси [7].

Усъвършенстването на процеса на планиране съдържа само военен аспект. Същият не изисква значителни финансови разходи и икономически потенциал, а може да се реализира чрез повишаване на подготовката на логистичните органи, които планират снабдяването на авиационните формирования при експедиционни операции. Необходимо е те да усъвършенстват своите знания и умения за:

- Точно определяне на потребностите от материални ресурси за операцията;
- Конфигуриране на потребностите по време и място на доставка.

Независимо от различните аспекти на двете възможности, тяхната крайна цел е насочена към редуциране на потребностите от материални ресурси за операции. Това от своя страна ще доведе до намаляване на:

- Броя на необходимите транспортните средства;
- Броя на личният състав и оборудването за обработка на товарите;
- Необходимата площ за съхранение на запасите.

Всичко това заедно ще повиши ефективността на снабдяването на авиационните формирования и в крайна сметка ще понижи разходите на държавата за участие в операцията.

References

1. Calway L., Tripp R., Ramey T., Drew J. (2000). A Global Infrastructure to Support Expeditionary Aerospace Forces. Expeditionary Logistics 2000. Air Force Logistics Management Agency. Pages 6-16

2. Diana J. (2004) Improving Bare Base Agile Combat Support. Air Force Journal and Logistics, Volume 28

3. Galway A., Amouzegar A., Hillestad J., Snyder D. (2002). Reconfiguring Footprint to Speed Expeditionary Aerospace Forces Deployment. RAND

4. Looney R. (1996). The Air Expeditionary Force – Taking the Air Force into the 21st Century. Air Power Journal.

5. Pathfinder. (2008). Air Bases – Sustaining Air Power. Air Power development Centre Bulletin, Issue 88.

6. Димитров М, Иринков В, Аспекти на развитието на военната логистика в процеса на планиране и изграждане на системата за колективна отбрана на НАТО, ВА, София, 2019.

7. Димитров М., Влияние на инициативата на НАТО „Интелегентна отбрана” върху развитието на военната логистика, Логистиката възможности и предизвикателства, Издателски комплекс УНСС, 2015, стр. 43-53.

8. Димитров М, Кирилов Д.,Развитие на органите за управление на интегрираната логистика в НАТО, Сборник доклади от университетска научна конференция, Том 6 - Сигурност и отбрана, Велико Търново, 2019, стр. 109-115.

Miroslav St. Dimitrov,

THEORETICAL ASPECTS OF THE SUPPLY OF AMMUNITION

Miroslav St. Dimitrov

*Logistics Department, National Defence College "G. S. Rakovski",
Sofia, Bulgaria, e-mail: dimitrovm @abv.bg*

***Abstract**: The paper considers the specifics of the ammunition as an object of supply in the context of logistical inventory management theory. The subsystems for the supply of military formations with ammunition in the operations are analyzed, accentuated on the study of material flows that occur in the implementation of logistics functions – warehousing, cargo handling and transportation.*

***Key words**: supply, ammunition, logistics system and military units*

ТЕОРЕТИЧНИ АСПЕКТИ НА СНАБДЯВАНЕТО С БОЙНИ ПРИПАСИ

Мирослав Ст. Димитров

Катедра „Логистика", Военна академия „Г. С. Раковски", София, България, е-мейл: dimitrovm@abv.bg

***Резюме:** Разгледани са особеностите на бойните припаси като обект на снабдяване, в контекста на логистичната теория за управление на запасите. Анализирани са подсистемите за снабдяване на военните формирования с бойни припаси в операциите, като е акцентирано на изследване на материалните потоци, протичащи при реализирането на логистичните функции - складиране, обработване на товарите и транспортиране.*

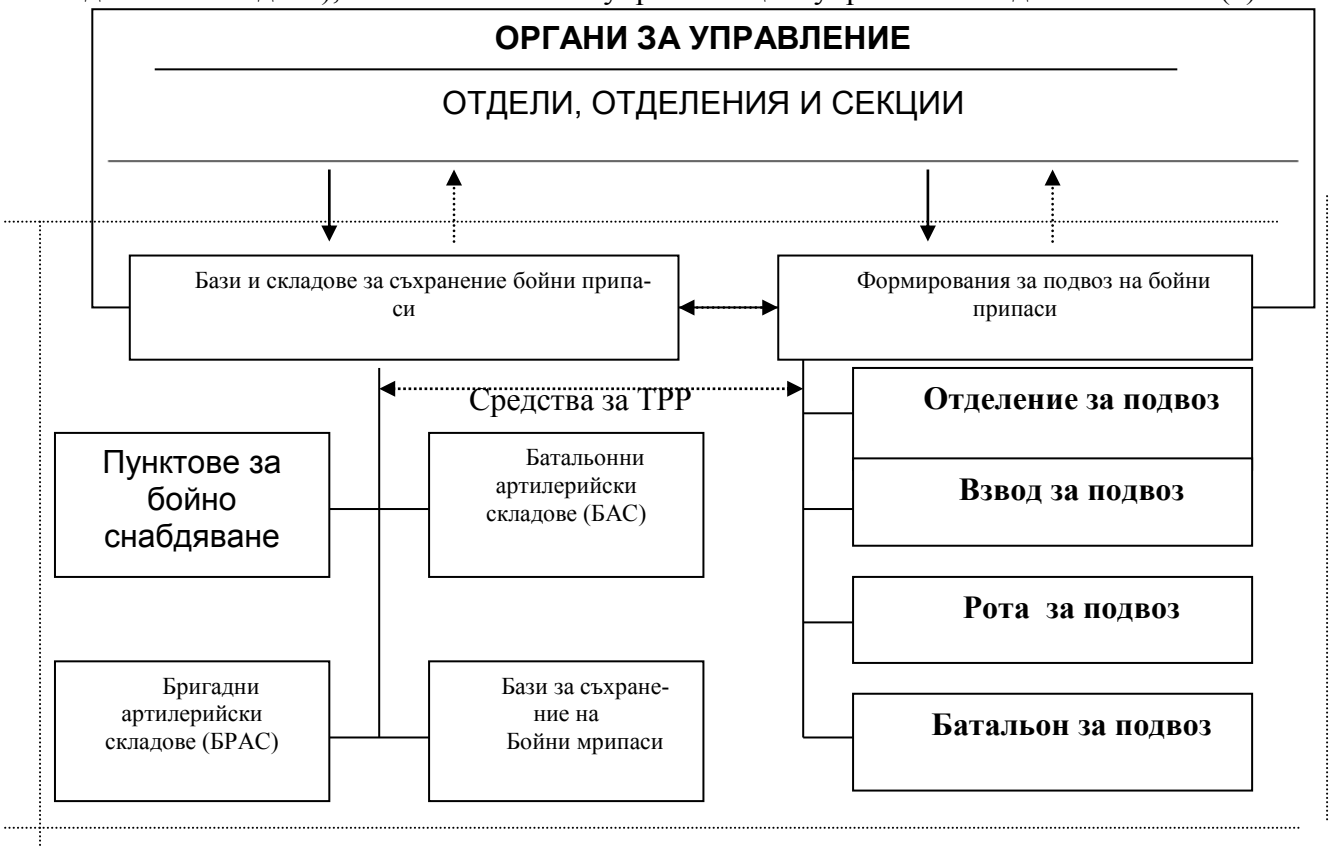
***Ключови думи**: снабдяване, бойни припаси, логистична система и военни формирования*

Изучаването и доброто познаване на богатия исторически опит от дейността на снабдителните органи по въоръжението и бойните припаси може до голяма степен да способства за изграждането на съвременна логистична система за осигуряване на войските с този основен вид материални средства за активно въздействие върху противника, без да се повтарят допусканите грешки.

Съгласно изискванията на регламентиращите документи в НАТО материалните средства от клас V - бойни припаси [5] се явяват решително средство за изхода на операцията, а като обект на снабдяване се характеризират с редица особености, които усложняват и затрудняват осигуряването им в операциите в сравнение с другите класове от системата на логистичното осигуряване [6]. Бойните припаси се характеризират с голяма техническа специфичност и сложност, изискващи спазването на строго определени изисквания при съхранението им в стационарни и полеви условия; при транспортирането им с различни видове транспорт и извършването на товаро-разтоварни дейности с тях; голямо количество и обем от бойни припаси подлежащи на транспортиране с различни видове транспорт; голямо разнообразие по системи, калибър и вид на действие на бойните припаси; значителните загуби в хода на боя; липсата на унификация и взаимно заменяемост между бойните припаси и други.

Така например докато през Първата световна война обемът на подвоза на бойните припаси е съставлявал едва 3,6% от общото количество подвозвани товари, то през Втората световна война той вече е съставлявал една трета (29,2%) от всички подвозвани товари. В съвременни условия подвозът на бойни припаси е 67% до74% от обема на подвоза на твърдите товари. Всичко това определя организирането и осъществяването на снабдяването с бойни припаси като сложна задача, която трябва да бъде решена в различни условия на обстановката, при определени ограничения в ресурси и време.

От позицията на общата теория на системите, снабдяването с бойни припаси може да се разглежда като система, структурата и функционирането, на която са обусловени от определен ред за снабдяване, който предвижда войските да се снабдяват с бойни припаси своевременно и пълно чрез създаване във войските и оперативните звена на ешелонирани по определен начин запаси от материални средства още от мирно време и чрез периодично попълване на изразходваните запаси до установените норми или до заповяданите запаси чрез подвоз за сметка на висшестоящите инстанции. Следователно структурата на разглежданата система може да се представи като съвкупност от взаимосвързани елементи на снабдяването и управлението, разположени на съответни нива на организацията на войските, а именно пунктове за бойно снабдяване, артилерийски складове и бази, транспортни формирования за подвоз и органи за управление (секции, отделения и отдели), т.е тя се състои от управляваща и управляема подсистеми Фиг. (1) .



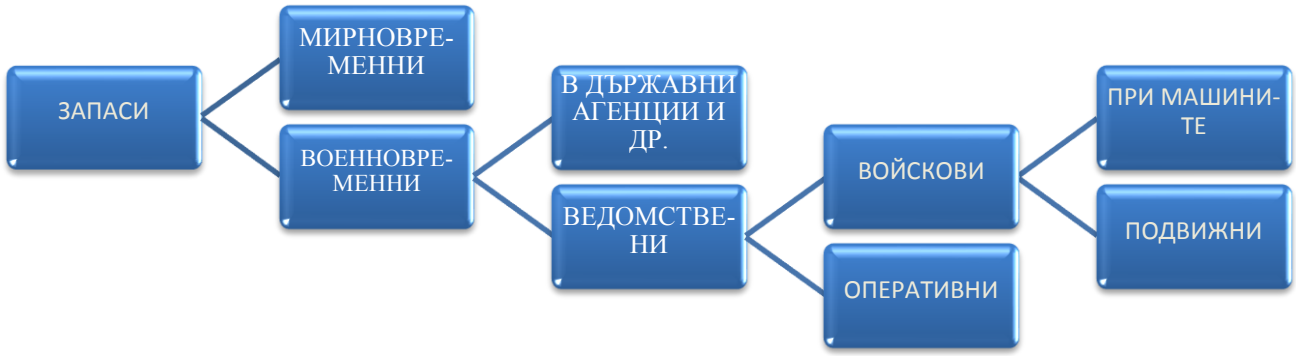
Фиг. 1. Структурно-функционална схема на системата за снабдяване с бойни припаси

Между структурните елементи на разгледаната система (пунктове за бойно снабдяване, артилерийски складове (батальонни, бригадни, на вид въоръжени сили (ВВС и ВМС), на Бригада «Логистика») се извършва подвоз, както и обмен на информация по въпросите на снабдяването бойни припаси. Това позволява функционирането на системата да се разглежда като процес, насочен към поддържане на установени или заповядани запаси във войските и складовете, чрез своевременното им подвозване и към оперативното управление на органите за снабдяване с материални средства.

Ако се анализира разглежданата логистична система ще се открият някои особености в характера на създаваните и поддържаните запаси. Това се дължи както на спецификата на самата система, така и на условията, в които тя ще функционира, т.е. на нейната вътрешна и външна логистична среда. В тази система, както е известно, по функционално предназначение запасите се делят на ведомствени и национални, а от своя страна ведомствените биват мирновременни и военновременни. Мирновременните запаси са за осигуряване на мирновременната дейност на формированията, за преминаване от мирно на военно положение, и за осигуряване на формирования, участващи в разрешаване на кризи и други операции, различни от война. По своето предназначение функция те се явяват текущи запаси. Остатъкът от текущите запаси при преминаване от мирно на военно положение съставлява приходящите запаси [2].

Военновременните запаси са предназначени основно за осигуряване на формированията на БА при привеждането им от мирно на военно положение, развръщането, прегрупирането им и попълване на разходите и загубите в хода на изпълнение на задачите. По предназначението си тези запаси във военно време са също текущи запаси, а по ниво следва да се разглеждат като максимални по икономическа целесъобразност от поддържане в мирно време и по съображения за надеждност на осигуряването във военно време. Във военно време тези запаси могат да се превишават (когато се създават допълнителни запаси) и да се занижават до определено ниво (когато в хода на бойните действия разходът и загубите превишават постъплението на материални средства).

Военновременните запаси са ешелонирани и се делят на войскови и оперативни в зависимост от местоположението си в разпределителната логистична система [3].От своя страна войсковите запаси също са ешелонирани по местоположението си: запаси при оръжията (бойците и машините), запаси в складовете на военните формирования разположени по йерархичната верига от изпълнителната подсистема за снабдяване с бойни припаси. Анализът на възприетия ред за осигуряване за бойните припаси в бойни условия, показва, че и в тази логистична система съществува праговия запас, достигането нивото, на който определя момента от време за подаване на заявка за попълване. В рамките на военно формирование с ранг на бригада, например, като такъв запас би следвало да се счита запасът при оръжията (бойците и машините) и в ротите (батареите), началото на разходването, на които е сигнал за попълване на запасите в батальонните (дивизионните) складове. Част от запасите при оръжията (бойците и машините) съставлява така наречения неприкосновен запас, който може да се разходва само с разрешение на командира на батальона (дивизиона). Този запас е постоянен и на практика се явява гаранционен и застраховащ запас (Фиг. 2).



Фиг. 2 Схема на запасите от материални средства в БА

Войсковите военновременни запаси от бойни припаси се съхраняват в складовете на съединенията и частите (самостоятелните подразделения), като част от тях могат да бъдат в бойните машини или на автомобилен транспорт от войскова наличност в зависимост от предназначението, времето за готовност и задачите на съединението.

Основната особеност на бойните припаси като обекти на снабдяване е тази, че за разлика от почти всички останали материални средства, бойните припаси, заедно с ракетите, са основни активни средства за въздействие върху противника. Във връзка с това в хода на операциите е не-

допустимо прекъсване в осигуряването с тях, докато за другите материални средства това е допустимо в определен интервал от време. Това се потвърждава и от бойния опит, когато несвоевременното осигуряване с бойни припаси в много случаи е водело до промяна в характера на бойните действия (от настъпление в отбрана, от отбрана в оттегляне и др.). За избягване възникването на дефицит от бойни припаси се е налагало да бъде използван транспорт, предназначен за подвоз и натоварен с други материални средства.

Отделните ключови и поддържащи функции при снабдяването (дистрибуцията) с бойни припаси се характеризират със следните особености:

- закупуване – бойните припаси се отнасят към изделията (продуктите) с така нареченото взаимообвързано търсене, тъй като те са предназначени за използуване от конкретна система оръжие, т. е. при тях отсъствува такава важна характеристика на почти всички останали видове материални средства като взаимозаменяемостта, което предопределя до голяма степен доставчика; освен това при определяне на потребностите и големината на поръчките трябва да се отчитат цената, голямата им специфична маса и обем, както и интензивността на разхода им;
- управление на запасите – при реализирането на тази логистична функция трябва да се отчитат: голямата им специфична маса, водеща до голяма маса на разчетно – снабдителната единица за снабдяване с бойни припаси бойния комплект (например в артилерията варира в обем от 60 до над 210 тона), което не позволява създаването и поддържането непосредствено при потребителите им (при бойците, в самите системи или влекачи) на запаси, адекватни на потребностите за един боен ден, и налага по-честото извършване на подвоз на бойни припаси в сравнение с другите материални средства. Поради това, че бойните припаси са активни средства за въздействие върху противника, с оглед недопускане на дефицит при потребителите е необходимо във военно време при осигуряването с тях да се използува ефективна система за управление на запасите;
- при осъществяване на придвижването (подвоза) на бойните припаси могат да се използуват всички видове транспорт, при което обаче трябва да се спазват редица изисквания при превозването и извършването на товаро –разтоварни работи с тях; освен това тук трябва да се отчитат: голямата специфична маса и големият разход на бойни припаси в бойните операции, изискващи по-голямата част от транспортните средства да се заделят за подвоз на бойни припаси (до 60-70 % от подвоза на материални средства се пада на бойните припаси); голямото разнообразие на бойните припаси, дължащо се както на многообразието на въоръжението, така и на необходимостта с едно и също въоръжение да се решават различни огневи задачи, налага да се извършва подбор на транспортните средства за подвоз на конкретни видове бойни припаси с оглед максимално използуване на товароподемността им, т. е. постигане на максимален коефициент за използуване на товароподемността (Кт); необходимостта от подвоз на бойните припаси непосредствено до самите потребители (огневите позиции) налага допълнителни изисквания за проходимостта и маневреността на транспортните средства за подвоз на бойни припаси; важно е да се има предвид също така, че подвозът на бойни припаси се извършва в условия на ограничена видимост, по черни пътища, особено при подвоз до огневите позиции, а също и в най – отговорните моменти на операциите;
- при осъществяване на логистичната функция “складиране” следва да се отчита, че големият разход на бойни припаси, вследствие на интензивното използуване на съвременно скорострелно въоръжение, налага създаването и поддържането не само на ешелонирани, но и на достатъчно големи по размери запаси от бойни припаси; значението на бойните припаси и голямата им маса налагат запасите от тях във войсковия тил да са подвижни (запаси на път), а на земята да се създават само запаси, необходими за изпълнение на конкретна огнева задача; бойните припаси изискват специални условия за съхранение, тъй като те са сложни и опасни електро–механични устройства, съдържащи барути и взривни вещества . Много важна особеност на бойните припаси като обект на снабдяването е, че те не са взаимозаменяеми, което налага много щателно да се планира и организира снабдяването с тях.

Съществена особеност на бойните припаси, водеща също до повишени изисквания към органите по логистика, при планиране на осигуряването с тях, е спецификата в организацията на осигуряването на най-големите им потребители – земната артилерия, зенитната артилерия, минохвъргачките, противотанковите средства, реактивната артилерия, танковете. Организацията на осигуряването с бойни припаси на всеки вид от тези средства трябва да отчита характера на бойното им използуване в различните видове бойни действия.

За осигуряването с бойни припаси е много важна и характерна поддържащата логистична функция събиране и връщане (евакуация) на празната опаковка и стреляните елементи. Разчетите показват, че те съставляват от 30 до 40 % от масата на подвозваните бойни припаси и почти 100 % от обема им.

В контекста на логистичната теория функционирането на изпълнителната подсистема на системата за снабдяване на военните формирования с бойни припаси в операциите може да се разглежда като процес на физическо разпределение на материалните средства, под което се разбира интегрирана логистична функция, включваща в себе си всички логистични операции, свързани с физическото преместване и съхранението на материалните средства в структурите за снабдяване [4]. Този процес обикновено се представя като динамична последователност от логистични операции, които се обединяват в комплексните логистични функции складиране, обработване на товарите и транспортиране, за които се счита, че изразяват същността на функционирането на изпълнителната подсистема на системата за снабдяване на активните сили с ракети и бойни припаси в операциите, т.е. на снабдителния процес. При това складирането се разглежда като логистична функция за поддържане и съхранение на определени запаси чрез управление на пространственото им разполагане (определяне на броя, дислокацията и възможностите на складовете за съхранение на запаси). Обработването на товарите е логистична функция, която обикновено се извършва паралелно със складирането и също осигурява поддържането и съхранението на запасите, но чрез извършване на такива елементарни логистични операции като: вътрешно складово преместване на материалните средства, правилното им разполагане в пределите на вместимостта (площта, обема) на съответните складове и други. Тази функция обикновено е свързана с избор на технологично оборудване за организиране преместването на материалните средства в склада, организиране на дейностите по сортиране, консолидиране и комплектоване на товарите за изпълнение на заявките.Транспортирането е една от ключовите логистични функции на снабдяването, тъй като без нея на практика не съществува материален поток. При това самият процес на транспортиране не се разглежда само като превоз на товари, а в по-широк план, като съвкупност от процесите на превоз, натоварване, разтоварване, експедиране и други съпътстващи операции. При него се решават такива задачи като избор на: превозвача (доставчика), вида на транспорта, транспортните средства за превоз на конкретни товари, рационални маршрути за подвоз.

Изхождайки от тези постановки в логистичната теория е целесъобразно изследването на функционирането на изпълнителната подсистема на системата за снабдяване на военните формирования с бойни припаси в операциите като логистична функция да се насочи към изследване на материалните потоци, протичащи при реализирането на посочените по-горе логистични функции - складиране, обработване на товарите и транспортиране. При това следва да се отчита много важната особеност при осъществяване на тези функции в процеса на снабдяването на военните формирования с бойни припаси в операциите, състояща се в това, че запасите в снабдителните звена трябва да са подвижни, т.е. складирането, обработването на товарите и транспортирането са неделими и се изпълняват от транспортните формирования за подвоз на бойни припаси, явявайки се по този начин основни структурни елементи на разглежданата подсистема.

На базата на изискванията към критериите за ефективност и от целта на функциониране на изследваната система е целесъобразно обобщеният критерий да се свърже с нейната фактическа производителност и с необходимата такава, обусловена от оперативните фактори (разстояние за подвоз, разрешен разход на бойни припаси).

Фактическата производителност на системата отразява възможностите й за извършване на определен обем от работа за един час и се определя по формулата:

$$P_{pc} = \mathbf{Q_Ф} . \mathbf{V_М} \ , \qquad (1)$$

където :

$\mathbf{P_{РС}}$ – производителност на системата [т.км/ч];

$\mathbf{Q_Ф}$ – фактическа товароподемност на транспортните средства [т];

$\mathbf{V_М}$ -средна скорост за движение на транспортните средства [км/ч].

Аналогично необходимата за успешно изпълнение на задачите от системата производителност може да се определи по формулата:

$$P_{\mathbf{п}} = \mathbf{Q_п} . \mathbf{V_п} \ , \qquad (2)$$

където:

$\mathbf{P_п}$ – необходима производителност на системата, обусловена от оперативните фактори [т.км/ч];

$\mathbf{Q_п}$ - необходима товароподемност на системата [т];

$\mathbf{V_п}$ - необходима скорост за движение на транспортните средства [км/ч].

Тогава обобщеният критерий за ефективност на подсистемата **G** може да се изрази с формулата:

$$G = \frac{Ppc}{Pn} \ , \qquad (3)$$

Целесъобразно е при разчитане на обобщения критерий за ефективност **G** на подсистемата производителността й де се изчислява по дни на операцията и за операцията като цяло.

Прието е фактическата товароподемност на транспортните следва $\mathbf{Q_Ф}$ да се определя по следната формула (4) [1]:

$$\mathbf{Q_Ф} = \mathbf{Q_Т} . \mathbf{К_{ит}} \mathbf{К_{тг}} \ , \qquad (4)$$

където:

$\mathbf{Q_Т}$ - техническа товароподемност на транспортните средства [т];

$\mathbf{К_{ит}}$ - средна стойност на коефициента за използване на товароподемността транспорта;

$\mathbf{К_{тг}}$ - коефициент на техническа готовност.

Освен обобщения критерий в математическите модели обикновено е прието да се използват и спомагателни (частни) критерии. Желателно е те да са съвместими с обобщения, т.е. с тяхна помощ трябва да могат да се оценяват съществени страни от функционирането на изследваната система и на елементите й. В този смисъл като спомагателни (частни) критерии в дадения случай могат да се разглеждат:

- показатели, характеризиращи възможностите на елементите на системата: товароподемност (фактическа и техническа); средна скорост за движение и среден денонощен пробег на транспортните средства; време за извършване на товарно-разтоварни работи;
- показатели, характеризиращи обема на задачите, стоящи пред системата: обем на подвоза; вероятен (реален) разход на материалните средства; необходим пробег на транспорта за извършване на подвоза и други.

От формула (4) се вижда, че най-съществено значение за ефективността на системата за снабдяване с материални средства клас пети имат следните тактико-технически показатели на автотранспорта: техническа готовност, товароподемност, проходимост и денонощен пробег.

Условията, в които ще функционира системата за снабдяване с бойни припаси ще са значително по тежки от тези за снабдяване с други материални средства. Това е обусловено от необходимостта в най-отговорните моменти от подготовката и воденето на операцията за кратко време да се подвозват големи количества бойни припаси в условия на ограничена видимост, по черни пътища, особено когато се доставят бойни припаси на огневите позиции на самоходната артилерия, танковете и на други средства монтирани на базови машини с висока проводимост. Изхождайки от характера на функционирането на системата за снабдяване с материални средства спецификата на бойните припаси като вид материални средства и от условията, в които ще се осъществява осигуряването с тях, могат да се направят следните най-общи изводи:

- транспортните формирования за подвоз на РАВ и бойни припаси трябва да са

комплектовани с автомобили с висока ефективност за изпълнение на тази отговорна задача. При това като най-важни параметри влияещи на тяхната ефективност, трябва да се разглеждат високата маневреност и скорост при експлоатация по черни пътища и достатъчно голяма товароподемност;

- личният състав непосредствено ръководещ и изпълняващ мероприятията по снабдяването с бойни припаси в основните структурни елементи на разглежданата система трябва да притежава много добри познания и умения, както по чисто техническите въпроси на устройството на бойните припаси, по комплектацията, маркировката и индексацията им, така и по въпросите за правилата за съхранение и извършване на товаро-разтоварни работи с тях в стационарни и полеви условия, за тяхното превозване с различни видове транспортни средства.

Ефективността на разглежданата система в голяма степен зависи от процесите на управление, които са насочени към достигане на крайната цел на функционирането им. Анализът на структурата на тези система показва, че от позициите на общата теория на управлението тя е йерархическа система за управление, във всяко звено, на която могат да се отделят органи за управление на снабдяването с бойни припаси на съответното звено, които образуват управляващата подсистема на дадената система за управление или управлявана подсистема. Много е важно да се отбележи, че йерархичността на тези системи произтича от организационната структура на органите за управление и тяхната подчиненост във всяко звено. Тази йерархичност способства за оптимална организация на информационните потоци и води до определено съответствие между количеството на обектите за управление във всяко звено и възможностите на органите за управление.

Под функциониране на системата за снабдяване с бойни припаси ще разбираме съвкупността от взаимно свързани функции по управление на силите и средствата за снабдяване с бойни припаси осъществяване от управляващата подсистема с цел да въздейства по необходимия начин на управляемата подсистема за достигане крайните цели на системата. Основни функции на управлението на снабдяването с този вид материални средства са събирането и обработването на информацията за оперативната и логистичната обстановка, за състоянието на подчинените сили и средства и на осигуряваните съединения и части; разработване на предложения за организацията за снабдяването; планиране на осигуряването; контрол и оказване на помощ на подчинените.

В съвременни условия значението на осигуряването на военните формирования с бойни припаси нараства поради големия разход и загуби на този вид материални средства в операцията. Същевременно условията за осъществяването на подвоз, ремонт и евакуацията им ще бъдат много сложни поради възможностите на противника да използува възможностите на космическото разузнаване и високоточните оръжейни системи. Всичко това повишава изискванията към органите за логистично осигуряване за своевременното и пълно снабдяване на формированията в операциите с този вид средства за активно въздействие върху противника.

References

1. Военни автомобилни превози, ВИ ,С., 1979.
2. Димитров. М и колектив, Военна логистика, част първа Основи на военната логистика, София, Военна академия, 2017.
3. Доктрина за логистика на Българската армия, НП-4А, С.,2019.
4. Митрохин В., Сергеев. В. Основи логистики, Москва, 2000, Инфра-М.
5. MC 319/3 - NATO Principles and Policies for Logistics, Brussels,NATO,2018.
6. NATO Logistics Handbook, Brussels, NATO, 2012.

Andrey I Bogdanov,

A NEW APPROACH TO STORAGE CAPACITY INCREASE

Andrey I Bogdanov

Konstantin Preslavski University Of Shumen, Shumen 9712, 115 Universitetska Str. anbog@abv.bg

***Abstract**: Warehouse operations are much more complex than when they appear at first glance. Profi ling (partitioning) of products and orders leads to a potential multitude of warehouses inside the warehouse. The paper presents an algorithm for increasing storage capacity in modern warehouses.*

***Keywords**: warehouses, storage capacity, storage area*

Introduction

Warehouses are places where materials and goods are stored [1]. Depending on the market demand, many operations such as loading distribution, packaging, marking, commercial conversion consolidated cargo forming are completed. Warehouses could be considered as a distribution channel for goods and materials. They could also be considered as an "insurance" against various difficulties in distribution channels and disruption of material flows in already established distribution chain.

Warehouses [5] accumulate material resources, which are necessary for dampering the volume fluctuations of demand and supply. They are also very important for synchronizing system from the producers to the customers or material flows in technological production systems.

Exposition

Warehouses can serve different roles within the larger organization. For example, a stock room serving a manufacturing facility must provide a fast response time. The major activities would be piece (item) picking, carton picking, and preparation of assembly kits (kitting). A mail-order retailer usually must provide a great variety of products in small quantities at low cost to many customers. A factory warehouse usually handles a limited number of products in large quantities. A large, discount chain warehouse typically “pushes” some products out to its retailers based on marketing campaigns, with other products being “pulled” by the store managers. Shipments are often full and half truckloads. The warehouse described here is a small, chain warehouse that carries a limited product line for distribution to its retailers and independent customers.

The purpose of the warehouse is to provide the utility of time and place to its customers, both retail and individual. Manufacturers of office supplies and furniture are usually not willing to supply products in the quantities requested by small retailers and individual customers. Production schedules often result in long runs and large lot sizes. Thus, manufacturers usually are not able to meet the delivery dates of small retailers and individuals. The warehouse bridges the gap and enables both sides, manufacturer and customer, to operate within their own spheres.

Modern big warehouse is a complex technical facility which consists of multiple interconnected elements. It has a fixed structure and performs a number of functions in the transformation of material flows, also in the accumulation, processing and distribution of goods among consumers. Moreover, because of the variety of parameters, technological and volume-planning solutions, equipment design and characteristics of the diverse nomenclature of processed goods stores belong to complex systems. At

the same time the warehouse itself is only an element of a system, which is on a higher level in the logistics chain. This position determines the main technical requirements to the warehouse system. It also determines the goals and criteria for its optimal function and the conditions for cargos processing.

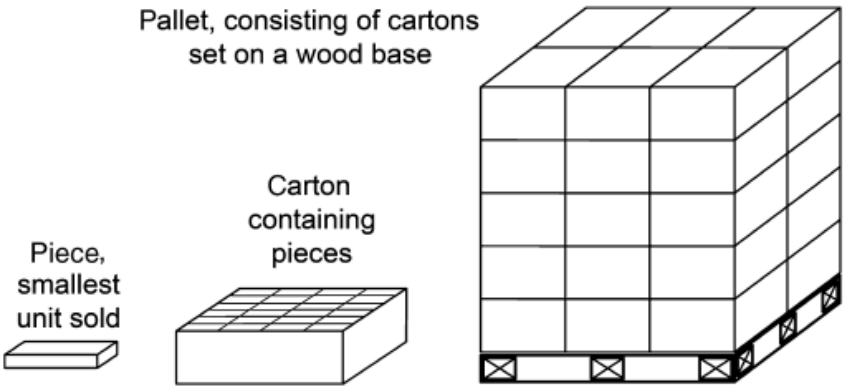


Figure 1: Load types.

Products are sold by the warehouse as pieces, cartons, and on pallets. Figure 1 shows the relationships among these load types. Individuals usually request pieces; retailers may also request pieces of slow movers, products that are not in high demand. Retailers usually request fast movers, products that are in high demand, in carton quantities. Bulky products like large desktop storage units may be in high enough demand so that they are sold by the warehouse in pallets. Furniture units are also sold on pallets for ease of movement in the warehouse and in the delivery trucks. The typical dimensions of a piece is 10 × 25 × 3.5 cm, with a typical volume of 0.875 liters. A carton has typical dimensions of 33 × 43 × 30 cm, with a typical volume of 42.6 liters. Thus, a typical carton contains 48.7 pieces. The typical dimension of a pallet is 80 × 120 × 140 cm, with the last dimension being the height. The pallet base is about 10 cm high, so the typical product volume is 1.25 m^3, corresponding to 29.3 cartons [3]. The pallet base allows for pickup by forklift truck from any of the four sides. Products in the pallet reserve storage area (see Fig. 2.) are assigned locations using a shared storage concept, with the more active products located closer to the receiving or shipping dock.

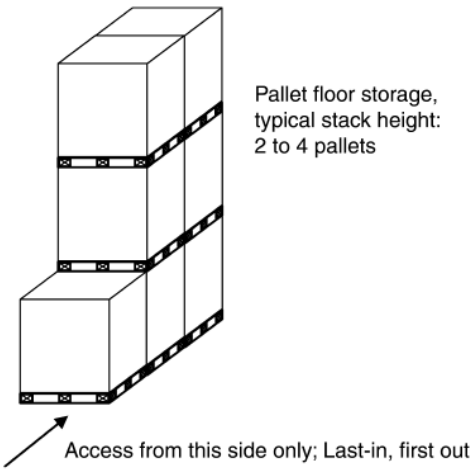


Figure 2: Pallet reserve storage area, floor stacking.

The high cost and limited availability of real estate near population centers - where most businesses would like to locate often forces firms to make the most of smaller facilities. In large cities it is common to find multi-level department stores, parking lots, all efforts to make better use of space.

Effective space utilization has long been a theme in material logistics and transportation as well. For example, ports must make the best use of limited acreage to store empty and full containers and other cargo; shipping and trucking firms must maximize freight per vehicle in order to reduce the total costs of transportation; and distributors strive for high utilization of warehouse space to decrease total facility and operating costs.

An automated form of dense storage is deep bulk storage, in which pallets are stored several deep in an automated handling system (Figure 3).

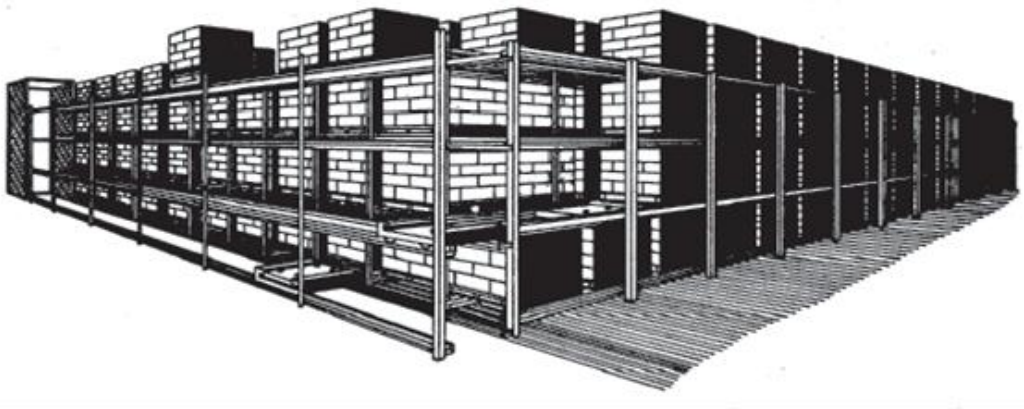


Figure 3: An automated deep bulk storage system.

Storage system has Very High Density (VHD) when it is sometimes necessary to move interfering items in the system in order to gain access to desired items. Generally speaking, double-deep pallet rack has very high density because one might have to move a pallet to retrieve the one behind it, but single-deep pallet rack does not, because every pallet is accessible directly from an aisle. Deep-bulk systems also have very high density, as do many container yards in ports, where containers are sometimes stored several units deep, and perhaps several units high.

If aisle cells are the same size as cells containing items, and so aisles have the same width as items. For many automated systems this is a reasonable assumption, but for other systems those involving fork-lifts in particular aisles are wider than items to allow the transporter to maneuver. Should wider aisles be necessary, there are at least two options. If aisle width is approximately an integer multiple of the width of a storage cell, we can redefine "cell" to mean the integer multiple and proceed as before. An alternative is simply to "stretch" the aisles to required width and then fill in newly created storage space with items. Figure 4 shows three example layouts: single-, two-, and three-deep, from left to right.

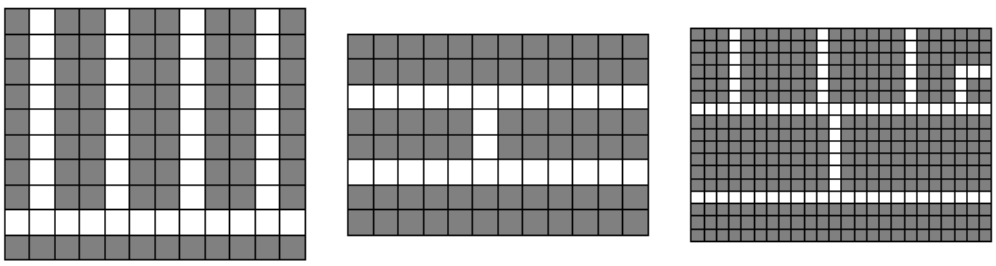


Figure 4: Example layouts

If we use algorithm, which is called Fill-and-Rotate, is based on a simple labeling procedure and a series of rotations of the grid (Figure 5):

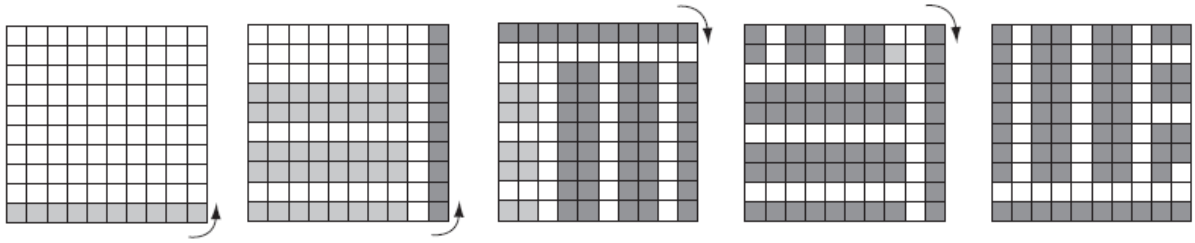


Figure 5: The Fill-and-Rotate algorithm applied to a 10 × 10

The best layouts for Very High Density storage spaces have a definite structure: items should be arranged in several aisles connected by a single cross aisle. For certain combinations of length, width, and lane depth it is best to arrange a slightly different region on one side to compensate for the lack of divisibility between the parameters.

Conclusion

The storage density in a space can be no greater and this bound is asymptotically tight as the storage space gets large. Logistics might use this as a rule of thumb when designing storage spaces that will be faced with the need for high density. This simple result can be used in other contexts as well for parking lots

References

1. Anikin B. s kolektiv. Logistika. M., izd. INFRA – Moskva, 2001.
2. Alzoubi, K. M., Wan, P.-J., and Frieder, O, Distributed heuristics for connected dominating sets in wireless ad hoc networks. Journal of Communications and Networks 2002.
3. Bassan, Y., Roll, Y., and Rosenblatt, M. J. Internal Layout Design of a Warehouse. IIE Transactions 2000
4. Kevin R. Gue Very High Density Storage Systems, Department of Industrial & Systems Engineering Auburn University, March 2015
5. Wooldridge, M. An introduction to Multiagent Systems – Second Edition. By John Wiley and Sons, USA, May, 2016

Conuy G. Conev, Hristo A. Hristov,

EXPERIMENTAL RESEARCH ON THE VARIATIONS IN HIT DISTANCE AND DEVIATION ELLIPSE DURING THE USE OF DIFFERENT GUNPOWDER TYPES WHEN OPERATING THE 82MM MORTAR AND 82MM REUSABLE TRAINING MORTAR ROUND FOR SHORT DISTANCE ENGAGEMENT

Conuy G. Conev, Hristo A. Hristov

Artillery, Air Defense and CIS Faculty, National Military University "Vasil Levski"
Shumen, Bulgaria, coni19@abv.bg

Abstract: *This paper explores a completed experimental study on the variations in hit distance and deviation ellipse when different types of gunpowder are used. During the research, an 82 mm mortar is used. The issued ammunition is an 82 mm reusable training mortar round for short distance engagement.*

Keywords*: mortars, simulator*

Introduction

Over the last two decades, there has been an ongoing trend in the implementation of simulators (training simulator) for the training of military personnel. Part of these simulators are targeted towards practical preparations related to fieldwork in conjunction with the execution of military tasks and tactical operations during mortar fire missions [2].

One of the developments of such type in the Republic of Bulgaria is a training simulator for the mortar crews with an 82mm reusable training mortar round for short distance engagements. It is intended for training mortar crews in the preparation for mortar deployment, execution of fire missions and fire correction.

The main elements of the simulator are:

- 82 mm mortar;
- 82 mm reusable training mortar round for short distance engagement;
- dummy fuse; for short distance engagement
- main charge;
- the charge of the dummy fuse.

Training simulator consumables are the main charge and the charge of the dummy fuse.

The contents of the main charge of the dummy fuse include a smoke-forming substance with which a mortar detonation is imitated. The delivery of this element by different manufacturers wound not lead to any significant disruption of the simulators performance.

The contents of the main charge include two types of gunpowder (black gunpowder and smokeless gunpowder). Black gunpowder serves only for strengthening the explosive train produced by the ignition device. The main source of energy for the launch of the training mortar round comes from the smokeless gunpowder [1].

For the use of the simulator short distance firing tables are made, utilizing main charges armed with smokeless nitroglycerin, ballistic, strip gunpowder type NLB-11(НБЛ – 11).

The data gathered from the conducted research indicates that different manufacturers of the main charge for the 82mm mortar rounds use different smokeless gunpowder types which in turn have differ-

ent characteristics. Therefore further research needs to be conducted on the possibility of significant differences in firing distances when firing with different primary charges armed with various types of smokeless gunpowder.

2. Experimental research

A proper flow of the paper is to first set the related work, description of the problem context, followed by the presentation of the proposed solution. Then the verification part includes the analysis, simulation and experimentation. Finaly, an evaluation of the solution according to the verification results is made in the conclusion and future work.

2.1.Research objective

The objective of this research is the determination on the presence of deviations in firing distances and the deviation ellipse when using different gunpowder types. In this research, the following equipment will be used: the 82 mm mortar and the 82 mm reusable training mortar round for short distance engagement used for mortar crew training.

2.2. Research tasks

- To experimentally determine the presence of deviation in firing distance with an angle of elevation allowing for maximum firing distance. Two types of smokeless gunpowder will be used for the primary charge of the 82 mm training mortar round.
- To experimentally determine the presence of variations in the deviation ellipse on the maximum range of the system. Two smokeless gunpowder types will be used for the main charge of the 82 mm training mortar round.

2.3. Research location

The research was conducted on the artillery training range "Markovo".

2.4.Conditions under which the research was conducted

- ambient temperature 20° C; with a relative air humidity 65%;
- fire missions are conducted in clear and windless weather conditions to eliminate the effects of crosswind.
- fire missions are conducted with an elevation angle of 45°, providing the maximum fire range;
- The fire mission was conducted with main charges, part of which (13 pc.) are armed with smokeless gunpowder, type PS-6642 (ПС-6642) and main charges (10 pc.) armed with smokeless nitroglycerin, ballistic, strip gunpowder type NBL-11(НБЛ – 11).
- The fire mission was conducted with 82mm mortar and 82mm reusable training mortar rounds for short distance engagement.

2.5. Restrictions

During the research, only the large axis of the deviation ellipse was noted.

2.6. Procedure for conducting the experimental research

A. Preparation of the weapon system and munitions.

Sequence::

- The bore of the mortar is cleared from lubricants, carbon and other contaminants before firing.
- The mortar is deployed;
- Dummy fuses are armed with their charges that imitate explosion on impact;
- The armed dummy fuses are then threaded to the training rounds;
- Distance indicators are deployed on the firing range with a distance of 10 meters in-between;

B. Execution of the experimental fire mission.

The experimental fire mission is conducted in the following sequence.

- 10 rounds are fired with the main charge armed with the smokeless nitroglycerin, ballistic, strip gunpowder type NLB-11 (НБЛ – 11) at an angle of 45° and after each shot the distance between the barel bore and the place where the mortar has landed is measured.

- 5 rounds are fired with the main charge weighing 2,5g, armed with smokeless grain gunpowder type PS-6642 (ПС-6642) at an angle of 45° and after each shot the distance between the barel bore and the place where the mortar has landed is measured;

- 4 rounds are fired with the main charge weighing 3g, armed with smokeless grain gunpowder type PS-6642 (ПС-6642) at an angle of 45° and after each shot the distance between the barel bore and the place where the mortar has landed is measured;

3. Results of the experimental research

For the approximate determination of the required amount of smokeless nitroglycerin, ballistic, strip gunpowder type NBL-11 (НБЛ – 11) for the main charge a formula was used 1 [5]:

$$\omega = \sqrt[b]{\frac{V_0}{a}} \tag{1}$$

where:

ω – the mass of the smokeless gunpowder in the main charge [kg];

V_0 –the desired initial velocity of the training mortar round for maximal firing range of 100 m (desired initial velocity has a speed of ≈ 30 m/s) [m/s];

a - coefficient depending on the caliber and mass of the mortar (for the 82 mm training mortar the value of this coefficient is 20,601892) [5];

b - coefficient depending on the caliber and mass of the mortar (for the 82 mm training mortar the value of this coefficient is 0,60068571 [5].

The required amount of smokeless gunpowder type NBL-11 (НБЛ – 11), calculated from formula 1 is approximately 2,4 g.

The results gathered from the experimental research of firing the training mortar rounds with a main charge armed with smokeless gunpowder type NBL-11 (НБЛ–11) at an angle of 45° are presented in table1.

Table 1

Results from the experimental research of firing the training mortar round with a main charge armed with smokeless gunpowder NBL-11 (НБЛ – 11) at an elevation angle of 45°

Mortar shot №	Elevation angle	Expected hit distance	Hit distance	Error
	[deg]	[m]	[m]	[%]
1	45°	100	86	-24%
2	45°	100	90	-10%
3	45°	100	97	-3%
4	45°	100	106	+6%
5	45°	100	111	+11%
6	45°	100	115	+15%
7	45°	100	89	-11%
8	45°	100	92	-8%
9	45°	100	103	+3%
10	45°	100	105	+5%
Average hit and error values			99,4	9,6%

The average firing distance is 99,4 m. The average error results gathered from the experimental research from using the training mortar round with the main charged armed with smokeless gunpowder type NBL-11(НБЛ–11) at a firing angle of 45° are 9,6% .

The big axis of the deviation ellipse is 29m.

Due to lack of data, the required quantity of smokeless gunpowder type PS-6642 (ПС-6642) for the main charge is not calculated. Therefore, main charges were made with a gunpowder mass of 2,5 and 3g.

The research from the conducted experimental fire mission are show in tables 2, 3 and 4.

Table 2

Results from the experimental research of firing the training mortar round with a main charge armed with smokeless gunpowder type PS-6642 (ПС-6642) with a gunpowder mass of 2.5g at an elevation angle of 45°

Mortar shot №	Elevation angle	Expected hit distance [m]	Hit distance [m]	Error [%]
1	45°	100	82,00	-18 %
2	45°	100	78,00	-22 %
3	45°	100	75,00	-25%
4	45°	100	84,00	-16%
5	45°	100	80,00	-20%
Average hit and error values			79,80	-20,2%

According to the data presented in the above table it is clear that the average firing distance is 79,8m and the average error results gathered from the experimental research from using the training mortar round with the main charged armed with smokeless gunpowder type PS-6642 (ПС-6642) with a gunpowder mass of 2,5g and an elevation angle of 45° are 20,2% .

Due to the high error percentage accruing in firing distance, firing was ceased. The research indicates that the charges with mass of 2,5g do not meet the necessary requirements being - when firing at an elevation angle of 45 ° the training mortar round must reach a distance of 90 to 100 m.

Table 3

Results from the experimental research of firing the training mortar round with a main charge armed with smokeless gunpowder type PS-6642 (ПС-6642) with a gunpowder mass of 3g at an elevation angle of 45°

Mortar shot №	Elevation angle	Expected hit distance [m]	Hit distance [m]	Error [%]
1	45°	100	84,60	-15,4 %
2	45°	100	90,00	-10 %
3	45°	100	107,00	+7,0 %
4	45°	100	109,00	+9,0 %
Average hit and error values			97,65	10,35 %

Average firing distance is 97,65m. The average error results gathered from the experimental research from using the training mortar round with the main charged armed with smokeless gunpowder type PS-6642 (ПС-6642) with a gunpowder mass of 3g and an elevation angle of 45° are 10,35%.

The big axis of the deviation ellipse is 24, 4 m.

Table 4

Results from the experimental research of firing the training mortar round with a main charge armed with smokeless gunpowder type PS-6642 (ПС-6642) with a gunpowder mass of 3g at an elevation angle of 83°

Mortar shot №	Elevation angle	Expected hit distance [m]	Hit distance [m]	Error [%]
1	83°	23	20,00	13,0 %
2	83°	23	19,00	17,4 %
3	83°	23	21,00	8,7%
4	83°	23	21,00	8,7%
Average hit and error values			20,25	11,95%

Average firing distance is 20,25m. The average error results gathered from the experimental research from using the training mortar round with the main charged armed with smokeless gunpowder type PS-6642 (ПС-6642) with a gunpowder mass of 3g and an elevation angle of 83° are 11,95% .

The big axis of the deviation ellipse is 2 m.

4. Conclusions

1. The conducted experimental research show that there are significant differences in the required amount of smokeless gunpowder for the main charge when manifactured from different types. This, in turn, does not allow the use of main charges manufactured by different companies for training mines since the firing tables will not be applicable.

2. A significant deviation in long distance hits was found. It is due to the presence of a small amount of gunpowder in the main charge (due to the requirement of maximum firing distance of up to 100 m). There is also a large passage of propellant gasses between the mortar round and the barrel bore. This, in turn, calls for the inclusion of an obturating band preventing the escape of propellant gasses.

References

1. Антонов С.И. (Possibilities for automation of designing elements of small arms using CAD/CAM/CAE systems). *Collection of papers: „Defense And Security, Mechanical Engineering And Military Technology, Communication And Computing Technologies, Social Science". 2016.* Shumen. ISSN 2367-7902.
2. Kalev, Krasimir. (A study of the influence of the parameters of a reaction zone on the burning rate.). *Collection of papers: „Defense And Security, Mechanical Engineering And Military Technology, Communication And Computing Technologies, Social Science". 2016.* Shumen. ISSN 2367-7902.
3. Христов Х.А. (Определяне на количеството барут на основния заряд при свръх къси дистанции на стрелба с 82 мм батальонен миномет.). *Сборник научни трудове на НВУ „В. Левски" Част 1, 2010.* Велико Търново. ISSN 1314-1953.
4. Христов Х.А. & Цонев Ц.Г. (Учебно-практическа мина за огнева подготовка на минохвъргачните разчети). *Годишник 1/2013 на ВА „Г.С. Раковски".* София. ISSN 1312-2991.
5. Христов Х.А. (Обобщен математичен модел на връзката начална скорост – енергия). *MATTEX 2012.* Шумен. ISSN 1314-3921.

Subi S. Minev,

PREPARATION OF GROSS PROPERTIES AFTER LONG STORAGE THROUGH INTERNAL BALLISTICS

Subi S. Minev

under. 26690 Pavlikeni, E-mail:subi.minev@abv.bg

Abstract: *The effect of aging of gunpowder charges due to their long-term storage is investigated. The relationship between the storage time of the gunpowder and the changes in their ballistic properties is determined using the obtained parameters of the inverse ballistics assignment.*

Keywords*: gunpowder, ballistic characteristics, gunpowder aging, gunpowder gases*

ПРОГНОЗИРАНЕ НА СВОЙСТВАТА НА БАРУТИТЕ ПРИ ПРОДЪЛЖИТЕЛНО ИМ СЪХРАНЯВАНЕ ЧРЕЗ ОБРАТНАТА ЗАДАЧА НА ВЪТРЕШНАТА БАЛИСТИКА

Съби С. Минев

В.ф. 26690 гр. Павликени, E-mail:subi.minev@abv.bg

Поради сложността на явлението изстрел всички негови процеси са свързани с промените във физико-химичните свойства на барутите особено при продължителното им съхранение (Анипко, с.4-6).

Срокът за съхранение на барутите за нашата страна средно е 20-35 години, което води до необратими физико-химични процеси поради комбинираното въздействие на температура, влажност, вибрации и т.н., в тях. (Бирюков,2005,с.55-57). Ефекта от стареенето на барутните заряди за посочените периоди се изразява в интегрални форми на последствията, които могат на кратко да се дефинират с възможността за поражението на целите (Kalev,2015, с.3-7). Този проблем разискван в е засегнат само информативно, а в литературата са представени частично, (Коновалов, 1979,с.52-89). Затова за определянето връзката между: времето за съхранение на барутите и измененията на балистическите им свойства е възможно да се използват някои основни зависимости на обратната задача на вътрешната балистика.

1. Постановка на проблема

За да се изследва ефекта от възрастовите промени в отклоненията на балистичните характеристики на оръжията, се налага да се вземе предвид барута и неговата чувствителност към външни влияния. При това, стойностите на тези отклонения могат да се определят от решаването на уравнението на втората или още обратната задача на вътрешната балистика. Но получените резултати дават само приблизителните стойности за: наляганeто на барутните газове, скоростта на

куршума и относителният път на куршума в цевта на огневата система. Или задачата за настоящото изследване се заключава в получаването на относително постоянни балистични характеристики на барутните състави, чиито стойности пряко се определят, от последствията в изменението на техните физико-химични характеристики, във функция от срокът им за съхранение. Това потвърждава актуалността на проблема по определяне състоянието на бойните припаси с продължителни срокове на съхранение, чрез използване резултатите от решенията на обратната задача на вътрешната балистика ОЗВБ -2.

2. Влияния на ефектите от стареенето на барутите върху балистичните елементи

Промените в бойни припаси поради негативното въздействие на срока за тяхното съхранение, предизвикват необратими физико-химични процеси. Те се дължат преди всички на преобразуването на техния химически състав, поради комбинираното въздействие на физико-химическите процеси протичащи в барутните състави, климатичните фактори при тяхното съхранение - температура и влажност на въздуха, механични вибрации при транспортиране или при манипулиране с тях в складовите бази и т.н. Те се изразяват в няколко направления:

Първо- Физико-химическите процеси при съхранение на барутите се съпровождат с ефекти на разлагане, молекулна дифузия и конвективен масов трансфер най-често на азотни компоненти, изграждащи техният състав. Това неминуемо води до промяната на процесите на явлението изстрел, главно в: плътността на барута - δ и скоростта на горене на барутното зърно u_1. Така например в барутните заряди при редукция на разтворителя с 1 до 2%, фабричната плътност на барута - δ , се редуцира почти с 10%, (Бирюков,2005,с.55-57).

Второ - продължителните срокове на съхранение на боеприпасите средно от 25…35 години за артилерийско и стрелково оръжие, спонтанно се наблюдава частично разлагане на барутните състави, съпроводено с масов трансфер на азот, изпарение на летливите вещества, абсорбция на влага в тях и др. Вследствие на това се получават отклонения в: началната дебелината на барутното зърно - $2e_1$; силата на барута - f ; скорост на горене - u_1.

Трето - като съществен недостатък на пироксилиновия барут е промяната на свойствата му при продължително съхранение в резултат на изпаряване на алкохолно-етерния разтворител в него. Резултатът от тази реакция е неговото разлагане с крайни химически елементи - азот и азотни киселини, които се образуват в резултат на автокаталитична реакция по време на масовия пренос на азот от барута към околната среда или свободният обем ограничен от параметрите на гилзата. Последното оказва влияние върху: силата на барута - f ; скоростта на горене - u_1 ; пълният импулс на налягането по време на горене на барута - I_k, което се свързва със скоростта на горене с величината e_1, а вследствие на това и върху началната скорост на куршума V_0.

Четвърто - интензитета на трансфера, формиращ дифузионният поток описващ движението на азота и разтворителите в барутният заряд, процесите ре-кристализация на някои от химическите елементи влизащи в състава на барута поради внасяне на енергия от вибрациите на барутните заряди при транспортиране. Следствие от това, главно на външните повърхности на барутните зърна се получават микропукнатини и дори малки фрагменти от зърната изграждащи барутният заряд на огневата система. Комплексното влияние на описаните последствия от стареенето на барута водят до изменения главно в редукцията на масата на заряда ω, което автоматически променя и плътността на зареждането Δ на огневата система.

Посочените последствия на влияние (1-4) върху балистическите елементи на изстрела поради продължителното съхранение на бойните припаси, оказват въздействие в протичането на явлението изстрел. Обобщено всичко това, например при промяна на съдържанието на летливите вещества в барутите само с 1% скоростта им на горене се изменя с 12%, съответно налягането на барутните газове – 15%, а началната скорост на снаряда –с 4% (Анипко, 2007, с.4). Освен това при продължително съхранение на барутните заряди се получава частично повърхностно разлагане на барута. Ускоряването на този процес в голяма степен се влияе от температурата на околната среда при тяхното съхранение, при което в практиката е установено, че нагряването на бару-

та само с 5 градуса ускорява процеса на разлагане на барутните състави от 1,5 до 2 пъти (Орлова, 1973, с.23-44,). При посочените последствия от процесите на стареенето на барута се налага да се определят величините на наляганeто и скоростта, задаващи ориентировъчно зависимостта за годините за съхранение на барутните състави.

3. Особености на решенията на обратната задача на вътрешната балистика

Известно е, че при решението на обратната задача на вътрешната балистика ОЗВБ-2 могат да се получат множество решения, при които за куршум от определен калибър и маса, може да се получат определени основни стойности на наляганeто P_{max} на барутните газове и начална скорост V_0 на куршума в цевната система. Това се реализира, чрез изменение на входните данни необходими за решението на задачата, като: марка и геометрически характеристики на барута, маса на барута в гилзата, плътността на барута, условия на зареждането др. Поради това, че броят на входните данни е значително голям може да се получи желаната начална скорост на куршума, чрез подбор и изменение на всяка една входна характеристика на барута. И затова се налага да се използват някои ограничения, при решаването на ОЗВБ-2, които се отнасят за определен тип огневи системи. Така например, решенията на ОЗВБ-2 за стрелковото оръжие се определят от следните негови параметри: коефициент на относителна маса на снаряда (куршума) - 20-30; относителна дължина на цевта -70 -100 калибъра,; калибър на огневите системи -5,45-14,5 mm (Костадинов, 2000,с.6); начална скорост на куршумите - 700-1000 m/s; плътност на зареждане - 0,8 - 0,95. Като пример за определяне на основните балистически характеристики на барутите с дълг срок на съхраняване, които да служат за прогнозиране на техните характеристики в зависимост от времето на тяхното съхраняването, може да се използва методологията за решаването на ОЗВБ-2 за този тип въоръжение. За целта, като модел за прогнозиране характеристиките на барутите дефиниращи стойностите на наляганeто на барутните газови и началната скорост на куршума във функция от времето на тяхното съхраняването се предлага де се използват:

Параметърът на условията за зареждане, наречен в балистиката още параметър на проф. Н. Ф. Дроздов - B, (Серебряков, 1962, с.243-249), обединява основните балистически характеристики на наляганeто P_{max} на барутните газове и началната скорост V_0 на куршума в цевната система. Влиянието на измененията в тези величини и следствията от тях са описани в (1-4). Параметърът на условията за зареждане притежава вида:

$$B = \frac{s^2 I_k^2}{f\omega\varphi m} = \frac{s^2 e_1^2}{u_1^2 f\omega\varphi m} = \frac{s^2 I_k^2 g}{f\omega\varphi q} = \frac{s^2 e_1^2 g}{u_1^2 f\omega\varphi q} \qquad (1)$$

От параметъра на проф. Н. Ф. Дроздов - B, могат да се определят основните балистически характеристики като:

-силата на барута:

$$f = \frac{s^2 I_k^2}{Bm\omega\varphi}; \qquad (2)$$

-тегло на барута:

$$\omega = \frac{s^2 I_k^2}{Bfm\varphi}; \qquad (3)$$

-пълен импулс на барутните газове в цевта на огневата система:

$$I_k = \frac{\sqrt{Bf\omega\varphi m}}{s}; \qquad (4)$$

-дебелина на барутното зърно:

$$e_1 = \frac{\sqrt{Bf\omega\varphi m u_1}}{s}; \qquad (5)$$

-скоростта на горенето на барутният заряд:

$$u_1 = \frac{e_1 s}{\sqrt{Bf\omega\varphi m}}; \qquad (6)$$

- коефициент на второстепенните работи:

$$\varphi = \frac{s^2 I_k^2}{Bfm\omega}; \qquad (7)$$

Освен това като показател на ефектите от стареенето на барута се явява и плътността на зареждането Δ, която може да се определи по:

$$\Delta = \frac{\omega}{w}\frac{kg}{dm^3} \qquad (8)$$

където: Δ - плътност на зареждане; ω - маса на заряда, kg; w - обем на зарядната камера на оръжейната система, литри[L]

Използвайки посоченият модел [1-7] за определяне настъпилите изменения в балистическите елементи (f, I_k, e_1, u_1), както и техните производни δ, σ, ν и др. на барутите намиращи се на дълговременно съхранение, става възможно определянето на стойностите на налягането P_{max} на барутните газове и начална скорост V_0 на куршума в цевната система. За целта е необходимо да се знаят табличните стойности на величините: параметър на условията за зареждане - $B_{таб}$, а също така и балистическите елементи (f, I_k, e_1, u_1). В този случай по метода на подобието, където се приема, че стрелковите (артилерийските) системи са балистически подобни, безразмерното налягане, скоростта, времето и пътят на (куршумите) снарядите в зависимост от избрания елемент ще съвпада или ще се различава само по мащабите. Подобието между огневите системи ще бъде пълно, ако то се изпълнява до излитането на снаряда и е ограничено, ако то се изпълнява само в периода на горене на барутният заряд в огневата система (Kalev, 2016, с.32).

В тази връзка посочената методика за определяне на променените стойности на балистически елементи (f, I_k, e_1, u_1) поради дълговременното съхранение на бойните припаси, започва с определяне табличната стойност на параметъра на условията $B_{табл}$. При което за таблични данни се приемат (Кирилов,1973, с.334: $s_{табл} = 0.00476\ m^2$, $\Delta_{табл} = 0.796 kg/dm^3$, $\omega_{табл} = 0.016 kg$, $g_{табл} = 9.80667 m/s^2$, $f_{табл} = 900000\ kg*dm/kg$, $e_{1табл} = 0.001\ m$, , $q_{табл} = 0.0079 kg$, $I_{k\_табл} = 133.3334 N$, $\varphi_{табл} = 1.09748$ $P^{max}_{табл} = 274.6 MPa$, $u_{1табл} = 0.0000075 \frac{dm/s}{kg/dm^2}$, $V_{0\_табл} = 715 m/s$.

Използвайки ги за табличната стойност на $B_{табл}$ получаваме:

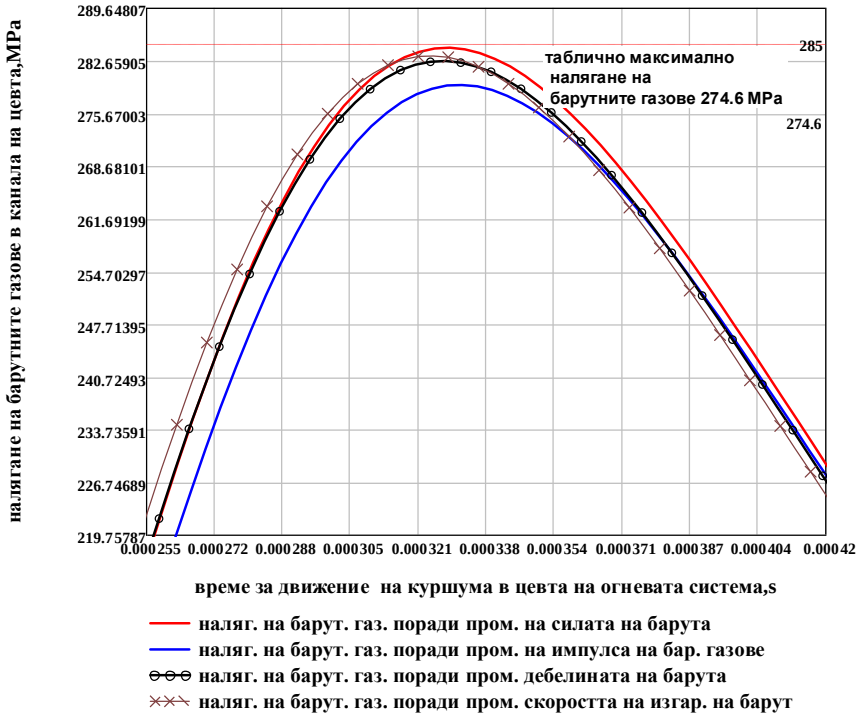
$$B_{табл} == \frac{s^2 I_k^2 g}{f\omega\varphi q} = \frac{0{,}00476^2 . 133{,}3334^2 . 9.80667}{900000 . 0.016 . 1{,}015 . 0.0079} = 2{,}98752 \qquad (9)$$

Тогава използвайки (9) за определяне стойността на балистическите елементи (f, I_k, e_1, u_1) променени от табличните, конструктивните само с - 0.5% на барут подложен на продължително съхранение имаме:

За силата на барута променен заради неговото стареене само с - 0.5% определен по (2) получаваме: $f = \frac{s^2 I_k^2}{Bm\omega\varphi} = 899990.2436 kg*dm/kg$; за пълният импулс на барутните газове в канала на цевта в края на горенето I_k определен по (4) имаме $I_k = \frac{\sqrt{Bf\omega\varphi m}}{s} = 131.3425 N$; за дебелината

на барутното зърно e_1 определено по зависимостта (5) се получава $e_1 = \frac{\sqrt{Bf\omega\varphi m u_1}}{s} = 0.00099mm$; за скоростта на горенето u_1 на барутният заряд в огневата система определена по (6) получаваме $u_1 = \frac{e_1 s}{\sqrt{Bf\omega\varphi m}} = 0.00000773 \frac{dm/s}{kg/dm^2}$.

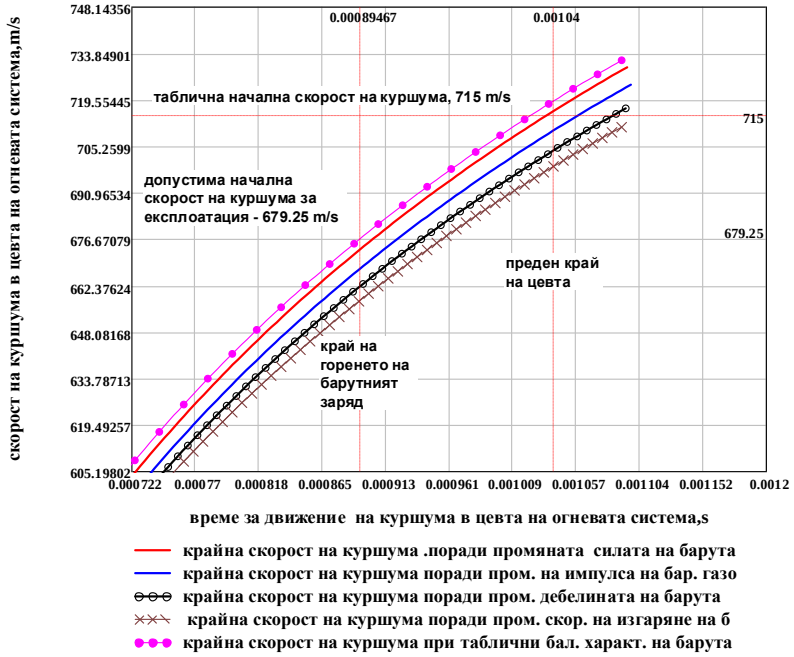
Получените резултати от промяната на балистичните елементи (f, I_k, e_1, u_1) на барутите със значителен срок на съхранение влияят по различен начин на стойностите на налягането P_{max} на барутните газове и съответно на начална скорост V_0 на куршума в цевната на система. При отчитането на отклоненията на всеки един от тях (f, I_k, e_1, u_1) стойността на P_{max} се променя по различен начин. Особеностите в стойността на P_{max} в зависимост от измененните (f, I_k, e_1, u_1) поради стареенето на барутите, спрямо табличните (f, I_k, e_1, u_1) са демонстрирани на фиг.1



Фиг.1.Максимално налягане на барутните газове в цевта на АК-47 при променени параметри на барута (f, I_k, e_1, u_1) *при срок за съхранение от 25 години .*

Анализът на относителното влияние на всеки един от променените параметри на барута (f, I_k, e_1, u_1) поради продължително съхранение от 25 години, стойността на P_{max} показва, че с най-голяма относителна тежест се явява промяната от проектните характеристики на силата на барута f, Фиг.1. Негативните влияния се изразяват в моментното повишаване на P_{max} поради физико-химическите промени главно свързани с дифузията на азота в барутните зърна. На второ място по влияние върху стойностите на P_{max} се явява импулса на барутните газове в канала на цевта в края на горенето I_k, където се наблюдава незначително повишаване на неговата стой-

ност, Фиг.1. Дебелината на горящият свод на барута e_1, най-динамично се променя поради дифузията на азота, ре-кристализацията и механическите въздействия на вибрациите. Поради това, геометрическите характеристики се променят и вследствие от това законът за горене на барутният заряд, нарежда на второ място по влияние формирането стойностите на P_{max}. Фиг.1. Всички негативи на старанието на барута се отразяват чувствително върху стойността на скоростта на горенето u_1 при формирането стойността на P_{max}. Освен като завишена моментна стойност на наляганието P_{max}, неговият център на получаване се измества по направление зарядната камера на огневата система. Това променя комплексно краят на изгарянето на барута и респективно води до редукция на началната скорост на куршума. Промяната на началната скорост на куршума поради променени параметри на барута (f, I_k, e_1, u_1) е представена на фиг.2.



Фиг.2.Начална скорост на куршума за АК-47 при променени параметри на барута (f, I_k, e_1, u_1) *при срок за съхранение от 25 години*

Формирането стойностите на наляганието на барутните газове поради променени параметри на барута (f, I_k, e_1, u_1) оказват влияние върху началната скорост V_0 на куршума в цевната система. Основно най-голяма редукция на V_0 се получава при промяната на стойността на скоростта на горенето на барута u_1 поради физико–химическите промени в барутните зърна, частичните механически разрушения на повърхностният слой получени от вибрациите при транспортиране на зарядите, както и други причини. Поради това от табличната началната скорост от $V_0 = 715m/s$, същата се редуцира $V_0 = 697m/s$ поради промяната на u_1, фиг.2. За относителното влияние промяната на e_1 върху V_0 е характерно, че то заема второ място поради генерираните стойности на P_{max} и бързината на изгарянето на барута след достигане неговата стойност в цевта на огневата система. Това води до редукция на началната скорост на куршума, спрямо табличната до

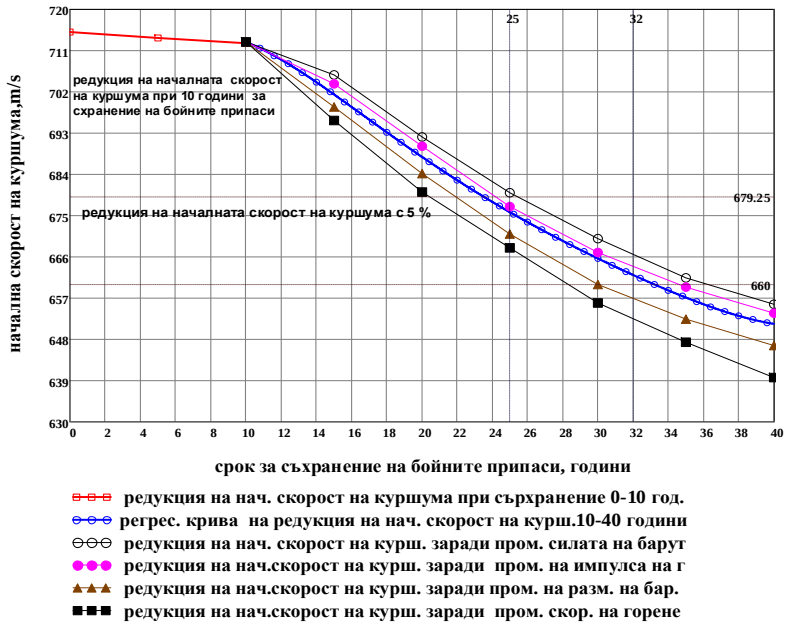
$V_0 = 702m/s$ фиг.2. Анализирайки останалите променени параметри на барута (f, I_k, u_1) и получените стойности от тях на P_{max} може да се направи извода че: винаги промените в (f, I_k, e_1, u_1) поради дълговременното съхранение на барутните заряди водят във всички случаи до редукция на началната скорост на куршумите. Посоченият ефект не съвпада с повишаване стойностите на налягането P_{max} в цевта на огневата система.

Тогава стойностите на редукцията на началната скорост на куршумите при отчитане на относителните тегла на промените в барута (f, I_k, e_1, u_1) вследствие годините за неговото съхранение могат да се използват, като един от индикаторите даващ връзката между годините за съхранение и прогнозната начална скорост V_0 на куршумите. За целта, чрез подбор на стойностите (f, I_k, e_1, u_1) в определени диапазони за тяхната промяна и не само посочените промени в барута може да се изведе емпирична зависимост между годините за съхранение на барутите и редукцията на началната скорост на куршумите. Обработените над 36 задачи по 8 броя за всяка промяна на всеки един от параметрите (f, I_k, e_1, u_1) съгласно математическият модел (1-8) позволяват да се изведе обща закономерност на стареенето на барута при отчитане на част от основните фактори ускоряващи процеса на стареенето. Към тях се отнасят: физико-химически процеси, механически въздействия на барутните състави поради многократното им транспортиране над 10 пъти на дистанции над 100 km с автомобилен транспорт, температурата на съхранение и др. В този случай, една от зависимостите на стареенето на барутите в нашата страна, даваща връзката между годините на тяхното съхранение при отчитане на посочените фактори и редукцията на началната скорост на куршумите, може да се зададе със следното уравнение:

$$C_{год}^{v_0} = 10.738x - 1.15x^2 + 0.047x^3 - 0.001x^4 + 628.238 \qquad (10)$$

където $C_{год}^{v_0}$ - връзка между годините на съхранение на барутите и редукцията на началната скорост на куршумите; x - е продължителността на съхранение на барутните заряди, години.

Зависимостта $C_{год}^{v_0}$ (10) определена с отчитане на относителните тегла на промените в барута (f, I_k, e_1, u_1), е представена на фиг.3.



Фиг.3. Сумарна зависимост на редукцията в началната скорост на куршума за АК-47 и годините за съхранение на барута, поради промяна на някои от основните му параметри (f, I_k, e_1, u_1)

Демонстрираната зависимост $C_{год}^{v_0}$, фиг.3. потвърждава основните относителни тегла на влияние на отделните променени балистически характеристики на барута при нейното определяне. Така например, относителното влияние в промените в силата на барута и пълният импулс в края на окончателното изгаряне на барутният състав, f, I_k при продължителното му съхранение оказват по-малко въздействие върху редукцията на началната скорост, фиг.3. Докато относителното влияние на дебелината на барута и неговата скорост на горене, e_1, u_1 имат решаващо значение за формиране на скоростта на куршумите във функция от годините за съхранение.

Грешката стойности на началната скорост на куршума, получени при решаването на правата задача по метода на проф. Дроздов с оглед на резултатите от обратната задача в сравнение с експерименталните стойности не надвишава 3 %. А прякото прилагане метода на проф. Дроздов при решаването на обратната задача на вътрешната балистика с използване на посочената методика се характеризира грешка до 5 %.

Заключение:

Предложената методология за определяне редукцията на началната скорост на куршума в зависимост от срока за съхранение на бойните припаси може да се използва при провеждане на опитни стрелби в полигонни условия за всяка една огнева система. Възприемането на началната скорост на куршума като диагностичен параметър, показващ стареенето на бойните припаси напълно може да се възприеме като модел за прогнозиране на техните балистически характеристики. Това дава основание да се направят практически препоръки за възможността за използване бойни припаси с различен срок за съхранение като стойността на редукцията на началната скорост се обозначи върху щатната им опаковка през определен период за съхранение, например 25 години. Тази информация относно редукцията на началната скорост ще позволи в значителна степен след въвеждане на съответните поправки да повиши ефективността на стрелбата с различни видове огневи системи.

Литература

[1].Анипко О.Б., Бирюков И.Ю. Зависимость начальной скорости снаряда от максимального давления в канале ствола при выстреле зарядами длительного срока хранения // Інтегровані технології та енергозбереження. – 2006. – №1. – С.83 – 86

[2].Анипко О.Б., Баулин Д.С., Бирюков И.Ю. Влияние длительности хранения боеприпасов на баллистические характеристики стрелкового оружия // Інтегровані технології та енергозбереження. Х.: Ізд-во НТУ “ХПІ”, 2007. – №2, С. 97-100.

[3].Бирюков И.Ю. Барутовые заряды длительных сроков хранения: проблемы, задачи и пути их решения // Інтегровані технології та енергозбереження. – Х.: 2006. – №2. – С.50 – 55.

[4]. Кирилов В.М. и др. Теория и расчет автоматического оружия. – Пенза: ПВАИУ, 1973. – 493 с.

[5].Коновалов А. А. и Ю. В. Николаев. Внешняя баллистика. Москва, ЦНИИ информации, 1979, 228 с.

[6]. Костадинов К.Н., Метод за определяне оптималният калибър на артилерийските системи в подразделенията от земната артилерия., Военен форум, ВВОВУ”В.Левски”, 2000

[7].Орлова Е.Ю. Химия и технология бризантных взрывчатых веществ. – Л.: Химия, 1973. – 688 с.

[8].Серебряков М. Е. Внутренняя баллистика ствольных систем и барутовых ракет. – М.: Оборонгиз, 1962. – 703с.

[9].Таблицы стрельбы по наземным целям из стрелкового оружие калибров 5,45 и 7,62мм ГРАУ № 61. Издание второе. Москва, 1977.

[10].Шерешевский, М., А.Гонтарев, и Ю.Минаев. Эффективность стрельбы из автоматического оружия. Москва, ЦНИИ информации, 1979, 328 с.

[11]. Kalev K., An approach for estimation of the geometrical parameters of the cannon barrel, International Scientific Session “Defense Technologies – Shumen 2015”. Faculty “A, AD and CIS”, Shumen, 2015, ISSN 2367-7902

[12].Kalev K., A study of the influence of the parameters of a reaction zone on the burning rate, International Scientific Session “Defense Technologies – Shumen 2016”. Faculty “A, AD and CIS”, Shumen, 2016, ISSN 2367-7902

COMMUNICATION AND COMPUTING TECHNOLOGIES

Anastas N. Madzharov,

TECHNICAL IMPLEMENTATION OF A REPORTING SYSTEM AND ITS WORKFLOWS

Anastas N. Madzharov

Institute of Information and Communication Technologies, Bulgarian Academy of Sciences, Sofia, a.madzharov@acad.bg

***Abstract**: This paper discusses the architectural decisions, flows and the implementation details of a reporting system and its workflows, as it is used within NMU. The system has been delivered as part of project BG051PO001-3.1.08-0024 "Improvements on the administrative systems of National Military University "V. Levski" (NMU). The paper is limited to the initial implementation of the reporting system and its workflows, while recent improvements on its code base and architecture are out of scope. Details are shared on its integration with reference database, especially the integration with the hierarchical employee structure of NMU "Vasil Levski". It is not a user guide. The implementation details are low level and aim at facilitating the long-term maintenance and improvements of the system. The main features of the system are (i) reports templating, input and archiving; (ii) daily summary reports and (iii) tracking the yearly holiday allowances for all employees.*

***Keywords**: Document Management Systems (DMS), Content Management Systems (CMS)*

ТЕХНИЧЕСКА РЕАЛИЗАЦИЯ НА СИСТЕМА ЗА ДОКЛАДИ И НЕЙНИТЕ РАБОТНИ ПОТОЦИ

Анастас Н. Маджаров

Секция „Високопроизводителни системи, мрежи и алгоритми“, Институт по информационни и комуникационни технологии, Българска академия на науките, ул. Акад. Г. Бончев, блок 25А, София, a.madzharov@acad.bg

Въведение

В тази статия се описва модула за молби и доклади от „Системата за управление на качеството“ в НВУ, към момента на неговото създаване. Разработван е по проект BG051PO001-3.1.08-0024 „Усъвършенстване на системите за управление в НВУ „В. Левски“. В настоящето описание не са взети предвид последващи изменения в структурата и кода на модула. Дават се подробности за интегрирането му с референтна бази данни, по-специално интеграцията с йерархичната структура на служителите в НВУ „Васил Левски“ [1]. То не е ръководство за потребители.

Целта на описанието е да се подпомогне поддръжката и експлоатацията на модула и евентуално неговото допълване и развитие.

Назначението на модула за доклади е да реализира въвеждане, резолиране, архивиране и отчетност на ежедневните доклади, да изчислява и отчита годишните отпуските на личния състав.

Системата поддържа над 60 бланки за доклади, които са разпределени според административните изисквания за водене на докладна книга. Всяка от бланките е реализирана чрез PHP мо-

дула Smarty, който поставя основата на динамично изграждане на документи чрез анотация на по-малки фрагменти. Всека бланка е в отделен php файл, като е разработена система за кодиране имената на файловете. Нова бланка се добавя като нов файл, с ново име. Това кодиране позволява при нормативни промени, старите доклади да се съхраняват в оригинален вид, а новите да постъпват с промените. Всеки потребител вижда само тези формуляри, които са му необходими. Този принцип също е заложен в системата за кодиране на имената на файловете.

1. Изграждане и съхраняване на доклад (молба)

Smarty е модул на PHP, който динамично попълва бланки на документи. Той предлага кеширане на документите във файловата система на сървъра, като това предотвратява ненужно натоварване на базата данни, както и предлага по-бързо показване на документите в браузър.

Моля на основание чл. 104 Правилника за вътрешния ред и дисциплината на НВУ „Васил Левски” да се разреши на **{$employeeName}** ваканция в размер на 10/20 (**{$daysString}**) дни за учебната **{$academicYear}** г., за времето **{$holidayDates}**. Ваканцията ще прекара в **{$address}**.

Моля същият да се отчисли от котлова храна от **{$meal}** на **{$date}** г. по приложение №2 от МЗ №ОХ-482/30.07.2010 г.

Фигура 1: Вид на бланка, съхранявана в базата данни като файл

Променливите от бланката се попълват по времена на заявката от браузъра както следва:

```
$this->smarty = new Smarty;
$smarty->assign($employeeName, “Иван Иванов Димитров”);
$this->smarty->display("string:" . $template);
```

1.1. Списък на разработените фрагменти за изграждане на бланка

Базовата функционалност на Smarty е недостатъчна за постигане целите на системата за доклади и са разработени множество разширения към модула, за да се поддържат различните типове доклади. Всичките тези разширения се наричат фрагменти за изграждане на бланка и основно имат две цели: 1) да визуализират фрагмента според изискванията, както и да 2) предложат специфична функционалност; например – търсене на курсант по име, падащи менюта за избиране на заместник, година за отпуск и други.

Според примера от фиг. 1, името “Иван Иванов Димитров” няма да е попълнено като текст в кода, а се използва подходящ фрагмент от допълнително разработените, за извличането му от модула „Личен състав“:

```
$this->smarty = new Smarty;
$employeeName = new \view\EmployeeNameView();
$smarty->assign($employeeName, $employeeNameView->display($nameFromDatabase) );
$this->smarty->display("string:" . $template);
```

Най-важните фрагменти за системата са следните:

• EmployeeName - Показва името на потребител в поле, което не може да се редактира.

• HolidayEmployeeName - Същото като EmployeeName, но се използва за бланки които са предназначени за отпуск и в които се следи календарното време.

• EmployeeNameSearch - Поле за търсене на име на потребител от базата данни.

• HolidayEmployeeNameSearch - Същото като EmployeeNameSearch, но в бланки, предназначени за отпуск и в които се следи календарното време.

• DatePicker - Поле за избиране на дати, с мини-календар като визуализация. Позволява да се избират дати от днес нататък.

• DatePickerUnbound - Същото като DatePicker, но позволява да се избират и отминали дати, отпреди днешния ден.

• HolidayDatesPicker - Група от два DatePicker-а, които са предназначени за избиране на начална и крайна дата на отпуск.

• HolidayDatesPickerUnbound - Същото като HolidaysDatesPicker, но позволява да се избират и отминали дати в първото поле за начална дата.

• OptionalParagraph - Използва се за обозначаване на специален параграф, чийто текст да може да се скрива.

• HolidayDeputyDropDown - Падащо меню за избор на заместник.

• HolidayYearDropDown - Падащо меню за избиране на годината, за която да се изчерпва заявения отпуск.

• TerminateDatesPicker - Същото като HolidayDatesPicker, но обозначава дати за прекъсване на отпуск. Тези дати са ограничени между датите на първоначално одобрения отпуск.

• InputField - Стандартно поле за редактиране.

• UnmodifiableInputField - Стандартно поле за показване на текст, който не може да бъде редактиран.

Реализация на фрагментите в код

Типовете фрагменти са дефинирани в таблицата dokladi_templateitemtype от базата данни.

Самите бланки се съхраняват в таблицата dokladi_template, в която полето contents съответства на бланката, така както Smarty я изисква.

Всяка бланка се асоциира с фрагменти от подходящ тип и това е реализирано чрез таблицата dokladi_templateitem.

Веднъж дефинирани, фрагментите са имплементирани с код, който е комбинация от PHP и JavaScript за визуализацията им.

Основният PHP пакет за работа с бланка е във директория /view/. Примерна реализация на фрагмент е:

```
abstract class AbstractFieldView {

   public abstract function displayAsHtml(\Entities\TemplateItem $templateItem, $defaultValue = "");

   public function displayInline(\Entities\TemplateItem $templateItem) {
      return $defaultValue;
   }
}


class InputFieldView extends AbstractFieldView {

   public function displayAsHtml(\Entities\TemplateItem $templateItem, $defaultValue = "") {
      return "<input  type='text' name='".$templateItem->name."' "
            ."value='". $defaultValue."' "
            ."class='tooltip borderless' title='".$templateItem->tooltipText."' "
            ."data-autosize-input='{ \"space\": 20}' "
            ."style='transition: width 0.25s; min-width: ".($templateItem->size)."'"
```

```
            ."/>";
    }
}
```

Функцията displayAsHtml се използва да покаже фрагмента в бланката по време на нейното попълване или редактиране, докато displayInline показва същият фрагмент, но като текст във вече попълнен доклад.

Много от фрагментите са допълнени с JavaScrit, който допринася за функционалността на потребителския интерфейс. Например, падащото меню за заместници (HolidayDeputyDropDown) се презарежда всеки път, когато датите за отпуск се променят в полетата на бланката (HolidayDatesPicker); промяната на датите води до преизчисляване на работните дните за които се иска отпуск и резултатът се показва на потребителя; полетата за прекратяване на отпуск не са активни, докато не се намери необходимия доклад за поискан отпуск, който ще се прекратява чрез въвеждане на неговия регистрационен номер, присвоен от системата след утвърждаването му от последна инстанция; и други.

1.2. Списък на типовете бланки

Типът на всяка бланка е зададен според това за какъв вид отпуска ще бъде съответния доклад. Типовете са:

• HOLIDAY – Отпуск.

• UNTRACKED_HOLIDAY – Друг вид отпуск, в която не се следят и изчисляват работни дни и не се изваждат от полагаемите се за избраната годината.

• ADDITIONAL_LEAVE – Допълнителен отпуск за балнеолечение и/или отпуснат според Кодекса на труда. Дните се следят.

• ADDITIONAL_LEAVE_STUDY – Допълнителен отпуск за обучение. Дните се следят заедно с тези от типа ADDITIONAL_LEAVE.

• SICK_LEAVE – Болничен.

• BUSINESS_TRIP – Командировка.

• NOT_HOLIDAY – Друг тип доклади, различни от горните типове, обикновено такива, в които няма периоди от време.

• LEFTOVER_OVERRIDE –Останали дни отпуск за годината.

• COMPESATION – резервиран за бъдещо развитие на системата при отчитане на компенсации от наряд или занятия през почивни дни.

Типовете на бланки за доклади са описани в таблицата dokladi_holiday_type. Съответно, всяка бланка е анотирана със своя тип в таблицата dokladi_template (holydayTypeId). Допълнително, всяка бланка е обозначена с ролята на потребител, който може да я упражнява. Те са: 0 – общи; 1 – военнослужещ; 2 – курсант; 3 – кадет; 4 – цивилен служител; 5 – студент (резервиран за бъдещо развитие).

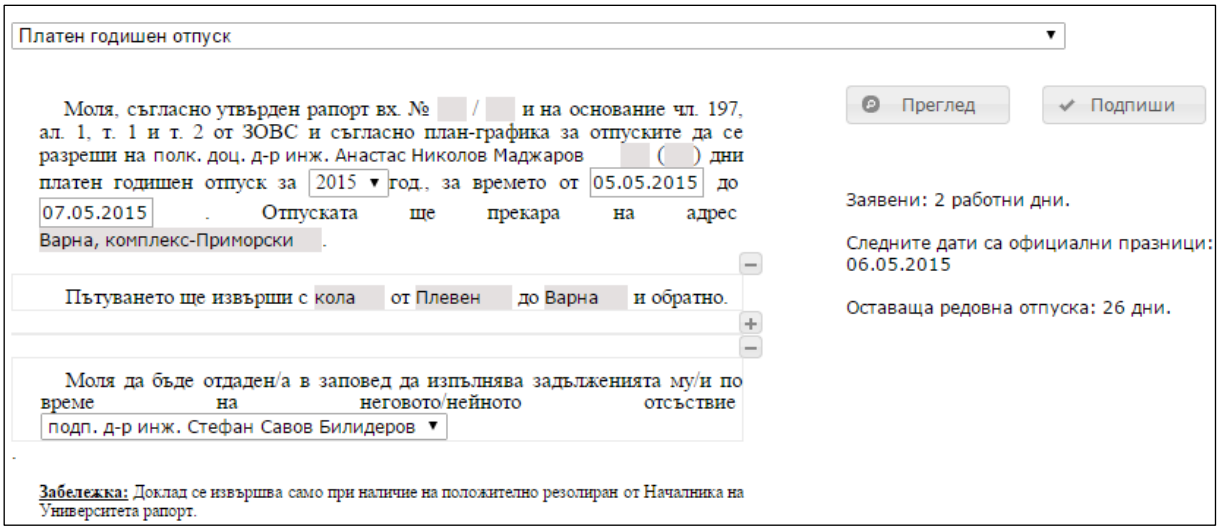
2. Функционални възможности за работа с доклади

2.1. Докладът като конкретна инсталация на бланка

Докладът представлява инсталация на бланка (фиг. 2) в брузер, която има конкретно зададени стойности за променливите и полетата. Докладите се записват основно в две таблици – 1) dokladi_request, която съдържа мета информация за доклада – коя бланка е използвана, кой и кога я е пуснал и т.н.; и 2) dokladi_requestdetails, която е аналогична на описаната по-горе dokladi_templateitem и още съдържа стойностите на фрагментите, които потребителят е задал.

Тук, е важно да се отбележи, че не всички стойности на фрагменти се записват в dokladi_requestdetails, а само тези, които са за фрагменти незапочващи с името Holiday. Тези, кои-

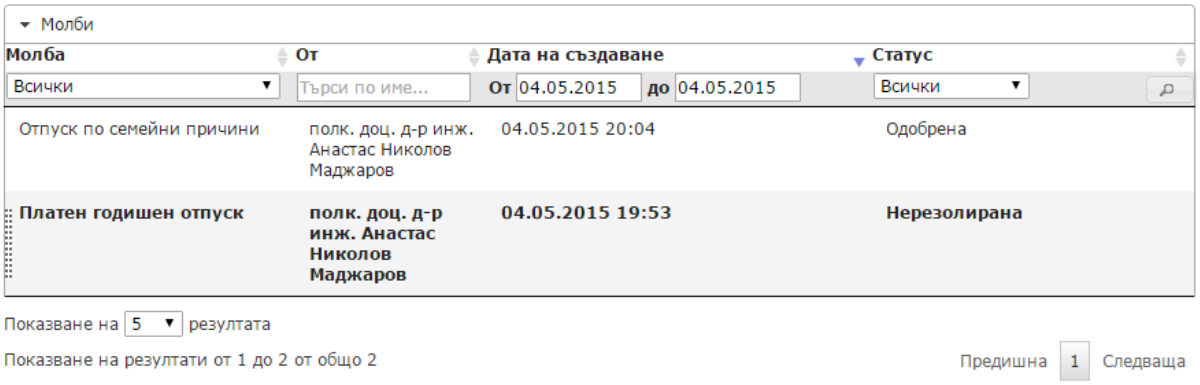
то започват с Holiday, специално се комбинират и обработват от системата, след което се записват в таблица dokladi_holiday. Тази таблица е подробен запис на зададен отпуск с дати; заместници; година на отпуска; работните дни за които е поискан отпуска и които са калкулирани по време на записа на молбата; и др.



Фигура 2: Вид на доклад с полетата за попълване

2.2. Преглед на доклад

Детайлите на доклада, които са записани в dokladi_request се използват за директното показване на списъка с доклади за всеки потребител. Това става от менютата “Молби” или “Мои молби”, като е реализирано в стил на пощенска кутия. Молбите в тъмно са тези, които логнатия потребител все още не е подписал (фиг. 3).



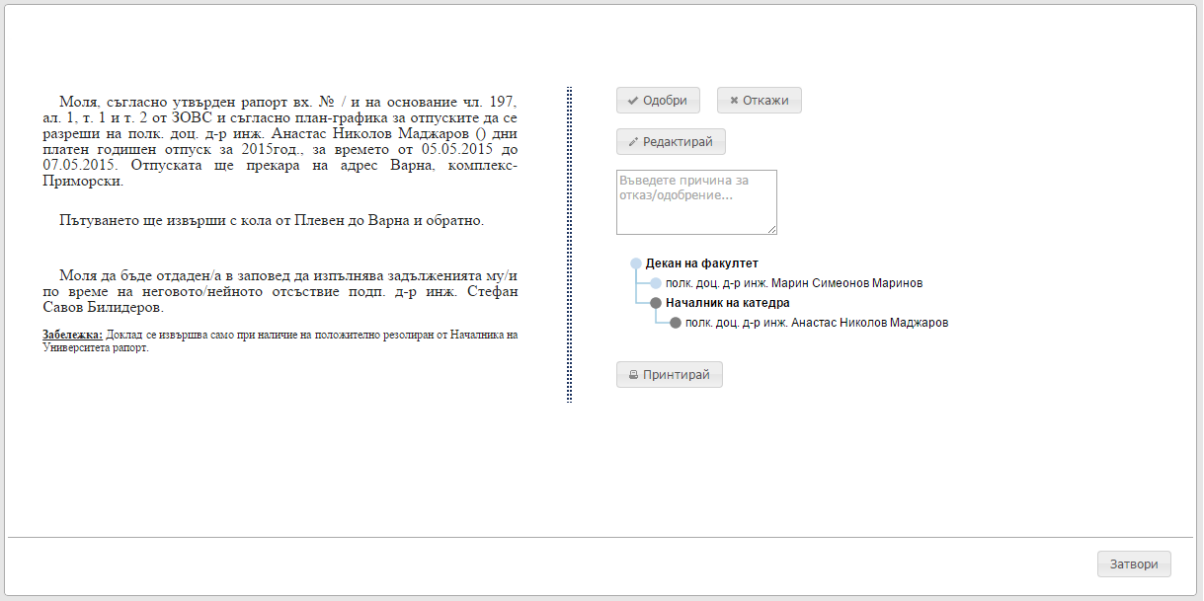
Фигура 3: Вид на справка за собствените молби

Подробните детайли от таблиците dokladi_holiday и dokladi_requestdetails се извличат от базата данни и цялата молба се показва на потребителя при поискване (избиране от падащо меню).

При прегледа на молба, според йерархията на потребителя, молбата може да бъде редактирана от него, преди да я подпише. При редакцията на молбата, бланката се показва, както при началното подаване на молбата, но полетата са попълнени според зададените им стойности. Потребителите от първо ниво на йерархията вместо бутон „Редактирай“ имат бутон „Преглед“, който показва молбата във форматиран окончателен вид.

По същество, кодът който визуализира бланката и молбата е един и същ, независимо от режима – пускане на нова молба, преглед при пускане, редактиране на молба, гледане на молба. По

този начин се избягват бъгове при форматиране и изгледът на дадена бланка се запазва еднакъв през целия и живот като молба.



Фигура 4: Преглед на молба с възможност за отпечатване, одобряване, редактиране, въвеждане на резолюция или отхвърляне

От гледна точка на реализация на функционалността, се използват два главни пакети от PHP код. Те са обособени в следните директории:

- /entities/ - са тези, които правят връзка с базата данни и конструират обекти директно от нея. Така всеки ред от таблиците в базата от данни се реализира като PHP обект.
- /domain/ - са тези, които преобразява обекти от /entities/ към обекти, с които системата ефективно може да следи отпуски, потребители, йерархия, коментари, да извършва визуализации и т.н.

2.3.Фази на живот за доклад (молба)

След като попълнена бланка се подпише, тя става молба и в зависимост от това как се придвижва по йерархията, може да премине през няколко фази:

- **Нерезолирана и чакаща подпис** – Логнатият потребител е получил молба от подчинен, която не е подписал все още (фиг. 4).
- **Нерезолирана** – Логнатият потребител е подписал молбата, но тя не се е придвижила до края на йерархията и все още е нерезолирана (фиг. 3 – текстът в тъмно).
- **Одобрена** – молба одобрена от всички в йерархията. Веднъж одобрена молбата се замразява – не може да се променя повече, независимо от бъдещите промените в йерархията. Ако молбата е за отпуск, работните дни, които съдържа отпуска се отчитат в момента в който молбата преминава в одобрена. В този момент и се присвоява и номер в системата. Независимо от възможни бъдещи промени в националните празници, дните които отпускът от тази молба покрива няма да се променят.
- **Отказана** – молба, може да бъде отказана на всяко ниво над първото в йерархията. Отпускът който е поискан чрез молбата ще остане вписана в dokladi_holiday, но няма да бъде отчетен. Веднъж отказана, молбата не може да се върне към по-ранен стадий. Опции за редактиране и манипулиране не се предлагат.

Заключение

Изградената система за доклади е реализирана за конкретните изисквания на потребителя. Предварително проведеното проучване на съществуващи Content Management Systems и документооборот с възможност за изчисляване и отчитане на годишните отпуските на личния състав не предоставяха необходимата функционалност и затова се премина към разработване на собствена, уникална структура на модула „Доклади“ от информационната система на Национален военнен университет.

За да се поддържа и развива вече изградена система е нобходимо да се познават детайлите от нейната структура и реализирани функционалности. Настоящата статия предоставя тази възможност.

Литература

1. Свилен Стефанов, Т. Йотков, Ц. Харизанов. Единен функционален модел на Национален военен университет „Васил Левски“, ПРОЕКТ BG051PO001-3.1.08-0024, Велико Търново, 2013.

Kolyo P. Kolev, Radoslav K.Velikov,

CALCULATION OF COMBUSTION CHAMBER DINAMIC CHARACTERISTICS OF AVIATION BOMB FOR FIRE EXTINGUISHING BY COMPUTER-ASSISTED MODELING

Kolyo P. Kolev*, Radoslav K.Velikov**

Aviation Faculty, National Military University „Vasil Levski", Dolna Mitropolia, Bulgaria
kolev_007@abv.bg, velikov@abv.bg***

ИЗЧИСЛЯВАНЕ НА ДИНАМИЧНИ ХАРАКТЕРИСТИКИ НА АВИАЦИОННА БОМБА ЗА ГАСЕНЕ НА ПОЖАРИ ЧРЕЗ КОМПЮТЪРНО МОДЕЛИРАНЕ

Кольо П. Колев*, Радослав К. Великов**

Факултет "Авиационен", НВУ "Васил Левски", Долна Митрополия, България,
kolev_007@abv.bg, velikov@abv.bg***

***Abstract**: We present the results of numerical modeling of the dinamic characteristics of fire extinguishing aviation bomb.The design methodology developed allows the simulation of dynamic characteristics of the aviation bomb under the different designed calculations.*

***Keywords**: simulation, "SolidWorks",aviation bomb,runaway,pressure.*

ВЪВЕДЕНИЕ

Математическото моделиране е процес на създаване и откриване на подходящо математическо представяне на авиационното средство.

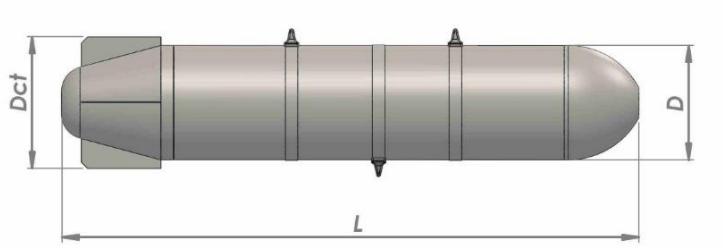
Днес, в много ситуации физичните модели са заменени с използването на компютърни *симулационни (имитационни),* обикновено те са компютърни програми, които изкуствено отразяват реална система, и при която могат да променят и тестват различни предположения за тази система. Симулирането се основава на принципа „опознаване чрез действие". За да се изучи системата, трябва да построи модел и да се тества многократно [3,5].

Конструктивният разчет се налага за определяне и обосноваване на основните тактико-технически характеристики.

В резултат от проучването е разработено тактико-техническо задание (ТТЗ) на авиационното средство за гасене на пожари (АСП) със следните изискванията:

- Калибър, kg - 500;
- Дължина -L, mm - 1445;
- Диаметър на корпуса-D, mm - 460;
- Разстояние от челния срез до масовия център , mm. – 1120;
- Височината на бомбопускане - от 300 до 1000 m.

- Окачване на изделието към всички съвременни носители.



Фиг.1 Геометрични размери на авиационно средство за гасене на пожари, L-дължина, D- диаметър на корпуса, D_{ct}- диаметър стабилизатора.

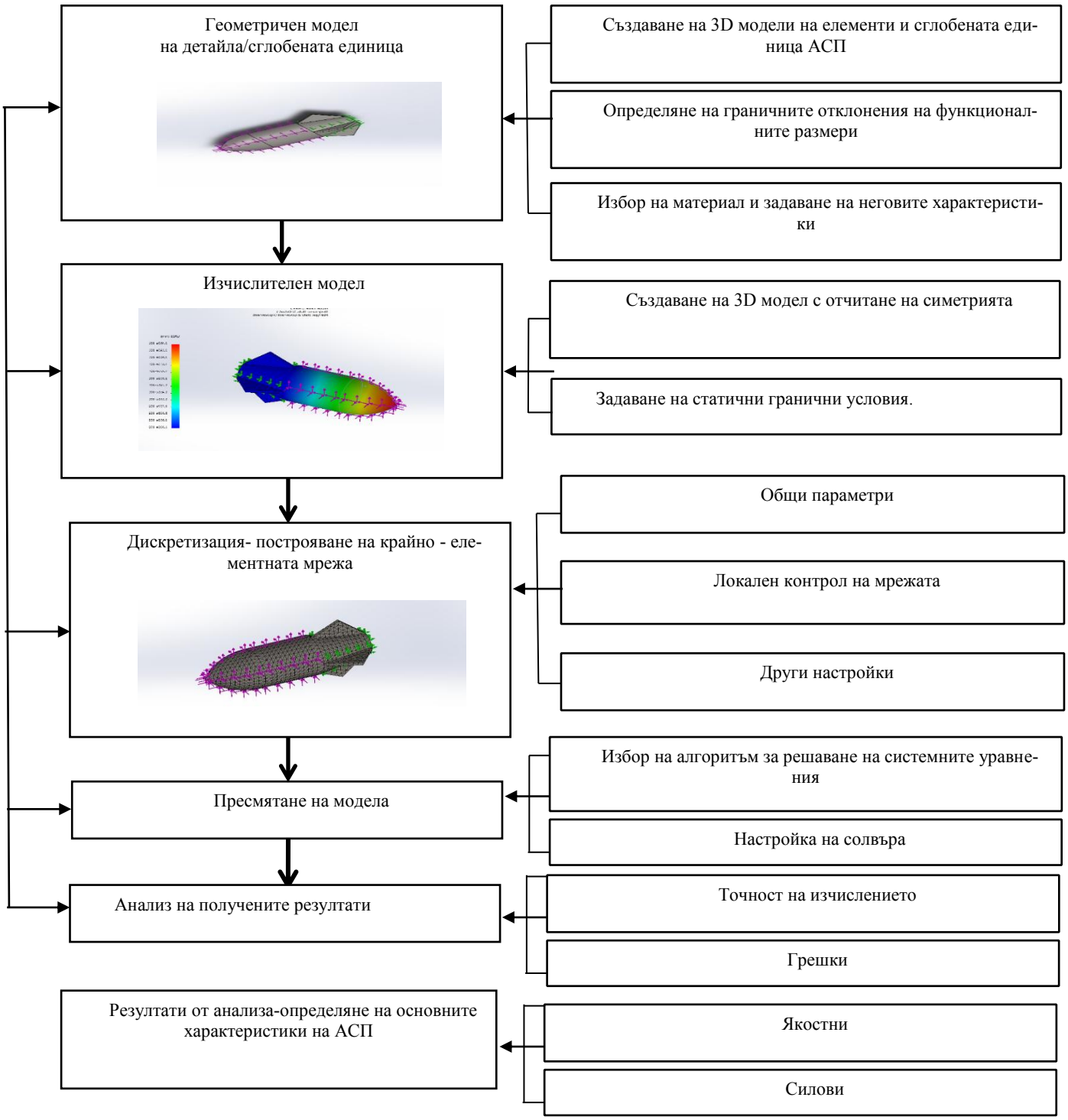
Изложение

Във връзка със сложната геометрия на АБ, за аналитично изследване на характеристиките на механизъма е целесъобразно използването на съвременни CAD/CAE системи. 3D графичната параметрична компютърна система SolidWorks и интегрирания в нея пакет за инженерни изследвания COSMOSWorks е единно решение за проектиране [1,2].

Проведен е числен експеримент, симулиращ работата на АБ при следните стойности на основните параметри на конструкциите цангови патронници: номинален диаметър на повърхнината на затяганата заготовка d = 96 mm; осова теглеща сила SΣ = 50000 N; Якостна проверка на конструкциите АБ се прави въз основа на диаграмите за разпределение на еквивалентните напрежения по von Mises, графика 1(деформация), 2(изместване), 3(натиск) [4].

Методика за проектиране на динамични характеристики на АСП се извършва по следен начин:

- създава се пространствен параметричен модел на АСП;
- определят се граничните отклонения на функционалните размери;
- избира се материал за елементите на АСП и се задават неговите характеристики (материалните характеристики за разглеждания пример съответстват на стомана $Ст_3$- модул на еластичност 2,1e+11 Pa, коефициент на Poisson 0,28 и др.);
- създава се изчислителен геометричен модел в основа на разработения обемен модел на АСП се явяващ се 1/z симетрична част от него, с цел намаляване на размерността и увеличаване на точността.
- избира се алгоритъм за решаване (в COSMOSWorks са вградени три алгоритъма за решаване на системите линейни уравнения). Кинематичните гранични условия водят към пораждане на „почти” кинематично подвижна сглобка;
- отчита се триенето между елементите в системата; в сглобената единица има тънкостенни обемни детайл; има материали, силно различаващи се по коравина и т.н..
- прави се анализ на получените резултати и се прилагат методи за контрол и повишаване на точността на изчислението.
- определят се големината и разсейването на основните характеристики на ЗМ (якостни, силови, точности, коравини и т.н.), тъй като те са функции от отклонението от номиналните размери (линейни, ъглови).



Фигура 2. Методика за проектиране на динамични характеристики на АСП

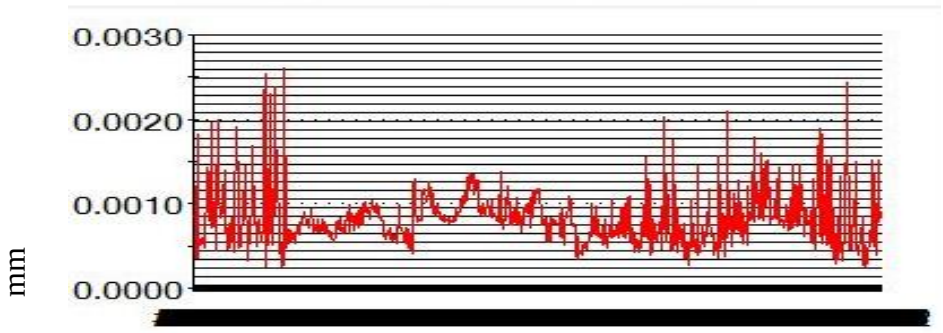
РЕЗУЛТАТИ

Проведен е числен експеримент, симулиращ работата на АСП при следните стойности на основните параметри на конструкциите:

- номинален диаметър на повърхнината на затягната заготовка d = 460 mm;
- осева теглеща сила SΣ = 20000 N;

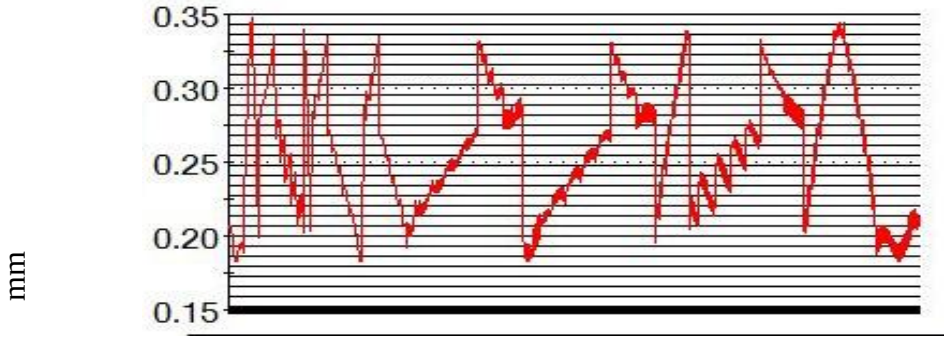
Якостна проверка на конструкциите АБ се прави въз основа на диаграмите за разпределение на еквивалентните напрежения по von Mises, графика 1 (деформация), 2(изместване), 3(натиск).

ДЕФОРМАЦИЯ



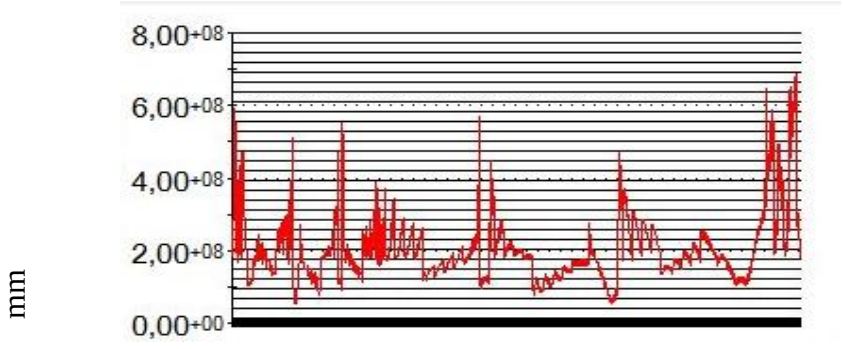
Граф.1 Деформация породена в специфичен участък на АСП

ИЗМЕСТВАНЕ



Граф.2 Изместване породено в специфичен участък на АСП

НАТИСК



Граф.3 Натиск породен в специфичен участък на АСП

Изводи

1. Разработената методика за проектиране позволява симулиране на АСП, при различни конструктивни разчети.

2. Създадените модели се явяват предпоставка за разработване на система за автоматизирано проектиране на АСП.

References

1. Antonov S., Tsonev T., (2016) Possibilities for automation of designing elements of small arms using CAD/CAM/CAE systems, Collection of papers: „Defense And Security, Mechanical Engineering And Military Technology, Communication And Computing Technologies, Social Science“, Shumen, Bulgaria 2016, p.p. 319-324, ISSN 2367-7902
2. Antonov S., (2017) Comparative analysis of the armament and equipment support modules in the field of command and control information systems of NATO armies, International Scientific Journal "SECURITY & FUTURE", Year I, Issue 4, p.p. 163-167, (2017), WEB ISSN 2535-082X; PRINT ISSN 2535-0668
3. Petrov Zh., Liliana Miron, (2019), Opportunities of a genetic algorithm for static calibration of mems accelerometers, International Annual Scientific Conference Aviation Faculty, National Military University, 2019, p. 246, ISBN 978-954-713-123-1
4. Petrova T., (2019), Application of geometrical transformations for the atachment of images to geographical maps // 21st International scientific conference: The teacher of the future, Budva, Montenegro, (07-09.06.2019), Institute of knowledge management – Skopje, Macedonia, 31, 2019, 6, pp.1917-1922, ISSN1857-923X (for e-version), ISSN 2545 – 4439 (for printed version)
5. Petrova T., (2019), Research on algorithms for filtration of aerial and radar images // 21st International scientific conference: The teacher of the future, Budva, Montenegro, (07-09.06.2019), Institute of knowledge management – Skopje, Macedonia, 31, 2019, 6, pp. 1923-1936, ISSN 1857-923X (for e-version), ISSN 2545 – 4439 (for printed version).

Kolyo P. Kolev, Radoslav K.Velikov,

CALCULATION OF DINAMIC CHARACTERISTICS OF AVIATION BOMBS FOR PENETRATION INTO MULTILAYER STRUCTURE BYCOMPUTER-ASSISTED MODELING

Kolyo P. Kolev*, Radoslav K.Velikov**

Aviation Faculty, National Military University „Vasil Levski“, Dolna Mitropolia, Bulgaria
kolev_007@abv.bg, velikov@abv.bg***

ИЗЧИСЛЯВАНЕ НА ДИНАМИЧНИ ХАРАКТЕРИСТИКИ НА АВИАЦИОННИ БОМБИ ЗА ПРОНИКВАНЕ В МНОГОСЛОЙНА СТРУКТУРА

Кольо П. Колев*, Радослав К. Великов**

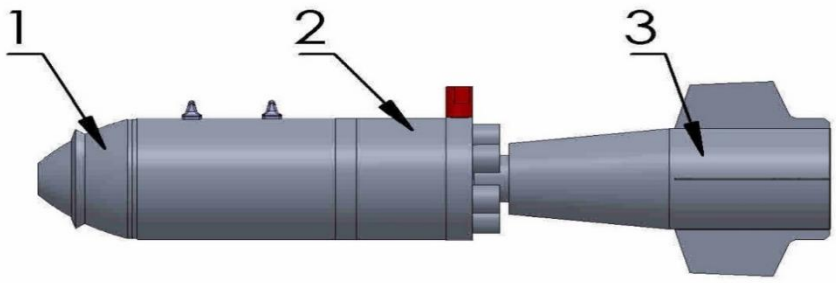
Факултет “Авиационен“, НВУ “Васил Левски“, Долна Митрополия, България,
kolev_007@abv.bg, velikov@abv.bg***

Abstract *We present the results of numerical modeling of the dinamic characteristics of of aviation bombs for penetration into multilayer structure by computer assisted modeling.The developed simulations of the elements of the aviation bomb construction make it possible to study and analyze their system and optimize their geometry in order to stabilize it..*

Keywords*: simulation, “SolidWorks“,aviation bomb,dynamic characteristics.*

Въведение

Фугасните АБ се явяват основен тип бомбово въоръжение за авиацията и са предназначени за поразяване на промишлени съоръжения, мостове, складове, фортификационни съоръжения и др (фиг.1).



Фиг.1

1. Челна част с корпус. 2. Барутно ракетен двигател. 3. Опашна част

Челната част на бомбата има оживална форма. Към челната част на корпуса е заварен балистическия пръстен.

Опашната част на бомбата представлява конус обърнат с голямата си основа на корпуса, служи за поместване на стабилизиращия парашут

Фугасните АБ съдържат сравнително голямо количество взривно вещество и вследствие на това притежават голяма разрушителна сила.

Разрушителното действие на ФАБ се определя от кинетическата енергия, която те притежават при среща с преградата. Знанието на закона за движение на боеприпаса при проникването му в непрекъснати твърди среди, позволява най-ефективно да се реши една от най важните задачи - задачата за поразяването на дълбоко укрити цели в грунда.

В настояще време във връзка с нарастване на скоростта и височината на бомбомятане, а също и с използване на толкова мощни средства за поражение, възниква задачата за разчет на здравина и безотказност на боеприпаса при удар в преграда.

Изложение

За решаване на задачата за проникване на тялото в среда е необходимо да се знае известни характеристики на телата /маса, форма и др./, известни физико-механични характеристики на средата, начални и гранични условия [1, 2].

Грунд се счита идеална непрекъсната среда, при която отсъстват касателни напрежения. Това предположение се приема при деформация на грунда под действие на големи напрежения [3,5]. При изучаване на явлението за проникване на телата е различни среди е необходимо да се има в предвид, че явлението се състои от три етапа:

1. удар по повърхността на средата;
2. проникване на тялото в средата;
3. движение на тялото в средата.

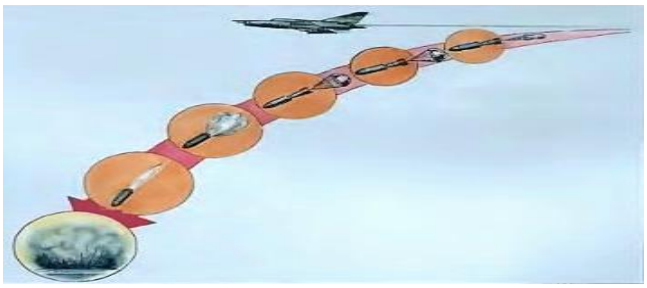
Началният етап - удар по повърхността на среда та се характеризира с възникване в мястото на удара такива условия, при които както в грунда, така и в тялото възниква ударна вълна на свиване. В този начален момент на среща на тялото е преградата, в резултат на рязко спиране възникват големи натоварвания [4].

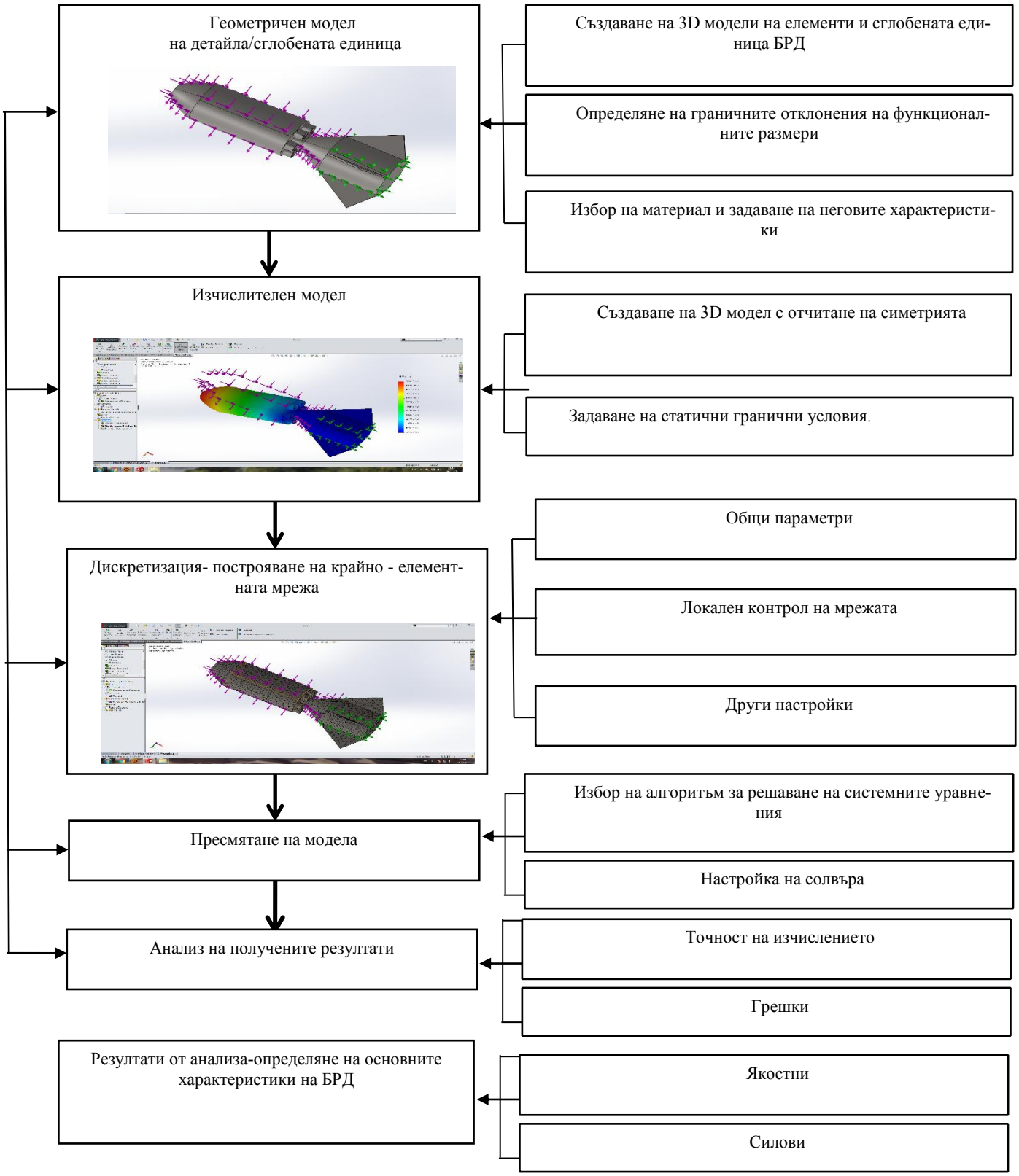
Проникването на тялото зависи от това, под какъв ъгъл АБ се среща с повърхността.

Разглеждането на процеса на проникване на боеприпаса в непрекъсната среда ще направим със следните допускания:

- среща на тялото с преградата е по нормалната. /нашата бомба е с парашутно устройства и дава възможност за увеличаване на ъгъла на срещата (фиг.1);
- траекторията на движение на тялото в средата е праволинейно.

За решаване на задачата за проникване на тялото в определена среда е необходимо да се извърши и анализ на динамичните характеристики на авиационната бомба, за да върши предназначеното и действие.

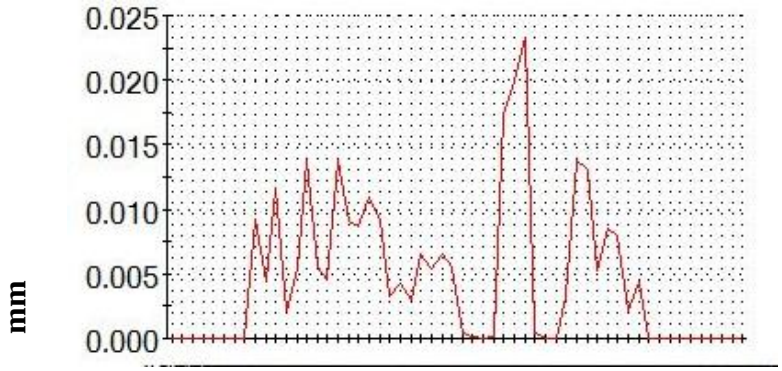




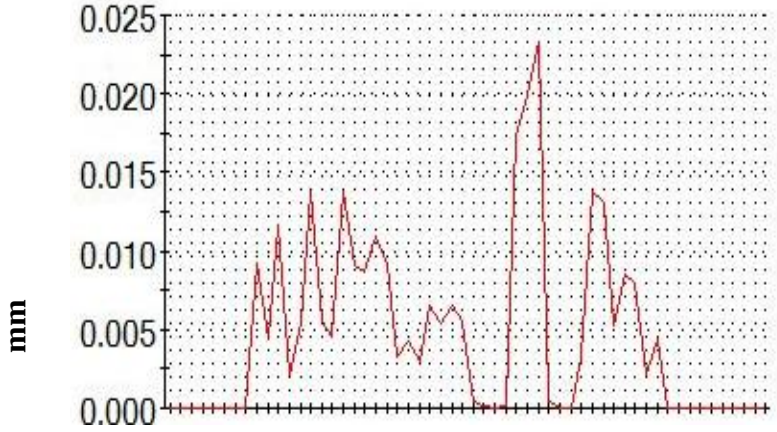
Фигура 2. Методика за проектиране на динамични характеристики на АБ

Резултати

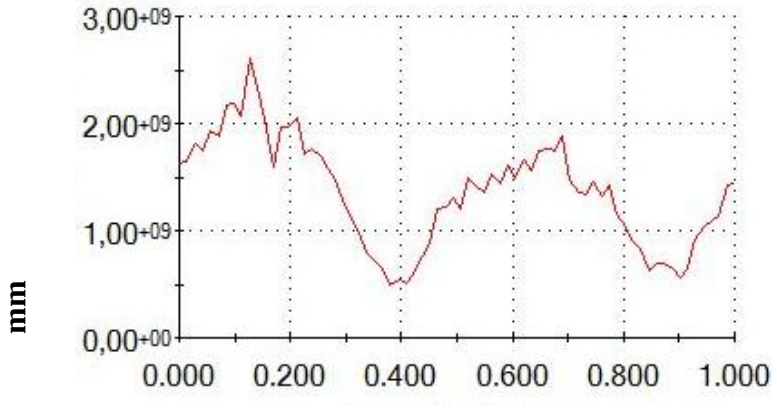
Проведен е числен експеримент, симулиращ работата на АБ при следните стойности на основните параметри на конструкциите: номинален диаметър на повърхнината на затяганата заготовка d = 296 mm; осева теглеща сила SΣ = 50000 N; Якостна проверка на конструкциите АБ се прави въз основа на диаграмите за разпределение на еквивалентните напрежения по von Mises, графика 1(деформация), 2(изместване), 3(натиск).



Граф.1 Деформация породена в специфичен участък на АБ



Граф.2 Изместване породено в специфичен участък на АБ



Граф.3 Натиск породен в специфичен участък на АБ

Изводи

1 Разработената методика за проектиране позволява симулиране на АБ, при различни конструктивни разчети.

2. Разработените параметрични крайно-елементни модели на конструкциите АБ дават възможност за изследване и анализ на динамичните им характеристики и оптимизиране на геометрията с цел стабилизиране на системата.

3.Създадените модели се явяват предпоставка за разработване на система за автоматизирано проектиране на авиационни бомби.

References

1. Antonov S., Tsonev T., (2016) Possibilities for automation of designing elements of small arms using CAD/CAM/CAE systems, Collection of papers: „Defense And Security, Mechanical Engineering And Military Technology, Communication And Computing Technologies, Social Science“, Shumen, Bulgaria 2016, p.p. 319-324, ISSN 2367-7902
2. Antonov S., (2017) Comparative analysis of the armament and equipment support modules in the field of command and control information systems of NATO armies, International Scientific Journal "SECURITY & FUTURE", Year I, Issue 4, p.p. 163-167, (2017), WEB ISSN 2535-082X; PRINT ISSN 2535-0668
3. Petrov Zh., Liliana Miron, (2019), Opportunities of a genetic algorithm for static calibration of mems accelerometers, International Annual Scientific Conference Aviation Faculty, National Military University, 2019, p. 246, ISBN 978-954-713-123-1
4. Petrova T., (2019), Application of geometrical transformations for the atachment of images to geographical maps // 21st International scientific conference: The teacher of the future, Budva, Montenegro, (07-09.06.2019), Institute of knowledge management – Skopje, Macedonia, 31, 2019, 6, pp.1917-1922, ISSN1857-923X (for e-version), ISSN 2545 – 4439 (for printed version)
5. Petrova T., (2019), Research on algorithms for filtration of aerial and radar images // 21st International scientific conference: The teacher of the future, Budva, Montenegro, (07-09.06.2019), Institute of knowledge management – Skopje, Macedonia, 31, 2019, 6, pp. 1923-1936, ISSN 1857-923X (for e-version), ISSN 2545 – 4439 (for printed version).

Kolyo P. Kolev, Radoslav K.Velikov,

CALCULATION OF COMBUSTION CHAMBER DINAMIC CHARACTERISTICS OF ROCKET MOTOR SOLID-PROPELLANT ENGINE BY COMPUTER-ASSISTED MODELING

Kolyo P. Kolev*, Radoslav K.Velikov**

Aviation Faculty, National Military University „Vasil Levski", Dolna Mitropolia, Bulgaria
kolev_007@abv.bg, velikov@abv.bg***

ИЗЧИСЛЯВАНЕ НА ДИНАМИЧНИ ХАРАКТЕРИСТИКИ НА БАРУТНО–РАКЕТЕН ДИВГАТЕЛ ЧРЕЗ КОМПЮТЪРНО МОДЕЛИРАНЕ

Кольо П. Колев*, Радослав К. Великов**

Факултет "Авиационен", НВУ "Васил Левски", Долна Митрополия, България,
kolev_007@abv.bg, velikov@abv.bg***

***Abstract**: We present the results of numerical modeling of the dinamic characteristics of the combustion chamber of gun-powder rocket engine.The developed design methodology allows to simulate the dynamic characteristics of the rocket engine,at different design calculations The results are compared to engine „РНДСИ 5-К"..*

***Keywords**: simulation, "SolidWorks",aviation bomb,rocket engine.*

ВЪВЕДЕНИЕ

Ракетните двигатели на твърдо гориво са получили в днешно време широко приложение. От публикациите следва, че повече от 90 % от съществуващите барутно-ракетни двигатели са изработени на основата на твърдо гориво. Тези двигатели имат висока надеждност, простота на експлоатация, постоянна готовност за действие, за кратко време тягата достига високи стойности. Наред с изброените достойнства барутно-ракетните двигатели имат и съществени недостатъци:

- зависимост на скоростта на горене на твърдото гориво от началната температура на заряда;
- относително ниски значения на специфичния импулс на твърдото гориво;
- трудни при регулиране и широк диапазон на работа.

Барутно-ракетните двигатели се използват във всички класове съвременни ракети с високо назначение. Разнообразните области на приложение и изпълняваните задачи е способствало за разработването на голямо число различни конструкции двигателя, отличаващи се по габаритни, масови, тягови и временни характеристики [1,2].

Тягата на най-слабите двигатели е от порядъка на 0,01N до 1600N. Тягата на най-големите двигатели (с диаметри 3,05; 4,5; 6,6 m) достигат десетки меганютона. Например за БРД с диаметър 6,6 m, тягата достига до 31 меганютона. Промеждутъчната област заемат двигателите със средни габарити, които се явяват като най-многочислени и разнообразни.

По изпълняваните функции всички ракетни двигатели могат да се разделят на три групи:

1. двигатели създаващи тяга, необходима за преместване на летателния апарат;
2. двигатели създаващи управляващи усилия и моменти;
3. двигатели за експериментални и технологични цели.

Първата група двигатели изпълняват основната функция, осигуряваща налитане и ускоряване на АБ.

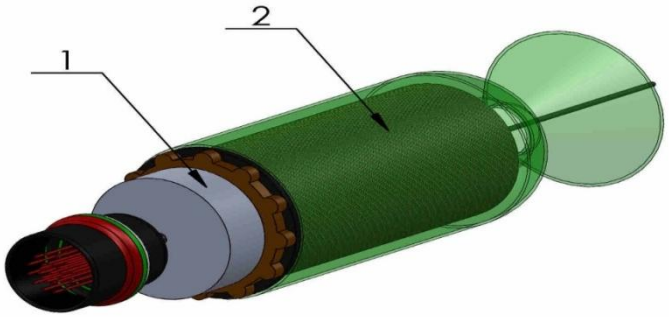
Втората група двигатели изпълняват спомагателни функции. Към група се отнасят релевите двигатели служещи за управление на полета по зададена програма. Корегиращи, необходими за стабилизация в необходимото положение, спирачни, предназначени за осъществяване на меко кацане.

Третата група е предназначена за провеждане на различен род изпитания.

ИЗЛОЖЕНИЕ

За да бъдат осъществени експерименталните изследвания първо трябва да се конструира и моделира барутно- ракетен двигател (БРД). Моделирането и изчисляването на геометричните характеристики е извършено с помощта на програмния продукт “SolidWorks” [3,5].

Конструктивният модел на БРД се състои от детайли оформени в следните сборки (фиг.1).



Фиг. 1 Типична схема на БРД

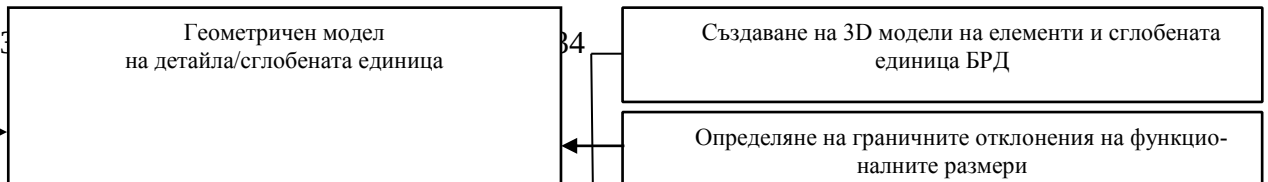
Корпуса на двигателя (2) се съединява с сборка инициатор (1), чрез резбово съединение. Вътрешният обем на двигателя е образуван от камера, която служи едновременно и за поместване на горивото. При горене на барутния заряд се образуват газови продукти, които се движат през камерата на горене към соплото и изтичат през него в атмосферата. Сечението на соплото има най-малка площ наричаща се критическа. В критичното сечение скоростта на газовете е равна на местната звукова скорост. Във входа на соплото се поставя решетка, която се нарича диафрагма. Ако заряда в процеса на горене се разруши, то големите парчета неизгорял барут се спират от диафрагмата и няма опасност от запушване на соплото.

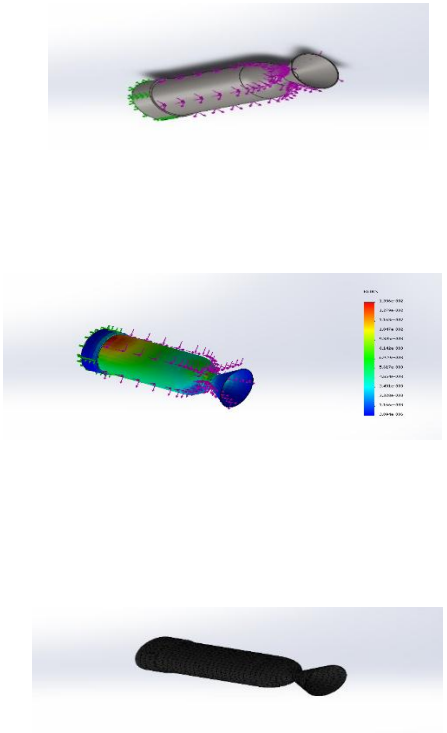
Във връзка със сложната геометрия на БРД, за аналитично изследване на характеристиките на механизъма е целесъобразно използването на съвременни CAD/CAE системи. 3D графичната параметрична компютърна система SolidWorks и интегрирания в нея пакет за инженерни изследвания COSMOSWorks е единно решение за проектиране [4].

Методиката за проектиране на ВЦП е дадена на фиг. 2 се извършва по следен начин:

- създава се пространствен параметричен модел на БРД;
- определят се граничните отклонения на функционалните размери;
- избира се материал за елементите на БРД, задават се неговите характеристики (материалните характеристики за разглеждания пример съответстват на стомана ХВГ- модул на еластичност 2,1e+08 Pa, коефициент на Poisson 0,32 и др.);
- в основа на разработения обемен модел на БРД, се създава изчислителен геометричен модел, явяващ се 1/z симетрична част от него.

ISSN 23





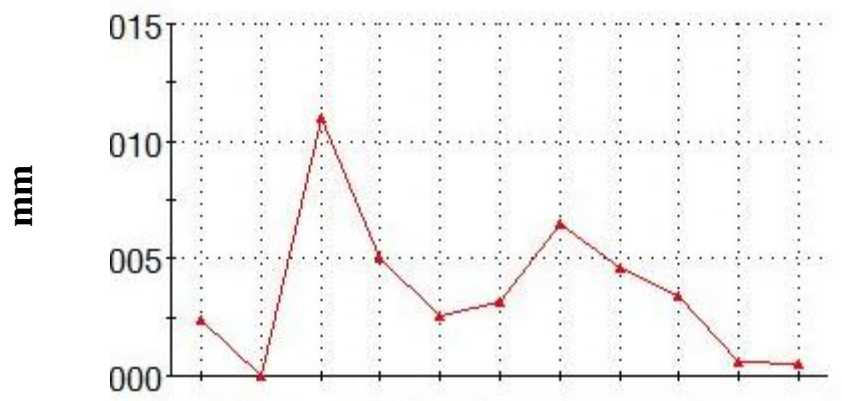
Фигура 2. Методика за проектиране на динмамични характеристики на БРД

РЕЗУЛТАТИ

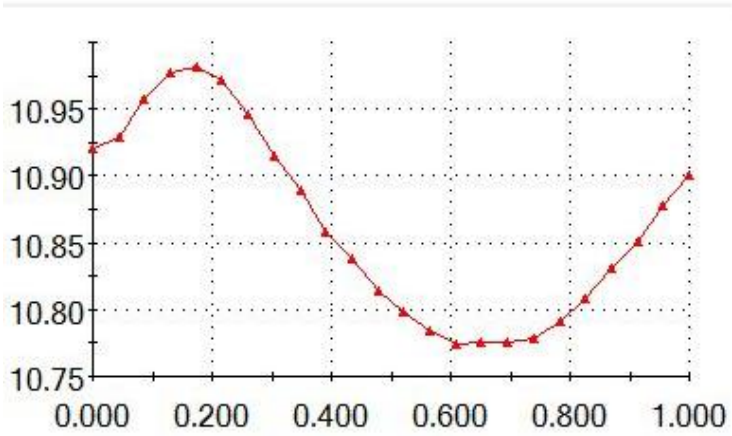
Проведен е числен експеримент, симулиращ работата на АБ при следните стойности на основните параметри на конструкциите цангови патронници: номинален диаметър на повърхнината на затяганата заготовка d = 96 mm; осова теглеща сила SΣ = 50000 N; Якостна проверка на конструкциите АБ се прави въз основа на диаграмите за разпределение на еквивалентните напрежения по von Mises, графика 1(деформация), 2(изместване), 3(натиск).

Таблица 1:
Резултати от РНДСИ- 5К.

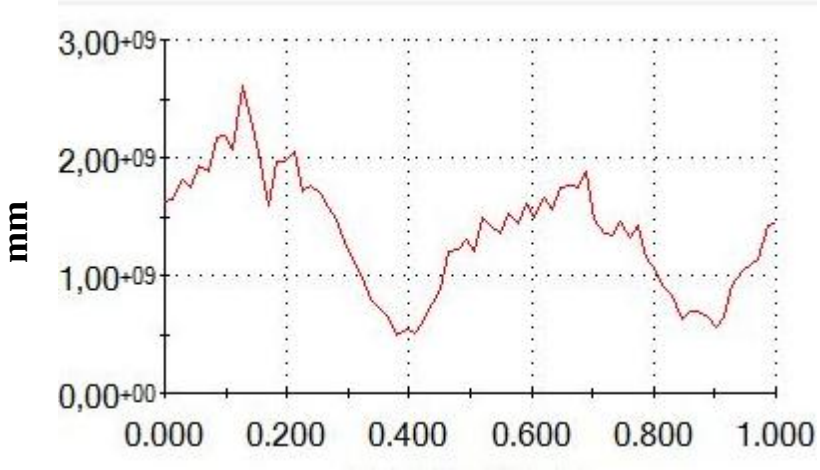
№	НАИМЕНОВАНИЕ		РЕЗУЛТАТ
1.	Тангенциалното напрежение		555 Mp_a
2.	Дебелина на стената на горивната камера б		1,86 mm
3.	Външния диаметър d		169 mm
4.	Осевото напрежение @z		223 Mp_a
5.	Масата на горивната камера q		5 kg
6.	Еквивалентното напрежение @екв.		492 Mp_a



Граф.1 Деформация породена в специфичен участък на барутно – ракетен двигател



Граф.2 Изместване породено в специфичен участък на барутно – ракетен двигател



Граф.3 Натиск породен в специфичен участък на барутно – ракетен двигател

Изводи

1 Разработената методика за проектиране позволява симулиране на динамичните характеристики на БРД, при различни конструктивни разчети.

2. Разработените параметрични крайно-елементни модели на конструкциите БРД дават възможност за изследване и анализ на динамичните им характеристики и оптимизиране на геометрията с цел стабилизиране на системата.

References

1. Antonov S., Tsonev T., (2016) Possibilities for automation of designing elements of small arms using CAD/CAM/CAE systems, Collection of papers: „Defense And Security, Mechanical Engineering And Military Technology, Communication And Computing Technologies, Social Science“, Shumen, Bulgaria 2016, p.p. 319-324, ISSN 2367-7902
2. Antonov S., (2017) Comparative analysis of the armament and equipment support modules in the field of command and control information systems of NATO armies, International Scientific Journal "SECURITY & FUTURE", Year I, Issue 4, p.p. 163-167, (2017), WEB ISSN 2535-082X; PRINT ISSN 2535-0668
3. Petrov Zh., Liliana Miron, (2019), Opportunities of a genetic algorithm for static calibration of mems accelerometers, International Annual Scientific Conference Aviation Faculty, National Military University, 2019, p. 246, ISBN 978-954-713-123-1
4. Petrova T., (2019), Application of geometrical transformations for the atachment of images to geographical maps // 21st International scientific conference: The teacher of the future, Budva, Montenegro, (07-09.06.2019), Institute of knowledge management – Skopje, Macedonia, 31, 2019, 6, pp.1917-1922, ISSN1857-923X (for e-version), ISSN 2545 – 4439 (for printed version)
5. Petrova T., (2019), Research on algorithms for filtration of aerial and radar images // 21st International scientific conference: The teacher of the future, Budva, Montenegro, (07-09.06.2019), Institute of knowledge management – Skopje, Macedonia, 31, 2019, 6, pp. 1923-1936, ISSN 1857-923X (for e-version), ISSN 2545 – 4439 (for printed version).

Plamen A. Ananiev,

COMPARISION OF DISCRETE SINE TRANSFORM BASED OFDM WITH DFT

Plamen A. Ananiev

29 "L. Karavelov" str., Sofia, Bulgaria, e-mail: pananiev@gmail.com

***Abstract**: The performance of high data rates communication systems is limited by frequency selective multipath fading which results in intersymbol interference (ISI). In the wireless channels, impairments such as fading, shadowing and interferences due to multiple user access highly degrade the system performance. As all the subcarriers are orthogonal to each other, they can be transmitted simultaneously over the same bandwidth without any interference which is an important advantage of OFDM. OFDM makes the high speed data streams robust against the radio channel impairments. OFDM is an efficient technique to handle large data rates in the multipath fading environment which causes ISI. With the help of OFDM, a large number of overlapping narrowband subcarriers, which are orthogonal to each other, are transmitted parallel within. the available transmission bandwidth. Thus, in OFDM, the available spectrum is utilized efficiently. The main aim of this paper is to examine BER vs. SNR performance of conventional DFT based OFDM system and DST based OFDM over different type of channel.*

***Keywords**: Orthogonal Frequency Division Multiplexing, Peak to Average Power Ratio, discrete sine transform (DST), discrete Fourier transform (DFT).*

Introduction

With the rapid growth in technology, the demand for flexible high data-rate services has also increased. The performance of high data rates communication systems is limited by frequency selective multipath fading which results in intersymbol interference (ISI). In the wireless channels, impairments such as fading, shadowing and interferences due to multiple user access highly degrade the system performance. Multicarrier modulation (MCM) is a solution that overcomes these problems in wireless channels. It is the technique of transmitting data that divides the serial high data rate streams into a large number of low data rate parallel data streams. OFDM)is a kind of multi-carrier modulation, which divides the available spectrum into a number of parallel subcarriers and each subcarrier is then modulated by a low rate data stream at different carrier frequency. The conventional OFDM system makes use of IFFT and FFT for multiplexing the signals and reduces the complexity at both transmitter and receiver.

OFDM is comprised of a blend of modulation and multiplexing. The original data signal is split into many independent signals, each of which is modulated at a different frequency and then these independent signals are multiplexed to create an OFDM carrier. As all the subcarriers are orthogonal to each other, they can be transmitted simultaneously over the same bandwidth without any interference which is an important advantage of OFDM. OFDM makes the high speed data streams robust against the radio channel impairments.

PAPR PROBLEM OF OFDM SIGNALS

Orthogonal frequency division multiplexing (OFDM) is one of the most promising techniques for high data rate transmission systems. It is currently the standard of IEEE 802.11a(Wi-Fi) Wireless LANs and is also being used for digital terrestrial television transmissions as well as digital audio broadcasting (DAB) digital radio . It is a parallel transmission scheme in which a single channel utilizes multiple sub-carriers on adjacent frequencies. It uses the spectrum much more efficiently by spacing all the channels more close and orthogonal. It offers high spectral efficiency, high data rate, low complexity for receivers and robustness against narrow band interference and frequency selective fading.

In spite of the advantages listed above, High Peak to Average Power Ratio (PAPR) is the major drawback of OFDM at the transmitter side. These peak values in the signal may make the high power amplifiers in the non-linear region and hence distort the signal. So, reduction in the value of PAPR is the major concern. Many PAPR reduction methods are proposed for its mitigation. These methods are divided into three categories. The first category is signal distortion techniques under which clipping, peak windowing techniques are included. The second category includes coding techniques like Block Coding, Transform techniques like Hadamard Transform, Companding, and Discrete Sine Transform (DST). The third category is scrambling techniques which includes selected mapping (SLM) and Partial Transmit Sequence (PTS).

DST BASED OFDM SYSTEM

Instead of using complex exponential functions, sinusoidal functions can be used as orthogonal basis to implement multi-carrier scheme. This can be synthesized using discrete sine transform (DST). For fast implementation algorithms DST can provide fewer computational steps than FFT based OFDM [3]. The effect of carrier frequency offset (CFO) will introduce inter-carrier interference (ICI) in both the DFT-OFDM and DST-OFDM. A single sinusoidal functions set $sin2\pi n\Delta Ft$ will be used as the orthogonal basis to implement MCM in DST-OFDM. The minimum ΔF required to satisfy Eq. (1) is 1/2T Hz [4].

$$\int_0^T \frac{2}{T} sin2\pi F_k t \; \frac{2}{T} sin2\pi F_m t dt = \begin{matrix} 1, k = m \\ 0, k \neq m \end{matrix} \quad (1)$$

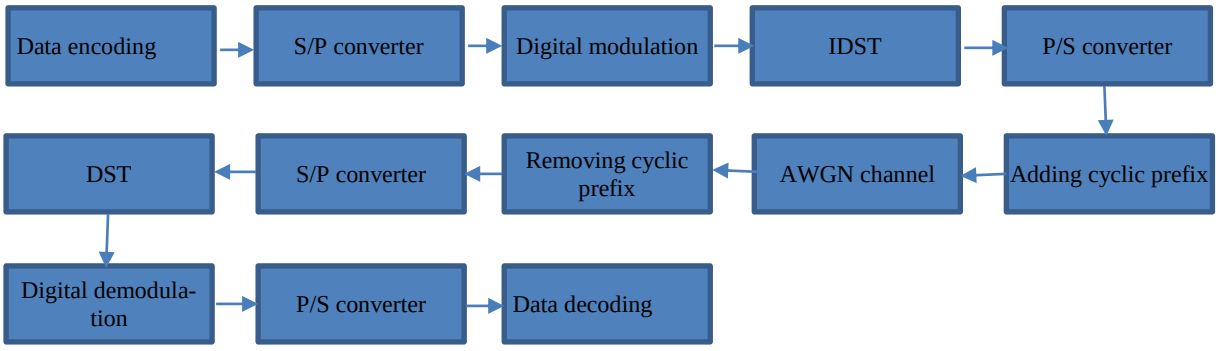


Figure 1. Block Diagram for Improved DST Based OFDM System

The Fig 1 block diagram based implementation involves separate sets of blocks which are:

Input module for OFDM system:

- Data encoding
- Serial to parallel converter

- Digital modulation
- Inverse Discrete Cosine Transform
- Parallel to series converter
- Adding Cyclic Prefix

Output Module for OFDM output:

- The Channel
- Inverse Cyclic Prefix
- Series to parallel converter
- Discrete Cosine Transform
- Digital demodulation
- Parallel to series converter
- Data decoding

Implementation Details.

Data encoding

Diferent modulation schemes can be used with DST based OFDM: On – Off keying, Amplitude shift keyng (ASK), Binary Phase Shift Keying (BPSK), Quadrature amplitude modulation (QAM) [1], [2], [5], [6].

Quadrature amplitude modulation (QAM) is both an analog and a digital modulation scheme. It c on ve ys two analog message signals, or two digital bit streams, by changing (modulating) the amplitudes of two carrier waves, using the amplitude-shift keying (ASK) digital modulation scheme or amplitude modulation (AM) analog modulation scheme. The two carrier waves, usually sinusoids, are out of phase with each other by 90° and are thus called quadrature carriers or quadrature components — hence the name of the scheme. The modulated waves are summed, and the resulting waveform is a combination of both phase-shift keying (PSK) and amplitude-shift keying (ASK), or (in the analog case) of phase modulation (PM) and amplitude modulation. In the digital QAM case, a finite number of at least two phases and at least two amplitudes are used.

Serial to Parallel Converter

The Serial to Parallel Converter converts the incoming serial data into parallel In-phase and Quadrature components which are 90 degrees out of phase so that real part can be separated from the imaginary part and a faster transmission can be achieved.

Constellation Mapping and De-mapping

The QAM technique involves constellation mapping of signal components using constellation diagram. A constellation diagram is a representation of a signal modulated by a digital modulation scheme such as quadrature amplitude modulation or phase-shift keying. By representing a transmitted symbol as a complex number and modulating a cosine and sine carrier signal with the real and imaginary parts (respectively), the symbol can be sent with two carriers on the same frequency. On the contrary, De-mapping just de-maps the constellation binary symbol components back to their original binary form. The constellation diagram for 16 bit QAM can be shown as below.

Symbol Generator and De-Generator

The symbol generator validates the input given to it and generates valid symbols only to be passed on the DST block. These symbols are binary symbols of course. The de-generator just converts the received noisy signal in the form required to be an input for the QAM block.

Zero Padding and Un-padding

Zero Padding is a technique involved to separate streams of data. The stream of data is padded with zeros both before and after the data, so that every two streams of data is separated and a proper transform can be performed. In this implementation, zero padding is 32 bits wide. So, every data stream, which is 64 bits, has 32 plus 32 zero padded bits ahead of and after it respectively.

DST and Inverse Discrete Sine Transform (IDST)

The multiple orthogonal subcarrier signals, which are overlapped in spectrum, need to be produced at the transmitter side. In practice, Discrete Sine Transform (DST) and Inverse DST (IDST) processes are useful for implementing these orthogonal signals. In the OFDM transmission system, N point IDST is taken for the transmitted symbols so as to generate the samples for the sum of N orthogonal subcarrier signals. The receiver will receive a sample corrupted by additive noise. Taking the N-point DST of the received samples the noisy version of transmitted symbols can be obtained in the receiver.

Cyclic Prefix and Inverse Cyclic Prefix

The OFDM scheme also inserts a guard interval in the time domain, called cyclic prefix (CP), which mitigates the inter-symbol interference (ISI) between OFDM symbols. Once the signal is received by the receiver, the effect of ISI is over and thus the cyclic prefix is removed by using Inverse Cyclic Prefix.

Output Module for OFDM output

The Output Module acts as an OFDM signal generating module, which apart from generating the OFDM output, filters the unwanted cosine terms from the Cyclic prefixed data. This OFDM output is passed on to the receiver through the channel.

The Channel

The channel is just a transmission medium between the transmitter and the receiver in which the data flows. The OFDM output generated is passed on to the receiver through the channel.

Parallel to Serial Converter

The Parallel to Serial Converter converts the incoming parallel data components which are 90 degrees out of phase into serial output data so that it matches the input data destined for the receiver, along with noise signals.

Bit interleaving

In order to maximize the diversity in a fading channel, the error correction coding coupled with interleaver is used. It separates the adjacent coded symbols farther than the coherence time of fading process by creating large Euclidean distance between the code words of a convolution code. The burst errors occurring in the channel or caused by the detector on the receiver side are dispersed by a de-interleaver at the receiver.

RESULT AND CONCLUSION

In this work, the conventional DFT based OFDM system using DPSK modulation technique under AWGN channel has been considered to evaluate the performance of the proposed DST based OFDM system. MATLAB simulation has been carried out to compare the performance of DFT OFDM with DST OFDM system.

Comparison of DST based OFDM with DFT

The simulation results are presented as follows (fig 2, fig.3):

Figure 2 shows the performance of DST OFDM and DFT OFDM system under AWGN channel using BPSK modulation As shown in figure, the BER of the OFDM system is exactly the same when DFT is replaced by DST while BER is plotted as a function of SNR.

Figure 3 shows the performance of DST OFDM and DFT OFDM system under AWGN channel using OOK modulation.

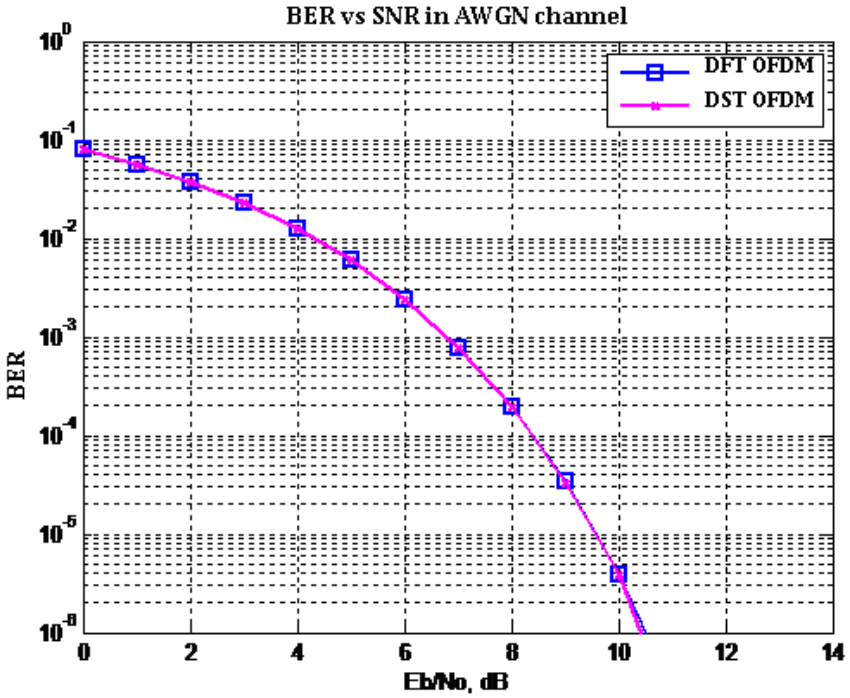


Figure 2. Performance of DST OFDM and DFT OFDM system under AWGN Channel with BPSK modulation

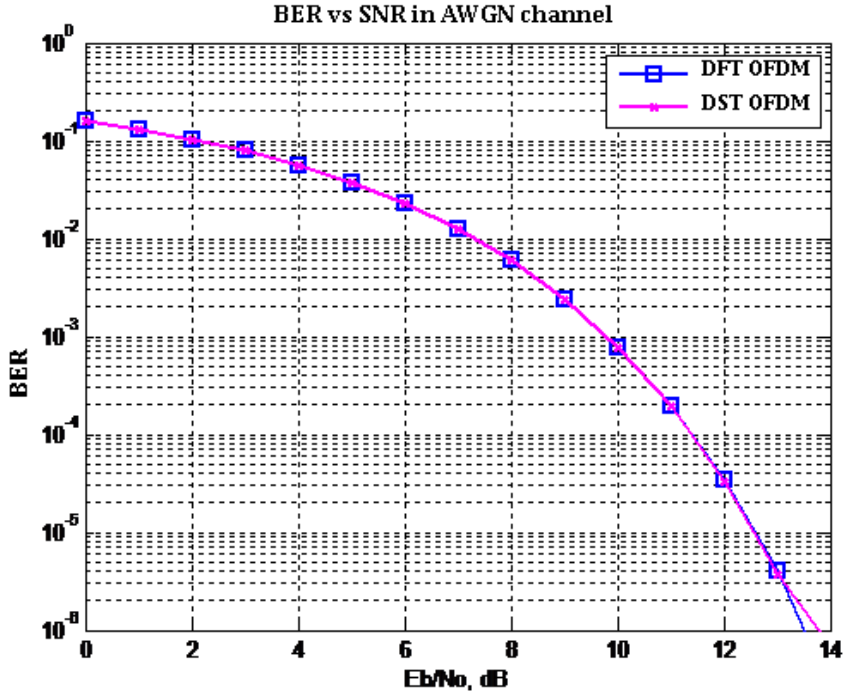


Figure 3. Performance of DST OFDM and DFT OFDM system under AWGN Channel with OOK modulation

References

[1] Rashmi, Sowmya, Nagaraja N. S. , „Comparision of discrete cosine transform based OFDM with DFT”, International Research Journal of Engineering and Technology (IRJET) Volume: 05 Issue: 07 | July 2018, pp. 594 – 597, e-ISSN: 2395-0056, p-ISSN: 2395-0072

[2] Чобанов Д. Г., „Ортогонално честотно разделяне и мултиплексиране с честотно отстояние между подносещите 1/2T, и M – кратна амплитудна манипулация“, Сборник доклади TechCo – Lovech 2019 том 1, с. 67 – 72, Университетско издателство “Васил Априлов” – Габрово, ISSN 2535-079X

[3] Чобанов Д. Г., „Алгоритъм за бързо синусово преобразувание“, Сборник доклади TechCo – Lovech 2019 том 1, с. 73 – 76, Университетско издателство “Васил Априлов” – Габрово, ISSN 2535-079X

[4] Чобанов Д. Г., „Ортогонално честотно разделяне и мултиплексиране базирано на дискретно синусово преобразование“, Сборник доклади от годишна университетска научна конференция 27 – 28 юни 2019 година, том 11, с. 83 – 87, Издателски комплекс на НВУ „В. Левски“, ISSN 1314 – 1937

[5] Чобанов Д. Г., „Система с ортогонално честотно разделяне и мултиплексиране базирана на дискретно синусово преобразование и “on-off keying” модулация на подносещите”, Сборник доклади от годишна университетска научна конференция 27 – 28 юни 2019 година, том 11, с. 88 – 94, Издателски комплекс на НВУ „В. Левски“, ISSN 1314 – 1937

[6] Чобанов Д. Г., „Система с ортогонално честотно разделяне и мултиплексиране базирана на дискретно синусово преобразуване при двукратна фазова манипулация на подносещите”, Сборник доклади от годишна университетска научна конференция 27 – 28 юни 2019 година, том 11, с. 95 – 101, Издателски комплекс на НВУ „В. Левски“, ISSN 1314 – 1937

Borislav A. Minchev,

IMPLEMENTATION AND CONTRASTING COMPARISION OF TRANSFORM TECHNIQUES OF OFDM

Borislav A. Minchev

Drujba – 1 Residential Quarter, Building 4, Sofia, Bulgaria, e-mail: boby_al@mail.bg

***Abstract**: Different type of transform techniques such as Discrete Hartley transform (DHT), Discrete Sine Transform (DST), Fast Fourier Transform (FFT) and their inverse are used for the fast computational algorithms in digital signal processing. These transforms are used to perform the modulation and demodulation operations for the OFDM system. In this paper the three transforms are describe, these transforms are used in OFDM and shows the comparison between these different schemes used in OFDM system and also the simulation results based on the BER performances.*

***Keywords**: DST, DHT, FFT, ICI, ISI, OFDM.*

Introduction

The different transforms used in this paper have their own applications, pros and cons in digital signal processing. These transforms have a wide importance in the orthogonal frequency division multiplexing. These transforms are adopted in OFDM because of their multiplexing and demultiplexing and because of their less computational time. A Fast Fourier Transform (FFT) is an efficient algorithm to compute the discrete Fourier transform (DFT) and its inverse. The Discrete Fourier Transform (DFT) is used to produce frequency analysis of discrete non-periodic signals. The FFT is a faster version of the Discrete Fourier Transform (DFT). The FFT utilizes some clever algorithms to do the same thing as the DTF, but in much less time.

The Discrete Hartley Transform is closely related to the Discrete Fourier Transform, but unlike the DFT, the DHT has the advantage of producing real numbers and it is (quasi-)symmetrical. The Hartley transform produces real output for a real input, and is its own inverse. It therefore can have computational advantages over the discrete Fourier transform.

The DST has found wide applications in image/video processing and other fields. Discrete sine transforms (DSTs) express a function or a signal in terms of a sum of sinusoids with different frequencies and amplitudes. A DST operates on a function at a finite number of discrete data points. The obvious distinction between a DST and a DFT is DST uses only sine functions, while DFT uses both cosines and sines[3]. DST implies different boundary conditions than the DFT or other related transforms. DST is used in JPEG image compression, MJPEG, MPEG, and DV video compression.

The modified discrete sine transform, or MDST is used in AAC, Vorbis and MP3 audio compression.

OFDM is the modulation technique used in many new and emerging broadband communication systems including wireless local area networks (WLANs), high definition television (HDTV) and 4G systems. To achieve high data rates OFDM is used in wireless LAN standards like IEEE 802.11a, IEEE 802.11g. Orthogonal Frequency Division Multiplexing (OFDM), which allows the overlapping of the subcarriers but keeps them orthogonal to avoid intercarrier interference (ICI) and inter-symbol interference (ISI) [1], has been adopted for mobile communication standards due to its ability to combat with the frequency-selective multipath fading channel effects and has high spectral efficiency. OFDM is robust against narrowband interference because such interference affects only a small percentage of the

subcarriers; also it increases robustness against frequency-selective fading. This paper considers the different sections which are – 2. OFDM system model, 3- Comparision between transforms used in OFDM, 4-simulation results, and 5- Conclusion.

Ofdm system model

Fast fourier transform (FFT)

The fast Fourier transform (FFT) is merely a rapid mathematical method for computer applications of DFT. It is the availability of this technique, and the technology that allows it to be implemented on integrated circuits at a reasonable price, that has permitted OFDM to be developed as far as it has. The main reason that the OFDM technique has taken a long time to become a prominence has been practical. It has been difficult to generate such a signal, and even harder to receive and demodulate the signal. The hardware solution which makes use of multiple modulators and demodulators. At the transmitter, the signal is defined in the frequency domain. It is a sampled digital signal, and it is defined such that the discrete Fourier spectrum exists only at discrete frequencies. Each OFDM carrier corresponds to one element of this discrete Fourier spectrum. The amplitudes and phases of the carriers depend on the data to be transmitted. The data transitions are synchronized at the carriers, and can be processed together, symbol by symbol. The FFT is a faster version of the Discrete Fourier Transform (DFT). FFTs are of great importance to a wide variety of applications, from digital signal processing to solving partial differential equations to algorithms for quickly multiplying large integers.

Let $x_0, \dots \dots . x_{N-1}$ be complex numbers. The DFT is defined by the formula (1):

$$X_k = \sum_{n=0}^{N-1} X_n e^{-\frac{2\pi}{N} nk} \quad (1)$$

where $k = 0 \dots N-1$

Evaluating these sums directly would take O(N^2) arithmetical operations An FFT is an algorithm to compute the same result in only O($N\ log\ N$) operations. In general, such algorithms depend upon the factorization of *N*, but there are FFTs with O($N\ log\ N$) complexity for all *N*, even for prime *N*. Many FFT algorithms only depend on the fact that $e^{-\frac{2\pi i}{N}}$ is a primitive root of unity. Since the inverse DFT is the same as the DFT, but with the opposite sign in the exponent and a $\frac{1}{N}$ factor, any FFT algorithm can easily be adapted for it as well.

Discrete Hartley transform

A discrete Hartley transform (DHT) is a Fourier-related transform of discrete, periodic data similar to the discrete Fourier transform (DFT), with analogous applications in signal processing and related fields. Its main distinction from the DFT is that it transforms real inputs to real outputs, with no intrinsic involvement of complex numbers. Just as the DFT is the discrete analogue of the continuous Fourier transform, the DHT is the discrete analogue of the continuous Hartley transform, introduced by R. V. L. Hartley in 1942.

Because there are fast algorithms for the DHT analogous to the fast Fourier transform (FFT), the DHT was originally proposed as a more efficient computational tool in the common case where the data are purely real. It was subsequently argued, however, that specialized FFT algorithms for real inputs or outputs can ordinarily be found with slightly fewer operations than any corresponding algorithm for the DHT. Formally, the DHT is a linear, invertible function $H\ R^n \rightarrow R^n$, where *R* is the set of real numbers. The N real numbers $x_0, \dots x_{N-1}$ are transformed into the *N* real numbers $H_0, \dots H_{N-1}$ according to the formula (2).

$$H_k = \sum_{n=0}^{N-1} x_n \left(cos\frac{2\pi}{N} nk + sin\frac{2\pi}{N} nk \right) \quad (2)$$

where $k = 0 \ldots N-1$

The IDHT is given by (3):

$$X_n = \frac{1}{N} \sum_{k=0}^{N-1} H_k \ \ cos\frac{2\pi}{N}nk + sin\frac{2\pi}{N}nk \quad (3)$$

where $n = 0 \ldots N-1$

The overall scale factor in front of the transform and the sign of sine term are differ and it does not affect the essential properties and it is matter of convention.

Discrete sine transform (DST)

A discrete sine transform (DST) is a Fourier-related transform similar to the discrete Fourier transform (DFT), but using only real numbers. DSTs are equivalent to DFTs of roughly twice the length, operating on real data with even symmetry (since the Fourier transform of a real and even function is real and even), where in some variants the input and/or output data are shifted by half a sample. The Discrete Sine Transform (DST) attempts to uncorrelated the image data. After decorrelation each transform coefficient can be encoded independently without losing compression efficiency.The DFT, like the Fourier series, implies a periodic extension of the original function. A DST, like a sine transform, implies an even extension of the original function.

However, because DSTs operate on finite, discrete sequences, two issues arise that do not for the continuous sine transform. First, one has to specify whether the function is even or odd at both the left and right boundaries of the. Second, one has to specify around what point the function is even or odd. In particular, consider a sequence *abcd* of four equally spaced data points, and say that we specify an even left boundary. There are two sensible possibilities: either the data is even about the sample a, in which case the even extension is *dcbabcd*, or the data is even about the point halfway between a and the previous point, in which case the even extension is *dcbaabcd* (a is repeated). Its DST is given by (4)[3]:

$$x_k = \sum_{n=1}^{N-1} sin\frac{\pi \ \ 2n+1 \ \ k}{2N} \quad (4)$$

where $k = 0 \ldots N-1$

And IDST is given by (5)[3]:

$$x_n = \sum_{k=1}^{N-1} sin\frac{\pi \ \ 2n+1 \ \ k}{2N} \quad (5)$$

where $n = 0 \ldots N-1$

The above two equations are the OFDM system transmitter and receiver sections. The IDST is perform by N*N DST matrix at receiver which is orthogonal to IDST, it recovers the original transmitted sequence.

Comparision of different transform scheme used in OFDM

PARAMETERS	FFT	DHT	DST
Pulse shaping	Required	Required	Required
Symmetric Extension	Not Required	Not Required	Required
Cyclic Prefix	Required	Required	Required
Transform	Complex valued	Real valued	Real valued
Implementation Complexity	Less	Less	Less

Time-Frequency Resolution	Fixed	Dynamic	Fixed

Simulation results

In the OFDM system implementation FFT, DST, DHT wereused to perform the modulation and demodulation operations. As possible modulation schemes OOK, BPSK, ASK are used as digital modulation technique[2], [4], [5], [6]. For OFDM-based transceivers, the modulator needs to compute a long-length inverse transform and the demodulator needs to compute a long length transforms, where the transform lengthis up to 512 or more. Software used for simulation is MATLAB R2018b. Simulation results show that the BER of the OFDM system is exactly the same when DFT is replaced by DST while BER is plotted as a function of SNR.

Conclusion

OFDM is a widely used and important modulation technique. It is computationally efficient because of FFT techniques. Using MATLAB software, the performance of OFDM system is taken for three different transform techniques namely FFT, DHT, and DST. By simulation results, it observed that BER is improved in noisy channel by using BPSK at maximum data transmission capacity. DST implies different boundary conditions than the DFT or other related transforms because of real valued nature and strong energy compaction property. DHT based OFDM, due to its real valued it require less computation complexity and implementation cost. From the results, it conclude that DHT,DST transform technique may be alternative of DFT for implementation of OFDM – based communication systems.

References

[1]. Gupta N., Saxena. D.K., „Implementation and Contrasting Comparision of Transform Techniques of OFDM”, International Journal of Computer Applications (0975 – 8887), Volume 72– No.19, June 2013, pp. 47 - 50

[2] Чобанов Д. Г., „Ортогонално честотно разделяне и мултиплексиране с честотно отстояние между подносещите 1/2T, и M – кратна амплитудна манипулация“, Сборник доклади TechCo – Lovech 2019 том 1, с. 67 – 72, Университетско издателство “Васил Априлов” – Габрово, ISSN 2535-079X

[3] Чобанов Д. Г., „Алгоритъм за бързо синусово преобразувание“, Сборник доклади TechCo – Lovech 2019 том 1, с. 73 – 76, Университетско издателство “Васил Априлов” – Габрово, ISSN 2535-079X

[4] Чобанов Д. Г., „Ортогонално честотно разделяне и мултиплексиране базирано на дискретно синусово преобразование“, Сборник доклади от годишна университетска научна конференция 27 – 28 юни 2019 година, том 11, с. 83 – 87, Издателски комплекс на НВУ „В. Левски“, ISSN 1314 – 1937

[5] Чобанов Д. Г., „Система с ортогонално честотно разделяне и мултиплексиране базирана на дискретно синусово преобразование и “on-off keying” модулация на подносещите”, Сборник доклади от годишна университетска научна конференция 27 – 28 юни 2019 година, том 11, с. 88 – 94, Издателски комплекс на НВУ „В. Левски“, ISSN 1314 – 1937

[6] Чобанов Д. Г., „Система с ортогонално честотно разделяне и мултиплексиране базирана на дискретно синусово преобразуване при двукратна фазова манипулация на подносещите”, Сборник доклади от годишна университетска научна конференция 27 – 28 юни 2019 година, том 11, с. 95 – 101, Издателски комплекс на НВУ „В. Левски“, ISSN 1314 – 1937

Rosen A. Bogdanov, Nikolay Zh. Kulev, Miroslav G. Nedelchev,

ESTIMATION OF DIRECTIONS OF ARRIVAL, APPLIED TO FIFTH GENERATION NETWORKS

Rosen A. Bogdanov, Nikolay Zh. Kulev, Miroslav G. Nedelchev

Communication Networks and Systems Department, Artillery, Air Defense Communication and Information Systems Faculty, National Military University „V. Levski", Shumen, Bulgaria

rab61@abv.bg, nz_kulev@abv.bg nedel4ew@abv.bg

МЕТОДИ ЗА ОЦЕНКА НА ЪГЛИТЕ НА ПОСТЪПВАНЕ НА СИГНАЛИТЕ, КОИТО СЕ ПРИЛАГАТ В МРЕЖИТЕ ОТ ПЕТО ПОКОЛЕНИЕ

Росен А. Богданов, Николай Ж. Кулев, Мирослав Г. Неделчев

Катедра „Комуникационни мрежи и системи", Факултет „Артилерия, протововъздушна отбрана, комуникационни и информационни системи", гр. Шумен, България

rab61@abv.bg, nz_kulev@abv.bg nedel4ew@abv.bg

***Abstract**: This paper presents an overview of estimation methods and techniques of narrowband direction of arrival and effective beamforming which represent spatial diversity, and mitigate spectrum use. There are numerous algorithms for generating different diagrams and beamforming, which used massive MIMO antennas and can be represented in fifth generation wireless cellular communication systems.*

***Keywords**: 5G, massive MIMO, beamforming, DOA estimation, MUSIC*

I. УВОД

В настоящия доклад са представени някои от методите за оценка на ъгъла на постъпване при детектиране на сигнали в условията на усложнена електромагнитна среда.

С развитието на безжичните комуникации, очакванията към системите от следващо поколение са за скорост от порядъка на 1 Gb/s в DL и 500 в Mb/s UL и изискванията към ъгловата разделителна способност, при оценка ъглите на постъпване в мрежите от пето поколение са завишени в сравнение с предходните стандарти. 3GPP дефинира следните изисквания [4]:

- за подвижно потребителско оборудване със скорост до 0,5 m/s – 5˚
- за подвижно потребителско оборудване със скорост до 10 km/h – 10˚
- за неподвижно потребителско оборудване – 30˚

В 4G мрежите такива изисквания не са предвидени и това налага напълно нови решения на проблема с определяне на ъгъла на постъпване и адаптивна промяна на излъчвания от антените лъч. Възможно решение предоставят многомерните (massive) MIMO антени, които значително повишават съотношението С/Ш, осигурява възможността за подобряване и ефективно използване на спектралните ресурси и са предпоставка за успешна борба с многолъчевостта [2].

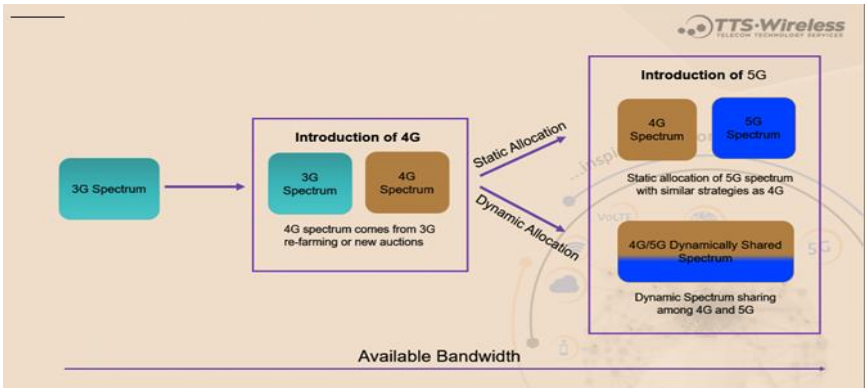
Определянето на ъгъла на постъпване по същество представлява техника за обработка на сигнала, която извършва оценка на местоположението на постъпващите от кореспондента елект-

ромагнитни вълни, докато адаптивната промяна на широчината и формата на ДНД е техника за сформиране и управление на излъчването, така че да се максимизира енергията в желаната посока и подтиснат страничните листи или излъчванията в нежелана посока [3].

Чрез комбиниране на двете техники се осигурява пространственото разнасяне, което е едно от основните предимства на massive MIMO технологията и има за цел да подобри надеждността на системата, като изпраща данни с минимална интерференция по различни пътища в пространството, което осигурява пространствено мултиплексиране.

Усложняването на процеса по определяне на местоположението при динамично уплътняване на честотния спектър, използван от когнитивни потребители и мрежите от пето поколение е вследствие на непрекъснатото движение на мобилния потребител и промените в заобикалящата среда, потребителското оборудване и мрежата изискват по-разширени възможности за непрекъснато координиране на връзката и управление на предаването на данни, с което да се постигне подобрена производителност [1].

На фигура 1 [5] е представено използването на честотните ресурси в мрежите от трето, четвърто и пето поколение.



Фигура 1. Използване на спектъра за мрежите от трето, четвърто и пето поколение

II. ТЕХНИКИ ЗА ОПРЕДЕЛЯНЕ НА ЪГЛИТЕ НА ПОСТЪПВАНЕ

Важно условие при формирането и управлението на лъч в базовата станция е наличието на система за оценка на ъгъла на постъпване, то се базира на измерване на закъсненията от постъпващите в антенните елементи вълни.

Съществуват различни методи за оценка на посоката приемане, като най - общо се разделят в четири групи [7]:

- Конвенционални техники – основаващи се на класическите техники за формиране на лъчи;
- Пространствени техники – се основават на неоптималното приемане на сигнали с висока резолюция, използващи структурата на матрицата от входни данни.
- Техники базиращи се на максималното правдоподобие - оптимални техники, които се характеризират с висока ефективност при ниски стойности на SNR и подлежат на лесна изчислителна обработка;
- Комбинирани техники - използват обработка на сигнала получен въз основа на възстановяването на постъпилите отразени сигнали и определяне на най- вероятното местоположение, чрез използване на пространствените техники.

Определянето на времезакъснението Δt_k в общия случай се извършва по следния начин:
В многомерна антенна решетка с M на брой елемента приема сигнали от L източници. Разстоянието между елементи от масива е d, а N е броя на отчетите и всички предаватели излъчват в тясна лента.

Фазата на сигнала в основната лента *s(t)*, приет в елемент *M=0* се приема за нула. За да се измери фазовата разлика в *k*-тия елемент е необходимо да се измери разликата във времето, в което сигналът *s(t)* постъпва в нулевият елемент и времето в *k*-тия елемент.

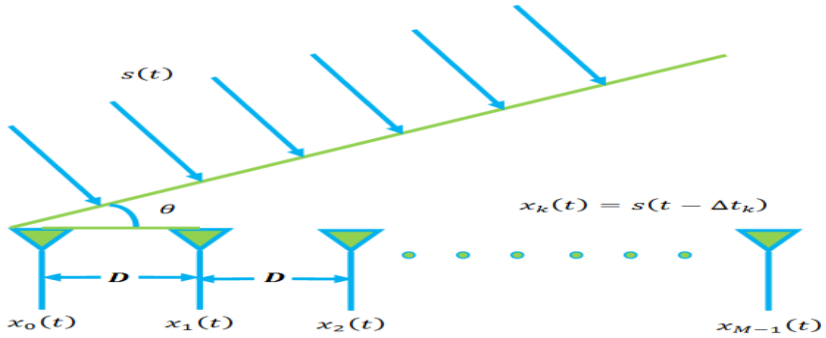
От фигура 1 е показан вариант с линейно разположени елементи и закъснението между *0*-вия *и k*-тия елемент, което може да се определи чрез тригонометричната зависимост

$$\Delta t_k = \frac{k\, D \sin\theta}{c} \qquad (1)$$

където *c* е скоростта на светлината.

За реален теснолентов сигнал с период на повторение *T* и носеща честота f_c, модулирана с $s_l(t)$ може да се запише

$$s\ t\ = \mathrm{Re}\ s_l(t)e^{j2\pi f_c t} \qquad (2)$$



Фигура 2. Линейно разположени елементи

За приетият в *k*-тия елемент сигнал може да се запише

$$x_k\ t\ = \mathrm{Re}\ s_l(t-\Delta t_k)e^{j2\pi f_c(t-\Delta t_k)} \qquad (3)$$

За дискретни сигнали при известна дължина на вълната и разстояния между елементите е в сила [6].

$$x_k\ n\ \approx s\ n\ e^{-j\pi k\sin\theta} = a_k(\theta)s\ n \qquad (4)$$

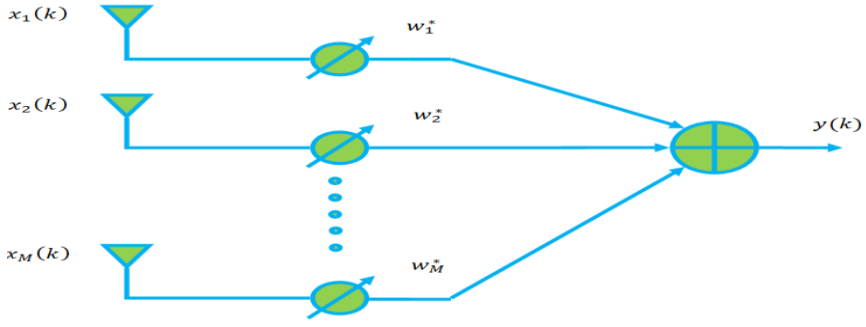
където $a_k(\theta)$ представлява управляващия (насочващ) вектор;

1. Конвенционални техники

Техниките за конвенционална обработка на оценката на ъгъла на приемане се основават по същество на форматирането на лъчи и определяне на техните закъснения и минималното отклонение без изкривяване или сканирането на лъч през пространството, както и измерване на получената от всеки ъгъл мощност. Решението за определяне на местоположението се определя от посоката с най-голяма стойност на мощността.

На фигура 2 е представен обобщен класически модел на антенна решетка за формиране на лъч за оценка на ъгъла на постъпване.

Изходният сигнал *y(k)* се получава чрез линейно сумиране на тегловите коефициенти, получени от изходите на елементите, в които е постъпил отразен сигнал.



Фигура 3. Модел за формиране на лъчи

Така може да се запише [6]

$$y\ k\ = \ w^{H}x(k) \tag{5}$$

Мощността излъчвана от конвенционален източник може да се запише, като

$$P = E\ \ y\ k\ ^{2}\ \ = E\ \ w^{H}x\ k\ ^{2}\ \ = w^{H}E\ \ x(k)x^{H}(k)\ w\ \ = w^{H}R_{xx}w \tag{6}$$

където R_{xx} е автокорелационната матрица на масива от постъпваща полезна информация. Чрез внимателна оценка на тази матрица е възможно да се определи вектора на отразения лъч.

Отчитайки постъпилия под ъгъл θ_0 в антенната решетка отразен сигнал *s(k)*, отчитайки (6) може да се запише

$$\begin{aligned} P\ \theta_0\ \ &= E\ \ y\ k\ ^{2}\ \ = E\ \ w^{H}x\ k\ ^{2}\ \ = E\ \ w^{H}(a\ \theta_0\ s\ k\ + n(k)\ ^{2} \\ &= \ w^{H}(a\ \theta_0\ \ ^{2}(\sigma_s{}^{2} + \sigma_n{}^{2})) \end{aligned} \tag{7}$$

където

$a\ \theta_0$ е вектора за управление на лъча, който се определя от алгоритъма за оценка на ъгъла на постъпване;

n(k) постъпилия на входа на антената шум;

$\sigma_s = E\ s(k)^2$ u $\sigma_n = E\ n(k)^2$ представляват мощността на сигнала и шума.

От това се вижда, че мощността се максимизира, когато $w = a(\theta_0)$ и тогава всички теглови коефициенти имат максимална стойност в направление θ_0. Постъпващите сигнали са симфазни и се получава конструктивно сумиране.

Чрез сканиране на даден регион през определени периоди от време и измерване на получената мощност е възможно да се изчислят отделните теглови коефициенти за различни ъгли θ.

Така уравнение (6) може да се запише в следния вид:

$$P = w^{H}R_{xx}w = \alpha^{H}(\theta)R_{xx}a(\theta) \tag{8}$$

Чрез оценка на автокорелационната матрица и известни стойности на управляващия вектор $a(\theta)$ за всички ъгли θ , позволява да се определи пиковата мощност, а от тук и ъгъла на постъпване θ_0.

Недостатъци на конвенционалния метод са слабата ефективност поради ограниченията в широчината на ДНД на лъча и нивата на страничните листи, при получаване на сигнали от различни ъгли на приемане или голям брой източници на енергия. Така разделителната способност е слаба. Възможно подобряване се постига чрез добавяне на допълнителен брой сензорни елементи, но с това следва да се увеличи необходимата памет и изчислителна мощ.

Усъвършенстван конвенционален метод е предложен от Капон. и се основава на определяне на минималната дисперсия и [8] се прилага в опит за преодоляване на проблема с влошената разделителна способност на конвенционалния метод, чрез използване някои степени на свободата при формиране на лъч в желаната посока и едновременно използвайки останалите степени на свобода за свеждане до нули, посоките на смущаващи сигнали.

Това поддържа постоянно усилване в направлението на главния лъч и минимизира изходната мощност на смущаващото оборудване.

$$\min_{w} E\ \ y\ k\ ^{2}\ \ = \min_{w} w^{H}R_{xx}w \tag{9}$$

при условие, че $w^{H}(a\ \theta_0\ \ = 1$

За определяне на мощността се използва следния израз [9] :

$$P_{Capon}(\theta) = \frac{1}{\alpha^{H}(\theta)R_{xx}{}^{-1}a(\theta)} \tag{10}$$

където α^H е постъпилия в антенната матрица отразен вектор за ъгъл θ;

R_{xx} отразява комплексно спрегнатото преобразуване на автокорелационната матрица.

Така метода на Капон с определяне на минималната дисперсия използва за изчисляване комплексно спрегнатата автокорелационна матрица, с което се подобрява разделителната способност, със сравнително малка изчислителна мощ.

2. Пространствени техники

Малката разделителна способност, която се постига с конвенционалния метод за оценка, оказва най-голямо ограничаващо влияние върху широкото му използване при лесната за реализиране изчислителна способност. Това налага да се търсят други техники за оценка на електромагнитната среда. Пространствените техники се базират на оценката на приетия единичен вектор и автокорелационна функция на сигнала и определяне на модел на шума, на базата на които се съставя структурна матрица за генериране на лъчи.

Типичен алгоритъм, които използва пространствени техники е алгоритъма предложен от Шмид през 1979 г. - т. нар. MUSIC (MUltiple SIgnal Classification) алгоритъм [10].

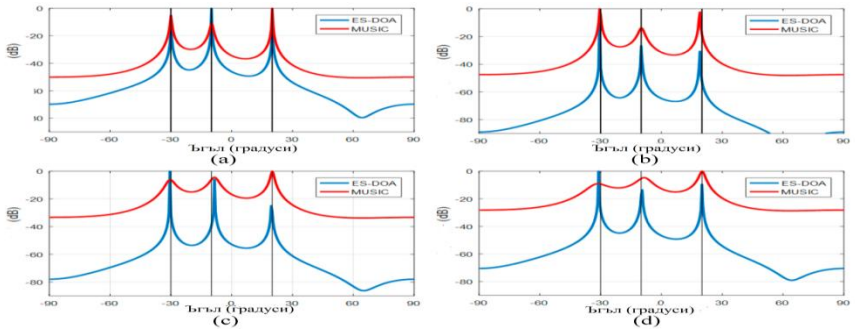
Чрез излъчване на ортогонални сигнали и съставяне на обратна матрица се съставя модел на шума и се определят максималният брой вектори в дадената среда, които са ортогонални на шума. Така при откриване на приет сигнал, кореспондиращ със стойностите на $a(\theta)$ (управляващия вектор), тогава $a(\theta)^H Q_n = 0$, а Q_n задава модела на шума.

Спектъра на сигнала определен, чрез MUSIC алгоритъм се дава с израза [6]:

$$P_{MUSIC}(\theta) = \frac{1}{\alpha^H \ \theta \ {Q_n}^H Q_n \, a(\theta)}$$

Алгоритъма е широко използван заради изключително добрата разделителна способност. Въпреки това не винаги самостоятелното му използване осигурява добра производителност и ефективност при оценка на некорелирани сигнали.

Друго ограничение налага сложността на изчисленията, породено от изчисляване на пиковете стойности на функцията и разходите за реализирането им. Грешно определяне се получава и при неправилна оценка на броя на източниците, вследствие наличието на други ортогонални на първоначално зададените сигнали [11].



Фигура 4. Ъгли на приемане при: a) С/Ш =20dB; b) С/Ш =10dB c) С/Ш =5dB d) С/Ш =0dB [11]

III. ЗАКЛЮЧЕНИЕ

В настоящия доклад са представени два от методите за оценка на ъгъла на постъпване и формиране на остро насочени лъчи с оглед подобряване на електромагнитната обстановка и начин за постигане на желаните в 5G скорости. Лесната реализация и малката изчислителна обработка са предимствата на метода на Капон, но добра разделителна способност се постига с алгоритъм MUSIC включително и при по – ниски стойности на отношението С/Ш. В [12].е доказано,

че с нарастването на броя на елементите в massive MIMO антенните решетки (напр. до 128 повишава не само точността на формиране на лъча (до 4 °), но и разделителната способност, при силно подтискане на интерфериращите лъчи) което отговаря на изискванията на 5G мрежите.

References

1. Д. И. Димитров и Д. К. Хубенов, „Приложение на когнитивното радио при уплътнение на честотния спектър,“ в *Научна сесия ,Сборник част 1*, Шумен, 2014
2. J. H. S. Emil Björnson, Massive MIMO Networks.Spectral, Energy, and Hardware Efficiency, 2017.
3. M. Shukair, „Qualcomm,“ [Онлайн]. Available: https://www.qualcomm.com/news/onq/2019/06/20/how-5g-massive-mimo-transforms-your-mobile-experiences.
4. . 3. T. 2. V16.5.0., „5G;Service requirements for next generation new services and markets,“ 2018.
5. TTSwireless. [Онлайн]. Available: https://www.ttswireless.com/dynamic-spectrum-sharing-within-5g-era/.
6. A. I. Ahmad Zeeshan, „Three Decades of Development in DOA Estimation,“ *TELKOMNIKA Indonesian Journal of Electrical Engineering,* 2014.
7. A. I. Ahmad Zeeshan, „Three Decades of Development in DOA Estimation,“ *TELKOMNIKA Indonesian Journal of Electrical Engineering,* August, 2014.
8. W. R. a. Y. Huang, „Analysis for Capon and MUSIC DOA estimation algorithms,“ в *IEEE Antennas and Propagation Society International Symposium Conference,* 2009.
9. G. P. Chowdary, „Performance Comparison of various DOA Estimation Techniques based on Antenna Parameter,“ *International Journal of Review in Electronics and Communication Engineering,* том Volume 4, April, 2016.
10. „Wikipedia,“ [Онлайн]. Available: https://en.wikipedia.org/wiki/MUSIC_(algorithm).
11. B. P. N. Ying Zhang, „MUSIC-Like DOA Estimation without Estimating the Number of Sources,“ *IEEE Transactions,* 2010.
12. G. F. A. M. Irina Stepanets, „Beamforming Techniques Performance Evaluation for 5G massive MIMO Systems,“ *Internet of Things, Networks and Security,* p. 67.

Todor G. Peshev,

RADAR SYSTEM WITH SYNTHESIZED ANTENNA APERTURE

Todor G. Peshev

Faculty of Artillery, Air Defense and Communication and Information Systems,
National Military University, Shumen, Bulgaria, iviv58@abv.bg

***Abstract**: The report addresses the problems of radar with a synthesized antenna aperture in the arbitrary motion of the aircraft under turbulent atmospheres and the presence of trajectory instabilities and elastic oscillations of the structure. Methods are proposed to compensate for these effects and to improve the quality of the radar image.*

***Key Words**: synthesized antenna aperture, trajectory instabilities, elastic oscillations of the structure.*

РАДИОЛОКАЦИОННА СИСТЕМА СЪС СИНТЕЗИРАНА АПЕРТУРА НА АНТЕНАТА

Тодор Г. Пешев

Факултет „Артилерия, ПВО и КИС"
Национален военен университет „В. Левски", Шумен, България, iviv58@abv.bg

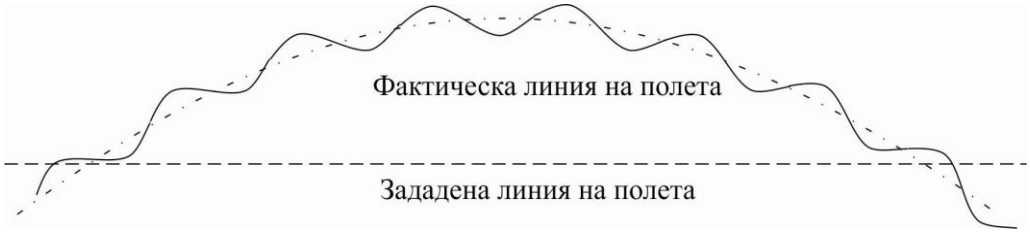
Въведение

При формиране на радиолокационното изображение (РЛИ) в радара със синтезирана апертура на антената се извършва управление както на реалната така и на синтезираната диаграма на насочено действие. Законите за управление се определят от зададения вид на обзор на земната повърхност при това сканирането на синтезираната диаграма на насочено действие (СДНД) се извършва посредством използването на специфични опорни функции. Независимо от вида за обзор на земната повърхност характера и параметрите на сигналите за управление се диктуват или от наличните априорни данни за режима на полет или по измерените параметри за движение на ЛА. Ако вида на фазовия център на антената (опорната траектория на полет на ЛА) е фиксиран и известен то опорната функция за синтезиране на ДНД може да се въведе предварително в паметта на системата за обработка на сигнала и получаване на РЛИ. При произволна траектория на движение на ЛА, когато тя се изменя от един интервал на синтезиране към следващ то следва опорната функция за обработка да се изчислява за всеки интервал на синтезиране по време на полета на основата на измерване на параметрите за движение на ЛА.

В качеството на фиксирана траектория обикновено се използва праволинейна траектория с постоянна скорост на движение на ЛА. При страничен обзор на земната повърхност в простия случай за получаването на РЛИ по принцип се изисква да се измерва само пътната скорост V_n на ЛА. На практика обаче нито един вид ЛА не може да лети равномерно и праволинейно в строгия смисъл на думата и особено това важи за най-разпространения носител на РСА – самолета. Това се дължи на факта, че полета на самолета в атмосферата се получава непрекъснато изменение на

посоката и скоростта навътъра, атмосферното налягане, плътността на въздуха и други подобни в резултата на което възникват случайни отклонения на режима на полета от зададения. Системата за управление на самолета от една страна не винаги успява да реагира на тези изменения и да поддържа автоматично зададения режим на полет на ЛА, но от друга страна самата тя въвежда елементи на случайност в движението му. Най-ярък пример в това отношение се явяват грешките на пилотирането от страна на летеца. Всички случайни отклонения от зададения режим на полет е прието да се наричат ***траекторни нестабилности*** (ТН). По важни от тях са: отклонение на ЛА от зададената траектория на полета; неговите ъглови колебания; случайното изменеие на величината и посоката на вектора на скоростта и други.

Траекторните нестабилности са реакция на самолета като твърдо тяло на въздействието на турболентната атмосфера и шумовете на системата за управление. Наред с това следва да се има предвид и факта, че конструкцията на самолета е гъвкава (еластична). Еластичните колебания на елементите от конструкцията на самолета под действието на аеродинамическите сили при полета в турболентна атмосфера се наричат ***еластични колебания на конструкцията*** (ЕКК). В реални условия на полета ТН и ЕКК се проявяват едновременно и предизвикват случайни отклонения на траекторията на фазовия център на антената от зададената. Това е представено на фиг. 1, където с прекъсната линия е показана зададената линия на полета (ЗЛП), а с пунктирна линия – отклонението от нея в следствие на ТН, а с непрекъсната линия – фактическата линия на полета (ФЛП) с отчитане на ТН и ЕКК.

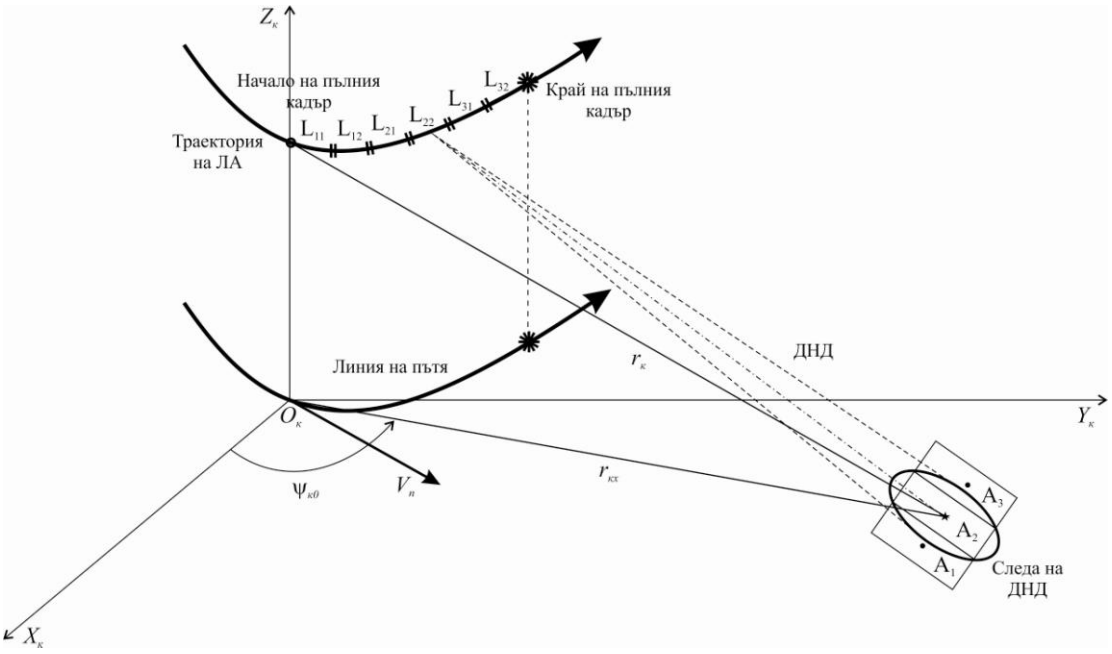


Фигура 1. Вид на зададената и фактическата линия на полета.

При фиксирана опорна траектория ТН и ЕКК предизвикват амплитудни и фазови изкривявания на отразените сигнали в РСА, който се наричат траекторни изкривявания. В резултат на тези изкривявания оптималността в обработката на сигналите в РСА се нарушава. С увеличаване интензивността на тези изкривявания се влошава разделителната способност на РСА по азимут, увеличават се грешките в определянето на местоположбението на обектите, свива се динамическия диапазон на сигнала на РЛИ. В някои случай РЛИ може напълно да се разруши [6, 2]. В резултат на теоретическите [5] и експериментални [3] изследвания, а така също и от цифровото моделиране [6] е доказана невъзможността да се осигури устойчиво РЛИ без прилагането на специални мерки по отношение на ТН и ЕКК. В тази връзка възниква проблема за тяхната компенсация. Възможен вариант за решаването на този проблем е постоянното измерване на параметрите на движение на ЛА и изчисляването на тяхна база на отклонението на фазовия център на антената от опорната траектория и корекция на отразения сигнал с отчитане на това отклонение. На свой ред възниква въпросът за състава, структурата и характериститките на измерителя на параметрите на движение (ИПД) на ЛА. За да се покаже ролята и мястото на ИПД при формирането на пълния кадър на РЛИ ще се разгледа работата на РСА при страничен обзор в случай на некохерентно натрупване на сигнала на РЛИ в парциалните кадри.

В момента на начало на формиране на пълният кадър на РЛИ в наземната свързана координатна система (НЗСК), Y_k, O_k, X_k Z_k (фиг. 2) наречена система на координатите на кадъра се задава азимуталния ъгъл на кадъра ψ_{k0} и хоризонталното $r_{кх}$ или наклоненото $r_к$ разстояние до центъра на участъка от местността, съответващ на пълния кадър(т. A_2 на фиг. 2). Зададените така също разделителна способност по разстояние и азимут се поддържат постоянни за цялото време на формиране на кадъра $T_к$. Постоянството в разделителната способност по азимут се постига посредством изменение на интервала за синтезиране при различни ъгли на наблюдение. По нататък

пълният кадър на РЛИ се разделя на парциални кадри и се изчисляват координатите на центъровете на всеки парциален кадър. На фиг. 2 са показани три парциални кадъра с центрове A_1, A_2 и A_3. След това ДНД се установява на линията $ЛА - A_1$ и се извършва запис на отразения сигнал. Управлението на ДНД се осъществява по такъв начин, че за цялото време на интервала на синтезиране (ИС) да се извършва облъчване на участъка от местността съответстващ на парциалния кадър. За да се осъществи следене на изменението на разстоянието от ЛА до центъра на парциалния кадър се изчислява пътя на ЛА в НЗСК Y_k, O_k, X_k, Z_k. Едновременно със записа на отразения сигнал по данните от ИПД се извършва и изчисление на опорната функция за обработка на сигнала в РСА. След което по избрания алгоритъм за обработка се формира сигнала на РЛИ на парциалния кадър. На следващия етап процесът на формиране на сигнала на РЛИ се повтаря или за същия парциален кадър, осигурявайки некохерентно натрупване или за следващия парциален кадър.



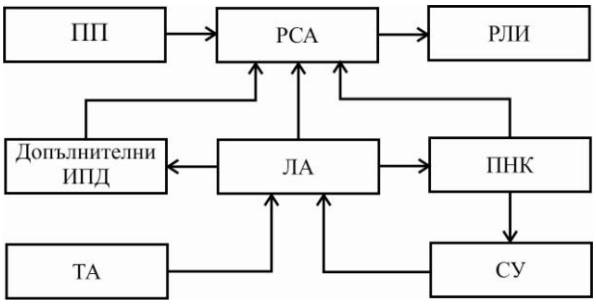
Фигура 2. Схема за формиране на пълния кадър при секторен обзор.

Общият брой на формираните в РСА парциални кадри $N_{пк}$ зависи от броя на некохерентни натрупвания $N_н$ и броя парциални кадри в пълния кадър на РЛИ $N_к$ т.е. $N_{пк}=N_кN_н$. Обикновено в практиката за увеличаване на вероятността за откриване и намаляване петнитостта на изображението се извършва три или четири кратно некохерентно натрупване ($N_н$=3 – 4). На фиг. 2 е представен случай на двукратно натрупване $N_н$=2, броя на парциалните кадри е $N_к$=3 то общия брой на парциалните кадри $N_{пк}$=6. Необходимо е да се добави и факта, че следенето за изменението на разстоянието до центъра на пълния кадър се извършва за времето на формиране му, а до центъра на парциалния кадър – за времето на некохерентното натрупване $T_н$.

Особено важно е да се подчертае, че при полет на ЛА в турболентна атмосфера по сложна траектория се увеличават ТН и ЕКК. Ето защо при структурирането (изчисляването) на опрната функция за обработка в РСА на всеки ИС се извършва с отчитане именно на ТН и ЕКК. А това от своя страна очевидно изисква при синтезирането на апертурата на антената и получаването на сигнала на РЛИ постоянно измерване на параметрите за движение. Използването на щатното пилотно-навигационно оборудване на ЛА, но повечето случаи то не е проектирано за съвместна работа с РСА [1]. Възниква въпроса за допълнителни измерители и тяхното съвместяване с щатните. По този начин РСА се оказва част от сложна радиолокационна система [4] със синтезирана апертура на антената. Блоковата схема на такава сложна радиолокационна система е показана на фиг. 3.

Основната задача на РСА е преобразуването на подстилащата повърхност (ПП) в РЛИ, показана с връзката ПП-РСА-РЛИ. На ЛА в общия случай му въздействат както системата за управле-

ние (СУ) така и турболентната атмосфера (ТА). Информация за параметрите на движение на ЛА постъпват от щатния пилотажно-навигационен комплекс (ПНК), но и от допълнителните ИПД. Посоченият модел на сложна радиолокационна система със синтезирана апертура на антената позволява използването на системния подход за изследвания, разработка и изпитания на РСА. Това е възможно само при условия, че са известни моделите на елементите на тази система и особено на самата РСА, на летателния апарат, на измерителите и техните грешки [2].



Фигура 3. Блокова схема на модела на РЛС със синтезирана апертура.

Моделът за движение на всяка точка от ЛА може да се получи посредством обединяване на зададената траектория и случайните отклонение от нея, като ТН и ЕКК в частност на първо приближение може да се приемат като стационарен случаен процес с нулево математическо очакване и съответната корелационна функция на линейните и ъглови отклонения съгласно израза [6]:

$$R_i(\tau) \approx D_i \exp\left\{-\frac{\tau^2}{T_i^2}\right\}\cos\left(\frac{\pi\tau}{2\tau_i}\right),$$

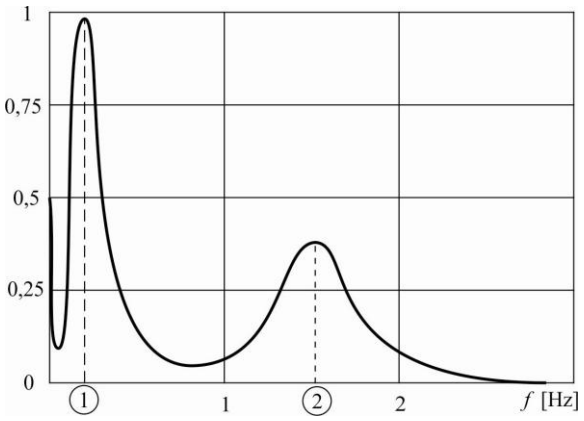
където: D_i – дисперсия на линейното или ъглово отклонение;

T_i, τ_i – параметри на функцията на корелация, където $T_i >> \tau_i$.

Средно-квадратичните стойности на линейните отклонения предизвикани от ТН са в порядъка на от единици до десетки метри, ъгловите отклонения по крен и курс са в границите на $1^0 – 2^0$ (по тангаж са от 3-5 пъти по-малки), а за еластичните колебания - десетки части от милиметъра до няколко сантиметра в зависимост от еластичността на конструкцията и положението на самолета. Разбира се конкретните параметри на ТН и ЕКК зависят от типа на самолета.

Самолетът може да се разглежда като филтър на входа на който постъпва случаен сигнал във вид на въздействие вследствие наличието на турболентна атмосфера. В този случай самолетът като носител на РСА може статичстически да се опише посредством АЧХ по отклоненията на фактическата траектория на полета от зададената. Пример на нормирана АЧХ на хипотетично тежък самолет е представена на фиг. 4. На фигурата с цифрата 1 е отбелязана честотата на колебания на самолета като твърдо тяло (ТН), а с цифрата 2 – честотата на елестичните деформации (ЕКК) с нисък тон.

Щатните навигационни системи (ИНС и ДИСС) за предназначени за решаването на основната задача на навигацията – определяне с минимална грешка местоположението на ЛА в географската (или ортодромичната) система от координати. ТН и ЕКК водя само до влошаване на точността на работа на тези системи. В тази връзка обикновено лентата на пропускане на тези системи се избира достатъчно тясна и е изчислена за пропускане само на нискочестотните отклонения на ЛА, което осигурява по-висока точност на навигацията. Тези системи сами по себе си имат постоянни и нискочестотни грешки, което води до това, че и допълнителните ИПД по отношение на РСА също притежават постоянни, нискочестотни и теснолентови грешки.



Фигура 4. АЧХ по отклоненията на хипотетично тежък самолет.

При определяне на състава и характеристиките на допълнителните измерители на параметрите за движение следва да се отчита и факта, че юатните навигационни системи се разполагат на самолета близо до центъра на масата му, а антената на РСА често е изнесена далеч от тях напред. Параметрите за движение на антената поради тази причина може значително да се различават от параметрите за движение на центъра на масата поради ъгловите и еластичните колебания на ЛА. В тази връзка закрепването на антената на РСА се прави на сечения с възможно най-малки еластични колебания, а допълнителните измерители се разполагат по възможност близо до самата антена на РСА.

Заключение

Следва да се отбележи, че неточното отчитане на траекторията за движение на ЛА се явява не единственият източник за изкривяване на сигнала на РЛИ. В изкривяването му свой принос имат атмосферните нееднородности (тропосферните флуктуации на амплитудата и фазата), приемо-предавателната част на РСА (апаратурните флуктуации), а така също и самите облъчвани обекти (флуктуации на преотражението). Средно-квадратичната грешка от изкривяването на фазата поради действието на тези източници може да достигне до няколко градуса, а средно-квадратичната грешка от изкривяването на фазата поради действието на ТН, ЕКК и грешката на датчиците да достигне до десетки или стотици градуси, което е значителна грешка [3]. Във връзка с това при изследванията и разработката на РСА една от главните задачи пред конструктурите е намаляване на средно-квадратичната грешка при измерване траекторията на фазовия център на антената до нивото на средно-квадратичната грешка на другите източници на изкривявания в сложната радиолокационна система със синтезирана апертура на антената.

References

1. Ахметьянов В.Р., Пасмуров А.Я., Пономаренко А.П., Цифровые методы получения изображения с помощью космических радиолокационных станций с синтезированной апертурой, Зарубежная радиоэлектроника, бр.5 1995.

2. Белоцерковский С.М., Толстов Е.Ф., Системный подход к исследованиям РЛС с синтезированной апертурой, Радиотехника, т.37 1992.

3. Богачев А.С., Толстов Е.Ф., Компенсация траекторных искажений сигналов в радиолокационных станциях с синтезированной апертурой антенны, Зарубежная радиоэлектроника, бр. 3 1991.

4. Михалевич В.С., Волкович В.Л., Вычислителные методы исследования и проектирования сложных систем, М, Наука, 1992.

5. Радиолокационные станции обзора земли. Под ред. Кондратенкова Г.С., М, Радио и связь, 1993.

6. Титов М.П., Толстов Е.Ф., Фомкин Б.А., Синтезирование апертуры антенны при полете самолета в турболентной атмосфере, М, Вопросы кибернетики, 1993.

Georgi N. Mazadzhiev, Sasho S. Evlogiev, Valentin T. Atanasov,

CONCEPTUAL MODEL OF SMART HOME MOBILE TECHNOLOGICAL SYSTEM

Georgi N. Mazadzhiev, Sasho S. Evlogiev, Valentin T. Atanasov

"Vasil Levski" National Military University, Faculty of Artillery, Air Defense and Communication and Information Systems
g_mazadviev@abv.bg, sevl@abv.bg, valopaint@yahoo.com

***Abstract**: This paper consider synthesizing of conceptual model as a part of development process of smart home mobile technological system, intended for practical teaching of the military cadets and students. The second aspect involves research activity and studies in the field of new ICT approaches in education. Main results are processes optimization and system deploying in condition of restrictions.*

***Keywords**: Home automation, smart home, IoT, model conceptualization, teaching tools*

КОНЦЕПТУАЛЕН МОДЕЛ НА МОБИЛЕН ТЕХНОЛОГИЧЕН КОМПЛЕКС „УМЕН ДОМ"

Георги Н. Мазаджиев, Сашо С. Евлогиев, Валентин Т. Атанасов

Национален военен университет „Васил Левски", Факултет „Артилерия, противовъздушна отбрана и комуникационно-информационни системи"
valopaint@yahoo.com, g_mazadviev@abv.bg, sevl@abv.bg

Въведение

Настоящето и близкото бъдеще на комуникационно-информационните технологии се определят като „пост-компютърни"[2,5]. Ускорители на тази еволюция са иновативни знания и концепции в комплексни научни области, както и революционни постижения в производствените технологии. Пост-компютърната фаза може да се разглежда и като преход към етапа на повсеместните изчисления (ubiquitous computing) - новата парадигма за информационна инфраструктура на 21-ви век"[3].

Програмата за развитие на отбранителните способности на въоръжените сили 2020 и развитието на военнообразователната система като източник на кадри за окомплектоване на българската армия изискват търсене и внедряване на нови, по-ефективни методи за обучение. В този контекст основна задача на факултет „Артилерия, ПВО и КИС" при НВУ „Васил Левски" е да подготвя висококвалифицирани и адаптивни към професионалната среда и технологичните предизвикателства курсанти и офицери за нуждите на военните комуникационни и информационни системи с реални и приложими знания, практически умения и компетентности, допринасящи за издигане на технологичното равнище и способностите в сферата на отбраната.

Повсеместното проникване и интегриране на компютърните информационни технологии трансформира дигитално както физическия свят, така и социума. Наблюдава се преход от отделни вградени системи към кибер-физически системи, основани на концепции за хиперсвързан свят и интелигентни пространства, формиращи високо интерактивно поколение [6]. Съществуващата учебно-планова документация предвижда адекватно учебно съдържание за студенти и курсанти,

но учебно-материална база за практическо обучение в интелигентна учебна среда, изградена с елементи, категория „*интернет на нещата*“ (IoT), както и иновативни интерфейси за взаимодействие с физически обекти липсват.

Целта на настоящата работа е да се синтезира концептуален модел като етап от физическата реализация на интелигентен високотехнологичен комплекс „*умен дом*“ с безжично управляеми контролери, посредством човеко-компютърен интерфейс в чиито състав влиза и набор от гласови команди. Основното предназначение на комплекса е учебно-изследователската работа на курсанти и студенти в областта на повсеместните информационни и комуникационни технологии, обвързана с налични комерсиални платформи от компоненти категория IoT.

1. Изложение

1.1. Изходни понятия

Съвременният „*автоматизиран дом*” („Home Automation”) обхваща управлението на осветление, отопление, климатизация, енергийно управление, сигурност, забавление и т.н. Редица компании предлагат продукти за автоматизиран дом - AMX, CommandFusion, Control4, Crestron, Idratek, Insteon, KNX, Rako. По-напредналите системи за автоматизация изискват мрежов протокол за комуникация на различна периферия с централното устройство (или т.нар. „майка”). Според нуждите се използват Z-Wave, Insteon, Zigbee, X10 и др. Мастър-контрол софтуерът комуникира с периферните устройства чрез радиоприемник/координатор, задаващ безжични команди към мрежата. Периферните устройства са два типа: сензори, с които се наблюдават условията на средата и състоянието на управляваните обекти; изпълнителни механизми, които реализират физически мрежовите команди”[4].

Квалификацията „*умен дом*” се различава от автоматизирания дом количествено и качествено - в степента на вътрешна и Интернет-свързаност, автономността, адаптивността и интелигентността в управлението на домашните системи, както и единното информационно пространство на взаимодействащите домашни подсистеми в интерес на обитателите – фиг.1

Фиг. 1 Концепция за „*умен дом*“

Технологиите „*умен дом*“ се развиват от една страна, за да се постигане на по-здравословен и комфортен микроклимат за работа или почивка при минимално изразходване на енергийни и комунални ресурси. От друга страна се повишава защитата от бедствия и неоторизиран достъп чрез мониторинг на неправомерно навлизане или възникнала аварийна ситуация. Важна тенденция е замяната на традиционния потребителски интерфейс от технологии, позволяващи по-пряка комуникация, базирана на говор, жестове и емоции – част от тенденцията за конвергенция „човек – компютър“.

Технологиите „*умен дом*“ могат да са особено полезни и в складовата инфраструктура на Българската армия. Контролът на влажността и температурата там засега се осъществява с морално и физически остарели аналогови датчици с ниска точност, чието използване е трудоемко

и с висока степен на субективност. Субективни грешки могат да повишат съществено вероятността за тежки аварии, да застрашат живота както на работещите, така и на използващите недобре съхранявано въоръжение и боеприпаси.

1.2. Съображения при синтеза на концептуален модел на „*умен дом*"

Като обект на моделиране „*умният дом*" е изключително сложна многомерна, разпределена, дискретно-непрекъсната динамична и стохастична система. Моделът на „*умния дом*" може да се дефинира като символичен и/или материален образ на реалния обект.

В [1] се дефинира сходството между модел и физически оригинал, както следва:

- ***адекватност*** – означава еквивалентност. Адекватен модел на практика не съществува, защото реалните обекти имат безкрайна размерност;
- ***изоморфизъм*** - еквивалентна структура между модел и оригинал;
- ***хомоморфизъм*** - непълна структурна еквивалентност (редукция);
- ***изофункционализъм*** - еднакво поведение при еднакви въздействия.

За целите на познанието се търсят изоморфни и изофункционални модели, а за целите на управлението се извършва синтез на хомоморфни и изофункционални модели.

Поставените цели с реализацията на технологичния комплекс са както познавателни, така и свързани с ресурси за възпроизвеждане на различни сценарии за управленски решения. Изоморфният модел на „*умен дом*" би бил твърде скъп и ще измести основния акцент за приложения в учебния процес. Ето защо, приемаме, че концепцията за мобилния технологичен комплекс трябва да предвижда редуцирани структурна еквивалентност и изофункционализъм.

Следователно, в концептуално отношение следва да се избере вариант за геометрично умален физически модел на част от „*умен дом*" – стая с врата и прозорец, отворена странично и отгоре за наблюдение и манипулации. В нея следва подходящо да се позиционират реални компоненти от система за управление на сигурността и контрол на електрически уреди и/или климатични параметри (редуцирани структурна еквивалентност и изофункционализъм). Така се осигурява степен на функционална и физическа съгласуваност с оригинала, която съответства на целите.

Управлението на процесите в „*умния дом*", както и съответните процеси в модела трябва да е устойчиво. Освен това, моделът трябва да бъде управляем (контролируем), наблюдаем (измерим), както и с крайна размерност съобразно зададената функционална рамка. Тези изисквания могат да се трансформират в следните ***характеристики*** на концептуалния модел:

- Използване на алгоритми за устойчиво управление на зададени процеси;
- Използване на налични автономни приложения за управление на компонентните контролери;
- Използване на операционна система (среда), съвместима с приложенията на компонентните контролери;
- Изграждане на система за централизирано управление и контрол посредством интерфейсна йерархична връзка с автономните приложения на компонентните контролери;
- Измеримост (наблюдаемост) на зададени физически величини с документиране и статистика;
- Ограничение в броя на управляемите и наблюдаеми физически величини.

От гледна точка на ***учебно-приложните аспекти*** концептуалният модел следва да предвижда:

- Работа в цифрови комуникационни и компютърни мрежи за некласифицирана информация и при нормални климатични условия;
- Мобилност за удобно транспортиране до учебна зала;
- Естетична реализация в хармонична цветова тоналност;

- Възпроизвеждане на множество сценарии за дистанционно наблюдение, управление, охрана и документиране на реални ситуации и процеси в умния дом в интерес на неговите обитатели през смарфон/таблет от произволна точка;
- Полезно използване както в демонстрационен вариант при фронтално обучение чрез система за визуализация, базирана на безжично управляем проектор, така и при индивидуално обучение в „действие“ (или за малки групи) чрез учебно-изследователски задачи;
- Интелигентно интерактивно гласово взаимодействие, т.е. обединение на функции за разпознаване на човешка реч със семантичен и синтактичен анализ, автоматично търсене и обработка на контекстна информация за конструиране на отговор/реакция и синтез на човешка реч до глас, близък до естествения.

Следователно, в структурно отношение концепцията за мобилния високотехнологичен комплекс ***интегрира*** четири системи:

- *Мобилна платформа*, която да е носител на геометрично умален физически модел на визуално достъпна стая от клас „*умен дом*“ с подходящо позиционирани реални компоненти категория IoT;
- *Система за безжично дистанционно управление и* визуализация на функционални възможности пред учебна група;
- *Система за управление на сигурността и безжичен контрол* на електрически уреди и/или климатични параметри в „*умен дом*“;
- *Интелигентна интерактивна система с гласов интерфейс* и функции за домашна автоматизация, базирана на облачен ИИ.

1.3. Синтезиране на концептуалния модел

В практиката съществуват редица подходи за представяне на концептуален модел - текстови репрезентации (предположения, списък на компоненти, описания), диаграми на процеси, блок-схеми, диаграми на езика UML (дейности, класове, случаи на употреба), графични репрезентации [7]. Степента на абстрактност при синтезирането на концептуалния модел е определяща в определени случаи. Настоящата статия ще представи концептуалния модел с няколко подхода с цел по-широк поглед и логическа обусловеност.

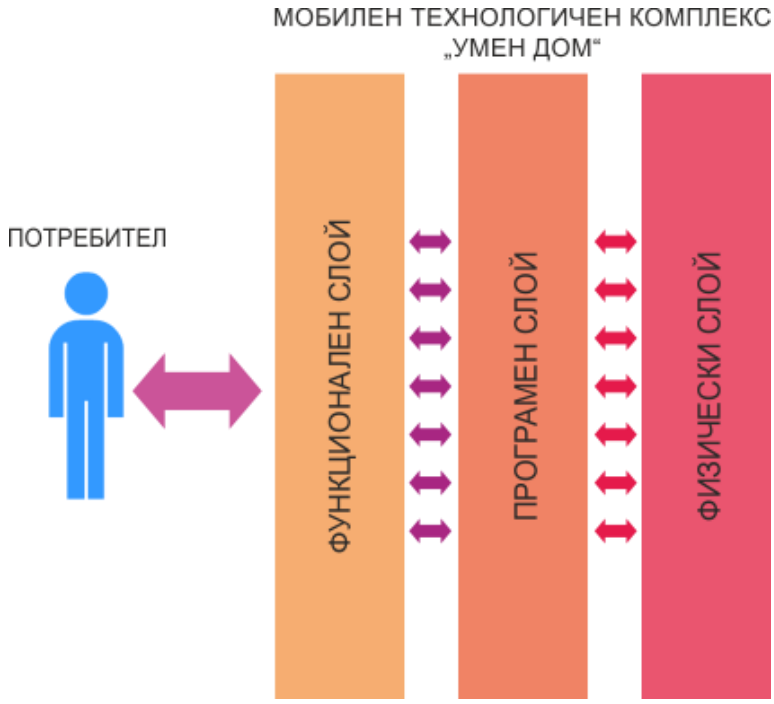
Изхождайки от разгледаните по-горе характеристики, аспекти и системна интеграция, концептуалният модел на мобилен технологичен комплекс „*умен дом*“, се представя в табличен вид в табл. 1.

Основни слоеве	Тип	Подслоеве	Характеристика	Подход
Функционален слой	Абстрактен	Дефиниране на изискванията. Основно предназначение и цели на комплекса.	Избор на спецификации и стандарти. (*Среди за разработка, език за моделиране, материали, елементи, инструментариум и др.*)	Итеративен
		Функционално моделиране на комплекса		
Програмен слой	Логически	Подслой за централизирано управление и контрол	Интегрирана система	
		Подслой на предефинираната среда	Автономни приложения(Applications)	
		Подслой на системното обкръжение	Операционна система	
Физически слой	Реален	Подслой на физическото обкръжение/контекст	Модели на обекти (Командни центрове, помещения, складове с ограничен достъп, учебни зали, кабинети и лаборатории в системата на отбраната и др.)	

		Подслой на инфраструктурата на модела	Комуникации, мрежа и електрозахранване	
		Компонентен подслой	Физически компоненти	

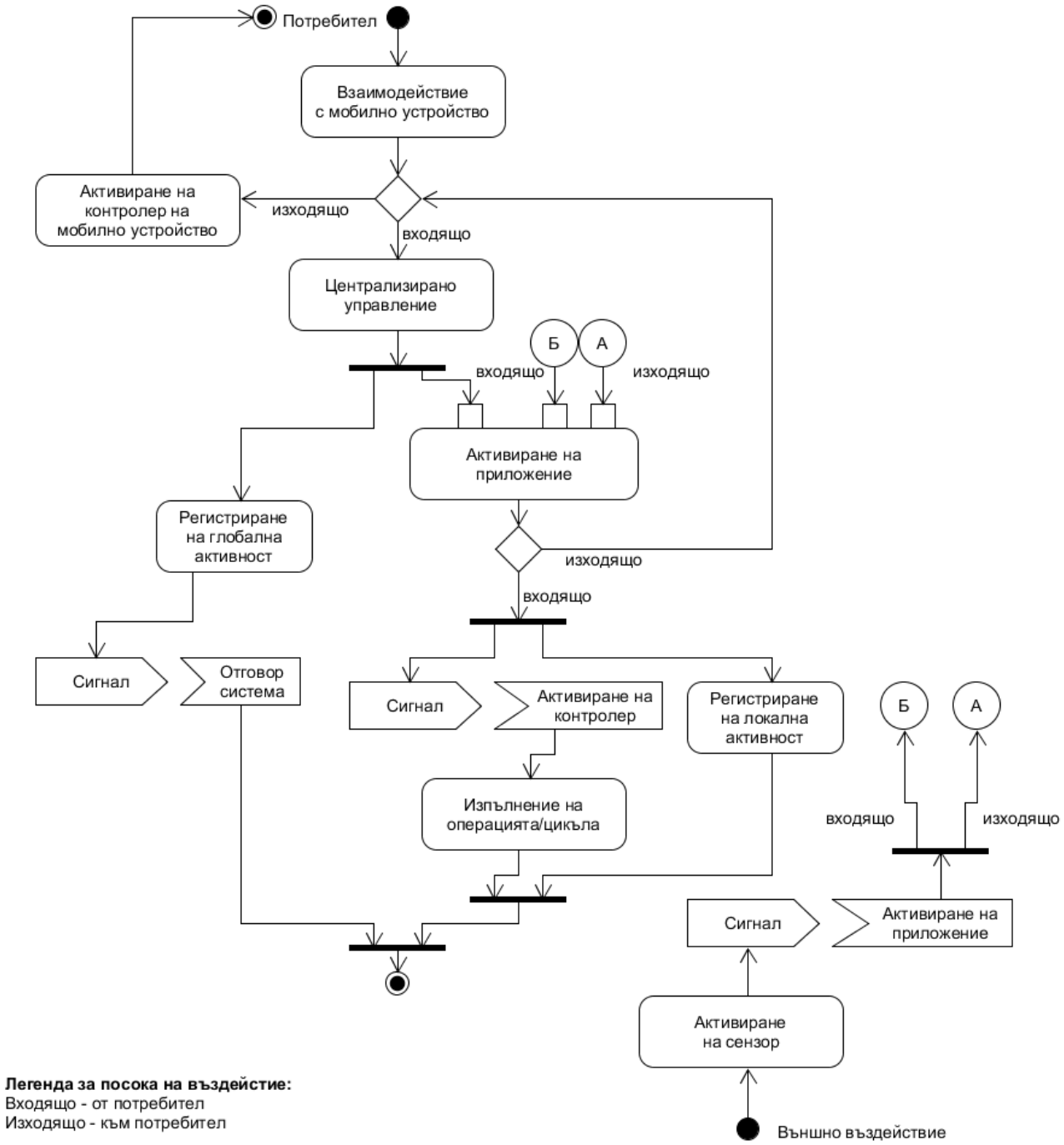
Табл.1. Таблично представяне на концептуален модел на мобилен технологичен комплекс „*умен дом*“

За по-пълно представяне и изясняване на йерархичността, взаимодействията ***потребител/система*** и взаимовръзките на изграждащите го обекти концептуалният модел се визуализира на фиг.2.



Фиг. 2 Графично представяне на концептуален модел на мобилен технологичен комплекс „*умен дом*“.

Необходимо е да се отбележи, че в този системен модел всички потребителски взаимодействия са на високо програмно ниво. Тоест взаимодействията на ниско апаратно(компонентно) ниво се осъществяват само и единствено от приложенията. Този подход определя интелигентната системна характеристика. На фиг.3 е представен концептуалният модел посредством диаграми на дейности, дефиниращ процедурната логика на системата.



Фиг.3. Концептуален модел на технологичния комплекс посредством диаграми на дейности.

Заключение

Ефектът от разработването на концептуален модел на мобилния технологичен комплекс с последваща физическа реализация може да се търси в направленията:

- Постигане на баланс между сложност (цена) и полезност (функционална използваемост) при ограничената финансова рамка на вътрешен за университета проект и налични комерсиални платформи с компоненти категория IoT;
- Преход към ново поколение учебно-материална база, съответстваща на съвременното равнище, на потребностите на високоинтерактивното поколение и близките перспективи в развитието на комуникационно-информационните технологии;
- Осигуряване на интелигентна среда за обучение и самообучение на млади преподаватели, докторанти, курсанти и студенти в областта на повсеместния компютинг и IoT като се изследват иновативни интерфейси за взаимодействие със сложни физически обекти;
- Повишаване интереса, мотивацията и резултатността в учебно-изследователския процес с курсанти и студенти в областта на съвременните комуникационно-информационни технологии;
- Научно-приложни резултати от изследване на функционалности за три вида интерфейси на взаимодействия, както и от сравнителен анализ на тяхната ефективност.

С реализацията и внедряването на интелигентен високотехнологичен комплекс с безжично управляеми контролери, посредством човеко-компютърен интерфейс, използващ фина моторика и гласови команди, както и с предвижданите бъдещи изследвания, се предлага иновативно решение, имащо за цел достигане качеството на високотехнологично практическо обучение на курсанти и студенти в областта на повсеместните информационни и комуникационни технологии.

Допълнително се натрупва експертен опит и се създават предпоставки за разработване и внедряване на интелигентни дигитални средства за автоматизирано пространствено наблюдение и контрол на критични параметри на вътрешната среда в складовата инфраструктура на Българската армия.

References

[1] Гарипов, Е., Идентификация на системи, ч.1, ТУ-София, 2004.

[2] Мазаджиев Г., Ст. Станев, „ Пост-компютърната ера и мобилния компютинг”, Научна сесия - НВУ “В.Левски”, Шумен, 2012.

[3] Мазаджиев Г., Преход към повсеместна информационна инфраструктура, списание CIO, ИКТ за отбраната(ч.1), юли, 2014, бр.7, ISSN 13112 – 5605

[4] Мазаджиев Г., Специализирани компютърни системи, Издателство: Химера ООД, Шумен, 2014, ISBN 978-954-9681-62-8

[5] Kleynhans Stephen, The New PC Era: The Personal Cloud, 2012, HTML.URL: http://www.gartner.com/resId=1890215

[6] Atanasov,V.T., Ivanova,A.S., A Framework for Measurement of Interactivity of Digital Learning Resources, 42nd International Convention On Information And Communication Technology, Electronics And Microelectronics MIPRO 2019 Proceedings, Croatia, May 20-24, 2019;

[7]Wang, W., Brooks, R., Empirical Investigations of Conceptual Modeling and the Modeling Process, In Proceedings of the 2007 Winter Simulation Conference

Dimitar G. Chobanov,

ASK DISCRETE SINE TRANSFORM BASED ORTHOGONAL FREQUENCY – DIVISION MULTIPLEXING

Dimitar G. Chobanov

Department of Communication Networks and System Faculty of Artillery, Air Defence and CIS
National Military University "Vasil Levski", Shumen,Bulgaria, chobanov.d@abv.bg

***Abstract**: Coherent ASK modulation is proposed for use in descrete sine transform (DST) based orthogonal frequency – division multiplexing (OFDM) systems. The frequency separation between sub-carriers is only 1/2T instead of 1/T. With a slightly wider bandwidth, an ASK – DST – OFDM can achieve the same bit – error rate (BER) of ASK – DFT – OFDM and allows using approximately twice more subcarriers.*

***Keywords**: Orthogonal Frequency – Division Multiplexing, Discrete Sine Transform, OFDM, DST, ASK*

СИСТЕМА С ОРТОГОНАЛНО ЧЕСТОТНО РАЗДЕЛЯНЕ И МУЛТИПЛЕКСИРАНЕ БАЗИРАНА НА ДИСКРЕТНО СИНУСОВО ПРЕОБРАЗУВАНЕ И М–КРАТНА ASK МОДУЛАЦИЯ НА ПОДНОСЕЩИТЕ

Димитър Г. Чобанов

Национален военен университет „В. Левски", Факултет „А, ПВО и КИС"
Шумен, България, chobanov.d@abv.bg

Въведение

Минималното честотно отстояние между подносещите в система с ортогонално честотно разделяне и мултиплексиране (OFDM) базирана на дискретно преобразование на Фурие (DFT) е $\frac{1}{T}$, при продължителност на OFDM символа T. С въвеждане на ограничението подносещите да се различават само по честота и амплитуда минималното честотно отстояние може да се сведе до $\frac{1}{2T}$. В този случай OFDM символът може да бъде генериран с помощта на обратно дискретно синусово преобразование (DST) и демодулиран чрез дискретно синусово преобразование (IDST).

В доклада е предложен вариант на OFDM система базирана на дискретно синусово преобразование и M – кратна ASK модулация на подносещите (ASK – DST – OFDM).

Изложение

ASK – DST – OFDM

Дефинираме ASK - OFDM сигнала като:

$$s\ t\ = \sum_{k=0}^{N-1} A_k\ sin2\pi\frac{k}{2T}t \qquad (1)$$

където A_kе амплитудата на съответната подносеща и N е броят на подносещите.

При M – кратна ASK модулация на подносещите символите се представят с различни амплитуди Ако максималната разрешена амплутуда е A то всички възможни амплитуди са в диапазона $[-A, A]$. Амплитудите се изчисляват съгласно формула 2.

$$A_m = \frac{2A}{M-1}m - A, \qquad m = 0{,}1 \dots \dots \dots M-1 \qquad (2)$$

Разликата между нивата се изчислява по формула 3.

$$\Delta = \frac{2M}{M-1} \qquad (3)$$

Честотата на подносеща с индекс k е $f_k = \frac{k}{2T}$, като k са последователни цели числа. Честотното отстояние е $\frac{1}{2T}$. Взаимната ортогоналност между подносещите лесно може да се провери чрез извършване на интегрирането:

$$\int_0^T A_i sin2\pi\frac{i}{2T}t\ A_j sin2\pi\frac{j}{2T}tdt = 0 \qquad i \neq j$$

На фигура 1 са изобразени енергийните спектри на подносещите на три – канална ASK – DFT – OFDM система с честотно отстояние $\frac{1}{T}$ и три – канална ASK – DST – OFDM система с честотно отстояние $\frac{1}{2T}$.

От фигура 1 е видно, че заеманата честотна лента определена по критерият “nul – nul bandwith” ΔF е:

$$\Delta F_{ASK-DFT-OFDM} = \frac{N+1}{T} \qquad (4)$$

и

$$\Delta F_{ASK-DST-OFDM} = \frac{N+3}{2T} \qquad (5)$$

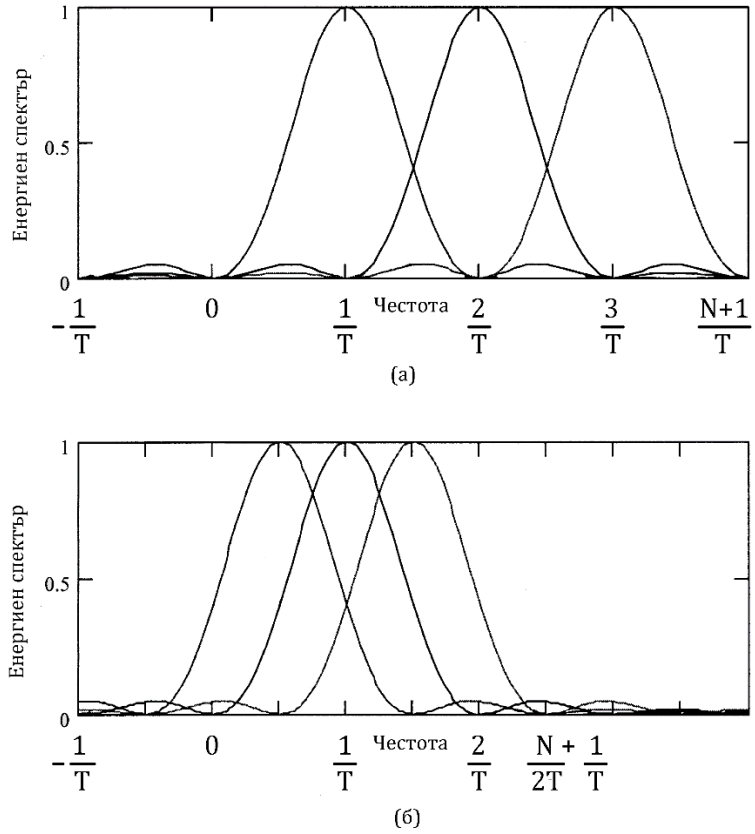
При N подносещи в ASK – DFT – OFDM система с честотно отстояние $\frac{1}{T}$ и M подносещи в ASK – DST – OFDM ситема с честотно отстояние $\frac{1}{2T}$, в една съща честотна лента е в сила равенството:

$$\frac{N+1}{T} = \frac{M+3}{2T} \qquad (6)$$

От (6) следва:

$$M = 2N - 1 \tag{7}$$

От (7) следва, че в една и съща честотна лента, ASK – DST – OFDM система с честотно отстояние между подносещите $\frac{1}{2T}$ позволява ползването на приблизително два пъти по – голям брой подносещи в сравнение с ASK – DFT – OFDM система с честотно отстояние $\frac{1}{T}$.



Фигура 1: Енергиен спектър на подносещи на OFDM система.
(а) честотно отстояние $\frac{1}{T}$; (б) честотно отстояние $\frac{1}{2T}$

Вероятност за битова грешка (BER)

Теоретичната вероятност за битова е анализирана при следните ограничения:
• На входа постъпва информационен поток x(i) представляващ поредица от некорелирани реализации на дискретната случайна величина с равномерен закон на разпределение и дефиниционно множество
• Предаването се извършва през канал с адитивен бял Гаусов шум (AWGN)
• Приемането е кохерентно

При посочените ограничения теоретичната вероятност за битова грешка в ASK – DST – OFDM система с честотно отстояние е:

$$BER_{ASK-DST-OFDM} = \frac{M-1}{Mlog_2 M} erfc \quad \frac{3log_2 M \ E_b}{M^2 - 1 \ N_0} \tag{8}$$

Полученият резултат напълно съвпада с вероятността за битова грешка в ASK – DFT – OFDM.

Дигитална имплементация

ASK – DFT – OFDM система може да бъде приложена с използването на обратно дискретно преобразование на Фурие (IDFT). В предложената ASK – DST – OFDM система обратното преобразование на Фурие е неприложимо заради честотното отстояние между подносещите, което е $\frac{1}{2T}$ вместо $\frac{1}{T}$.

В ASK – OFDM система с честотно отстояние $\frac{1}{T}$ е приложимо дискретно синусово преобразование (DST). DST се дефинира като [4]:

$$x\ k\ = \sum_{n=0}^{N-1} x\ n\ sin\frac{\pi nk}{N}, \quad n = 0,1 \dots \dots \dots N-1 \text{ и } x\ n\ \equiv 0 \tag{9}$$

Съответно обратното дискретно синусово преобразование (IDST) е:

$$x\ n\ = \sum_{k=0}^{N-1} x\ k\ sin\frac{\pi nk}{N}, \quad \text{к} = 0,1 \dots \dots \dots N-1 \tag{10}$$

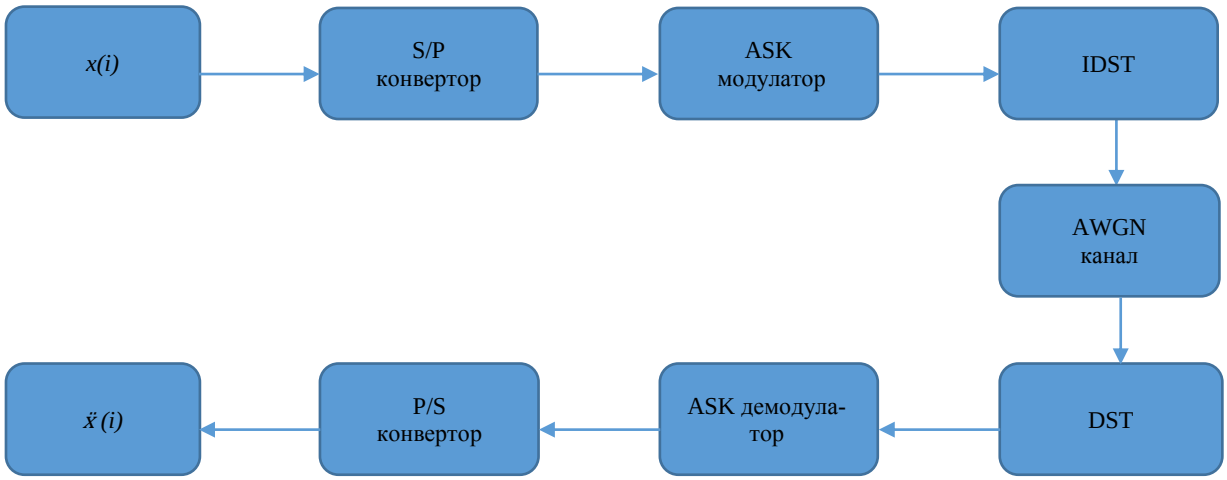
След заместване в (1) на t с $n\Delta t$ и T с $N\Delta t$, където е интервал на дискретизация, дискретният във времето ASK – DST – OFDM сигнала е:

$$s\ n\ = \sum_{k=0}^{N-1} A_k sin\frac{\pi nk}{N} \tag{11}$$

Така ASK – DST – OFDM сигналът може да бъде генериран чрез обратно дискретно синусово преобразование и демодулиран чрез дискретно синусово преобразование. Изрази (9), (10) и (2) дефинират OFDM система базирана на дискретно синусово преобразование с M – кратна ASK модулация на подносещите (ASK – DST – OFDM).

Блокова схема на ASK – DST – OFDM система

Блоковата схема на ASK – OFDM базирана на дискретно синусово преобразование е представена на фигура 2.

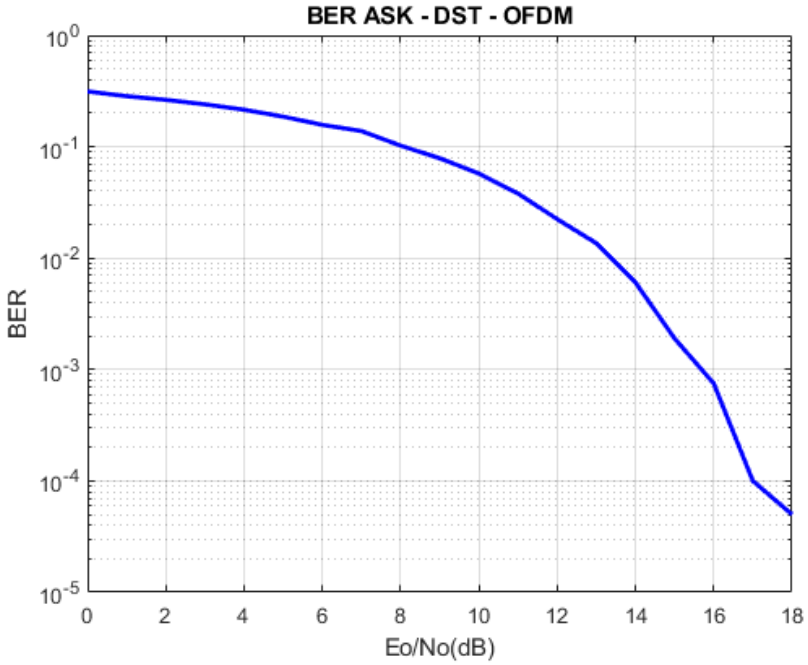


Фигура 2: Блокова схема на ASK – DST – OFDM система

Последователно – паралелният конвертор (S/P) акумулира серийната последователност от входни данни в блок от данни с размерност N . N – размерните потоци от данни се модулират съгласно (1) в ASK модулаторът. Блокът за обратно дискретно синусово преобразование (IDST) синтезира ASK – DST – OFDM сигналът. След преминаване през AWGN канала сместа ASK –

DST – OFDM сигнал и бял Гаусов шум постъпва в кохернтната приемната част (ASK демодулатор, P/S ковертор), в която се извършват обратните операции за демодулиране на ASK – DST – OFDM сигнала.

Въз основа на така описаната блокова схема на ASK – DST – OFDM система е извършена симулация в MATLAB. Резултатите от симулацията са представени на фиг. 3.



Фигура 3: Вероятност за битова грешка в ASK – DST – OFDM система

Заключение

В доклада е изследвана кохерентна система с ортогонално честотно разделяне и мултиплексиране и ASK модулация на подносещите, базирана на дискретно синусово преобразование. Честотното отстояние между подносещите е $\frac{1}{2T}$. Резултатите от направеното изследване сочат, че в една и съща честотна лента, при едни и същи качествени показатели (битова вероятност за грешка) предложената ASK – DST – OFDM система позволява ползването на приблизително два – пъти повече подносещи.

Трябва да се подчертае, че анализът и резултатите в това изследване се отнасят за AWGN канали. Очаква се предложената ASK – DST – OFDM система да влоши качествените си показатели в условията на предаване в канали със затихване, многолъчеви канали и пр., обект на бъдещи изследвания.

References

1. Proakis John G. Digital Communications McGrawHill, 4th edition, 2000
2. F. Xiong, Digital Modulation Techniques. Boston, MA: Artech House, 2000.
3. Press William H., Teukolsky Saul A., Vetterling William T., Flannery Brian P. NUMERICAL RECIPES: The Art of Scientific Computing, Copyright (C) 1986-1992 by Cambridge University Press.
4. Ахмед Н., Рао К. Р. Ортогональные преобразования при обработке цифровых сигналов. Пер. с англ. - М.: Связь, 1980.

Angela R. Borisova,

CONTEMPORARY LANGUAGES FOR PROGRAMMING ARTIFICAL INTELLIGENCE

Angela R. Borisova

ANGELA.BORISOVA@ABV.BG

***Abstract**: Almost all social networks use Artificial intelligence for enhancing user performance nowadays. By choosing a programming language, providing proper data, and applying a suitable algorithm, a program could be raised up that, like a human, will learn how to respond to specific situations. The most popular programing languages to AI are presented in the paper and some examples are shown.*

***Keywords:** Artificial Intelligence, Machine Learning, Deep Learning, Python, R, Java, Lisp, JavaScript.*

СЪВРЕМЕННИ ЕЗИЦИ ЗА ПРОГРАМИРАНЕ НА ИЗКУСТВЕН ИНТЕЛЕКТ

Ангела Р. Борисова

ANGELA.BORISOVA@ABV.BG

***Абстракт**: В днешно време почти всички социални мрежи използват изкуствен интелект. Избирайки език за програмиране, предоставяйки подходящи данни и прилагайки подходящ алгоритъм, може да се създаде програма, която като човек ще се научи как да отговаря в конкретна ситуация. В настоящия доклад са представени някои от най-известните езици за програмиране на изкуствения интелект.*

1. Изкуственият интелект и някои от неговите подкатегории – Machine Learning и Deep Learning

В нашето съвремие понятието „Изкуствен интелект“ придоби изключително важно значение. Изкуствения интелект навлиза все повече в обкръжаващата ни среда, като доказателство за това са автономните превозни средства, алгоритмите в социалните мрежи, бързите отговори при онлайн запитванията от потребители и много други[10]. Едно от най-актуалните приложения на изкуствения интелект се явява това в изследването на програмни кодове в киберсигурността и вземане на решение, че даден такъв е злонамерен [9]. В изкуствения интелект трите основни термина са: Artificial intelligence (AI), Machine Learning (ML) и Deep Learning (DL). Те често пъти биват взаимозаменяеми, но има съществена ралика между тях. AI традиционно се отнася до изкуствено създаване на човекоподобна интелигентност, която може да учи, разсъждава, планира,

възприема, навигира и обработва естествен език [1]. Реализирани са огромен брой приложения с изкуствен интелект в сферите на сервизните роботи, целенасоченото лечение, транспорта, здравната диагностика, обществената безопасност, образованието и развлеченията, но областите им на приложение тепърва ще се разрастват все повече през следващите години. Благодарение на AI технологиите се повишава производителността. Това включва машини, които могат да изпълняват нови задачи, като например усъвършенствани роботи, интелигентни асистенти, самоуправляващи се автомобили, подкрепящи хората в ежедневието им.

Днес компаниите инвестират десетки милиарди долари всяка година, за да развият Machine Learning, което го прави повсеместно средство за анализ и интерпретация на данни. Някои компании като Google и Facebook използват алгоритми за машинно обучение, за да показват реклами, други като Amazon и Apple използват машинно обучение за обработка на говорим език и за синтезиране на реалистични звукови гласове, трети пък като Tesla го използват за разработване на превозни средства със самостоятелно управление.

Deep Learning е подмножество на Machine Learning, включващо невронните мрежи като основна технология за анализ на данни. След като е съставен алгоритъм на базата на Deep Learning, той може да се използва за решаване на проблеми в реалния свят, като откриване на болести, авто-управление на автомобили, намиране на плевели или вредители в поле или намиране на неизправности в машините.

2. Python

Цялостният език Python може да се нарече и платформа, която може да бъде използвана както за научноизследователска и развойна дейност, така и за разработване на производствени системи [2]. Python е един от най-често използваните езици за програмиране, когато става въпрос за изкуствен интелект. Това е така, заради многото му вградени библиотеки и предварително вкоренени инструменти за прилагане на Machine Learning алгоритми и модели, които внасят лесnота при писането на програми. Някои от по-известните библиотеки на Python, с отворен код са: “TensorFlow”, “KERAS”, “PYTORCH”, “CAFFE2”, “Hebel”, “Seeborn”, “Chainer”, “SymPy”, “Theano”, “Matplotlib”, “Scipy”, “Pandas”, “MILK”, “Bob”, “Pybrain”, “Pipenv”, “NumPy”, “Ramp”, “NuPIC”, “Scikit-learn” [6].

Tensorflow е framework, написан на Python, съставен на базата на Deep learning. На фигура 1 е показан програмен фрагмент, служещ за разработване на конволюционни невронни мрежи за откриване на обекти чрез използване на една от вградените в Python библиотеки, а именно TensorFlow.

```
import tensorflow as tf

input_layer = tf.reshape ( features["x"], [ -1, Hight, width, channels] )

convolution = tf.layers.conv2d( inputs=input_layer,
                                filters = 32,
                                kernel_size = [5, 5],
                                padding= "same“,
                                weight,
                                bias,
                                activation = tf.nn.relu)

pooling = tf.layers.max_pooling2d( inputs=input layer,
                                   pool_size=[2, 2],
                                   strides=2 )
```

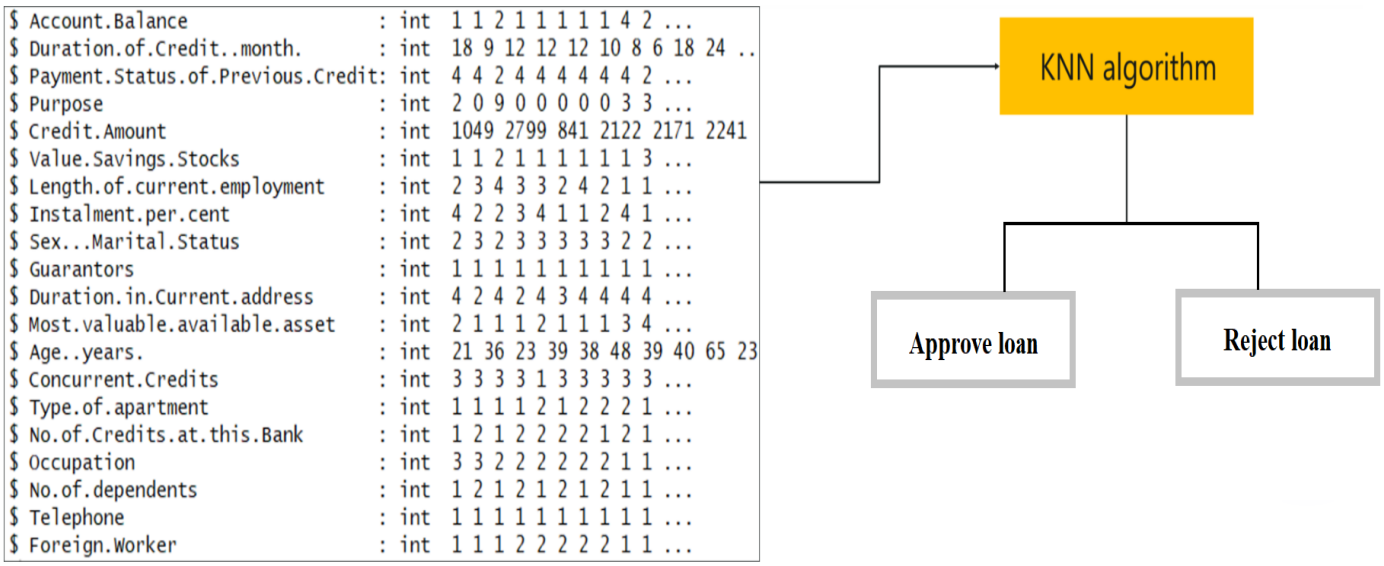
Фигура 1. Разработка на модел с TensorFlow [3]

3. Език “R”

Езикът „R“ се използва за проучване и за изграждане на Machine learning модели. Той е статистически, мощен език за програмиране, с отворен код, с помощта, на който се изчисляват и графично изобразяват различни данни. Паралелно с това, R е и развойна среда за разработване на проекти. Писането на програми с R е много лесно и интуитивно, защото не се изисква компилиране след всяка стъпка, а кода се изпълнява по време на писането. R използва алгоритъм за машинно обучение, наречен „KNN“ (k-nearest neighbors) [4].

KNN е най-простия алгоритъм за машинно обучение, изграден на базата на сходство между обектите. Класификацията на обект към съответен клас зависи от принадлежността на най-близкия до него обект.

На фигура 2 е показан пример за KNN алгоритъм, който цели да събере информация за социално-икономически профил на дадено физическо лице, относно отпускане на банков кредит и на базата на събраната информация, да изгради модел за машинно обучение, който предвижда, дали заемът на кандидата може да бъде одобрен или не.



Фигура 2. Модел на алгоритъм KNN за отпускане на кредит [5]

На фигура 3 е представена същинска част от програмен фрагмент за изграждане на модел на машинно обучение с помощта на алгоритъм KNN.

```
#Install class package
install.packages('class')
# Load class package
library(class)

#Find the number of observation
NROW(train.loan_labels)
[1] 700
knn.26 <- knn(train=train.loan, test=test.loan, cl=train.loan_labels, k=26)
knn.27 <- knn(train=train.loan, test=test.loan, cl=train.loan_labels, k=27)
```

Фигура 3. Изграждане на модел с алгоритъм KNN, написан на R [5]

Изборът на броя на най-близките съседи, т.е. определянето на стойността на k, играе съществена роля при определянето на ефикасността на модела. По този начин изборът на k ще определи доколко добре данните могат да бъдат използвани за обобщаване на резултатите от kNN алгоритъма.

4. Java

Java е лесен за програмиране, хетерогенен (способен да прехвърля съдържанието на различни приложения от едни софтуерни и хардуерни платформи на други) и използващ динамична памет, обектно-ориентиран език. Някои от по-известните работни програми, написани на Java и използвани за изследване, разработване и експоатация на Machine Learning, са “Weka”, “MOA” (Massive On-line Analysis), “Encog Machine Learning Framework”, “Java-ML”, “MLlib(Spark)”, “H2O”, “Signa”, “RapidMiner”, “Smile”. За пример е взета библиотеката, Encog Machine Learning Framework. Encog е усъвършенстван фреъймлърк за машинно обучение, който поддържа различни усъвършенствани алгоритми (невронни мрежи и генетични алгоритми) и класове за поддръжка и обработка на данни. Освен от Java, Encog се използва и от C# и от Silverlight. За изграждане на невронни мрежи се използват три основни библиотеки: DeepLearning4j, Neuroph и Arbiter. Проста невронна мрежа може да се създаде с помощта на обектите BasicLayer и BasicNetwork. На фигура 5, елемент 1 и 2 е представена примерна невронна мрежа, написана на Java. В елемент 1 е показана програмирана част включваща : входен слой с два неврона, скрит слой с три неврона и изходен слой с един неврон. В елемент 2 се вижда, добавяне на функция на активация към кода.

елемент 1

```
BasicNetwork network = new BasicNetwork();
network.addLayer(new BasicLayer(2));
network.addLayer(new BasicLayer(3));
network.addLayer(new BasicLayer(1));
network.getStructure().finalizeStructure();
network.reset();
```

елемент 2

```
BasicNetwork network = new BasicNetwork();
network.addLayer(new BasicLayer(null,true,2));
network.addLayer(new BasicLayer(new ActivationSigmoid(),true,3));
network.addLayer(new BasicLayer(new ActivationSigmoid(),false,1));
network.getStructure().finalizeStructure();
network.reset();
```

Фигура 4. Невронна мрежа, написана на Java [6]

елемент 1
```
org.encog.examples.neural.persist.EncogPersistence
```

елемент 2
```
public void trainAndSave() {
  System.out.println(
    "Training XOR network to under 1% error rate.");
```

елемент 3
```
System.out.println("Saving network");
EncogDirectoryPersistence.saveObject(new File(FILENAME), network);
```

елемент 4
```
public void loadAndEvaluate()
{
  System.out.println("Loading network");
  BasicNetwork network =
   (BasicNetwork)EncogDirectoryPersistence.loadObject(
   new File(FILENAME));
```

Фигура 5. Encog Persistence [6]

На фигура 5 елемент 1 е изобразен програмен фрагмент, включващ библиотекта Enlog Persistance, чиято цел е да придаде устойчивост на кода. Фигура 5, елемент 2, създаване на невронна мрежа, включваща метод trainAndSave, обучаваща се с XOR оператор. Фигура 5, елемент 3, следва запазване на невронна мрежа във файл Encog EG. Фигура 5, елемент 4, зареждане и оценка на вече съществуващата невронна мрежа, с помощта на метода loadAndEvaluate.

Encog използва GPU(Graphics processing unit), благодарение, на което ускорява бързодействието на системата. Java е лесен за използване инструмент, създаден за проектиране на различни софтуерни приложения, които да бъдат защитени и сигурни.

5. Lisp

Lisp все още се използва като език за програмиране на изкуствен интелект, но неговата популярност все повече намалява, заради развитието на съвременните езици, разполагащи с множество библиотеки и най-нови техники. Основна конструкция за работа на Lisp е списъкът, самата програма е списък. На фигура 6 е представен начина, по който се дефинира променлива, в случая „employee“ и нейните характеристики (slots) – name, address, serial-number, department, selary във фрейм (използва се за представяне на по-обща информация на клас обекти с общи характеристики). Фигура 7 показва просвояване на стойност на вече декларираната променлива “employee”.

```
(defstruct employee
    name
    address
    serial-number
    department
    salary)
```

Фигура 6. Дефиниране на променлива във фрейм [7]

```
(setq new-employee
    (make-employee
        :name '(Doe Jane)
        :address "1234 Main, Randolph, Vt"
        :serial-number 98765
        :department 'Sales
        :salary 4500.00))
```

Фигура 7. Присвояване на стойност на вече дефинираната променлива [7]

6. JavaScript

JavaScript е функционален и обектно-ориентиран език, чиято задача е вмъкване на динамичност в приложенията. JavaScript е много по-лесен за използване в сравнение с някои от другите езици за програмиране, като например Python. Javascript отваря нови хоризонти за приложенията, благодарение на многото му вградените инструменти. Някои от по-известните работни програми, използвани в машиното обучение с JavaScript са:

На първо място отново е TensorFlow (както и при Python), изписван TensorFlow.js. На следващо място “Brain.js”, “stdlib-js”, “machinelearn.js”, “math.js”, “face-api.js”, “R-js” и “natural”.

За пример е изследван “Brain.js”. Библиотеката Brain.js улеснява писането на Machine Learning и Deep Learning, благодарение на множеството му заложени функционалности. В примера на фигура 8 е представена графика на обучение на мрежа, като са комбинирани данни за обучение и тест в един масив, чрез използване на CrossValidate (валидиране на модела, оценка на това как резултатите от статистическия анализ ще се обобщят до независим набор от данни). CrossValidate предоставя начин за обучение на по-големи масиви данни. Вътрешно създава множество невронни мрежи и след обучението предоставя достъп до мрежата с най-добра точност.

```
const fs = require('fs');
const mnist = require('./mnist');
const brain = require('brain.js');


async function run() {

    const trainLabels = await mnist.getTrainLabels();
    const trainDigits = await mnist.getTrainImages();

    const testLabels = await mnist.getTestLabels();
    const testDigits = await mnist.getTestImages();

    const labels = [...trainLabels, ...testLabels];
    const digits = [...trainDigits, ...testDigits];
```

Фигура 8.Обучение на невронна мрежа [8]

7. Заключение

Машините с изкуствен интелект започнаха да заместват човека в много области, като например науката и техниката. Това обаче води със себе си до негативни резултати по отношение на трудовата заетост в човешките ресурси, като много от кадрите ще станат непотребни и могат да загубят работа си. Също така, машините все още не са достигнали достатъчна зрялост по начин, по който да заместят истински човешки мозък. Работата по изграждане на истински изкуствен интелект продължава в научните среди, като езиците за програмиране следват тази тенденция.

Създават се нови езици и подходи за алгоритмизация, получаването на знания и оформянето на машинен интелект. Разгледаните езици за програмиране в изкуствения интелект показват посоките на развитие, като се повишава удобството при използването им чрез добавена функционалност, но с това се увеличава и сложността им.

References

1. Интернет източник: Artificial Intelligence and Machine Learning: Policy Paper, URL: https://www.internetsociety.org/resources/doc/2017/artificial-intelligence-and-machine-learningpolicypaper/?gclid=Cj0KCQjwqs3rBRCdARIsADe1pfTA69Nv1TDuU33irZpblBeHZFC51xpsTJ7R08wyJqnAnuOTnfytL5UaAnjeEALw_wcB
2. Интернет източник: Your First Machine Learning Project in Python Step-By-Step – URL: https://machinelearningmastery.com/machine-learning-in-python-step-by-step/
3. Интернет източник: TensorFlow Meetup, Riadh Ayachi, URL: https://www.researchgate.net/publication/334626389_TensorFlow_Meetup/stats
4. Интернет източник: Machine Learning in R for beginners, URL: https://www.datacamp.com/community/tutorials/machine-learning-in-r
5. Интернет източник: KNN Algorithm: A Practical Implementation Of KNN Algorithm In R, URL: https://www.edureka.co/blog/knn-algorithm-in-r/
6. Heaton, Jeff, “Programming Neural Networks with Encog3 in Java”, Heaton Research Inc., 2011, ISBN: 978-1-60439-021-6
7. Интернет източник: Machine Learning in Lisp, URL: https://www.cs.unm.edu/~luger/ai-final2/LISP/CH%2019_Machine%20Learning%20in%20Lisp.pdf
8. Интернет източник: Machine Learning with brain.js and Tensorflow.js, URL: https://golb.hplar.ch/2019/01/machine-learning-with-brain-and-tensorflow-js.html
9. Nikolov, L., „Network Infrastructure for Cybersecurity Analysis“, Proceedings of International Scientific Conference “Defense Technologies”, Shumen, 2018, ISSN 2367-7902, URL: http://aadcf.nvu.bg/scientific_events/dft2018
10. Slavyanov, K.O. “An algorithm of fuzzy inference system for human resources selection tools”, Proceedings of the International Scientific Conference “Society. Integration. Education”, Vol. V, 2018, ISSN 1691-5887, p. 445-454, http://dx.doi.org/10.17770/sie2018vol1.3311

Dimitar I. Sumulyov,

FORMATION OF TARGET RADAR IMAGE, BY COMPARING OF TWO CORES FOR ANALIZE THE RADIOLOCATION INFORMATION

Dimitar I. Sumulyov

AAD and CIS Faculty, "Vassil Levski" NMU, Shumen, Bulgaria

ФОРМИРАНЕ НА ИЗОБРАЖЕНИЕ ОТ РАДИОЛОКАЦИОННА ЦЕЛ ЧРЕЗ СРАВНЕНИЕ НА ДВЕ ЯДРА ЗА ОБРАБОТКА НА РАДИОЛОКАЦИОННАТА ИНФОРМАЦИЯ

Димитър И. Сумульов

Факултет „А, ПВО и КИС", НВУ „В. Левски", Шумен, България

Abstract: *An algorithm with time-frequency transformation for signal processing and image forming of target is studied. Research on different cores of time-frequency transformation, different signal to noise ratios and different orientation of target are made. Results showed that the certain cores are better for lower signal to noise ratio.*

Keywords: *UWB radar, Time-frequency transforming, Radar image, target*

1. ВЪВЕДЕНИЕ

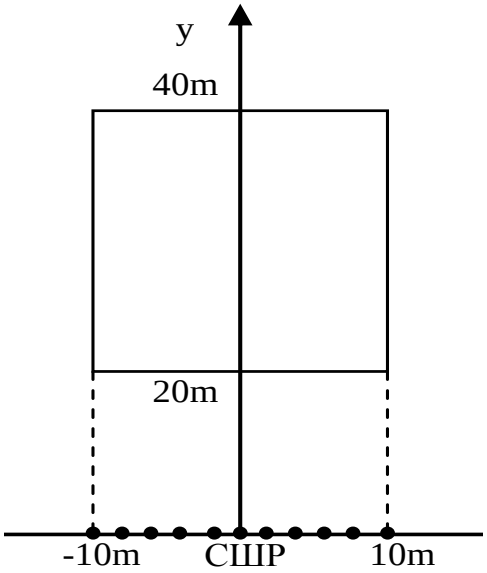
Развитието на свръхшироколентовите (UltraWideBand – UWB) технологии в последните десетилетия, доведе до внедряването на различни радари за откриване на обекти върху и под земната повърхност, системи за формиране на радиолокационно изображение на обекти, автомобилни радарни системи, комуникационни системи, системи за извършване на измервания, медицински системи и др. Тези системи поставят и нови изисквания както към използваните антени, така и към методите, използвани за анализ и проектиране .

В свръхшироколентовите радари (СШР) се използват различни алгоритми за обработка на сигналите и за формиране на изображения на наблюдавания сектор [1]. За да се определят условията, при които даден алгоритъм е подходящ за използване е необходимо да се извършват изследвания. Изследванията трябва да обхващат използване на различни параметри на алгоритмите и работата на алгоритмите при различни отношения сигнал/шум.

В доклада е изследван алгоритъмът, предложен в [2] при различни условия на работа. Предложен модел на цел, състояща се от няколко блестящи точки, за която може да се задава различна ориентация спрямо радара. Направени са изследвания при използване на различни ядра на преобразуването при различни отношения сигнал/шум и при различна ориентация на целта.

2. ИЗСЛЕДВАНЕ НА АЛГОРИТЪМ ЗА ОБРАБОТКА.

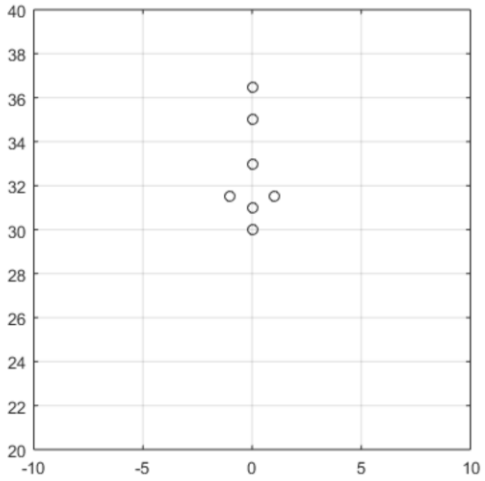
При изследванията е използвана геометричната постановка на разположение на радара и сектора на наблюдение, показана на фигура 1 [2]. Антените на СШР са разположени по оста *y* през разстояние от 2 метра. Всеки пиксел в изображението отговаря на квадрат от сектора със страна $dx = dy = 0{,}05m$. Времевият интервал, в който радара приема отразени сигнали, се определя от максималното и минималното разстояние от елемент на антенната система до координатите на точка от наблюдавания сектор [2,3].



Фигура 1. Геометрично разположение на радара и наблюдавания сектор.

Номерата на дискретите от времевия маргинал, които съответстват на даден пиксел от изображението се определят отделно за всеки елемент от антенната решетка по алгоритъма, предложен в [3]. Индексите за всеки пиксел се изчисляват предварително и се запаметяват, като по този начин по време на обработката не е необходимо те да бъдат изчислявани.

На фигура 2 е показано геометричното разположение на блестящите точки на тестовата цел при ориентация по оста *y*.



Фигура 2. Цел, състояща се от блестящи точки.

При симулациите се използва сигнал във вид на нормиран гаусов импулс, като отразения сигнал е сума от отразените сигнали от блестящите точки на целта:

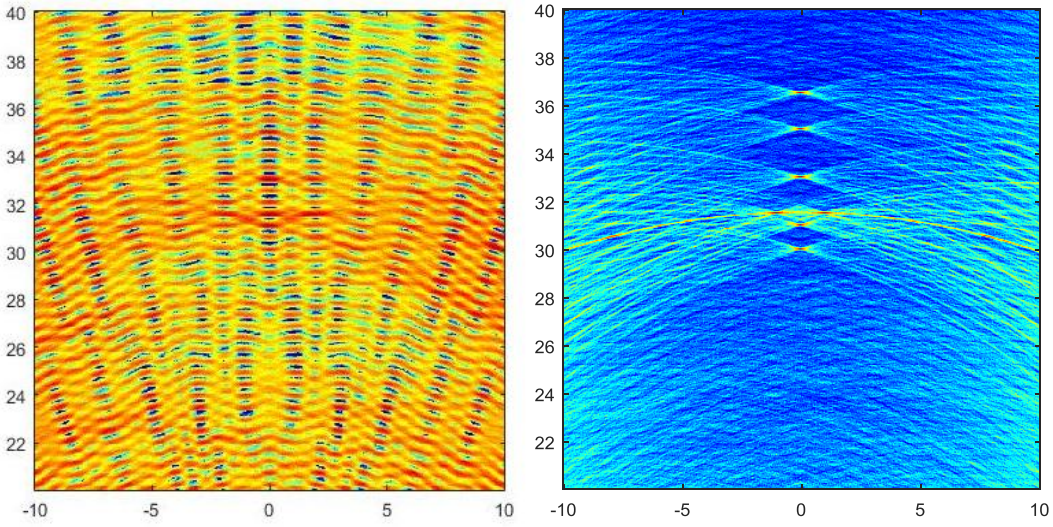
$$s_k(n) = \sum_{i=1}^{7} A_i(nt_s - t_{ki}) e^{-\pi \frac{(nt_s - t_{ki})^2}{\tau_u^2}}, \quad (1)$$

където $t_{ki} = 2\left[\sqrt{y_i^2 + (x_i - x_k)^2} - R_{\min}\right]/c$ е времезакъснението на сигнала, отразен от i-та блестяща точка, при работа на k-тия елемент на антенната система; x_i и y_i са координатите на i-та блестяща точка; x_k е координатата по оста x на k-тия елемент на антенната система; $A = \sqrt[4]{t_s^2 32\pi^2 / \tau_u^6}$ е амплитудата на импулса; $\tau_u = 0{,}2ns$ е продължителността на импулса.

Амплитудата на сигнала в (1) е подбрана така, че енергията на дискретизирания сигнал да бъде равна на единица.

Направени са изследвания на алгоритъма при използване на две различни ядра – на Вигнер и разделно ядро. Вида и изразите за описание на тези ядра са дадени в [4,5]. В доклада са направени изследвания за две ориентации на целта. Едното е при ориентация на целта по оста y (0°), а другото при ориентация на целта по оста x (90°). Изследвана е работата на алгоритъма при 3 различни отношения сигнал/шум (ОСШ).

На фигура 3 са показани формираните изображения за цел ориентирана по оста y при обработка с двете ядра и ОСШ 0,1.

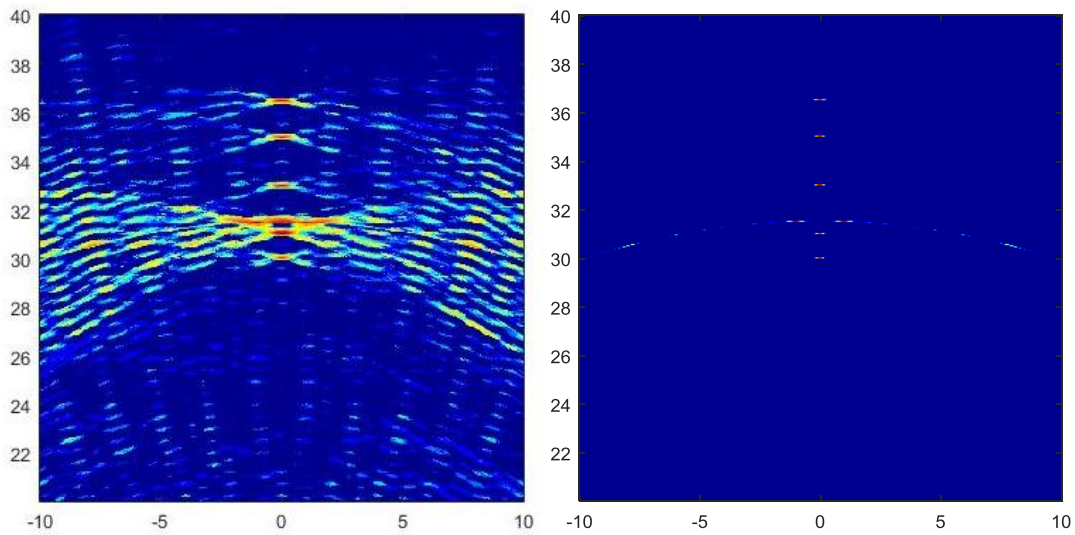


а) ядро на Вигнер *б) разделно ядро*

Фигура 3. Изображения на цел, ориентирана по оста y, при ОСШ 0,1 (-10dB).

Получените изображения показват, че при ОСШ 0,1 ядро на Вигнер не формира разпознаваем образ на целта, а при използване на разделно ядро изображението е с наличие на много шумове. Следователно алгоритъма не може да бъде използван при толкова малко ОСШ, независимо от използваното ядро.

На фигура 4 са показани формираните изображения за цел ориентирана по оста y при обработка с двете ядра и ОСШ 0,5.

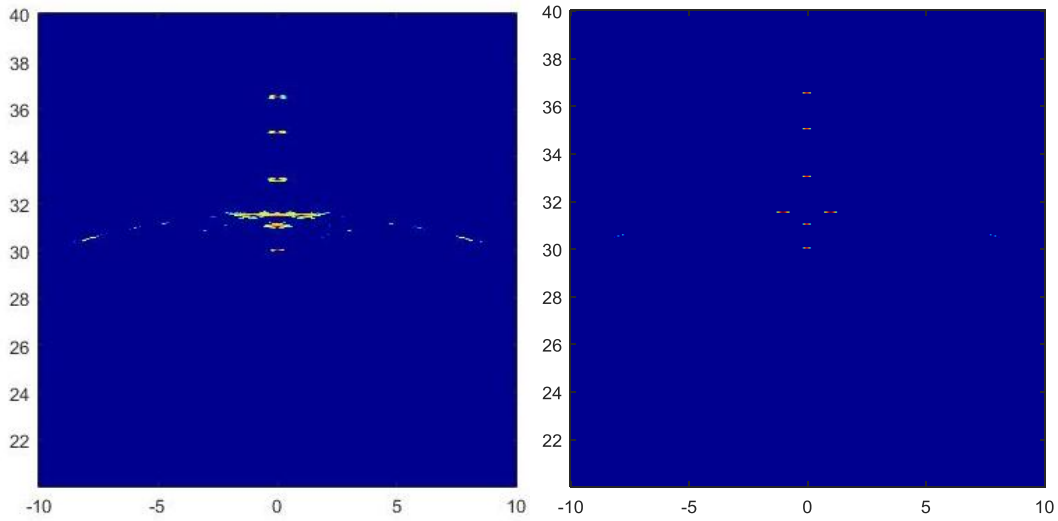


а) ядро на Вигнер *б) разделно ядро*

Фигура 4. Изображения на цел, ориентирана по оста y, при ОСШ 0,5 (-3dB).

Резултатите от изследванията показват, че формираното изображение при използване на ядро на Вигнер е с много шумове и практически е невъзможно да се различи целта. При използване на разделно ядро се формира ясно изображения на целта. Върху него се наблюдават известен брой зашумени пиксели, но те не пречат на категоричното разпознаване на целта. Сравнението с фигура 2 показва, че местоположението и ориентацията на целта върху формираното изображение съвпада с истинските.

На фигура 5 са показани формираните изображения за цел ориентирана по оста *y* при обработка с двете ядра и ОСШ 2.

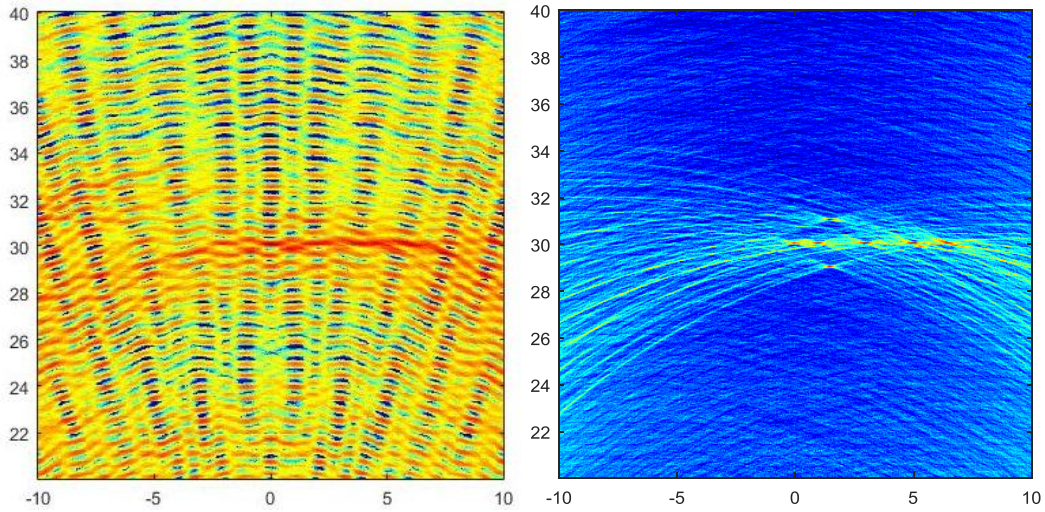


а) ядро на Вигнер *б) разделно ядро*

Фигура 5. Изображения на цел, ориентирана по оста y, при ОСШ 2 (3dB).

Получените резултати показват, че и при двете ядра се различава формата и ориентацията на целта. При използване на разделно ядро изображението е със значително по-високо качество и върху него не се забелязват шумове. Вижда се, че белезите от блестящите точки са с по-големи размери върху изображението при обработка с ядро на Вигнер.

На фигура 6 са показани формираните изображения за цел ориентирана по оста *x* при обработка с двете ядра и ОСШ 0,1.

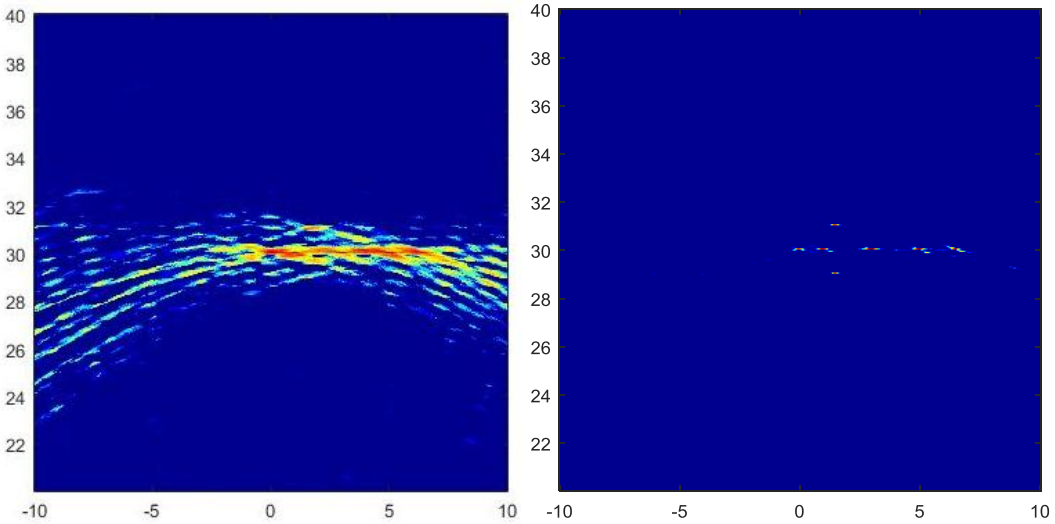


а) ядро на Вигнер *б) разделно ядро*

Фигура 6. Изображения на цел, ориентирана по оста x, при ОСШ 0,1 (-10dB).

При използване на ядро на Вигнер, изображението на целта от фигура 6 е много слабо различимо, като на фона на смущенията, тя се наблюдава само като силует. При използване на разделно ядро се формира по-ясна картина на целта, може да се определи нейната ориентация, но не и конкретното разположение на блестящите точки.

На фигура 7 са показани формираните изображения за цел ориентирана по оста *x* при обработка с двете ядра и ОСШ 0,5.

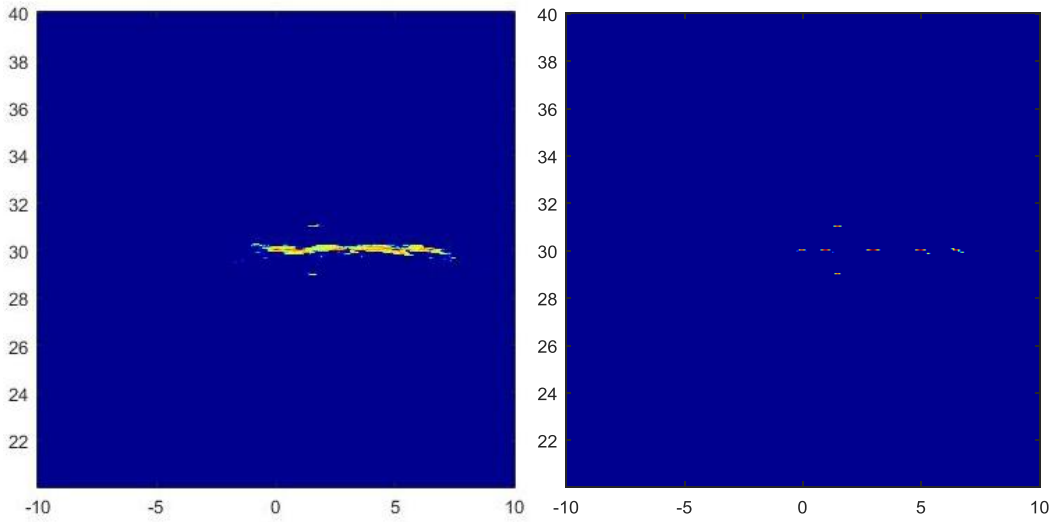


а) ядро на Вигнер *б) разделно ядро*

Фигура 7. Изображения на цел, ориентирана по оста x, при ОСШ 0,5 (-3dB).

Получените резултати показват, че при използване на разделно ядро се получава ясно изображение на целта, като се различават отделните блестящи точки. При използване на ядро на Вигнер може да се определи, че има цел, но не и нейните блестящи точки. При обработката с ядро на Вигнер се наблюдават области със шумове, което се дължи на интерференцията между зоните на неопределеност на радара. Сравнението между фиг. 4 и фиг. 7 показва, че при ориентация на целта по оста *x* изображенията са с по-малък шум, което се дължи на различните зони на неопределеност, които интерферират. Следователно ориентацията на целта оказва влияние върху качеството на радарното изображение, като това влияние е значително по-голямо за ядро на Вигнер.

На фигура 8 са показани формираните изображения за цел ориентирана по оста *x* при обработка с двете ядра и ОСШ 2.



а) ядро на Вигнер *б) разделно ядро*

Фигура 8. Изображения на цел, ориентирана по оста x, при ОСШ 2 (3dB).

Получените резултати показват, че и върху двете изображения се различава силуета на целта. При ядрото на Вигнер се наблюдава сливане на блестящите точки, разположени по оста *x*, което показва по-лошата разделителна способност на това ядро.

Получените резултати доказват, че при по-високи ОСШ могат да се използват и двете изследвани ядра, но изображенията, получавани при обработка с разделно ядро, са с по-висока разделителна способност. При по-малки ОСШ разделното ядро осигурява по-високо качество на изображенията. И при двете ядра се наблюдава зависимост на качеството на изображението от ориентацията на целта при по-малки ОСШ, но за разделното ядро тя е слаба, докато при ядрото на Вигнер е значителна.

3. ЗАКЛЮЧЕНИЕ

В доклада е изследван алгоритъм за обработка и формиране на изображение на цел, съставена от няколко блестящи точки, в свръхшироколентов радар, използващ време-честотно преобразуване. При изследванията е разработено математическо описание на геометрията на целта, позволяващо завъртането ѝ на произволен ъгъл. Получени са резултати от обработката на сигналите в радара и формиране на изображение при различни отношения сигнал/шум и различна ориентация на целта.

Получените резултати показват, че изображенията формирани чрез разделно ядро са с по-високо качество в сравнение с тези, получени при използване на ядро на Вигнер. Разделното ядро осигурява формиране на изображение, върху което се различава положението на блестящите точки при по-ниски отношения сигнал/шум.

Сравнението на изображенията при различна ориентация на целта показва, че ориентацията влияе върху качеството на изображението, като при ядрото на Вигнер то е много по-забележимо. За получаване на по-точна информация за това влияние е необходимо да се изследва формирането на изображения при повече положения на ориентация на целта и при използване на по-голям набор от ядра при обработката.

References

1. Иванова С. И., Изследване на ефективността на методите за обработка на информацията в свръхшироколентовите електронни системи, дисертация, 2012.

2. Сумульов Д. И., Димов Р. С., Маринов М. С., Алгоритъм за обработка на сигнали в свръхширококолентов радар и формиране на радиолокационно изображение, Годишна международна научна конференция, факултет „Авиационен“, 19-20 април 2018.

3. Сумульов Д. И., Маринов М. С., Изследване на алгоритъм за обработка и формиране на изображение на точкова цел в свръхширококолентов радар, Годишна международна научна конференция, факултет „Авиационен“, 19-20 април 2018.

4. Hlawatsch F.,G. Matz: “Time-frequency methods for signal estimation and detection in Time-Frequency Signal Analysis and Processing: A Comprehensive Reference”, ed. B. Boashash , Oxford, UK: Elsevier, 2003.

5.Jeong J., W. J. Williams: “A new formulation of generalized discrete-time-time frequency distributions”, IEEE International Conference on Acoustics, Speech, and Signal Processing, volume 5, April 1991.

Dyanko K. Hubenov, Nikolay Zh. Kulev, Rosen A. Bogdanov,

ADALM-PLUTO BUILD SDR SYSTEM PROGRAMMING

Dyanko K. Hubenov, Nikolay Zh. Kulev, Rosen A. Bogdanov

Communication Networks and Systems Department,
"Vasil Levski" National Military University, 1 "Karel Shkorpil" str., Shumen, Bulgaria

e-mail: d_hubenov@abv.bg, nz_kulev@abv.bg, rab61@abv.bg

Abstract: *In this paper are given programming models for software reconfiguration of Adalm-Pluto build SDR system.*

Keywords: *SDR, Analog Devices, Zynq, Xilinx*

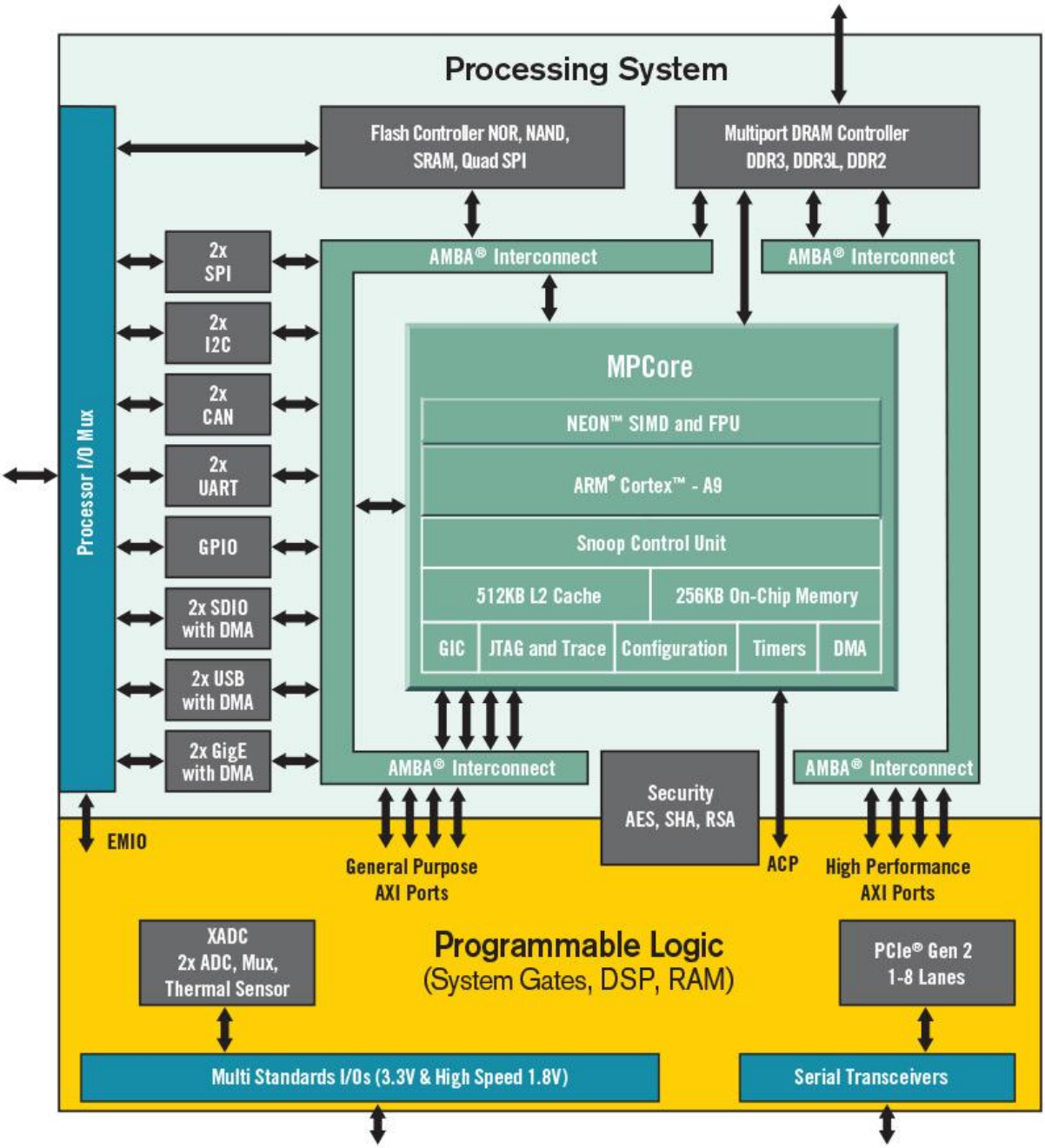
ПРОГРАМИРАНЕ НА SDR СИСТЕМА, БАЗИРАНА НА ADALM-PLUTO

Дянко К. Хубенов, Николай Ж. Кулев, Росен А. Богданов

Катедра „Комуникационни мрежи и системи, Факултет „Артилерия, ПВО и КИС",
Национален военен университет „Васил Левски", гр. Шумен, ул. „Карел Шкорпил" 1

Въведение

SDR системите изпълняват комбинация от множество задачи за обработка на данни, комуникация и потребителски интерфейс, които имат различни изисквания за ширина на лентата за обработка и ограничения при работа в реално време. Затова, хардуерната платформа, избрана за изпълнение на такава система трябва да е стабилна и мащабируема в същото време позволяваща бъдещи подобрения и разширения на системата. Xilinx Zynq-7000 All Programmable SoCs отговаря на тези изисквания чрез предоставяне на високопроизводителна система за обработка, комбинирана с програмируема логика, както е показано на фигура 1. Комбинацията от програмируема логика и система за обработка осигурява изключителна паралелна мощност на обработка, ефективност в реално време, бързи изчислителни скорости и гъвкавост на свързаността.



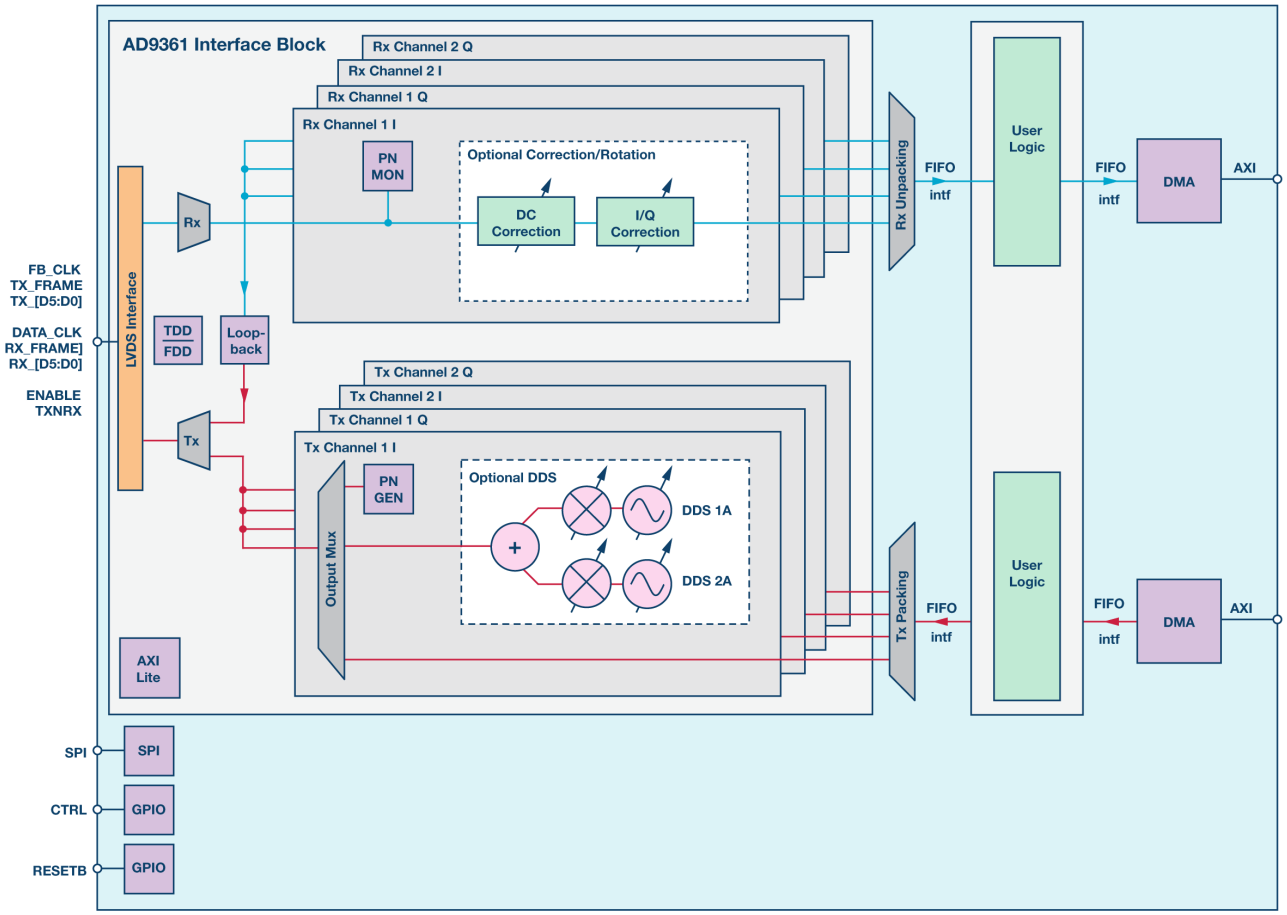
Фигура. 1. Функционална блокова схема на Xilinx Zynq SoC [3]

1. Софтуерна инфраструктура

Програмируемата система Xilinx Zynq All Programmable System on Chip (AP SoC) интегрира софтуерната програмируемост на ARM-базиран процесор с хардуерната програмируемост на FPGA, което позволява хардуерно ускоряване при интегриране на CPU, DSP, стандартен продукт със специфично приложение ASSP (Application-Specific Standard Product) и смесена сигнална функционалност в едно устройство. Устройството разполага с двуядрен процесор ARM Cortex ™ -A9, който е свързан с 28 nm програмируема логика, базирана на Artin® 7. Оборудван е и с най-често използваните хардуерни периферни устройства като USB и SPI.

Фигура 2 показва инфраструктурата на Analog Devices Zynq за поддръжка на ADALM-PLUTO и платките FMCOMMSx с възможности за използване на hardware description language HDL и софтуерен дизайн.

Всички ADI Linux драйвери са базирани на Linux индустриална входно/изходна подсистема Linux IIO, която е включена във всички основни Linux ядра. IO Scope е приложение с отворен код за Linux, разработено от Analog Devices [2], което работи на двуядрения ARM Cortex-A9 процесор в Xilinx Zynq и има способността да представя данни в реално време, придобити от всички аналогови устройства с FPGA Mezzanine Card (FMC) карта, свързани към платформата Xilinx Zynq. Данните може да се представят както във времева и честотна област, така и като констилация.



Фигура 2. ADI HDL и софтуерна инфраструктура [4]

2. Програмиране на SDR системата

За тестване на софтуерните възможности за пренастройване на когнитивната радиосистема, базирана на хардуерната платформа ADALM-PLUTO, са използвани възможностите за програмиране на вградения FPGA, което предоставя няколко варианта за генериране на предаваните данни. Първата възможност използва вградения директен цифров синтезатор DDS (Direct Digital Synthesizer) за предаване на едно- и дву-тонален сигнал по канали I и Q на DAC. Втората възможност използва функцията за директен достъп до паметта DMA (Direct Memory Access) за предаване на персонализирани данни, които са съхранени във файл [1].

Управлението на приемопредавателя [5,6] в PlutoSDR се осъществява чрез IIO подсистемата на Linux. Драйверите на устройството позволяват да се вземат проби чрез IIO подсистемата на Linux ядрото, управляваща функциите за аналоговоцифрови или цифровоаналогови преобразуватели и свързаните с тях хардуер. IIO комуникира с потребителското пространство чрез sysfs и символни устройства чрез извикване на функция или метод. Библиотеката LibIIO осигурява всякакъв вид абстракция на устройства и обработва всички видове вътрешни IO.

- **Управление на приемопредавателя**

Управлението на приемопредавателя се извършва в четири стъпки:
Създаване на IIO IP Network, зададена чрез IP адрес ip:xxx.xxx.xxx.xxx или usb:XX.XX.X
Получаване на структурата на физическия слой на AD936x PHY device
Задаване на честотата на TX LO
Задаване на честотата на дискретизация RX
Програма на C++ за управление на предавателя е представена на Листинг 1.

Листинг 1. *Управление на приемопредавателя*

```
#include <iio.h>

int main (int argc, char **argv)
{
        struct iio_context *ctx;
        struct iio_device *phy;

        ctx = iio_create_context_from_uri("ip:192.168.2.1");

        phy = iio_context_find_device(ctx, "ad9361-phy");

        iio_channel_attr_write_longlong(
                iio_device_find_channel(phy, "altvoltage0",
true),
                "frequency",
                2400000000); /* TX LO честота = 2.4GHz */

        iio_channel_attr_write_longlong(
                iio_device_find_channel(phy, "voltage0",
false),
                "sampling_frequency",
                5000000); /* RX скорост = 5 MSPS */

        receive(ctx);

        iio_context_destroy(ctx);

        return 0;
}
```

- **Управление на приемането на данни**

Управлението на приемането на данни се извършва в 6 стъпки:
Получаване на RX структурата на устройството;
Получаване на входните IQ канали;
Разрешаване на I и Q каналите;
Създаване на RX буфер;
Запълване на буфера;

1. Обработка на пробите.

Програма на C++ за управление на приемането на данни е представена на Листинг 2.

Листинг 2. *Управление на приемането на данни*

```
int receive(struct iio_context *ctx)
{
        struct iio_device *dev;
        struct iio_channel *rx0_i, *rx0_q;
        struct iio_buffer *rxbuf;

        dev = iio_context_find_device(ctx, "cf-ad9361-lpc");

        rx0_i = iio_device_find_channel(dev, "voltage0", 0);
        rx0_q = iio_device_find_channel(dev, "voltage1", 0);

        iio_channel_enable(rx0_i);
        iio_channel_enable(rx0_q);

        rxbuf = iio_device_create_buffer(dev, 4096, false);
        if (!rxbuf) {
                perror ("Could not create RX buffer");
                shutdown();
        }

        while (true) {
                void *p_dat, *p_end, *t_dat;
                ptrdiff_t p_inc;

                iio_buffer_refill(rxbuf);

                p_inc = iio_buffer_step(rxbuf);
                p_end = iio_buffer_end(rxbuf);

                for (p_dat = iio_buffer_first(rxbuf, rx0_i);
p_dat < p_end; p_dat += p_inc, t_dat += p_inc) {
                   const int16_t i = ((int16_t*)p_dat)[0];
//Real(I)
                   const int16_t q = ((int16_t*)p_dat)[1];
//Imag(Q)

                        /* Обработка на пробите */
                }
        }
        iio_buffer_destroy(rxbuf);
}
```

Програмируемата хардуерна архитектура на когнитивна радиосистема, базирана на ADALM-PLUTO, позволява да се изпълняват множество задачи в реално време, като обработка на данни, комуникация и потребителски интерфейс. Комбинацията от програмируеми RF интерфейс, логика и система за обработка предоставя възможност за паралелна обработка, бързи изчислителни процеси, ефективност при работа в реално време, и гъвкавост на свързаността. Това от своя страна, осигурява възможност за бъдещи подобрения и разширения на когнитивната радиосистема.

References

1. Analog Devices, ADALM-PLUTO: SDR Active Learning Module, 2017, Available at http://www.analog.com/media/en/news-marketing-collateral/product-highlight/ADALM-PLUTO-Product-Highlight.pdf .

2. Analog Devices, RF Agile Transceiver AD9363, 2016, Available at http://www.analog.com/media/en/technical-documentation/data-sheets/ad9363.pdf .

3. Xilinx, Zynq-7000 SoC Data Sheet: Overview, 2018. Available at https://www.xilinx.com/support/documentation/data_sheets/ds190-Zynq-7000-Overview.pdf .

4. Xilinx, Zynq-7000 SoC Technical Reference Manual, 2018. Available at https://www.xilinx.com/support/documentation/user_guides/ug585-Zynq-7000-TRM.pdf .

5. Димитров, Д. И., Анализ на информационния потенциал на радиотехнически системи, използващи ефекта на нелинейно отражение на електромагнитните вълни, Научни трудове, Русенски университет „А. Кънчев“, Том 47, Серия 3.2, с. 68-72, 2008, ISSN 1311-3321.

6. Димитров, Д. И., Василев, В. М., Особености на параметрите на сондиращия сигнал в нелинейна радиолокационна станция, „Военно издателство“, София, с. 36-50, 2008, ISSN 1312-2916.

Dyanko K. Hubenov, Nikolay Zh. Kulev, Rosen A. Bogdanov,

ADALM-PLUTO BUILD SDR SYSTEM TESTING

Dyanko K. Hubenov, Nikolay Zh. Kulev, Rosen A. Bogdanov

Communication Networks and Systems Department,
"Vasil Levski" National Military University, 1 "Karel Shkorpil" str., Shumen, Bulgaria

e-mail: d_hubenov@abv.bg, nz_kulev@abv.bg, rab61@abv.bg

Abstract: *This paper shows the results of multiple test of the capabilities for software reconfiguration of Adalm-Pluto build SDR system.*

Keywords: *SDR, Analog Devices, Zynq, Xilinx*

ТЕСТВАНЕ НА SDR СИСТЕМА, БАЗИРАНА НА ADALM-PLUTO

Дянко К. Хубенов, Николай Ж. Кулев, Росен А. Богданов

Катедра „Комуникационни мрежи и системи, Факултет „Артилерия, ПВО и КИС",
Национален военен университет „Васил Левски", гр. Шумен, ул. „Карел Шкорпил" 1

Въведение

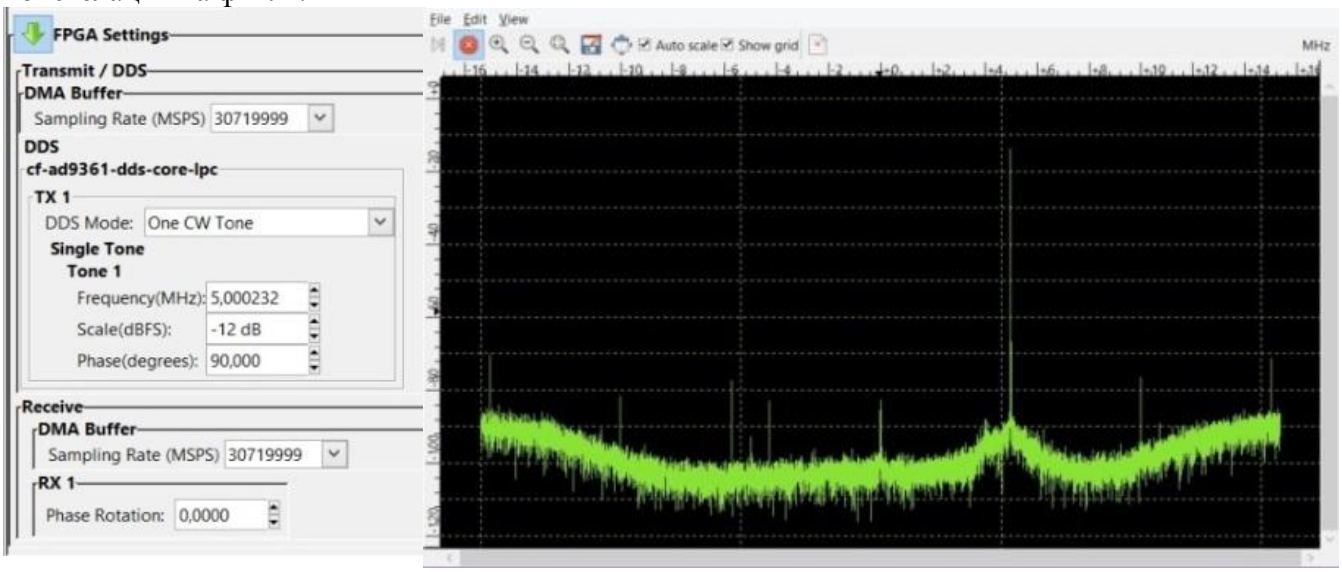
Модулът ADALM-PLUTO (PlutoSDR) е лесен за използване инструмент, предлаган от Analog Devices Inc., който може да се използва за изследване на основите на софтуерно дефинираното радио (SDR), безжичните и радио комуникации. Той предоставя лична преносима RF лаборатория, която може да се използва с управляващ хост. Въз основа на приемо/предавателя AD9363, той предлага един канал за приемане и един предавателен канал, който може да работи в пълен дуплекс, способен да генерира или измерва RF аналогови сигнали от 325 до 3800 MHz, до 61,44 MSPS с 20 MHz честотна лента. PlutoSDR е напълно самостоятелен, портативен джобен модул и се захранва изцяло от USB с фърмуера по подразбиране. Може да работи с помощта на OS X ™, Windows ™ и Linux ™ операционни системи. Освен управление от командната линия, той позволява разработки чрез софтуерни пакети като MATLAB или Simulink, които осигуряват иновативен интуитивен графичен потребителски интерфейс GUI за минимизиране времето на обучение и изследване.

Тестване на SDR системата

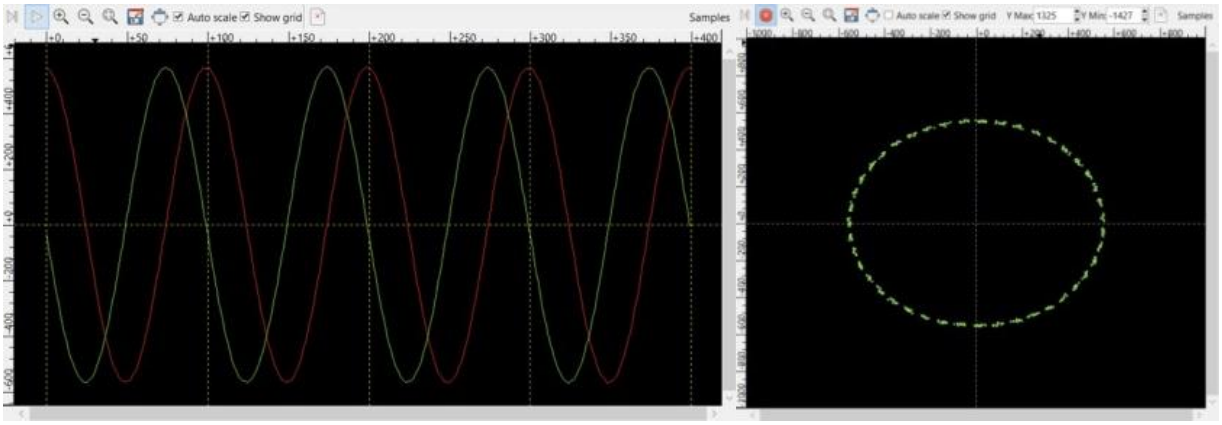
За тестване на възможностите за реконфигуриране на SDR устройството са програмирани и изследвани следните три режима на предаване и приемане на данни: една тонална честота, две тонални честоти и независимо управление на I/Q каналите. За всеки режим са представени сигналите на I/Q каналите във времевата област, получения спектър и констелацията на сигнала.

✓ **Една тонална честота**

В режим на една тонална честота „One CW Tone“ се извежда един тон с непрекъсната синусоида Continuous Wave (CW). Плъгинът показва контролите за задаване на честота, амплитуда и фаза само за един тон и настройва амплитудата на другия тон на 0. Сигналът се извежда на канал I на DAC и дефазираният на 90 градуса сигнал се извежда на канал Q на DAC. Параметрите на предаваната тонална честота и спектърът на сигнала са представени на фиг. 1, а неговото времево представяне и констелация на фиг. 2.



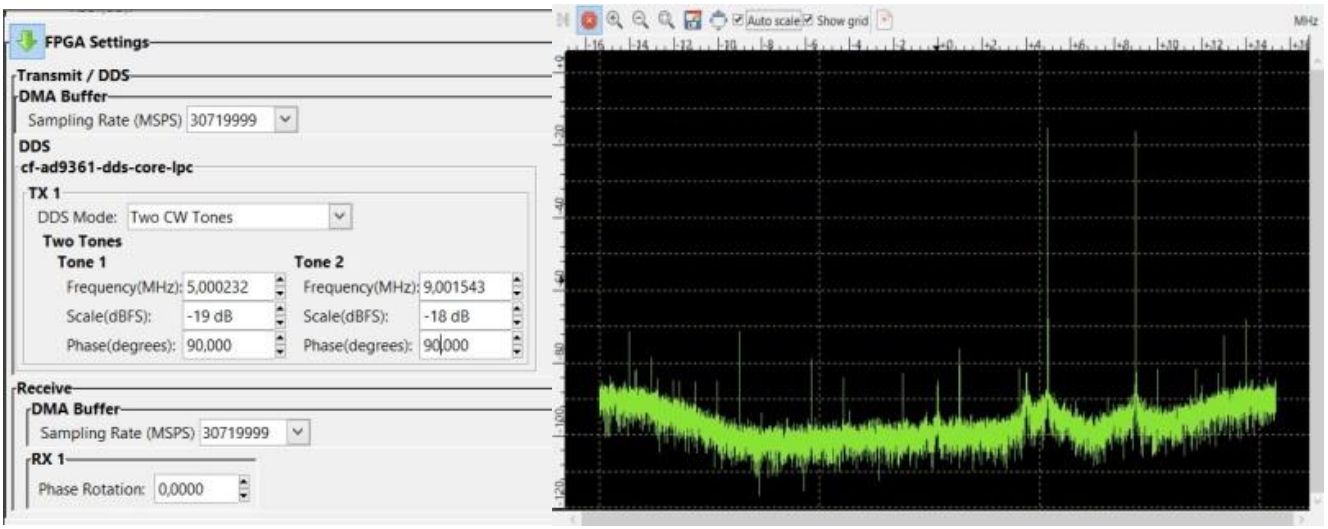
Фигура 1. *Параметри и спектър на предавания сигнал с една тонална честота*



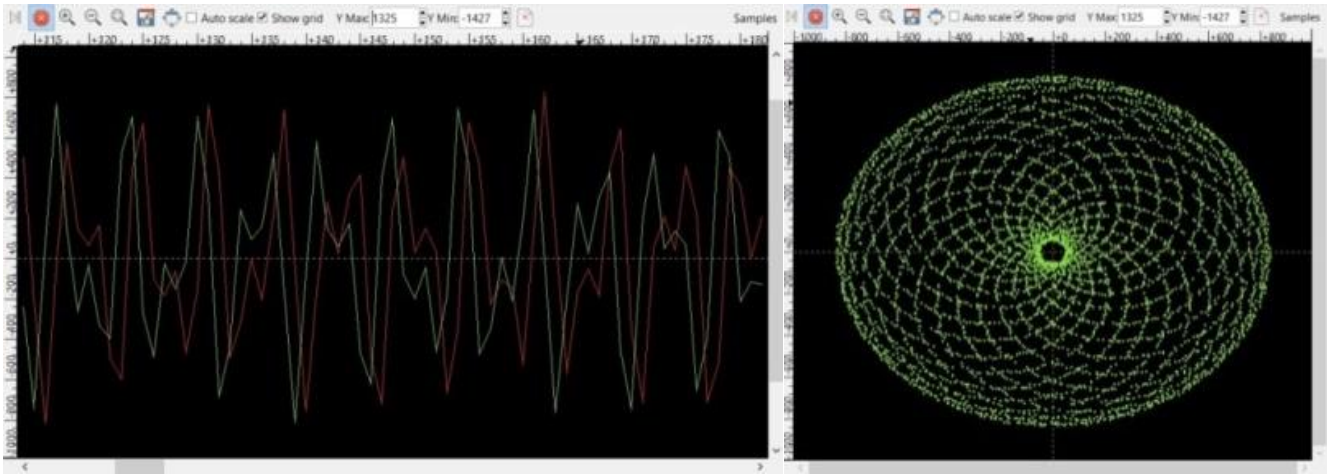
Фигура 2. *Времево представяне и констелация на предавания сигнал с една тонална честота*

✓ **Две тонални честоти**

При режима на две тонални честоти „Two CW Tone“ се извеждат два тона с непрекъснати синусоиди CW. Плъгинът показва контролите за задаване на честотите F_1 и F_2, амплитудите A_1 и A_2, както и фазите P_1 и P_2 за двата тона. Полученият сигнал се извежда на канал I на DAC и сигналът, дефазиран на 90 градуса, се извежда на канала Q на DAC. Параметрите на предаваните две тонални честоти и спектърът на сигнала са представени на фиг. 3, а неговото времево представяне и констелация на фиг. 4.



Фигура 3. *Параметри и спектър на предавания сигнал с две тонални честоти*



Фигура 4. *Времево представяне и констелация на предавания сигнал с две тонални честоти*

✓ **Независимо управление на I/Q каналите**

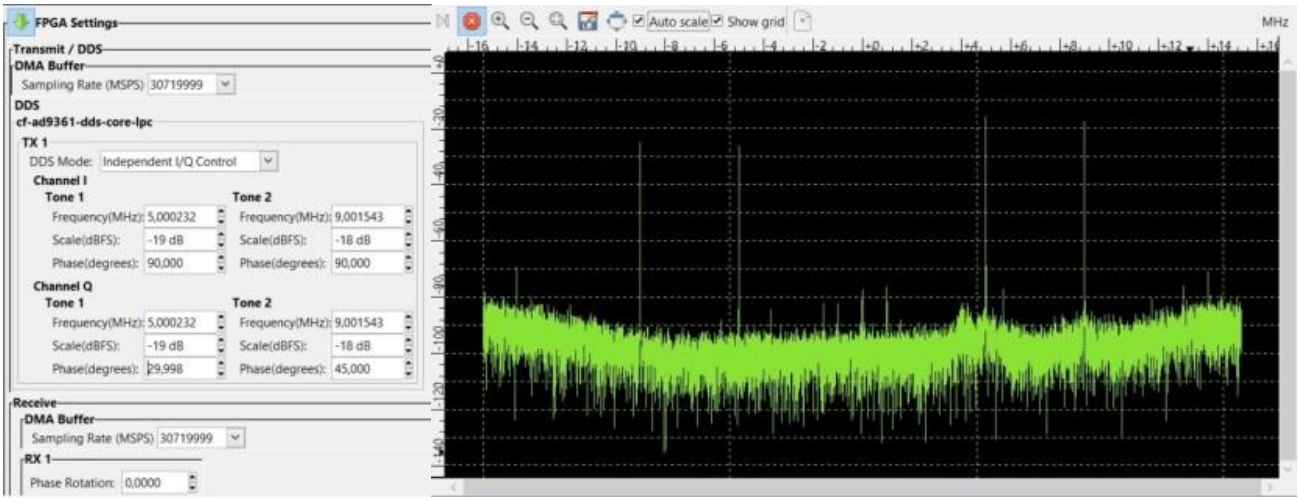
При независимото управление на I/Q каналите „Independent I/Q Control“ се задават честотите, амплитудите и фазите за двата тона, които ще бъдат изведени на канал I и двата тона, които ще бъдат изведени на канал Q. Те могат да се конфигурират независимо един от друг.

Двутоналният сигнал T се дефинира като сума от двата тона:

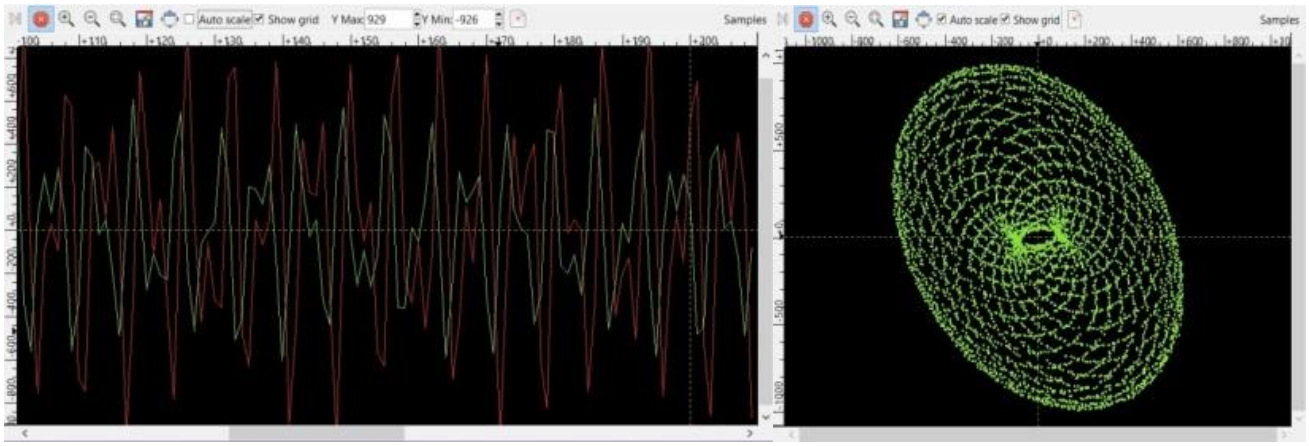
$$T(t) = A_1.\sin(2\pi F_1 t + P_1) + A_2.\sin(2\pi F_2 t + P_2), \qquad (4.1)$$

където A е амплитудата, F – честотата, а P – фазата на тона.

Параметрите на предаваните две тонални честоти и спектърът на сигнала са представени на фиг. 5, а неговото времево представяне и констелация на фиг. 6.



Фигура 5. *Параметри и спектър на предавания сигнал с независими I и Q канали*



Фигура 6. *Времево представяне и констелация на предавания сигнал с независими I и Q канали*

Реализираните тестове на SDR системата в режим на предаване и приемане на данни при една тонална честота, две тонални честоти и независимо управление на I/Q каналите доказват функционалността за реконфигуриране на радиоустройството.

References

1. Analog Devices, ADALM-PLUTO: SDR Active Learning Module, 2017, Available at http://www.analog.com/media/en/news-marketing-collateral/product-highlight/ADALM-PLUTO-Product-Highlight.pdf .
2. Analog Devices, RF Agile Transceiver AD9363, 2016, Available at http://www.analog.com/media/en/technical-documentation/data-sheets/ad9363.pdf
3. Xilinx, Zynq-7000 SoC Data Sheet: Overview, 2018. Available at https://www.xilinx.com/support/documentation/data_sheets/ds190-Zynq-7000-Overview.pdf .
4. Xilinx, Zynq-7000 SoC Technical Reference Manual, 2018. Available at https://www.xilinx.com/support/documentation/user_guides/ug585-Zynq-7000-TRM.pdf.

Dyanko K. Hubenov, Nikolay Zh. Kulev, Rosen A. Bogdanov,

ADALM-PLUTO BUILD SDR SYSTEM FREQUENCY BAND SWITCH TESTS

Dyanko K. Hubenov, Nikolay Zh. Kulev, Rosen A. Bogdanov

Communication Networks and Systems Department,
"Vasil Levski" National Military University, 1 "Karel Shkorpil" str., Shumen, Bulgaria

e-mail: d_hubenov@abv.bg, nz_kulev@abv.bg, rab61@abv.bg

Abstract: *ABSTRACT: In this paper are given the results of testing the reconfiguration abilities of Adalm-Pluto build SDR system.*

Keywords: *SDR, E-UTRA, LTE, Analog Devices*

ТЕСТВАНЕ НА ВЪЗМОЖНОСТИТЕ ЗА ЗАЕМАНЕ НА РАЗЛИЧНИ ЧЕСТОТНИ ЛЕНТИ НА SDR СИСТЕМА БАЗИРАНА НА ADALM-PLUTO

Дянко К. Хубенов, Николай Ж. Кулев, Росен А. Богданов

Катедра „Комуникационни мрежи и системи, Факултет „Артилерия, ПВО и КИС",
Национален военен университет „Васил Левски", гр. Шумен, ул. „Карел Шкорпил" 1

Въведение

Тестването на възможността за заемане на различна честотна лента на SDR система, базирана на ADALM-PLUTO, е реализирано чрез един от специфицираните E-UTRA тест модели E-TM (E-UTRA Test Models). E-UTRA е усъвършенствания въздушен интерфейс за мобилни мрежи в 3GPP LTE (3rd Generation Partnership Project стандарт Long Term Evolution).

В E-UTRA тест моделите се използват следните основни параметри:

- Тестовите модели са дефинирани за порт с една антена (p = 0), 1 кодова дума (q = 0), 1 слой; повторно кодиране не се използва;
- Продължителността е 10 подкадри (10 ms);
- Нормален цикличен префикс CP (Cyclic Prefix);
- Виртуални ресурсни блокове от тип за локализация, без вътрешен подкадър за скачане в PDSCH (Physical Downlink Shared CHannel);
- Не се използват специфични UE (User Equipment) еталонни сигнали;
- Настройките на захранването на физическите канали се определят от физическия канал EPRE (Energy Per Resource Element) по отношение на EPRE на RS (Reference

Symbol). Относителната точност на физическия канал EPRE, както е посочена в EPPE на RS, трябва да има толеранс от ± 0,5 dB.

1. Параметри на тестовия модел

За реализиране на тестовете е избран тестовият модел E-TM3.1, който се използва за проверка на динамиката на предаваната мощност и качеството на предавания сигнал. Той е един от най-натоварващите тестове, защото при него се използва 64 QAM. Параметрите на физическия канал при E-TM3.1 са показани в табл. 1.

Таблица 1. *Параметрите на физическия канал при E-TM3.1*

Параметри	1.4 MHz	3 MHz	5 MHz	10 MHz	15 MHz	20 MHz
Еталонни сигнали RS, Сигнали за синхронизация						
RS усилване, $P_B = E_B/E_A$	1	1	1	1	1	1
Сигнал за синхронизация EPRE/E_{RS} [dB]	0.000	0.000	0.000	0.000	0.000	0.000
Reserved EPRE/E_{RS} [dB]	-inf	-inf	-inf	-inf	-inf	-inf
PBCH (Physical Broadcast Channel)						
PBCH EPRE/E_{RS} [dB]	0.000	0.000	0.000	0.000	0.000	0.000
Reserved EPRE/E_{RS} [dB]	-inf	-inf	-inf	-inf	-inf	-inf
PCFICH (PCFICH Physical control format indicator channel)						
# of symbols used for control channels	2	1	1	1	1	1
PCFICH EPRE/E_{RS} [dB]	3.222	0	0	0	0	0
PHICH (Physical hybrid-ARQ indicator channel)						
# of PHICH groups	1	1	1	2	2	3
# of PHICH per group	2	2	2	2	2	2
PHICH BPSK symbol power/E_{RS} [dB]	-3.010	-3.010	-3.010	-3.010	-3.010	-3.010
PHICH group EPRE/E_{RS} [dB]	0	0	0	0	0	0
PDCCH (Physical downlink control channel)						
# of available REGs	23	23	43	90	140	187
# of PDCCH	2	2	2	5	7	10
# of CCEs per PDCCH	1	1	2	2	2	2
# of REGs per CCE	9	9	9	9	9	9
# of REGs allocated to PDCCH	18	18	36	90	126	180
# of <NIL> REGs added for padding	5	5	7	0	14	7
PDCCH REG EPRE/E_{RS} [dB]	0.792	2.290	1.880	1.065	1.488	1.195
<NIL> REG EPRE/E_{RS} [dB]	-inf	-inf	-inf	-inf	-inf	-inf
PDSCH (Physical downlink shared channel)						
# of QPSK PDSCH PRBs which are boosted	6	15	25	50	75	100
PRB $P_A = E_A/E_{RS}$ [dB]	0	0	0	0	0	0
# of QPSK PDSCH PRBs which are de-boosted	0	0	0	0	0	0
PRB $P_A = E_A/E_{RS}$ [dB]	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.

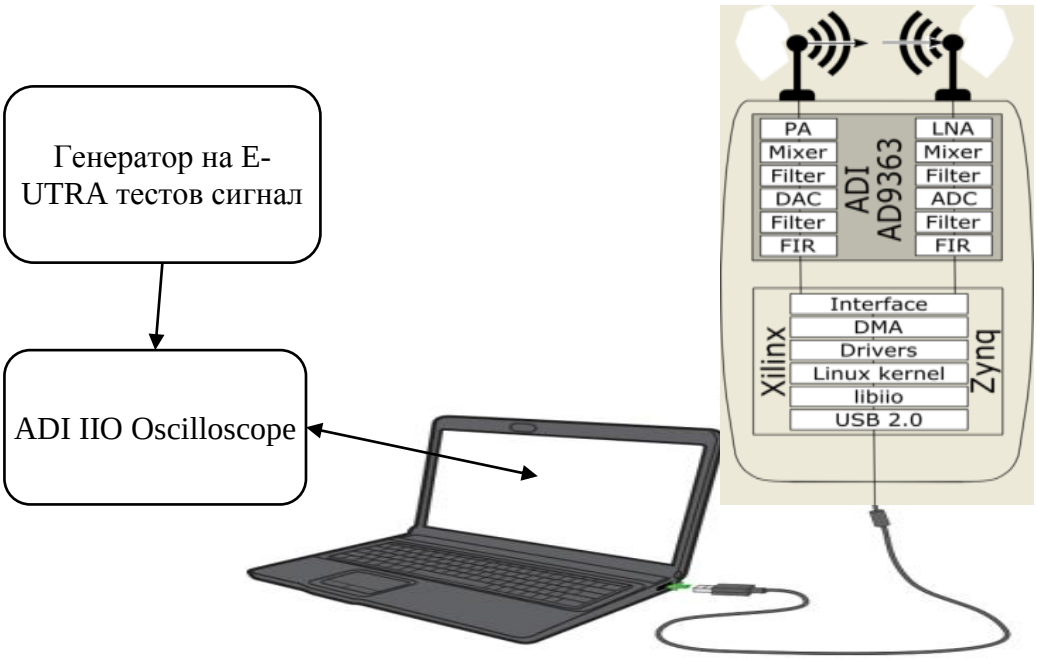
Сигналите на физическия канал при E-TM3.1 са генерирани в среда MATLAB чрез lteTestModelTool (Листинг 1).

Листинг 1. *Генериране на тестовия модел в низходящата връзка*

```
//Генерира сигнал във временната област txWaveform и двумерен масив
от ресурсни елементи txGrid за тест модел TS 36.141 E-TM 3.1
с 10MHz честотна лента.
tmn = '3.1';
bw = '10MHz';
tmCfg = lteTestModel(tmn,bw);
[txWaveform,txGrid,tm] = lteTestModelTool(tmCfg);
```

2. Резултати от тестването на SDR системата

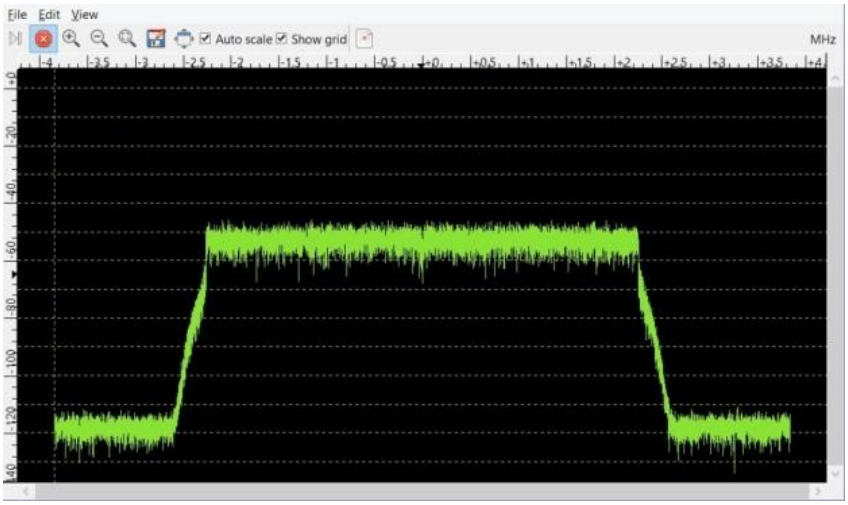
Реализирани са над 100 теста с тест модел TS 36.141 E-TM 3.1 съответно при честотни ленти 5, 10 и 20 MHz. Блоковата схема на опитната тестова постановка е показана на фиг. 1.



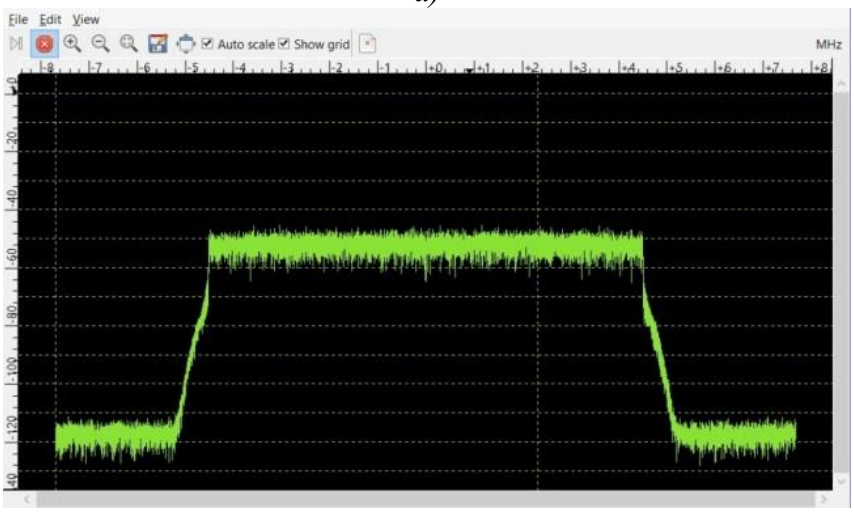
Фигура 1. *Блокова схема на опитната тестова постановка*

При всеки от тестовете са изследвани честотната лента, I и Q каналите, и констелацията на приетия сигнал. Резултатите са представени на фигури 2, 3 и 4.

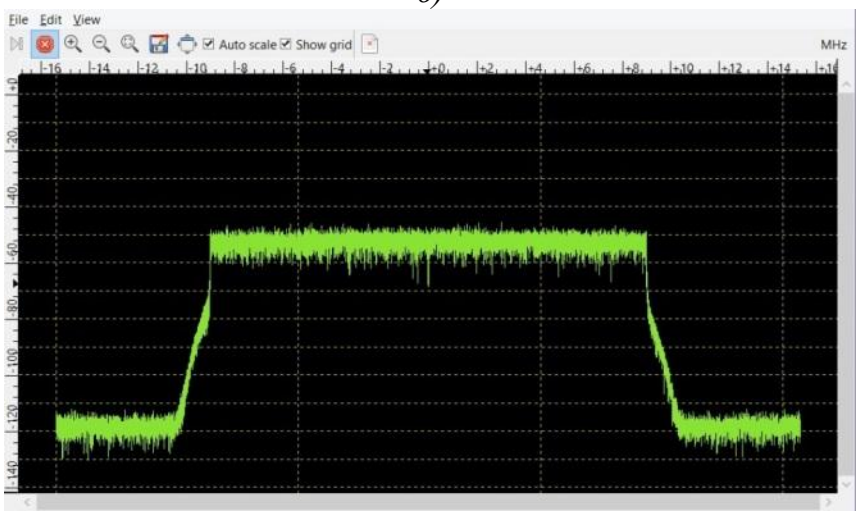
Анализът на резултатите от направените тестове потвърждава възможността на когнитивната радиосистема, базирана на ADALM-PLUTO, за бърза пренастройка (по-малко от секунда) от една честотна лента на друга, както и устойчивост в честотната лента и формата на приетите сигнали в устройството.



а)

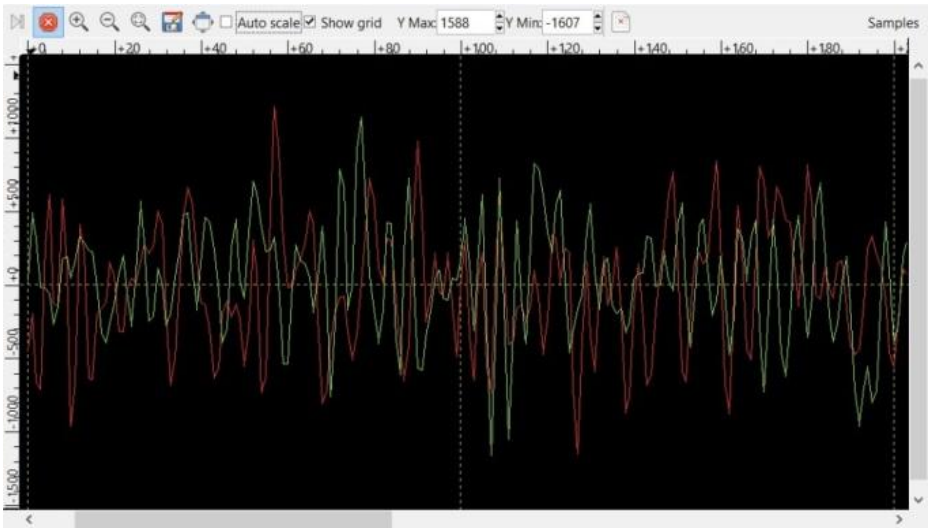


б)

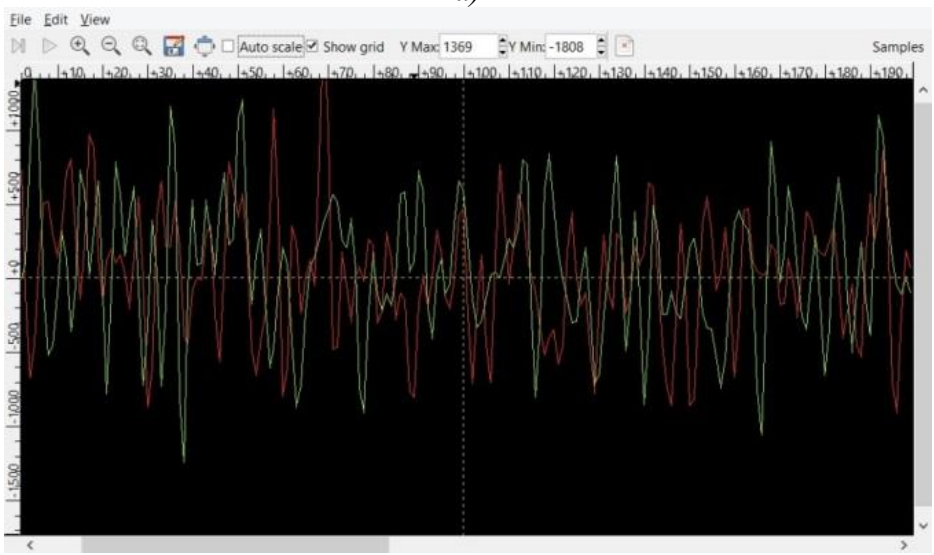


в)

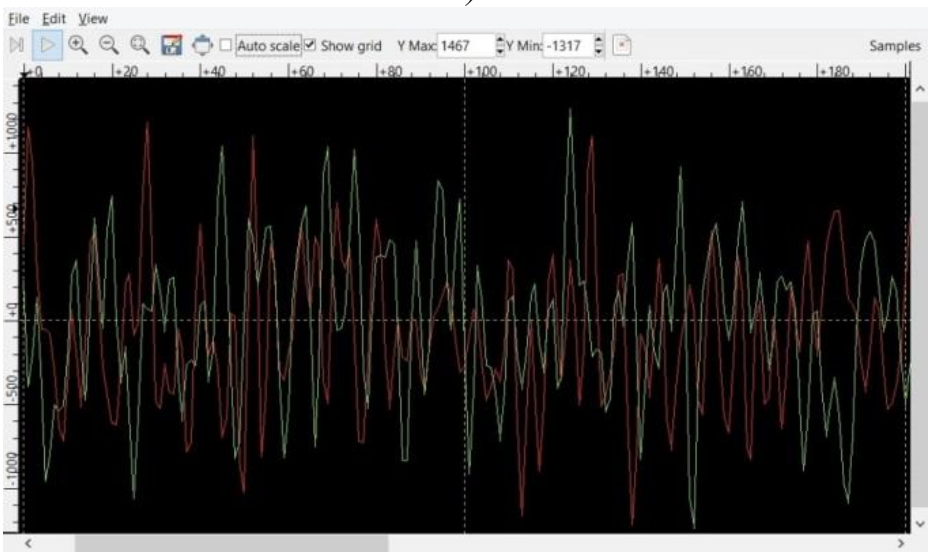
Фигура 2. *Честотна лента на приетия сигнал при тест модел E-TM 3.1*
а) 5 MHz б) 10 MHz в) 20 MHz



а)

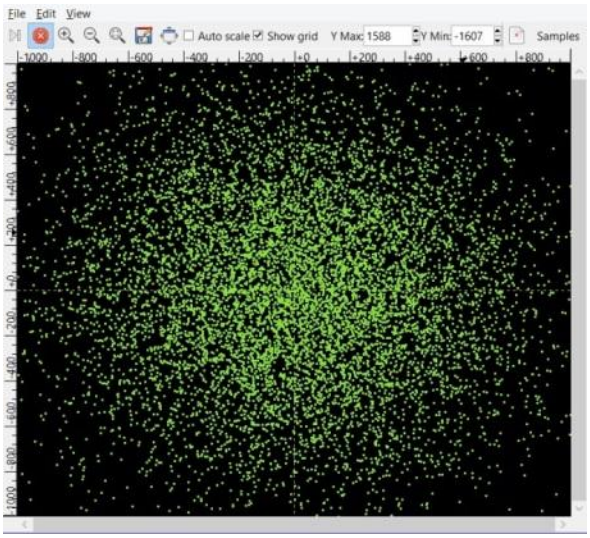


б)

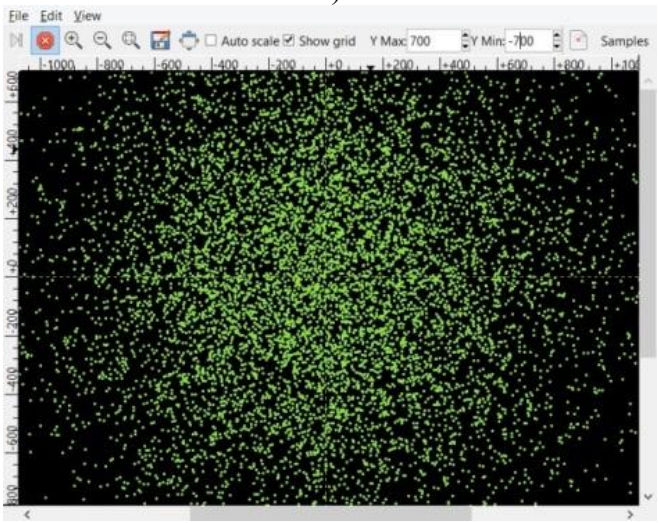


в)

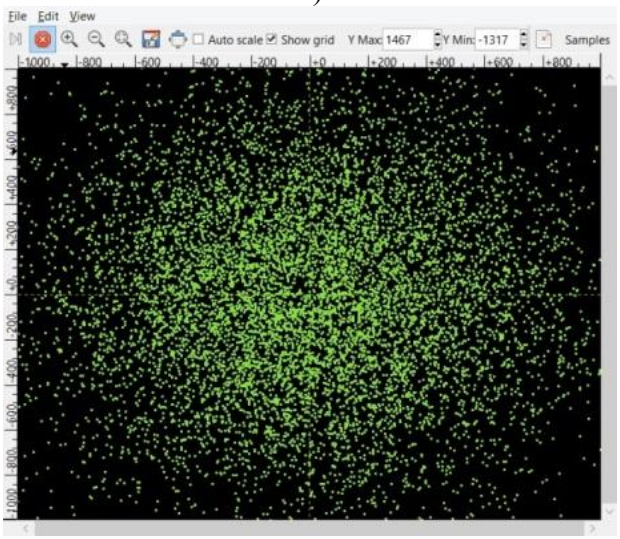
Фигура 3. *I и Q канали на приетия сигнал при тест модел E-TM 3.1*
а) 5 MHz б) 10 MHz в) 20 MHz



а)



б)



в)

Фигура 4. *Констелация на приетия сигнал при тест модел E-TM 3.1*
а) 5 MHz б) 10 MHz в) 20 MHz

References

1. Analog Devices, ADALM-PLUTO: SDR Active Learning Module, 2017, Available at http://www.analog.com/media/en/news-marketing-collateral/product-highlight/ADALM-PLUTO-Product-Highlight.pdf .
2. Analog Devices, RF Agile Transceiver AD9363, 2016, Available at http://www.analog.com/media/en/technical-documentation/data-sheets/ad9363.pdf
3. ETSI, *LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Base Station (BS) conformance testing (3GPP TS 36.141 version 12.5.0 Release 12),* Document Number ETSI TS 136 141 V12.5.0 (2014-10), 2014, Available at https://www.etsi.org/deliver/etsi_ts/136100_136199/136141/12.05.00_60/ts_136141v120500p.pdf
4. ETSI, *LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Physical channels and modulation (3GPP TS 36.211 version 14.2.0 Release 14),* Document Number ETSI TS 136 211 V14.2.0 (2017-04), 2017, Available at https://www.etsi.org/deliver/etsi_ts/136200_136299/136211/14.02.00_60/ts_136211v140200p.pdf.

CYBERSECURITY

Георги Т. Герасимов,

СЪВРЕМЕННИ РЕШЕНИЯ ЗА ЗАЩИТА НА СТАЦИОНАРНИ СТРАТЕГИЧЕСКИ ОБЕКТИ

Георги Т. Герасимов

Intellect TGK, Gate-92 DG, Sofia-Sevlievo, Bulgaria, office@g-92.com

***Abstract**: In the following article are dicussed contemporary methods for passive and active protection of strategic industrial objects. The advantages of some of the commonly used methods for counteracting high precision weapons are analyzed, and also are discussed the advantages and disadvantages of different forms of passive and active protection. In its final part the article propose and highline some important research aspects and benchmarks, that could be taken into account in future R&D work in this area.*

***Keywords**: passive protection, active protection, prompt global strike, pgs, high-precision weapons protection, automated security systems, autonomous cybernetic modules*

Дефиниция

Под уязвимост на стационарните обекти ще разбираме степента на поражение върху тях, при използване на различни по вид и функционалност средства за въздействие.

Степента на уязвимост се определя от разположението на обекта, неговите размери, начина по който функционира, използваната защита, тактико-техническите характеристики на средствата за въздействие и други фактори. Това налага прилагане на *комплексен подход* при изготвяне на анализи и формиране на мерки за защита на стационарни стратегически обекти.

1. Анализ на съществуващите проблеми

Защитата на стационарни обекти със стратегическо значение е въпрос, който добива все по-голяма актуалност. В съвременния свят те са не само цел, но също така все по-често са обект на различни по характер атаки в т.ч. кибернетични и диверсионно-терористични извършвани с помощта на *автоматизирани нападателни средства (АНП)*.

Анализът на проведените военни операции в Югославия, Либия, Ирак, Афганистан и Сирия показаха, че използваните към момента методи за активно и пасивно противодействие са все по-малко ефективни.

Съгласно концепцията за „*мълниеносен глобален удар*" (*Prompt Global Strike - PGS*), стационарните обекти, поради своята специфика, са основна цел на една евентуална кинетична бомбардировка, основаваща се на орбитален удар върху наземни цели *(tungsten telephone pole, проект Thor*). В същото време съществуващите активни средства за ПВО-защита не са в състояние да се противопоставят дори на *перспективните хиперзвукови оръжия* с висока точност (*Advanced Hypersonic Weapon – AHW),*

Сериозен проблем е и все по-масовото навлизане на баражни боеприпаси с голям обсег на действие. Те са с относително ниска цена, изключително висока степен на мобилност и висока точност. В съчетание с радиуса на поражение би могло да се каже, че на практика те представляват много-по-голяма заплаха от високоточните боеприпаси. Като основна причина за това, бихме

могли да посочим тяхната достъпност. На състоялото се от 17 до 21 февруари 2019 година в Абу Даби (ОАЕ) изложение на военна техника IDEX, бяха демонстрирани много нови решения в тази област.

Друг фактор, който за съжаление рядко бива отчитан, е невъзможността за гарантиране на енергийна автономност. Това е сериозна слабост, тъй като дори кибернетична атака (*която към момента не се счита за военна агресия*) е в състояние да изведе от строя важен стратегически обект за неопределен период от време прекъсвайки достъпа до базови мощности.

Целта на настоящият доклад е да обобщи основните принципи, въз основа на които би следвало да се формира защитата на стационарните обекти, както и да предложи съвременни решения за повишаване на общата ефективност на провежданите пасивни и активни мероприятия, съобразно развитието на технологиите.

2. Изисквания към средствата за пасивната защита

Развитието на военните технологии налага прилагане на нови методи за маскировка на стационарните обекти и критичната инфраструктура, така че да не бъде нарушена нейната функционалност в случаите на агресивно въздействие.

Ако през XX век традиционните видове маскировка се считаха за „*пасивна защита*”, то с появата на високоточните боеприпаси и комплексните средства за самонасочване този подход стана не само неефективен, но и икономически неизгоден.

Проблемите при пасивните методи за защита произтичат от стационарния характер на обектите и тяхната площ. Редица критични обекти притежават демаскиращи признаци, които са обвързани с предмета на тяхната функционалност (*машини, железопътни линии, силози, цехове, топлообменници и др.*). За да се постигне ефективно замаскиране на тези обекти са нужни принципно нови решения. Тези решения би следвало да се базират на реципрочно време за реакция и комплексна маскировка. Това предполага автоматизирани системи за ранно предупреждение, контрол на периметъра, съпровождане на целите и управление на противодействието. Времето за реакция на тези комплексни решения би следвало да е в рамките на 2 до 3 минути. Това време е определено въз основа на тактико-техническите показатели на съвременните високоточни оръжия и автономни оръжейни комплекси.

Съвременните разработки в тази сфера позволяват генериране на лъжливи физически полета в широк честотен спектър (*инфрачервен, оптичен, радиочестотен и др.*), както и прикриване на конфигурацията и реалното разположение на отделните компоненти, изграждащи обекта. Към подобен вид средства бихме могли да причислим специализираните боеприпаси за създаване на смущения, дистанционно управляемите аерозолни завеси, средствата за имитация на физически полета и др..

Най-ефективни, спрямо експлотационните разходи са средствата, използващи аерозоли. Друго тяхно предимство е възможността за дистанционно управление и пълната автоматизация на процесите, свързани с прилагането им.

Всички тези средства обаче притежават един сериозен недостатък. Той се изразява в незадоволителните маскиращи показатели в инфрачервената част на спектъра. Това ги прави неефективни срещу системи, използващи топловизионни датчици.

Друг проблем е невъзможността да се предвиди как метереологичните промени (*влажност на въздуха, скорост на вятъра и др.*) ще повлияят на разпространението на електомагнитните вълни и до колко това няма да доведе до поява на демаскиращи признаци.

За противодействие на високоточните боеприпаси, използващи отразени радиовълни, е добре да се използват наклонени отразителни екрани, които са основен елемент на инженерните маскировъчни комплекти. За повишаване на ефективността е необходимо те да се комбинират с хибридни решения за „*изкривяване*” на ландшафта. Също така е добре още в етапа на проектиране да се помисли за използване на топлоотразителни покрития. Това решение има и чисто икономически ефект, защото позволява рязко снижаване на енергийните разходи.

Съществуват редица решения за „*отклоняване*" на високоточните боеприпаси от обекта и тяхното детониране на безопасно разстояние. За тази цел се използват специализирани боеприпаси, бойните глави на които носят комбинирани радиолокационни и топлинни примамки.

За повишаване ефективността на защитата на критично важни обекти от високоточни оръжия, които ползват корелационно-екстремални системи за насочване може да бъдат използвани системи за изменение физическото поле на местноста. По този начин не се позволява на управлението, използващо отразени сигнали, да извършва корекцията в траекторията. Най-лесният начин за реализиране на подобен подход е използването на химическа пяна или друг вид нискобюджетни средства и решения, създаващи покрития с високо повърхностно напрежение.

Имитацията на поражения може да бъде реализирана посредством имитационни покрития. Това могат да бъдат синтетични платна, с изобразени на тях физически разрушения, пиротехнически средства, използвани за генериране на фалшиви пожари и др.. През последните години все по-често се използват решенията, базирани на аеростати.

Комплексното прилагане на така изброените средства за пасивна защита позволява запазване на функционалните характеристики на стационарния обект, след всяко следващо въздействие от страна на високоточните и класически боеприпаси.

Основните елементи, изграждащи една хибридна система са:

- Средства за откриване и проследяване на високоточни оръжия;
- Генератори на смущения и компоненти за радиоелектронно противодействие;
- Системи за залпов огън, използващи светлоотразителни, радиоотразяващи, инфрачервени, димообразуващи и друг вид елементи;
- Използване на класически аеростати и съвременни цепелини, с вградени радио и светлоотразителни елементи;
- Универсални и радиопоглъщащи и отразяващи маскировъчни покрития;
- Макети на радио, топло и светло излъчващи елементи в стационарно и мобилно изпълнение и др..

Едни от най-важени елементи при комплектовката на всяка една хибридна система за пасивна защита са геометричните размери и конфигурацията на отделните елементи, от които е съставена.

С оглед на гореизложеното маскируемите обекти биха могли условно да бъдат разделени на следните групи:

- Малогабаритни обекти – Размери *50x50 m*. При този вид обекти площта съвпада с радиуса на поражение на високоточните боеприпаси. Като такива може да посочим компресорните станции (*използвани при газопроводната мрежа*), трафопостовете, складовите бази и др..
- Средно големи обекти – Размери до *200x300 m*. Това са преди всичко технологични участъци, извеждането от строя на които води до прекъсване на производствения цикъл. Тук могат да бъдат добавени и малките хидро-технически съоръжения, разрушаването на които би довело до регионални наводнения.
- Големи обекти – Размери *400x600 m*. Преди всичко в този клас обекти може да включим атомните централи. Химическите комбинати, терминалите за разтоварване и съхраняване на нефтопродукти и др.. Тяхното унищожаване е съпроводено с екологично замърсяване, пожари и сериозни поражения сред цивилното население.

- Линейни обекти – Това са обекти с дължина над *1200 m*. Тук включваме железопътни линии, магистрали, далекопроводи и др..

Оценката на риска и ефективността на използваните средства е комплексно мероприятие, което би следвало да се осъществява въз основа на емпирично обосновани коефициенти.

Таблица 1

Системи за пасивна защита	Малогабаритни	Средни	Големи	Линейни
Аерозолни генератори	0,01	0,4-0,5	0,4-0,5	0,2-0,3
Топлинни примамки	0.8 – 0,9	0,6-0,7	0,6-0,7	0,4-0,6
Физични деформации	0.8 – 0,9	0,1-0,2	0.1-02	0,4-0,7

Въз основа на посочените в таблицата коефициенти се извършва проектиране и изграждане на комплексна система от защитни мерки, която би следвало да включва инженерни средства за маскировка, използване на специализирани боеприпаси, средства за радиоелектронна борба, защитни системи, основаващи се на нови физични принципи и др.. По този начин рязко се снижава вероятността от поразяване на стационарните обекти от високоточните оръжия на противника.

В зависимост на принадлежността на обекта към една от така изброените групи могат да бъдат предложени повече от едно решения. За един малогабаритен обект, могат да бъдат използвани системи за прихващане и проследяване на нисколетящи високоточни оръжия (*в т.ч. бражни боеприпаси*), както и системи за изкривяване на физическите полета и маскировъчни покрития. Използването на аерозолни генератори в този случай би било слабоефективно и на практика икономически неизгодно.

Разработката и въвеждането в експлоатация на мерки за пасивна защита на критични за икономиката обекти е основен елемент от изпълнение на плановите задания за съхраняване и повишаване на тяхната физическа устойчивост на външни въздействия. Това важи най-вече в случаите, когато се изисква да бъдат изпълнени програми за противодействие на диверсионни мероприятия и антитерористична защита. В този случай е задължително да се добавят системи за контрол на достъпа, охранителни системи, реагиращи на опит за терористична и кибер атаки, централизирана система за регистрация, контрол и анализ на събитията (*събитийни анализатори*), елементни бази данни и специализиран софтуер. На практика само така може да се изгради единна система за защита, която би била ефективна в съвременните условия.

От изключително значение е средствата за пасивна защита да бъдат разработвани като унифицирани решения с двойно предназначение. По този начин те ще могат да бъдат използвани както в инфраструктурните обекти, така и във военните подразделения. Това е въпрос с изключителна икономическа значимост.

3. Изисквания към системите за активна защита

Разработката на средстава за активна защита на стратегически стационарни обекти е от изключително значение при изграждането на военните доктрини.

Съвременните активни системи трябва да се базират на нискобюджетни решения, използващи хибридни модули. Те би следвало да се активират в изключително кратки времеви интервали.

Всяка високо ефективна система за активна защита (SAO OVO) би следвало да решава следните основни задачи:

- Пълна автономност при прихващане и последващо унищожаване на високоточни боеприпаси;

- Гарантирано устойчиво функциониране в случаите на въздействие със специални средства за поразяване, използващи нови физични принципи;
- Противодействие на базирани на ниска и висока орбити космически навигационни и ударни системи;
- Автоматизирано противодействие на наземни атаки, с използване на автономни кибернетични модули;
- Защита от съвременни конвенционални оръжия със сухоземно, морско и въздушно базиране;
- Противодействие на диверсионни, терористични и кибер-атаки.

Съвременните средства за ефективна защита на стратегически обекти представляват автономни разузнавателно-огневи структури, с висока степен на автоматизация. За да бъде гарантирана тяхната ефективност те би следвало да използват мобилни или контейнерни (*стационарни*) решения. При всички случаи обаче е необходимо да се отчитат специфичните особености на обекта и съпътстващата го инфраструктура.

Така изброените препоръки позволяват да се проектират и създават *полигамни системи* за активна защита с *открита архитектура*. Този вид защитни системи са в състояние безпроблемно да се трансформират в елемент от действащите структури на ПВО за региона, в който са разположени.

В резултат на поредица от експерименти, бе доказано, че не е възможно да бъде гарантирана ефективна защита, ако се разчита на само и единствено на еднородни структури. Дори да бъдат създадени смесени групировки, при които се използват различни по вид средства за активна защита, управлявани от независими командни пунктове, проблемите не могат да бъдат решени.

Една възможна алтернатива е изграждане на *информационно-технически координационни звена*, които да позволят обединяването на защитните модули в хибридни защитни комплекси. Подобен вид комплекси биха позволили многократно повишаване на общата ефективност, без това да изисква увеличаване на инвестиционните и експлоатационни разходи.

В този случай е важно автоматизираните разузнавателно-защитни комплекси да се управляват от *единен команден център*, като при това съхранят своята автономност. По този начин ще се гарантира изпълнението на поставените цели, дори в случаите, когато комуникацията с централното командване е нарушена.

Разузнавателните модули трябва да бъдат в състояние да гарантират разпознаване на целта (*наземна, въздушна и с морско базиране*), в реално време. Това изисква разработката на прецизни таймери, работещи на микро, нано и пико секунди, съвременни средства за пасивна радиолокация, модули за обработка на радиолокационна информация и др..

Всички системи за връзка и обмен на данни, трябва да бъдат снабдени с „*информационни шлюзове*”, посредством които да се извършва обмен на оперативна информация с други системи за отбрана. За целта е наложително спешно да се пристъпи към създаването на специализирани протоколи за обмен на данни и съпътстващите ги програмни и апаратни решения.

4. Съвременни решения за защита на стационарни обекти

Всички съвременни системи за защита на стационарни обекти се характеризират в висока степен на автономност и изключително кратко време за реакция.

Типичен пример за практическа реализация на локална активна защита е използването на зенитноракетен комплекс Skyshield.

Фигура 1: Зенитноракетен комплекс Skyshield

Основната функция на Skyshield е да гарантира поразяване на тактически самолети, ударни вертолети, крилати ракети и безпилотни летателни апарати (БЛА), действащи на малки и предел-но малки височини, а също така наземни бронирани цели. Пункта за управление се разполага на разстояние от *500 m* от активните компоненти на комплекса. В случай на извеждане от строя на централното управление и/или радарните установки на комплекса, всяка една огнева точка про-дължава да функционира автономно, посредством локалните оптико-електронни системи за уп-равление на огъня. Skyshield притежава изключително малко време за реакция - *4,5 sec*. Летящите цели могат да бъдат прихванати на растояние от *20 km*, при ъгъл на отклонение по азимут от 360º.

Фигура 2: Мобилен зенитноракетен комплекс N/TWQ-1 Avenger

На фиг.2 е показан мобилен зенитно-ракетен комплекс N/TWQ-1 Avenger на та Boeing (САЩ). Системата е разположена върху High Mobility Multipurpose Wheeled Vehicle - HMMWV и е предназначена да унищожава въздушни цели (самолети, вертолети, ударни БЛА и др.).

N/TWQ-1 Avenger е снабден с лазерна установка за поразяване на БЛА, както и със система за автоматично съпровождане на целта. Позволява изстрелване на зенитна ракета в движение, при скорост от *35 km/h.*

Един от най-перспективните проекти в сферата на активната защита е миниатюрната проти-воракетна система МНТК (Miniature Hit-to-Kill) на компанията Lockheed Martin. При диаметър *38 mm*, дължина *610 мм* и тегло от *2,3 кg*, МНТК позволява в един многоцелеви пусков контейнер (Multi-Mission Launcher – MML) да бъдат разположени до 9 броя ракети.

Фигура 3: Миниатюрната система за активно противодействие МНТК (Miniature Hit-to-Kill)

Основното предимство на този вид боеприпас е възможността за пряко попадение в малки по размер цели (*82x120 mm*), каквито са минометните снаряди или 155 милиметровите гаубични боеприпаси. Подобна точност се постига посредством вградената радиолокационна система, работеща в милиметров диапазон на излъчване.

Изключителен интерес представлява и решението обединяващо SHORAD на Boeing и модифицираната версия на Stryker Mobile SHORAD Launcher (MSL), на компанията General Dynamics.

SHORAD (SHOrt Range Air Defense) shoot-off е типична мултифункционална ПВО система с малък радиус на действие. Системата се комплектова с ракети AGM-114 Hellfire, AGM-114 Hellfire Longbow, AI-3 и AIM-9X Sidewinder, както и с боен лазер. Предназначена е да унищожава всички видове въздушни цели. Проведените изпитания, показват нейната изключителна ефективност при защита на стационарни обекти.

Фигура 3: Мобилно изпълнение SHORAD (SHOrt Range Air Defense) shoot-off

Решение, което обединява в едно активна защита от въздушни и наземни цели е дистанционно управляемият модул Turra 30 на словашката компания EVPU. Системата може да бъде използвана както при стационарни, контейнерни решения, така и да бъде монтирана на колесни или гъсенични бронирани машини. Позволява ефективно унищожаване на наземни и въздушни цели на разстояние до *2500 m.* Това, което я отличава от гореизброените е вградената система за автоматично управление на огъня и начина, по който тя се интегрира с оперативно тактическите командни системи. Това е типична система, обединяваща в общ корпус модули за разузнаване, как-

то и такива за управление на огъня и поразяване на наземни и въздушни цели (*комплексна интеграция на система за активно противодействие*).

Фигура 4: Дистанционно управляемият модул Turra 30.

Компанията, която е водеща при автоматизацията на активни системи за защита е турската Aselsan. Основната причина за това е, че Турция влага изключително голям ресурс в развитието на съвременни оръжейни системи и разработката на електронни компоненти за тях. На изложението IDEF 2019 в Истанбул. Aselsan презентираха SAPR Zafer.

Компактната конструкция на SARP позволява интегриране върху тактически машини, стационарни постове за наблюдение или контролни кули. Всички процеси, свързани с автоматичното следене на целта и определяне на балистичните параметри са изцяло автоматизирани. Към настоящият момент Aselsan произвежда по 150 броя SARP месечно.

Фигура 5: Дистанционно управляем SARP

Заключение

Ефективното управление на процесите, касаещи националната сигурност, изисква постоянно усъвършенстване на отбранителната индустрия. В настоящият момент сме свидетели на качествен преход във военната наука. Крупномащабните оперативни действия постепенно биват изместувани от асиметрични мобилни операции, провеждани в сравнително кратки времеви интервали. Стратегическите усилия са насочени към контрол над въздушно-космическото пространство, кибернетичната инфраструктура, енергийните източници и екологията. Всички тези процеси се развиват динамично и налагат търсене на нови решения. Тези решения са обвързани най-вече с повишени изисквания към държавното управление, инфраструктурата, функционирането на икономиката, както и тиловото обезпечение на армията.

Изхождайки от гореизложеното може да заявим, че гарантирането на активната и пасивна защити на стационарните стратегически обекти остава първостепененна задача за въоръжените сили и спомагателните структури, отговарящи за гарантиране на сигурността. Независимо от развитието на военните технологии все още съществуват проблеми, които очакват своето решение. Стационарните обекти са с постоянна локация с всички произтичащи от това последици. Ако обаче тяхната функционалност бъде частично или напълно разрушена, това би имало много тежки последици в дългосрочен план.

За да има напредък в тази област е нужно да бъдат обединени усилията на научните звена, университетите, промишлените предприятия и държавните ведомства. Това е направление, което се разраства с бързи темпове и при което търсенето многократно надвишава предлагането.

В настоящия доклад бяха разгледани много малко от възможните решения. Не бе отделено място за системите, базирани на нови физични принципи, нанотехнологиите, методите кибернетично противодействие и др.. Не бяха разгледани изключително важните въпроси, свързани със защитата на стратегически обекти от проникване на роботизирани, автономни агрегати, в т.ч. и такива без директно задвижване. Всички тези въпроси са предмет на бъдещи разглеждания. Това, което спешно трябва да бъде направено е да се пристъпи към създаване на програма, която би гарантирала развитието на военната индустрия и технологии в направления, свързани със създаване на хибрдни решения, които могат да бъдат използвани както в отбранителната промишленост така и в гражданската сфера. Необходимо е да се търсят нискобюджетни решения за асиметрично противодействие, да се изграждат специализирани бази знания, да се провеждат изследвания в перспективни направления като фотоника, биохимия (*взаимодействие между живата и нежива материя*), физика на средните взаимодействия и др.. Това означава подготовка на кадри, научно-развойна дейност и практически експерименти. За да се случи това е нужно бързо интегриране на теоретичните разработки в практиката.

References

1. *Woolf, Amy F., 7 July 2017 , Conventional Prompt Global Strike and Long-Range Ballistic Missiles: Background and Issues, Congressional Research Service.*
2. *Mikhail I.Uliyanov, 2015, Acting Head of the Delegation of the Russian Federation at the 2015 Review Conference of the Parties to the Treaty on the Non-Proliferation of Nuclear Weapons (General debate) .*
3. *James M. Action, 2013, Asking the Right Questions About Conventional Prompt Global Strike,* Carnegie Endowment for International Peace, Washington, DC 20036.
4. *Vince Manzo, 2008, CDI Research Assistant, An Examination of the Pentagon's Prompt Global Strike Program: Rationale, Implementation, and Risks, Center for Defense Information,.*
5. *M. Elaine Bunn and Vincent A. Manzo, December 2006, Conventional Prompt Global Strike: Strategic Asset or Unusable Liability?, Strategic Forum National Defense University,*
6. *Pavel Podvig, Russia and the Prompt Global Strike Plan, PONARS Policy Memo No. 417, Stanford University.*
7. *А.В. Маринин, И.А. Ростовцев, А.С. Балакирев, В.В. Сироткин, Л.А. Маринина, Применение лазерного излучения в системах охраны, Пенза, Пензенский филиал военной акаде-*

мии материально-технического обеспечения, ФГБОУ ВПО "Пензенский государственный университет" Сердобский филиал

8.Защита стратегических и режимных объектов от проникновения разведывательной робототехники. Спецслужбы России.

9.Гарсиа М., 2003,Проектирование и оценка систем физической защиты, М.: Мир, 392 с.

Павел Г. Герасимов,

ХИБРИДНИ ОБЛАЧНИ ТЕХНОЛОГИИ ОТ НОВО ПОКОЛЕНИЕ

Павел Г. Герасимов

Intellect TGK, Gate-92 DG, Sofia-Sevlievo, Bulgaria, p.g.gerasimov@gmail.com

***Abstract**: During the last 15 years, cloud architecture, and the based on it systems and technological solutions became fundamental parts of the global IT-ecosystem. The rapid and accelerated development of this technology, set many questions like "Do we know what types of dangers can expect in the cloud?, "How protected am I, my Organization, and the information stored on the cloud? "What means and methods should I use in order to protect myself and my information from attack on the cloud, and how to treat the consequences concerning me?", and "What the hybrid cloud can give me, that the standard can't?" In the following article, we will discuss some of the benchmarks in the nature of the cloud platforms, that could let us propose new type of Hybrid Cloud, and of course to present some new methods and solutions, for protecting the information on the cloud. In the end of the article, the reader will be able to understand a new type of hybrid cloud system, that gives the user the ability to control and manage the level of his protection, and to manage the risk concerning the storage of sensitive information on cloud storage.*

***Keywords**: Cloud, Hybrid Cloud, Protected Cloud Storage, Encryption, SECaaS, Cloud computing*

Въведение

По дефиниция облачната архитектура представлява тип специализирана компютърна услуга, предоставяна на потребителя чрез отдалечен компютър, към който потребителят се свързва посредством internet или специална комуникационна линия.

Националният Институт по Стандартизация и Технологии на САЩ (The National Institute of Standards and Technology - NIST) в своя бюлетин специално посветен на дефиницията на облачната архитектура дефинира четири основни модела на предоставената услуга: [1]

- **SaaS** ***(Software as a Service)*** – Софтуер като услуга или Приложно ниво (*Application layer*)
- **IaaS** ***(Infrastructure as a Service)*** – Инфраструктура като услуга или Хардуерно ниво (Hardware layer)
- **PaaS** ***(Platform as a Service)*** – Платформа като услуга или Междинно ниво (*Middleware layer*)
- **DaaS** ***(Database as a Service)*** – База данни като услуга.

През годините са се развили различни модели, в резултат на все по-разширеното използване на облачните услуги. В настоящата публикация ще се фокусираме върху една специфична форма, която е и предмет на теоретичните разглеждания.

С развитието на облачната архитектура, се достигна до четири базови структури:

- **Частен облак** *(Private Cloud)* – При него инфраструктурата на облака се притежава или наема от една организация и се използва само и единствено от нея.
- **Общностен облак** *(Community Cloud)* – Инфраструктурата на облака се споделя от няколко организации и служи за поддържането на специфична общност от потребители. Всички потребители споделят обща мисия, обща политика и общи изисквания към информационната сигурност.
- **Публичен облак** *(Public Cloud)* – Инфраструктурата на облака се притежава от една организация, която продава облачно-базирани услуги на широк спектър от клиенти.
- **Хибриден облак** *(Hybrid Cloud)* – При този тип архитектура, инфраструктурата на облака е съчетание от горе-представените три решения, които остават разграничими на база вътрешна политика за сигурност. В същото време те са свързани посредством стандартизирана или авторска технология, използвана от компанията провайдер.

В настоящата публикация, ще разглеждаме модификация на типа архитектура „Хибриден облак" и ще се опитаме да представим нови технически решения, към които този тип архитектура предполага.

Технико-икономическа обосновка

Според проучване на консултантската компания KPMG [2], около 25% от правителствата по света са насочили своя фокус за следващите 15 години към облачно-базираните системи и по-конкретно към разработка на хибридни системи с високо ниво на защита. Според посоченото проучване засиленият интерес се дължи основно на факта, че се налага значително оптимизиране на разходите по поддръжка на съществуващата IT-инфраструкура. В същото време изискванията за подобряване на общата сигурност, оптимизация на протоколите при реакция в случай на кибернетични атаки както и на противодействие на опитите за несанкциониран достъп до чувствителна информация все повече нарастват.

Отново, според същото проучване, все по-често на дневен ред се поставят въпроси касаещи защитеността на аутсорснатите информационни масиви, както и унификацията на методите за защита и тяхната междуплатформена съвместимост.

Друг много важен проблем е *зоната* (*територията*), на която се намират сървърите на компанията, поела дейността по обработка и защитено съхранение на информационните масиви. Проблемът е в резултат на тежката регионална и международна юридическа рамка, обхващаща функционирането на този вид технологични решения, както и на строгите процедури на сертификация по ISO.

Хибридният облак е изключително полезен и удобен за компании и държавни органи работещи с големи масиви от данни, изпитващи нужда от допълнителни системи за съхранение и обработка на информация, които нямат възможност да поддържат скъпоструваща IT-инфраструктура.

Съвременните хибридни облачни решения са изправени пред следните четири проблема [3, 4]:

- **Цена** – проблемът е свързан с необходимостта от наличие на локална сървърна инфраструктура при потребителя и отдалечен ресурс при провайдера на облачната услуга.
- **Режийни разходи** – енергийни разходи, вода, разходи за климатизация и вентилация, разходи за физическа сигурност и други.

- **Оперативни разходи** – свързани със системата на функциониране и обслужване на хибридния облак.
- **Амортизация** – важно е амортизацията да бъде отчетена като перо при поддръжката на хибридния облак, тъй като в зависимост от натовареността на системата трябва да бъдат прогнозирани с абсолютна точност периодите на обслужване на физическите устройства

Развитието на хибридните облачни решения, поставя въпроса за защитеността на информацията намираща се на тях и минимизиране на рисковете за потребителя на съответната услуга.

В течение на развитието на технологията се развива модела **SECaaS** – *(Security as a Service)* Сигурност като услуга. SECaaS предоставя на потребителя определен набор от инструменти, които подпомагат обезпечаването на неговата сигурност, както и инструменти за контрол на достъпа, инструменти за защита на информацията, защитени линии на достъп и други.

Използването на SECaaS има както свойте предимства така и някои недостатъци. [5]

Глобално погледнато за потребителя, облакът е „черна кутия", за която той няма информация от гледна точка на сигурността. Друг сериозен проблем е, че към момента степента на защитеност трудно може да бъде измерена, поради липса на утвърдена методология.

М.Карвало (M.Carvalho) в своя публикация от 2011, поставя въпроса за предоставяне на инструментариум на потребителя, посредством който той (*потребителят*) ще може да управлява защитата на информацията съхранявана на облака като по този начин се създава възможност за формиране на политики за определяне на риска.

Много е важно да отбележим, че SECaaS не е услуга, която може да се предоставя само на един потребител. Това е услуга предназначена за голям набор от потребители, както крайни, така и големи корпоративни структури.

Структура на Хибридния облак

Хибридните облаци като услуга са рискови, независимо от това, което се твърди за тях. На практика те са типични трислойни приложения, с всички произтичащи от това последствия.

Един от основните проблеми е, че контролът основно се извършва от административни структури, които обслужват сървърната част и бизнес слоя. В същото време клиентските приложения са мултифункционални и слабо защитени.

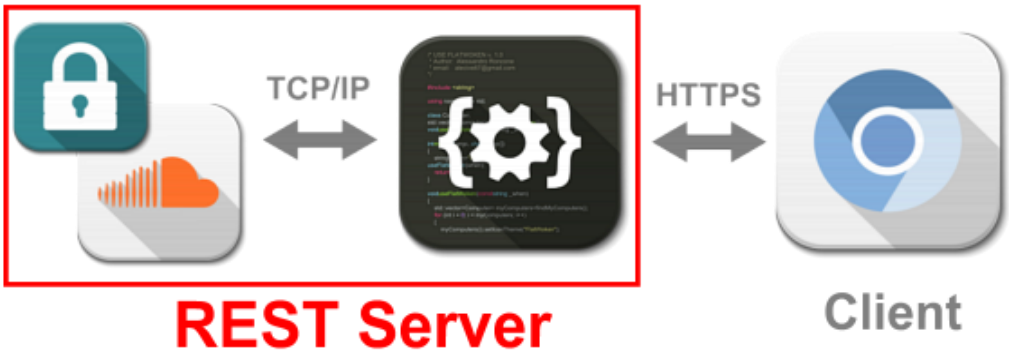
Поради тази причина е необходимо да се намери решение, което да позволи на крайните потребители да защитават използваната от тях информация, съобразно своите политики за сугурност, без това да нарушава общите правила за ползване на облака.

В зависимост от използвания клиент хибридните решения от ново поколение, могат да бъдат обособени в следващите три групи:

- **Web-базиран клиент** – Това са приложения, при, които като клиент за достъп се използва web-браузър. Този тип хибриден облак е достъпен под формата на internet-базирано хранилище. Това, което отличава този хибриден облак от други популярни алтернативи, съществуващи днес, е възможността потребителят да избира сам криптиращият механизъм за защита. Комуникацията с облака се извършва при използване на HTTP или FTP протокол. Управлението на жизнения цикъл на сесията се реализира при използване на TCP/IP проткол. Управлението се извършва от специализиран REST-сървър.
- **Специализиран клиент** – при тази реализация хибридният облак е достъпен посредством защитено крайно приложение. Този вид решения са извънбраузърни (*out of browser*), мултиплатформени решения, при които се елиминира частично или изцяло използването на HTTP протокол. Както и при web-базираните, така и тук потребителят може сам да избира криптографския алгоритъм, посредством който да защити своята информация. При този

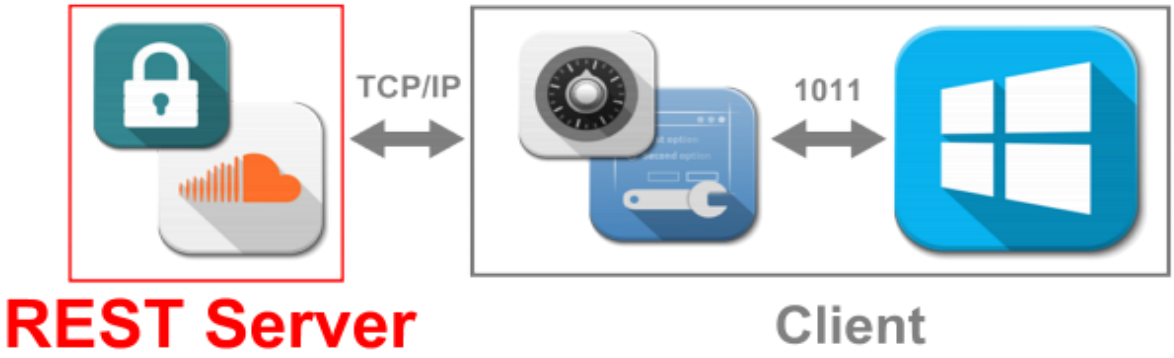
тип решение се извършва предварително криптиране от страна на потребителя. В този случай преносът е надеждно защитен дори тогава, когато не се използва VPN-канал или друго подобно решение.

-



Фигура: Схема на структурата на web-базирано приложение

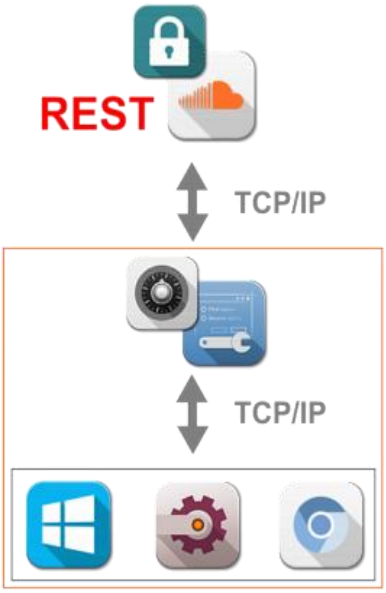
- **Специализиран клиент** – при тази реализация хибридният облак е достъпен посредством защитено крайно приложение. Този вид решения са извънбраузърни (*out of browser*), мултиплатформени решения, при които се елиминира частично или изцяло използването на HTTP протокол. Както и при web-базираните, така и тук потребителят може сам да избира криптографския алгоритъм, посредством който да защити своята информация. При този тип решение се извършва предварително криптиране от страна на потребителя. В този случай преносът е надеждно защитен дори тогава, когато не се използва VPN-канал или друго подобно решение.



Фигура 2: Използване на специализиран клиент

- **Специализирани решения (*специализиран пакет*)** – това е реализация на хибриден облак, подходяща за държавни и общински институции, малки и средни предприятия, обработващи големи масиви от разнородна информация (финасово-счетоводна, технологична, специализирана и др.) и нуждаещи се от гарантирана защита. Този потребителски пакет

позволява изграждане на нискобюджетна локална инфраструктура. Функционалността е аналогична на предходно описаните потребителски пакети.



Фигура 3: Трислойна хибридна структура.

Фигура 4: Двуслойна, хибридна структура

Защита на информацията съхранявана в хибридния облак

Както споменахме по-горе в нашите разглеждания, хибридният облак позволява както криптиране на информацията съхранявана на него така и криптиране от страна на крайния клиент. При трислойната архитектура това се извършва от бизнес слоя на приложението. При двуслойните решения механизът е различен.

Към самият хибриден облак е свързан специален оперативен модул, който е отговорен само и единствено за криптирането на съхраняваната информацията. Оперативният модул комуникира с

потребителя, като провайдера на услугата. Директната връзка оперативен модул-потребител, позволява на потребителя да поеме частично или напълно управлението на риска, свързан с отдаленото съхранение на информацията.

Контролът на жизнения цикъл за всяка една сесия се осъществява в реално време и се документира, съобразно действащите стандартни зисквания. За реализиране на този процес се използва контролен модул. При еднопроцесорните 32 разрядни апаратни решения се използва многопоточна обработка на данните. При многопроцесорните 64 разрядни се използва паралелна обработка.

Контролният модул на Хибридния облак следи за правилното разпределяне на изчислителните ресурси на облака, неговото дисково пространство и балансираното разпределение на заявките за обслужване, подавани от потребителите. Една от най-важните функции на контролът на сигурността (Information Security Control – ISC), който се изразява в превенция на опити за злонамерен достъп, DDoS – атаки, SQL – инжекции, нерегламентирано извличане на потребителски данни за достъп и други.

Друг важен аспект при реализацията на хибридни системи е възможността за автоматично изграждане на виртуални контейнери. За целта се използва специализиран by-pass механизъм., който изпълнява предпазна функция в случай на недопустимо натоварване на системата. В случай на невъзможност за обслужване на заявката се генерира виртуален контейнер, към който тя се пренасочва. Преди да бъде записана заявката се анализира и класифицира. Подредбата се извършва по приоритет, регламентиран от вътрешни правила. След като заявката бъде обработена, резултатът се съхранява в друг временен контейнер. При приключване на сесията двата виртуални контейнера се самоунищожават без да оставят остатъчна информация.

При специализираните пакети хибридният облак предоставя опцията за формиране на Защитено Работно Пространство (ЗРП).

Защитеното локално работно пространство има за цел да предостави на потребителя локално генериран виртуален контейнер, който да гарантира защитена среда за работа с чувствителна информация. В този случай информацията може да бъде прехвърлена към защитен облак или да бъде използвана като алтернативно решение за съхраняване на цифрови данни.

Фигура 4: Вътрешна структура на хибридния облак

При ЗРП данните се съхраняват в бинарен вид, като могат да бъдат частично или напълно криптирани. Физически ЗРП съществува до момента в който се осъществи пълна миграция на съхраняваната информация към хибридния облак и/или краен получател. Когато работната сесия приключи се извършва миграция или се задейства протокол за пълно унищожаване на данните.

За да бъдат предотвратени опити за несанкционирани действия от страна на неоторизирани потребители, процесът на миграция и унищожаването при ЗРП, е автоматизиран.

В случаите, когато се извършва миграция, системата прави проверка за наличие остатъчни елементи или електронни следи. Ако бъде констатирано наличието на такива автоматично се включва протокол за тяхното унищожаване.

При унищожаването на ЗРП се премахва всяка остатъчна информация. В този случай се генерира цифров маркер, който подготвя създаването на ново ЗРП, предназначено за изпълнението на нова задача.

Важно е да се отбележи, че хибридният облак и използването на ЗРП, гарантират надеждна анонимизация, а също така елиминират необходимостта от събиране на лични данни и тяхната последваща обработка и анализ.

Заключение

Хибридните облачни технологии са надеждна алтернатива на много изисквания, пред които са изправени съвременните системи за обработка и съхранение на информацията.

Все по-нарастващите регулации в сферата на защитата на личните данни, неизбежно ще доведат до излишно усложняване, а от там и до възникване на нови затруднения при проектирането и изграждането на системи за обработка, съхранение и трансфер на цифрова информация.

Анонимизацията на потребителите е компромисно решение. По този начин се създава баланс между нуждите на крайния потребител, нормативните разпоредби, финансовите ограничения и техническите решения, които съставляват една съвременна информационна система.

Абсолютизирането на сървърните технологии е подход, който води до нарастване на проблемите. От друга страна общият обем да данни расте, като това се случва най-вече в резултат на увеличаващият се информационен шум. Не бива да се забравя, че дейтацентровете са сериозни консуматори на електро енергия. Това поражда допълнителни проблеми, които към момента не се отчитат.

Хибридните решения са само една от възможните алтернативи. Все още има много въпроси, които чакат своя отговор, но бъдещето ще изисква един различен и по-гъвкав подход.

References

1. P. Mell and T.Grace, Sep-2011, “The NIST Definition of Cloud Computing.” National Institute of Standards and Technology
2. KPMG, “KPMG – Exploring the cloud – A global study of governments’ adoption of Cloud.”
3. Koushik Annapu reddy, “Security Challenges in Hybrid Cloud Infrastructures”, Aalto University – School of Science and Technology
4. Philipp C. Heckel “Hybrid Clouds: Comparing Cloud Toolkits”
5. M. Carvalho, 2011, “SECaaS – Security as a Service”, Inf. Syst. Secur. Assoc., vol.9, no.10.pp. 20-24
6. Adrian Yanes, “Reputation in Cloud Computing”, Aalto University, School of Science and Technology
7. Nedzelský R., “Hybrid cloud computing: Security Aspects and Challenges”, University of Economics Prague

Yana E. Kolegova-Delcheva,

CRYPTOGRAPHY - A PART OF CYBER SECURITY IN THE ARMED FORCES

Yana E. Kolegova-Delcheva

***Abstract**: In the following report, we examined the topic cybersecurity and cryptography as part of it. The concept of cryptography is being defined along with a brief description of the main terms and objectives. A brief classification of the different cryptography types according to the types of cryptography keys used is also present. The need of using cryptography in the armed forces as one of the main means of achieving cybersecurity has been analysed too.*

***Keywords**: cybersecurity, cryptography, armed forces, cryptosystem, key*

КРИПТОГРАФИЯТА - ЧАСТ ОТ КИБЕРСИГУРНОСТТА ВЪВ ВЪОРЪЖЕНИТЕ СИЛИ

Яна Е. Колегова-Делчева

kolegova@abv.bg

1. Увод

Още от древността различните племена са водили битки помежду си за завладяване на територии. С развитието на човечеството, със създаването на националната държава, светът навлиза в една нова фаза от своето съществуване. Пред лидерите на страните се появява един нов спектър от задачи и приоритети, които трябва да изпълнят, за да съумеят да запазят и съхранят националната си идентичност и просперитет. Една такава задача е опазване на сигурността и гарантирането на спокойно съществуване на гражданите в периметъра на националните граници. Светът преминава през две катастрофални войни – Първата и Втората световна война, а страхът от избухването на трета взема превес и държавите осъзнават, че осигуряването на мир и стабилност ще доведат до пълноценно развитие на човечеството. След тези войни вече започва да се говори не само за национална, но и за глобална политика на сигурност. Бързото развитие на технологиите, компютрите, появата на интернет и цифровизацията на системите служат както в помощ на правителствените структури, но също така крият своите опасности за националната и световната сигурност. Осигуряването на киберсигурност се е превърнало в неизменна част от политиката на всяка страна. Киберсигурността се свързва с осигуряването на «*защита на свързаните с интернет системи, включително хардуер, софтуер и данни, от кибератаки*» [12] .Киберсигурността представлява приемането на защитни механизми и мерки срещу неоторизирания достъп до центрове за данни и други компютърни системи. Изграждането на ефективни и адекватни мерки за киберзащита е сравнително нова област на загриженост от страна на военните и правителствените организации. Ниската цена на компютърните устройства и компоненти, както и свободното разпространение на технологиите са предпоставка за превръщането на много хора в потенциални

„контрабандисти" на информация. Пазарът за откраднатa информация е доста богат и се превръща дейността по търговията с информация в процъфтяващ и печеливш бизнес по целия свят. [7]

2. Криптография

Информационните системи на Министерство на отбраната и въоръжените сили, както и всички специализирани организации имат нужда от особено мощна киберзащита, защото загубата на класифицирана информация или данни не е опция в отбранителния сектор и военните организации. Голяма част от приложенията и класифицираната комуникация са силно защитени чрез жизненото и необходимо криптиране[13].

2.1. Дефиниция

Криптографията е свързана с процеса на преобразуване на текстово съобщение от разбираем текст в неразбираем и обратното. Тя представлява метод „*за съхраняване и предаване на данни в определена форма, така че само тези, за които е предназначен, могат да го четат и обработват* [11] ". В чл. 84, Раздел 4 от Закон за защита на класифицираната информация /ЗЗКИ/ криптографската сигурност е дефинирана, като „*...система от криптографски методи и средства, които се прилагат с цел защита на класифицираната информация от нерегламентиран достъп при нейното създаване, обработка, съхраняване и пренасяне.*[1]" Именно чрез криптографията се защитават голяма част от мрежите и системите, защото тя служи не само за защита на данните от кражба или промяна, *„но може да се използва и за удостоверяване на потребителя* [1]". В съвременния свят криптографията представлява пресечна точка между математическата теория и практиката на компютърните науки.

2.2. Основни понятия

Няколко са основните понятия свързани с криптографията, а именно:

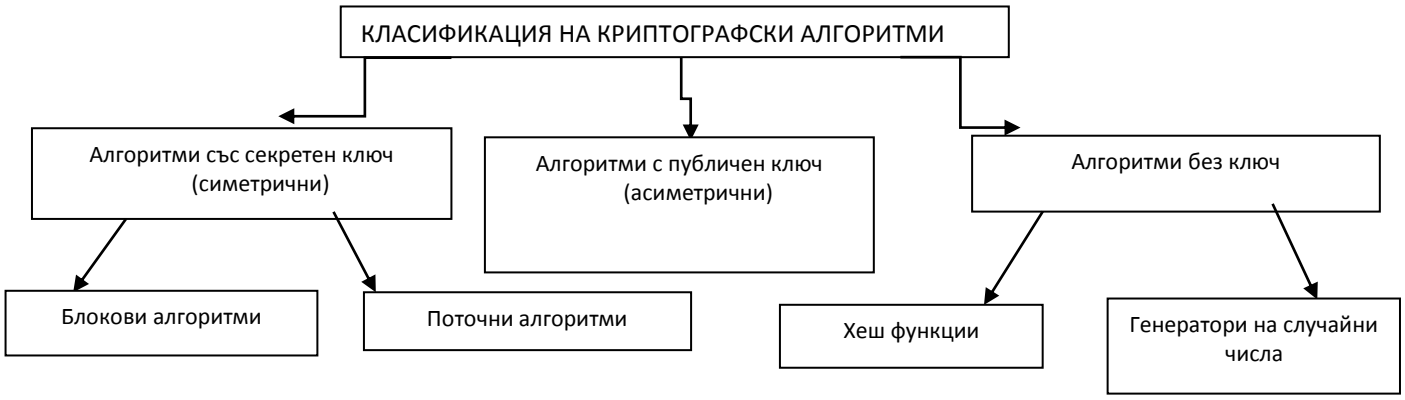
- Криптиране (encryption) – преобразуване на текстовото съобщение, по такъв начин, че то да остане неразгадаемо, за всеки, за който не е предназначено.
- Декриптиране (decryption) – обратната операция. Декодиране на съобщението в явен текст.
- Криптографски алгоритъм (cryptographicalgorithm) – преобразуването на данни в неразбираеми последователности от символи и тяхното правилно обратно възстановяване.
- Явен текст (plaintext) – първоначалния, оригинален текст, преди той да бъде шифриран с криптографски алгоритъм.
- Криптиран текст (ciphertext) – получената символна поредица, след криптирането на явния текст.
- Криптографски протокол (cryptographicprotocol) - правилото за обмен на данни и използване на криптографския алгоритъм.
- Криптосистема (cryptosystem) - съвкупността от криптографския алгоритъм и критрографския протокол.
- Криптографски ключ (key) - множество от числа или символи, което се използва за криптиране или декриптириране на съобщенията . Ключът бива два вида: ако е запазен в тайна (secretkey) и ако е известен, се нарича публичен ключ (publickey).
- Криптоанализът (cryptanalysis) е наука, занимаваща се с разработката на методи и средства за разкриване (на тайната) на криптографските системи и за оценка на тяхната сигурност.
- Криптология (cryptology) е обобщена дисциплина, включваща криптографията и криптоанализа [14].

2.3. Цели

Целта на криптографската система е да се предотврати нерегламентирано проникване в системите и неразрешеното извличане на информация и данни, т.е. да се осигури нейната **конфиденциалност**. Друга основна цел на криптографията е да се осигури **целостта** на информацията, т.е. да се предотврати възможността данните да бъдат променени или манипулирани по някакъв начин. **Истинността** определя дали дадено лице в интернет е реално, като се проверява не само самоличността на подателя на съобщението, но и на получателя. Друга основна цел е осигурява-

нето на **достъпност** на информацията, т.е. да се гарантира, че кодираните данни ще попаднат в правилните ръце.

2.4. Класификация на криптографски алгоритми



Таб. 1 – Класификация на криптографски алгоритми, спрямо използването на ключове - http://netseclab.tu-sofia.bg/vbook/Glava10.pdf, стр.228 [2]

3. Криптографията и въоръжените сили

Когато говорим за военните криптографски системи, трябва да се имат в предвид редица практически измерения. Тя трябва да представлява единна универсална система, предназначена за практична употреба от най-високо до най-ниско йерархично равнище. Използването на криптографията за защита на военната информация има своите немалко предимства. На първо място, криптографията представлява надежден механизъм за защита на база данни, независимо от броя на съобщенията, които се изпращат. От друга страна тя работи при всички климатични условия и не изисква специално обучение на потребителите. Разбира се не всяка система отговаря на тези условия. Изборът на криптографска система за военна употреба трябва да се свързва с осигуряване на сигурността, запазване на целостта, достоверността и поверителността на информацията. Същевременно, защитавайки информацията от нерегламентиран достъп, системата трябва да осигурява бърза и надеждна комуникация и да обслужва нуждите на всички участници в нея. Ако се използва криптографска система, която изисква един час за криптиране на данните, която е толерантна към направата на грешки при използването ѝ, ако не може да се използва при определени климатични условия, ако поддържа нисък обем от съобщения и изисква скъпо и сложно оборудване, то тя би била напълно неподходяща за използването за военни цели. Разбира се нито една система не отговаря на абсолютно всички изисквания за сигурност, надеждност, гъвкавост и цена. Затова при изборът на криптографска система за опазване на военна информация трябва да се търси баланс между тези практически изисквания и да се избере системата, която има най-малко уязвимости, която би могла да осигури сигурността при обмена на информацията.

Когато говорим за криптографските системи, трябва да отчетем и фактът, че са податливи на уязвимости. Има няколко фактора, които могат да спомогнат за осъществяването на криптоаналитична атака. Един от най-важните фактори е криптографската стабилност, т.е. колкото по-малко повтаряне на ключовете и ограничени модели за използване има, толкова по-голяма е устойчивостта на системата. Колкото по-дълго време се използват ключовете без промяна, толкова по-голяма е вероятността да се открие уязвимост в системата и да се проникне в нея. Една от най-важните роли за сигурността в системата играят системните потребители, за които има написания ясни правила за употреба. Смесването на явен текст с кодиран в едно съобщение, направата на неоторизирани промени или опростяване в системата, обсъждането на съдържанието на крипти-

раните съобщения и на системата и нейните ключове, могат да доведат до осъществяването на успешна кибератака [15].

4. Изводи

4.1. Сигурността на държавите отдавна е преминала отвъд националните граници и се е превърнала в транснационална, което налага приемането на общи политика за сигурност и сътрудничество в сферата на отбраната, комуникацията, транспорта, енергетиката и др.

4.2. Криптографията е едно от надеждните средства за осъществяването на адекватна, ефективна и ефикасна политика за киберсигурност.

4.3. Използването на уязвимостите в мрежите на критичните инфраструктури, налага използването на криптографията, като алгоритъм за защита на поверителността, целостта на данните.

4.4. Когато се говори за криптографска сигурност трябва специалистите по киберзащита да са наясно с определените дефиниции, понятия, цели и типове криптография.

4.5. Необходимо е да се инвестират повече средства в хора, технологии, научноизследователска дейност, за да могат военните да проучат съвременните заплахи в киберпространството и да открият възможните начини да защитят своите мрежи от неправомерни действия.

5. Заключение

Съвременното бойно поле отдавна е излезнало извън рамките на традиционното и вече започват да се появяват все повече неконвенционални оръжия. Бойният терен се прехвърли в киберпространството, което поражда нуждата от вземането на специални механизми за киберсигурност във всички сфери от обществения и личния живот. Компютърните системи са все по-чувствителни и уязвими, а процеси като глобализацията, разпространението и производството на компютърна техника, не достатъчната подготовка на хората за работа със системите, многобройните заплахи от нападения или манипулации застрашават работата на модерните информационни системи. Киберсигурността включва защита на военните мрежи срещу киберзаплахи. Киберпространството е мрежа от мрежи, която включва безброй компютри по целия свят, поради което нито една държава или организация не може едностранно да поддържа ефективна киберсигурност [9]. Именно в такъв тип мрежа, която се използва от голям брой потребители, криптографията често е от съществено значение за защитата, както на съхранените, така и на предаваните данни. Всяка една мрежа изисква използването на определен крипрографски алгоритъм, който да отговаря на нуждите на системата, за да гарантира сигурността. Колкото и да е сигурна, дори криптографската система има своите уязвимости и слаби места и основна задача на експертите по киберсигурността е да откриват тези „слаби места” и да създават алгоритми, с които системите да останат неприкосновени.

References

1. **Закон** за защита на класифицираната информация. https://www.lex.bg/laws/ldoc/2135448577

2. **Ненова** М. Въведение в приложната криптография. http://netseclab.tu-sofia.bg/nsk/lectures_nsk/L6.pdf

3. **Трифонов** Р. Системи за сигурност. Подписване на електронен документ с последваща валидация. http://archive.uktc-bg.com/SISTI_SIGURNOST/UPR-3_06-14.pdf

4. **Al-Vahed Ahmed, Haddad Sahhavi** (2011). An overview of modern cryptography. https://pdfs.semanticscholar.org/46d6/fee601a4f89b448deff8af7fce9c52d68501.pdf

5. **Diffie** Whitfield, Martin E. Hellman. Multiuser cryptographic techniques. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.892.6389&rep=rep1&type=pdf

6. **Koch** Robert, Mario Golling (2016). Weapons Systems and Cyber Security – A Challenging Union. https://ccdcoe.org/uploads/2018/10/Art-12-Weapons-Systems-and-Cyber-Security-A-Challenging-Union.pdf

7. Mulazzani Fabio**,** Lt.Col. Salvatore A. SARCIA (2011). Cyber Security on Military Deployed Networks. A Case Study on Real Information Leakage.
https://ccdcoe.org/uploads/2018/10/CyberSecurityOnMilitaryDeployedNetworks-Mulazzani-Sarcia.pdf

8. Rashid Awais, George Danezis, Howard Chivers, Emil Lupu and Andrew Martin (November 10, 2017) – CYBOK. Scope for the Cyber Security Body of Knowledge.
https://www.cybok.org/media/downloads/CyBOKScopeV2.pdf

9. Seng Alan Ho Wei. Cyber Attacks and the Roles the Military Can Play to Support the National Cyber Security Efforts -
https://www.mindef.gov.sg/oms/safti/pointer/documents/pdf/v42n3%204%20Cyber%20Attacks%20and%20the%20Roles%20the%20Military%20can%20play.pdf

10. **Snyder**, Don, James D. Powers, Elizabeth Bodine-Baron, Bernard Fox, Lauren Kendrick, Michael H. Powell. Cybersecurity of Air Force Weapon Systems. Ensuring Cyber Mission Assurance Throughout a System's Life Cycle.
https://www.rand.org/content/dam/rand/pubs/research_briefs/RB9800/RB9835/RAND_RB9835.pdf

11. https://economictimes.indiatimes.com/definition/cryptography

12. https://searchsecurity.techtarget.com/definition/cybersecurity

13. https://www.stormshield.com/solutions/by-industry/defense-and-military-organizations/

14. http://netseclab.tu-sofia.bg/vbook/Glava10.pdf

15. http://www.umich.edu/~umich/fm-34-40-2/ch2.pdf

Petar Kr. Boyanov, Zhaneta N. Savova,

IMPLEMENTATION OF CREDENTIAL HARVESTER ATTACK METHOD IN THE COMPUTER NETWORK AND SYSTEMS

Petar Kr. Boyanov[1], Zhaneta N. Savova[2]

[1] *Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, Department "Communication and Computer Technologies", peshoaikido@gmail.com*
[2] *National Military University "Vasil Levski", Faculty of Artillery, Air Defense and Communications and Information Systems, Department „Communication Networks and Systems", zh.savova@mail.bg*

Abstract: In this paper some sophisticated implementation of credential harvester attack method in the computer network and systems is made.

Keywords: Credential Harvester, Cybersecurity, Footprinting, Government agencies, Information Security, Modern cyber-attacks, Social engineering, Vulnerability, Threat

Introduction

The cyberattacks cause the greatest damage to businesses, companies, organizations and individuals through unauthorized intrusion into the resources of computer and network systems [1], [2] regardless of the firewalls built in, IDS intrusion detection systems, anti-theft systems IPS penetrations, virtual local area networks, and virtual public networks. The types of social engineering attacks are Human and computer based attacks. Characteristic of human-based attacks is that the malicious perpetrator can be presented as a legitimate end user [12], a very important user, or as a technical support person [13]. In all three types, the masked abuser aims to gain access to confidential information about the company, company or organization [6], [7], [8], [9], [10]. It should be noted that this type of attack also includes techniques in which cybercriminals monitor and observe everything behind their victim. In this way, a cybercriminal can obtain the desired information only by gently spying and looking behind the back or shoulder of an organization employee. It is even more dangerous when it is behind the back of the system administrator who is responsible for all information security of the organization. The malicious perpetrator may also use Special Intelligence Means (CPCs) [15] for real-time audio and video calls. Another way a cybercriminal can get information about his victim is to search through trash cans to find letters, important documents, sketches, written passwords and usernames, projects, plans, and more. [12], [13], [14]. Disguising and presenting a cybercriminal as a legitimate representative of a large organization can also help him get information about his chosen victims, with the ultimate goal being, in most cases, financial fraud and demanding bribes in large sums of money [1], [2], [3], [5], [6, [7], [8].

Computer-based attacks are characterized by the fact that various malicious programs and software applications are used [9], [10] such as infected letters sent via e-mail, use of computer viruses, Trojans, etc. The types of computer-based attacks are [1], [2], [11], [14], [15], [16], [17], [18]:

• Send false emails [1].

• Pop-ups. These attacks use pop-ups that alert the average user to disconnect from the computer network [5] and need to re-enter their username and password [7]. The most commonly used email is a hyperlink that redirects to a fake web page requesting the introduction of personal information or downloading a malicious program such as a Trojan horse or spyware that keeps track of every key on the keyboard.

• Mobile-based cyberattacks. They are divided into:

• Publishing malicious applications. In these attacks, cybercriminals create malicious applications with attractive configurations similar to real trusted applications in a large online application store. Then, unwary ordinary users download these applications and are then infected by malware that sends all their personal information to the cybercriminal computer machine [1], [2], [6].

• Send fake short messages on mobile phones.

2. Phases and victims of social engineering

Social engineering is one of the most powerful and almost always successfully completed by cybercriminals. They are characterized by the following features:

• In most cases, people are most susceptible to different assumptions and influences and thus the cybercriminal can take advantage of this fact and get the information he or she wants.

• In computer practice, it is almost impossible to detect or detect attempts at social engineering.

• The fact is that no effective or almost no methods and means have been found so far to provide full protection from social engineering.

• In practice, there are neither hardware nor software protections against social engineering cyberattacks.

The phases that one must go through in order for an effective and successful social engineering cyberattack are:

• Finding a way to visit the victim organization. It is also possible to go to the trash can of the organization in order to search for and retrieve recorded passwords and employee usernames.

• Identify disgruntled or offended employees of the victim organization.

• Associate with certain employees of the organization to obtain more confidential information such as financial statements and bank accounts, telephone numbers, e-mails, social network profiles, future plans and projects of the organization, current and future products and services, etc. [1], [3].

The major victims of social engineering cyberattacks are:

• System administrators.

• Automated Information Systems and Networks Security Officers.

• Development and Operation Officers.

• Users as call center staff, receptionists, host organization.

• Technical managers for information problems in an organization or company.

• Ordinary users or customers of the company, company and organization.

• Representatives of large and small companies for software and hardware products and services.

3. Experiment

The experiment on a Local Area Network of 13 hosts in a computer lab at the Faculty of Technical Sciences at Konstantin Preslavsky University of Shumen is made. Similar lab is proposed in [4]. The operating system installed on the computer victim is Windows 10 Pro x64, version 1709, OS Build: 16299.371. The operating system installed on the attacking computer is Kali Linux 4.12.0-kali-amd64 #1 SMP Debian x86-64 GNU/Linux.

The purpose of the science experiment is to create a cloned site for stealing your username and password. The SET machine toolkit for this purpose will be used. This suite of tools was developed by TrustedSec in order to test the computer and network security of a particular host. This is shown on Fig. 1.

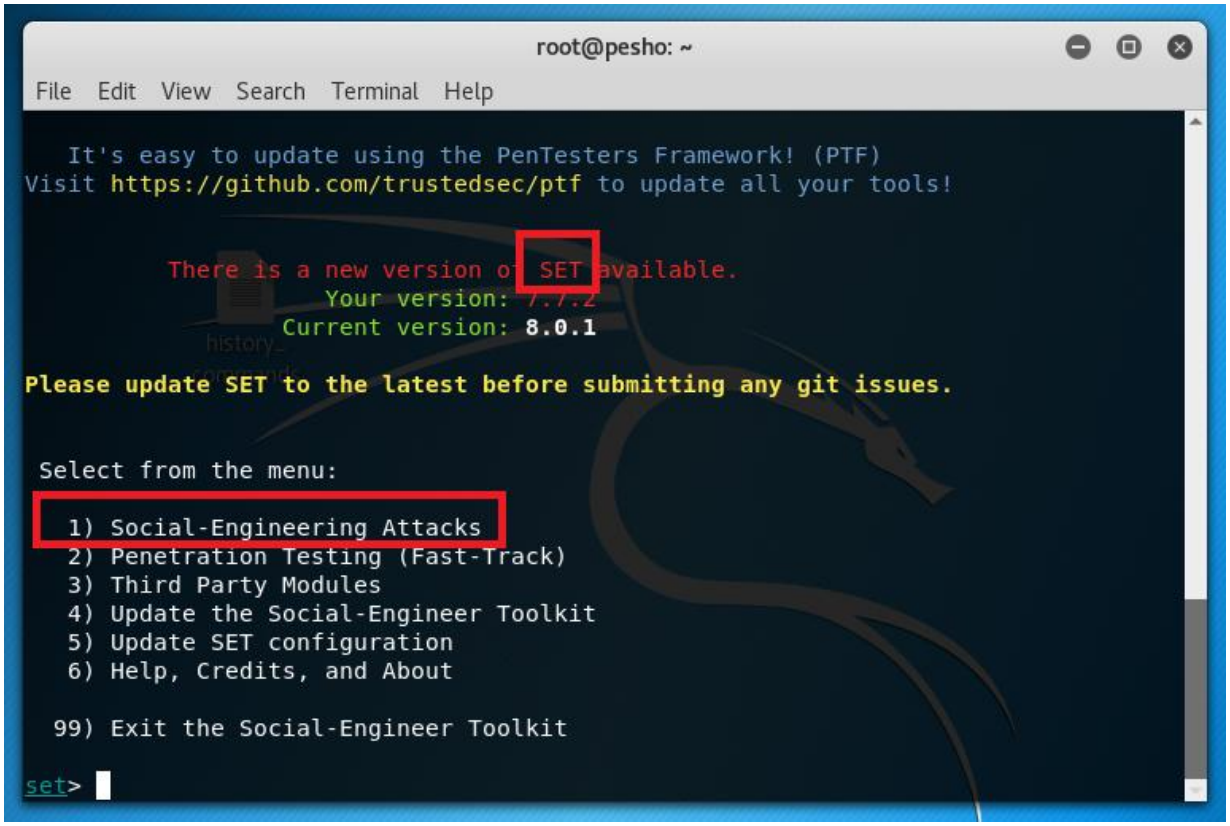


Figure 1. Initial screen of the toolbox SET

After the initialization of the toolbox the main menu is being visualized. Then menu number 1 with name “Social-Engineering Attacks” is selected. A new menu appears with possible attack vectors. It consists of 11 different attack vectors, which on Fig. 2 are shown.

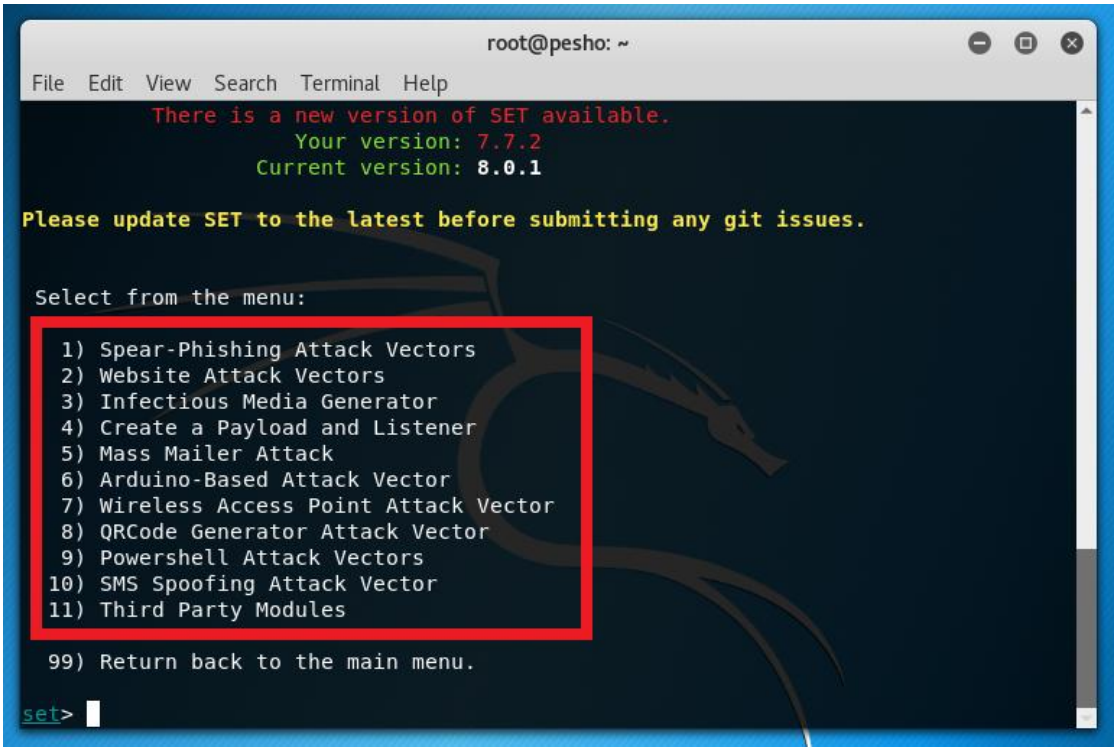


Figure 2. The attacking vectors

Menu „Website Attack Vectors” consists of the following attacking methods:

1) Java Applet Attack Method;
2) Metasploit Browser Exploit Method;
3) Credential Harvester Attack Method;
4) Tabnabbing Attack Method;
5) Web Jacking Attack Method;
6) Multi-Attack Web Method;
7) Full Screen Attack Method;
8) HTA Attack Method.

The most appropriate attacking method is Credential Harvester Attack Method. It will utilize web cloning of a web site that has a username and password field and harvest all the information posted to the website. The next menu displays three options (shown on Fig. 3).

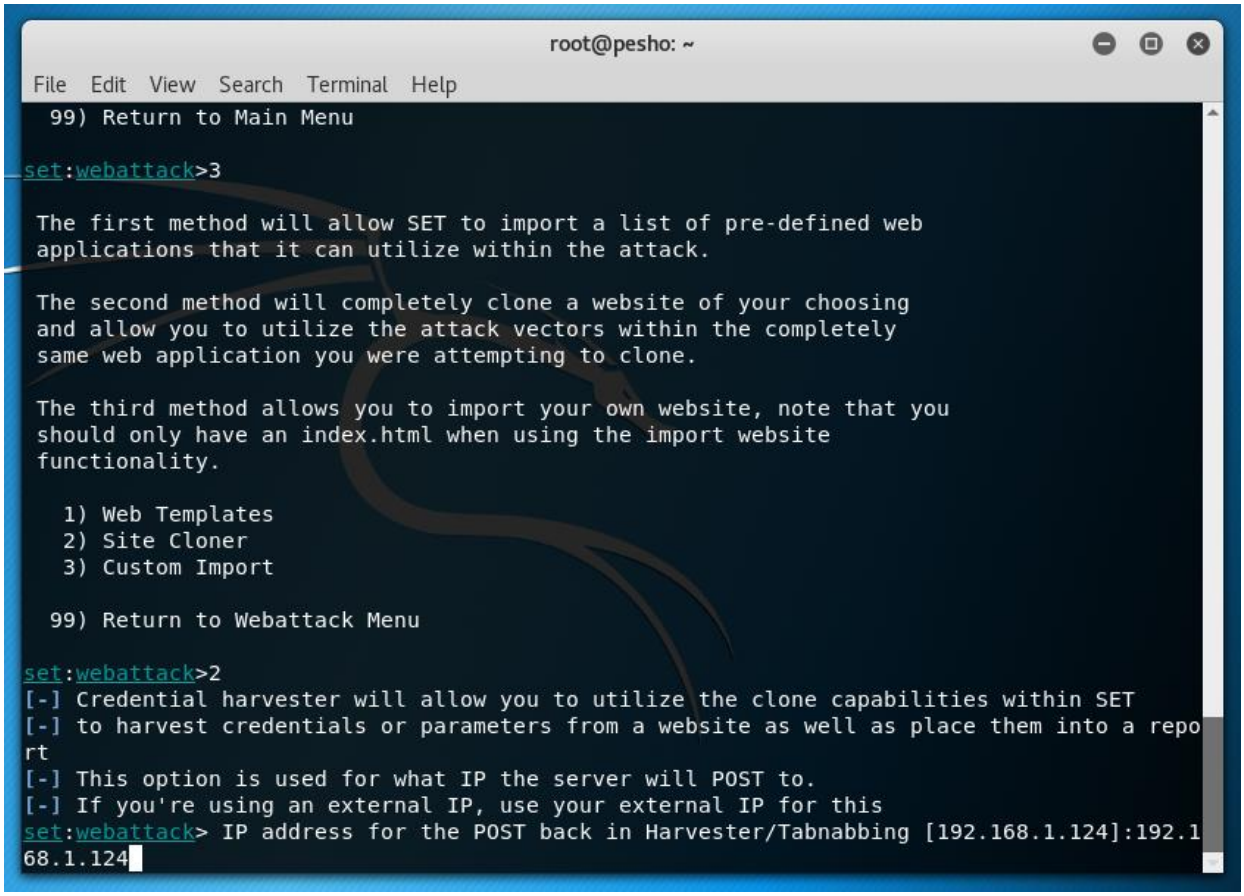


Figure 3. The menu of Credential Harvester Attack

After selecting “Site Cloner” the program asks for the IP address that the cloned site will contact when it is opened on the victim's computer. The IPv4 address of the attacking machine is 192.168.1.124. If this attack is carried out over the Internet, the public IP address is entered. When using a public network and a router, the port to be used for the connection will need to be routed from the router to the attacker's private address.

The last parameter that must be entered is a web page that will clone. The URL of the cloned web site will be - https://twitter.com/login. This is shown on Fig. 4.

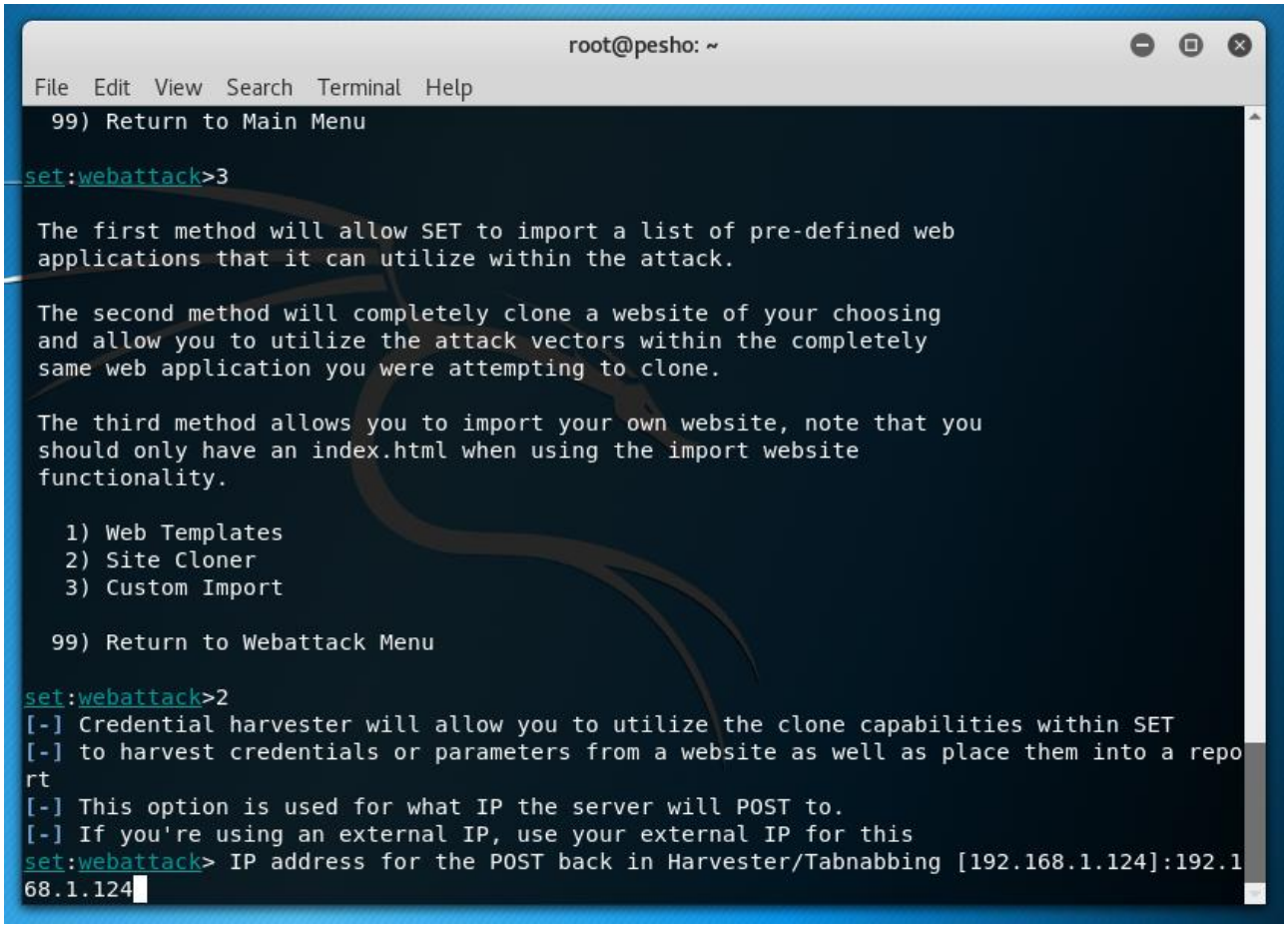


Figure 4. Credential harvester parameters

After that the Credential harvester vector is running on port 80 and clones the web site https://twitter.com/login. When everything is configured, then the victim computer is expected to enter their data on the cloned website and this is shown on Fig. 5.

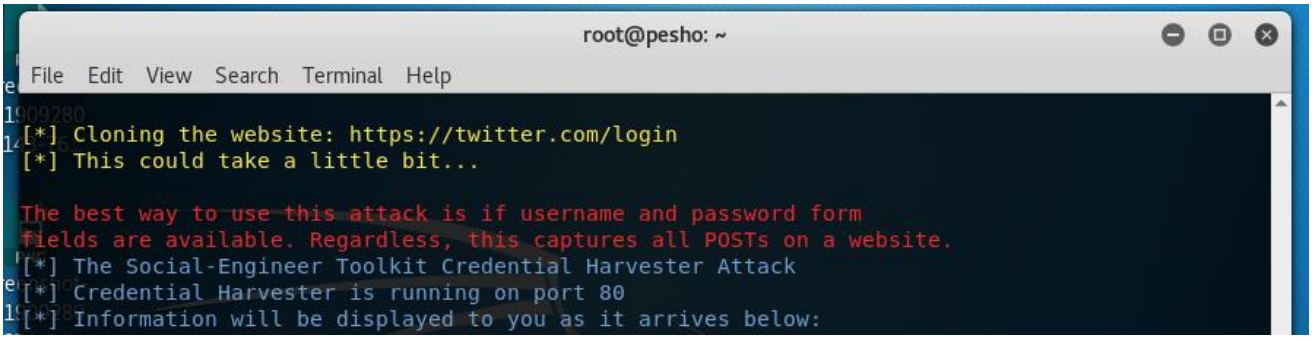


Figure 5. The configured parameters of the Credential harvester vector attack

When the victim’s computer enters its information, then it will appear on the screen in plain text format. After that the victim will be redirected to the official Twitter web page. The victim

Fig. 6 illustrates the loading the Twitter cloned web site with IPv4 address of the attacking machine. Fig. 7 shows the process of entering the username and password of the victim with working operating system Windows 10 Pro x64. The victim’s web browser Google Chrome version 77.0.3865.90 is used.

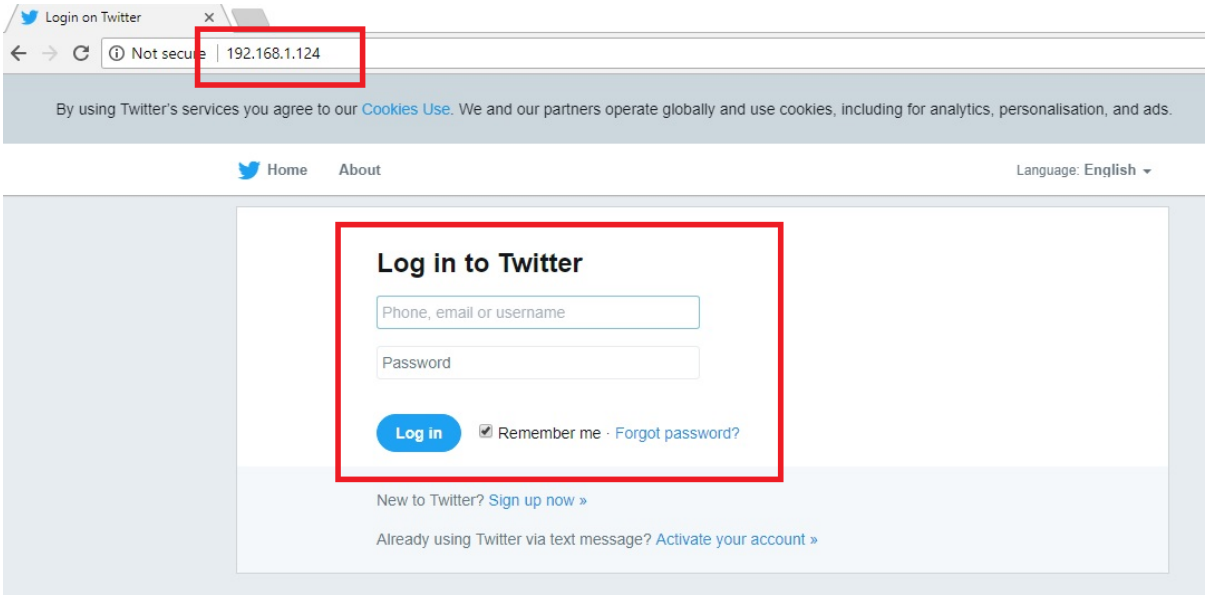


Figure 6. The Loading the Twitter cloned web site

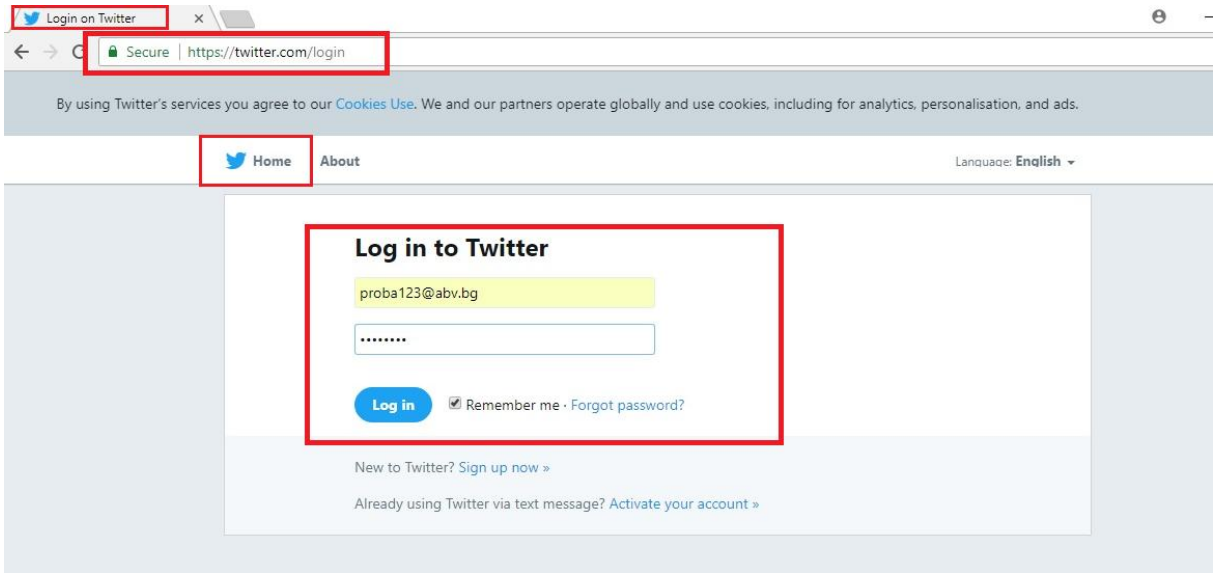


Figure 7. Entering the username and password of the victim

The possible found username or email is "proba123@abv.bg" and possible found password is "parola123". The fetched information is saved as a report file. The content of the generated report file is shown on Fig. 8.

NOTE: All of the scientific experiments and studies in this paper were conducted in a specialized computer lab at the Faculty of Technical Sciences at the Konstantin Preslavsky University of Shumen, consisting of several hosts. Everything illustrated and explained in this paper is for research purposes and the authors are not responsible for any misuse.

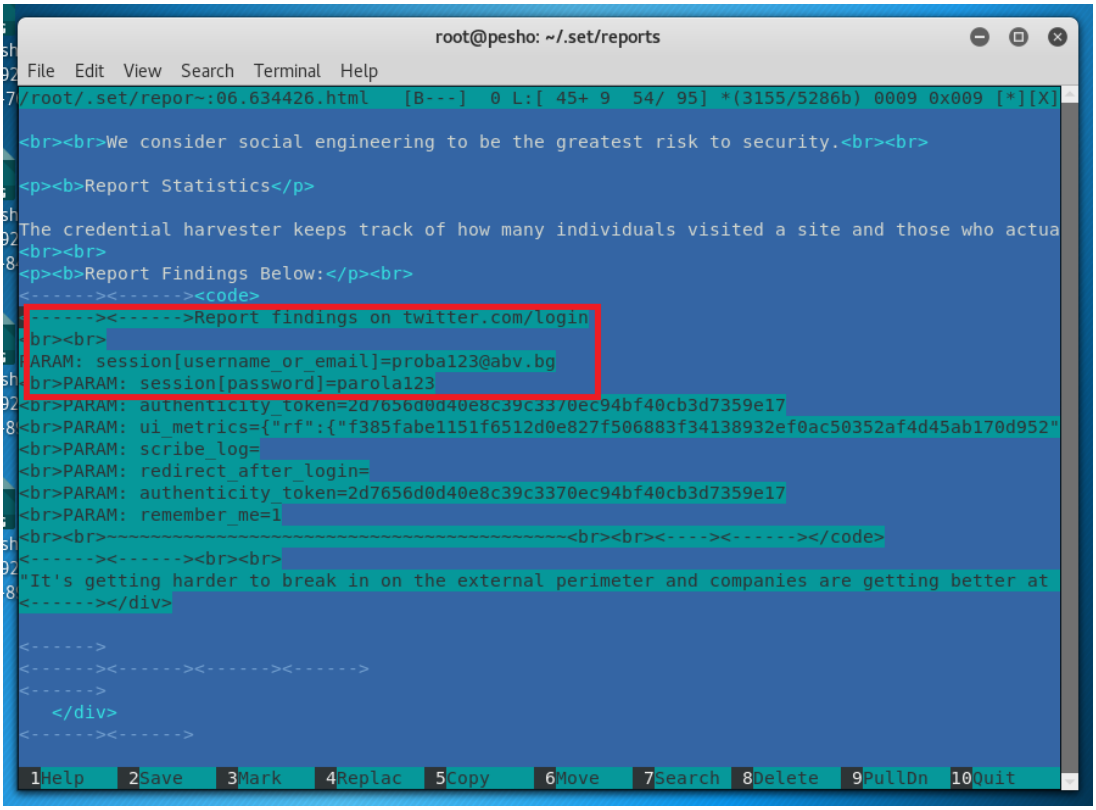


Figure 8. The content of the generated report

Conclusion

Automated Information Systems and Networks Security Officers and the Security Administrator must take and take the following security actions, such as:

• Mandatory periodic change of employee passwords.

• Blocking an employee's user account if more than three or more unsuccessful attempts have been made. The blocking time can be set for 1 day.

• Use of special machines for destroying Schroeder documents. This way, the cybercriminal will not be able to find any stored sheets of paper in the organization's trash cans.

• Mandatory employee identification through unique ID cards, fingerprints, special uniforms, hand bracelets, eye retina scanners, and more.

• When there is an open day at the organization, there is a need for special staff to monitor all guests what they are doing and where they are going.

• Compulsory undergraduate special training courses for employees and signing special documents to ensure that they understand and comply with information security policies. In case the employee does not comply with the regulated internal rules, he is liable to criminal liability according to the Criminal Code and the Criminal Procedure Code of the Republic of Bulgaria.

References

1. Linko Nikolov, Krasimir Slavyanov, „*On the contemporary cybersecurity threats*“, I st CONFSEC 2017, 11-14.12.2017, Borovets, ISSN Print: 2603-2945, ISSN Online: 2603-2953, стр. 142-144; url: http://confsec.eu/sbornik/2-2017.pdf.
2. Linko G. Nikolov, Ognyan M. Fetfov, Angela R. Borisova, „SECURITY CONCERNS IN JAVASCRIPT CODING“, MATTEX 2018, Volume 2, part 2, CONFERENCE PROCEEDING, v. 2, pp. 27 – 31, SECTION Communication and Computer Technologies, ISSN: 1314-3921

3. Linko G. Nikolov, „*Wireless network vulnerabilities estimation*“, International Scientific Journal “Security & Future”, Vol. 2 (2018), Issue 2, pg(s) 80-82; WEB ISSN 2535-082X; PRINT ISSN 2535-0668
4. Nikolov, L., Slavyanov, V. Network infrastructure for cybersecurity analysis. International scientific conference 2018, “Vasil Levski” National Military University - Artillery, Air Defense and CIS Faculty, Shumen, Bulgaria, 2018, ISSN 2367-7902.
5. Савова, Ж., Богданов, Р., *Анонимна система за комуникации в киберпространството, използваща протокол TOR*, Сборник научни трудове на научна конференция на Факултет „А, ПВО и КИС” „Новата парадигма за сигурност в киберпространството” Шумен 2014, стр. 259-265, ISBN 978-954-9681-49-9.
6. Савова, Ж., Богданов, Р., *Оценка на изчислителната сложност на алгоритмите за генериране на големи прости числа за целите на криптографията*, Сборник научни трудове на Научна конференция „Проблеми на информационната сигурност”, гр. Шумен, 2010, ISSN 1314-0647.
7. Савова, Ж., Богданов, Р., *Приложение на недвоичните псевдослучайни последователности в криптографията*, Сборник научни трудове Немус'2012. Институт по отбрана Проф. „Цветан Лазаров”, 2012, ISSN 1312-2916.
8. Досев, Н., Петров, В., *Съвременни тенденции и аспекти на информационната сигурност в автоматизираните информационни системи и мрежи (АИС/М)*, Научна конференция с международно участие MATTEX 2018 , Шуменски университет „Епископ Константин Преславски“, Университетско издателство, Сб. научни трудове том 2, част 1, стр. 85¸95, ISBN 1314-3921.
9. Фетфов, О., Боянов, П., Ташева, Ж., Трифонов, Т., *Анализ на съвременните видове уязвимости и експлойти в компютърните мрежи и системи*, Annual of Konstantin Preslavsky University of Shumen, Shumen, Университетско идателство „Епископ Константин Преславски“, ISSN 1311-834X, Vol. VI E, 2016, с. 112-122.
10. Savov, I., Edin pogled varhu sashtnostta na kiberprestapleniyata, spisanie „Politika i sigurnost”,VUSI, 2017, ISSN 2535-0358, s. 36-47.
11. Savov, I., The collision of national Security and Privacy in the age of information technologies, European Police Science and Research Bulletin, European Union Agency for Law Enforcement Training, 2017, ISSN 2443-7883, p. 13-21.
12. Камарашев, Г., Димитрова, С., *Финансовия мениджмънт като елемент на военната логистика*, Trans&Motauto 2005 с.37-41.
13. Kamarashev, G., Dimitrova, S., *Outsourcing as a part of the management of resources for security and defense*, SIBIU 2011, pp.643-647.
14. Kamarashev, G., Dimitrova, S., A*spects of defence and security resource allocattion,* Sibiu 2007.
15. Kamarashev, G., Banabakova, V., *Acquisition – theoretical and practical aspects of application in the defense system*, Brno 2005 с.30-37.
16. Parashkevanova, G., Tsankov, Ts., *CERT Bulgaria*. Научна конференция с международно участие „Киберсигурността в информационното общество“, НВУ „Васил Левски“, Шумен, 2017.
17. Parashkevanova, G., Tsankov, Ts., *Cybercrime as the main contemporary threat to large organizations*, Conference proceedings Mattex 2016, ISSN 1314-3921.
18. Tsankov, Ts., Denev D. R., *Use in Internet of Protocols Transport Layer Security and its now-deprecated predecessor Secure Sockets Layer*. Annual of Konstantin Preslavski University of Shumen, Vol. VIII E, 2018.

SOCIAL SCIENCE

Krasimir M. MarkoV,

FOR BASIC CONCEPTS IN EXTREME PSYCHOLOGY

Krasimir M. Markov

Faculty Artillery, PVO and KIS – Shumen, National Military Inuversety "Vasil Levski" Bulgaria, e-mail markov_kr@abv.bg

ЗА ОСНОВНИ ПОНЯТИЯ В ЕКСТРЕМАЛНАТА ПСИХОЛОГИЯ

Красимир М. Марков

Факултет Артилерия, ПВО и КИС – Шумен, Национален военен университет „В. Левски“ България, e-mail markov_kr@abv.bg

***Abstract**: Basic concepts in extreme psychology related to experiences in extreme situations and implications for the human psyche are discussed*

***Keywords**: extreme psychology, extreme situation, stress, frustration, conflict, crisis, affect*

Общоприето е авторите и изследователите занимаващи се с екстремална психология, когато описват екстремалните, тежките или критичните ситуации да извеждат четири ключови понятия с които в екстремалната психология се описват подобни ситуации [1,2,6,8,9]. Тези основни понятия са: стрес, фрустрация, конфликт, кризис и афект. Независимо от единодушие на авторите за тези понятия като основни в екстремалната психология доста от тях влагат различно съдържание при описването им.

Стрес – стресът е особено състояние на психиката и на организма като цяло, характеризиращо се с мобилизация на всички резерви на организма за преодоляване на някакво вредно или опасно за здравето и живота въздействие. Това въздействие трябва да бъде достатъчно силно, за да може да предизвика защитна хормонална реакция на организма свързана с преустройството на функционалните системи и адаптация към новите условия, и имаща цел да запази и съхрани организма. Тези въздействия, които наричаме стресови като правило се делят на физиологични свързани с болка, глад, жажда, висока или ниска температура, прекалено физическо натоварване и т.н., и психологически към които включваме опасност, заплаха, загуба, лъжа, обида, информационна претовареност и др.

Стресът става травматичен, когато в резултат на въздействието на стресора се появява нарушение в психичната сфера. В този случай се нарушава структурата на Аз-а, когнитивният модел на света, афективната сфера и механизмите управляващи процесите на паметта, ученето и т.н.

Това означава, че стресора трябва да бъде травмиращо събитие притежаващо много мощно негативно въздействие в последствие от което се явява ситуация на заплаха за живота на човека или неговите близки. Ясно е, че такива събития нарушават чувството за безопасност на човека, предизвиквайки травматичен стрес, психологическите последици от който са доста разнообразни. Факт е, че преживяването на травматичен стрес от някои хора става причина за проявление у тях на наченки на посттравматично стресово разстройство [1,9].

Като причини за появата на стреса можем да посочим и такива като постоянен недостиг на време, налага се да правим нещо по задължение, а не ни се прави, нещо ни препира, постоянно недоспиване, конфликти в семейството и работата, неудовлетвореност от живота, чувство за самотност и липса на човек с когото да споделим проблемите си и т.н.

Етапите на стреса са описани още от Ханс Селие, но в тях се влага относително ново съдържание. Те са следните:

- Етап на мобилизация, през който се повишава вниманието, мобилизира се активността;
- Етап на стенични отрицателни емоции – проявява се гняв, ярост, агресия, а увеличеното натоварване води до последващо изтощение на организма;
- Етап на астенични отрицателни емоции, при който се усеща чувство за безсилие, настъпва депресия и човек е обхванат от мъка и отчаяние.

Като резултат на протичане на тези етапи в човешкия организъм настъпва нервен срив и се появяват неврози.

Травматичен стрес, това е особено преживяване в резултат от специфично взаимодействие на човека и околната среда. Всъщност става дума за нормална реакция на ненормални обстоятелства, която възниква в човека преживял нещо излизащо извън рамките на нормалния човешки опит. Става дума за много ситуации, но всички те са свързани със заплаха за живота и здравето на човека и неговите близки, или с нарушаването на Аз-образа. Психическата реакция на травмата включва три относително самостоятелни степени на развитие, което позволява да я разглеждаме като процес развиващ се във времето.

Първа степен – психичен шок, съдържа два основни компонента – загуба на активност, нарушаване на ориентацията, дезорганизация на дейността и отрицание на случващото се. По принцип нормално тази степен е относително кратка.

Втора степен – въздействие, характеризира се с изразени емоционални реакции по повод на събитието и неговите последствия. Това могат да бъдат страх, ужас, тревога, гняв, плач или другояче казано емоции, които се проявяват непосредствено и с висока интензивност. Постепенно те се сменят с реакция на критика или съмнение в себе си и се съпровождат с болезнено осъзнаване на невъзвратимостта на случилото се и признаване на собственото безсилие. Тази степен е критична за човека тъй като след нея започва или процес на възстановяване, адаптация към нововъзникналите обстоятелства и възприемане на новата реалност, или настъпва фиксация върху травмата и последващ преход към постстресово състояние в хронична форма. Този тип нарушения, които се развиват след преживяната психологическа травма засягат всички нива на функциониране на човека като организъм, довеждат до значителни личностни изменения не само у хората, които са преживяли това събитие, но и в техните близки. Особеното е, че в резултат на много изследвания се доказва, че това състояние което се развива под действието на травматичен стрес не попада в нито една от познатите в клиничната практика класификации [1,8.9].

Фрустрация – този термин се използва с две значения, от една страна като акт на блокиране или прекъсване на поведение насочено към постигане на определена цел и тогава говорим за фрустрационна ситуация, и от друга страна като емоционално състояние на човека възникващо след неуспех при неудовлетворяване на някаква силна потребност или критично отношение на останалите към даден човек. Последиците от това са възникване на силни емоции като враждебност, гняв, вина, тревога.

В литературата [9] се определят няколко основни вида фрустрационно поведение на личността:

- Двигателна възбуда – безцелни и непоследователни поведенски реакции;
- Апатия;
- Агресия и деструкция – човек се стреми към разрушаване на предмети от околната среда, причиняване на вреда или щета;
- Стереотипизация – проявява се като тенденция на безсмислено поведение на фиксирани форми на поведение;
- Регресия – тя се разбира като обръщане към поведенски модели, които са доминирани в по-ранни периоди от живота на човека или като примитивизация на поведението.

Състоянието на фрустрация не възниква изведнъж, за да се появи то трябва да се преодолее така наречения фрустрационен праг. Той се определя със следното:

- Повторение на неудовлетворението – всяко последващо неудовлетворение води до сумирането му с емоционалната следа от предишния неуспех;
- Дълбоко неудовлетворение – колкото по-силна е била потребността, толкова по-занижен е прага при който настъпва фрустрацията;
- Емоционална възбудимост – колкото тя е по-висока, толкова по-нисък е фрустрационния праг;
- Ниво на претенциите на човека – колкото човек по-рядко се е сблъскал с неудачи и провали, толкова по-нисък е прага на фрустрацията;
- В зависимост от етапа на дейността – ако препятствието възникне в началото на определена дейност фрустрацията се проявява по-слабо в сравнение с тази, която настъпва в края или при завършване на определена дейност.

Самата фрустрация има и негативни, и позитивни последствия за човека. Позитивните последствия са свързани с мобилизирането на психичните ресурси и откриващите се възможности за личностно развитие. Усиленото в резултат на фрустрацията напрежение може да помогне на човека да има нов поглед върху ситуацията, да преоцени своите предишни действия и да види нови различни пътища за достигане на поставената цел, а негативните ефекти се заключават в увеличаването на напрежението от емоционалната възбуда, което може да се окаже толкова силно, че под въздействието на афекта човек да загуби способност за конструктивност на действията, да загуби контрол и да изпадне в паника. Ако човек изпада често във фрустрация, това води до формиране на негативни черти в поведението като агресивност, възбудимост, враждебност.

Конфликт – понятието в социалната психология, личностовата психология и конфликтологията се трактува по различен начин, но винаги става дума за това, че се създава ситуация на сблъсък на някой с някого за нещо. Този конфликт може да бъде вътрешен, когато възниква в човека, който е поставен пред дилемите мога и не мога, искам и не искам, трябва и не трябва и т.н. За да възникне междуличностния конфликт трябва да са налице интереси и противоречия между хората, които са несъвместими от гледна точка на крайната цел на достигането им. В екстремалната психология се среща често понятието невротичен конфликт, под което се разбира противоречие между личността и значими за нея аспекти от действителността, които се разрешават непродуктивно и нерационално и водят до болезнени преживявания на неуспех, на неудовлетворимост на потребностите, непостигане на целите на живота, невъзвратими загуби и т.н.

Кризис – самото понятие кризис реално означава остра ситуация в която попада човек, повратен пункт, важен момент. Това е нарушение на емоционалния баланс настъпващ под влияние на заплаха създавана от външни обстоятелства. Чисто психологически това е ситуация водеща до невъзможност на по-нататъшното съществуване на човек в досегашния му статус [2,9].

Имаме два типа кризисни ситуации в зависимост от това каква възможност предоставят на човека в живота след ситуацията:

Първи тип – сериозно сътресение, което обаче съхранява определен шанс за връщане към предишния живот.

Втори тип – зачертва всичко случило се досега в живот на човек и му оставя единствения изход промяна на собствената личност и смисълът на собствения живот.

Каплан [по 9] описва четири последователни стадии на кризи при човек:

- Първичен ръст на напрежението – който стимулира обичайни начини за решаване на проблемите;
- По-нататъшен ръст на напрежението – тогава, когато тези резултати и способи се окзват нерезултатни;
- Още по-силно увеличаване на напрежението – което изисква мобилизация на вътрешни и външни ресурси;
- Ако това се окаже също безрезултатно настъпва четвъртия стадий, който се характеризира с повишена тревога, депресия, чувство за безпомощност или депривация на личността.

Той подчертава също и факта, че кризиса може да приключи във всеки един от тези стадии, ако изчезне опасността или бъде намерено адекватно решение за решаване на проблема.

Ще се спрем на някои видове кризиси:

Невротични кризиси – предпоставките за възникване на които се формират още в ранното детство и могат да се развиват даже при отсъствие на въздействие на някои външни дразнители, травмиращи събития и промени (З. Фройд, К. Хорни).

Възрастови кризиси – възникващи при прехода от една възраст към друга, които са свързани с преобразование в системата на социалните отношения, дейността, съзнанието (Ж. Пиаже, Л. Виготски, Е. Ериксон).

Травматични кризиси – възникват в резултат на психотравмиращи ситуации и зависят от оценката на тази ситуация от личността и съответно преценената степен на субективна значимост.

Биографичен кризис – той е особеност на вътрешния свят на човека, която се проявява от преживяване в различни форми на непродуктивността на собствения жизнен път. Самият биографичен кризис има три типа направления: кризис на нереализираността – възниква тогава, когато по една или друга причина човек трудно намира връзка между отделните събития на собствения си живот; кризис на опустошеността – възниква при ситуации, когато субективната картина на жизнения си път човек не открива връзките, които го водят от миналото през настоящето към бъдещото; кризис на безперспективността – възниква в ситуации, когато по една или друга причина, човек трудно прави планове, проекти или липсват мечти свързани с неговото бъдеще.

Кризис на загубата – свързан със загуба на близък човек. Преживяването му се описва с картината на голяма мъка (Линдеман).

Екзистенциален кризис – загуба на смисъла на съществуването, загуба на най-значимите ценности и цели на живота, преразглеждане на целия собствен живот.

Афект – той е състояние на внезапно възникващо силно душевно преживяване предизвикано от насилие, издевателство, тежко оскърбление, продължителна посттравматична ситуация и др. За афекта е важно да се установят основните признаци на всеки вид афект, тъй като в правото афекта може да се разглежда като смекчаващо обстоятелство, което може да освободи човек от наказателна отговорност. Афектът забавя включително психични процеси, които не са пряко свързани с него, като вниманието което се концентрира върху източника на чувствата, а всички останали детайли на обстановката изобщо не влиза в проекта на съзнанието, затова състояние е характерно свиване на съзнанието. Състоянието на афекта възниква по-често у неуравновесените и слабохарактерни хора. Външно той може да се проявява в прекомерна активност или агресия, или от друга страна като задръжка в движенията и вцепеняване. Силната възбуда се разпространява и върху механизма на физиологичната регулация на емоциите. Човек или побледнява, или почервенява, неговите движения са сковани или хаотични, а речта е накъсана.

В психологията и психиатрията се определят три вида афекти:

- Физиологичен афект – с този афект се занимават преди всичко психолозите и той се свързва с внезапно възникване на силно, но кратковременно емоционално състояние, при което про-

тича дезорганизация на психичната дейност. Човек не разбира напълно разбирането си за ситуацията и действията, които извършва, но практически не ги контролира. Основните признаци на физиологичния афект са: внезапност на възникването, взривоопасна динамика, развива се за много кратко време и достига своя предел; кратковременност – продължава секунди или минути; интензивност и напрежение при протичането – в състоянието на афект у човек се появяват допълнителна сила и възможности; дезорганизиращо влияние на психичната дейност – свиване на съзнанието, снижаване качеството на мисловните процеси, рязка загуба на самоконтрол; засилена двигателна активност – в някои от случаите се стига до особена жестокост на поведението; вегетативни изменения – изменя се цвета на кожата, модулацията на гласа, интензифицира се сърдечната дейност; като последствие на афекта може да се наблюдава частична амнезия и астеничен синдром, когато човек не си спомня отделни детайли на това, което е направил и изпада във физическа и нервно-психическа слабост.

- Патологичен афект – с него се занимават психиатрите и клиничните психолози, той представлява кратковременно болезнено психическо разстройство съпроводено с дълбоко замъгляване на съзнанието, импулсивни актове и частична или пълна амнезия. Действията на човек в това състояние са съпроводени с несвързан говор и прекалена жестикулация.

Приведената типология предоставя възможност за по-диференцирано описание на екстремалните житейски ситуации. Разбира се, всяко конкретно събитие може да засегне всички показани промени като предизвиква едновременно и стрес, и фрустрация, и конфликт, и кризис, но именно различията в екстремалните ситуации създават необходимостта от разграничаването на понятията стрес, фрустрация, конфликт и афект от гледна точка на екстремалната психология.

References

1. Alexandrov, Iv. (2018) Post-traumatic stress disorder. Clinical-psychological aspects. "STENO" -Varna
2. Атанасова-Кръстева, Н. (2018) Психология на кризиса. В. Търново : Нац. воен. унив. "Васил Левски",
3. Антипов, В. В. (2002) Психологическая адаптация к экстремальным ситуациям. М., Владос,
4. Анцыферова, Л. И. (2001) Личность в трудных жизненных условиях: переосмысление, преобразование ситуаций и психологическая защита. СПб.
5. Голованевская В. И. (2003) Характеристики Я-концепции и стратегии совладания с трудными жизненными ситуациями. В. Московского университета.
6. Малкина-Пих (2005), Экстремальные ситуации. М.
7. МКБ-10. (2003) Психични и поведенчески разстройства. С.
8. Стасенко В.Г. М.Л Хуторная. — «Экстремальная психология и психотерапия экстремальных состояний»Учеб. пособие. – Воронеж: НОУ ВПО «Международный институт компьютерных технологий», 2010
9. Стоянов, В. (2008) Посттравматично стресово разстройство. В.
10. Magnusson, D. A. (1981) Psychology of Situations. Toward a Psychology of Situations: An Interactional Perspective. New Jersey
11. Paul, M. Lehrer; P. L. Woolfolk. (1993) Principles and Practice of stress management. N. Y.; Guilford Press.

Veliko P. Petrov, Hristo A. Hristov,

INTERNATIONAL ORGANIZATIONS AND INSTITUTIONS WORKING ON ENVIRONMENTAL PROBLEMS

Veliko P. Petrov, Hristo A. Hristov

*Faculty of Artillery, Air Defense and Communication and Information Systems,
National Military University, Shumen, Bulgaria, veliko_pp@abv.bg,
Shumen university ,,Bishop Konstantin Preslavski’’, Shumen city, Faculty of technical sciences, Department ,,Management of security systems’’*

***Abstract**: This report aims to familiarize readers with international organizations and institutions working on environmental issues that find adequate solutions to address the world's universal environmental problems. International and national institutions and organizations, including UN entities and its specialized organizations and the EU, are developing systems of measures and regulations aimed at reducing environmental risks.*

***Key words:** international organizations and institutions, environment*

МЕЖДУНАРОДНИ ОРГАНИЗАЦИИ И ИНСТИТУЦИИ, РАБОТЕЩИ ПО ПРОБЛЕМИТЕ НА ОКОЛНАТА СРЕДА

Велико П. Петров, Христо А. Христов

През последните десетилетия глобалните и регионалните екологични проблеми са сред основните предизвикателства пред съвременното човечество. От една страна, нараства загрижеността относно ефекта от различните икономически дейности върху националната и глобална околна среда. От друга страна, постигането на по-висок икономически растеж е обвързано пряко с природните ресурси, с които разполагаме.

Международните организации обслужват международните отношения, така както вътрешнодържавните институции са в служба на националните общности, но с много по-ниска ефикасност. Различните международни организации и институции започват да проявяват определен интерес към околната среда най-вече след втората половина на XX век и вземат активно участие в повечето провеждани общи и специализирани конференции по екологични проблеми. Те имат отношение и дават компетентни мнения по много аспекти и измерения на екологичната проблематика. В рамките на своите правомощия международните организации често са инициатори за изготвянето на договорености по различните аспекти на околната среда. Един от най-важните елементи на сътрудничеството в рамките на международните организации, които се занимават с екологични проблеми е събирането и предоставянето на всякакъв вид информация свързана със състоянието на околната среда. По редица конвенции опазването на околната среда и рационалното използване на природните ресурси се възлага на международни организации.

Бурното развитие на научно-техническия процес особено през последното столетие доведе до увеличаване на човешкото въздействие върху околната среда. Глобалните екологични проблеми придобиват нови измерения поради факта, че с напредъка на научните познания става ясна

и разбираема необходимостта от овладяване на негативните последици от човешката дейност върху околната среда. Отрицателните последици от това въздействие се проявяват понякога в много по-късен момент от извършването на вредоносното влияние и поради това са трудно предвидими. Замърсяването и увреждането на околната среда в настоящия момент има своите проекции и засяга бъдещето на следващото поколение, не само неговото здравословно състояние, но и необходимостта да влага много повече средства за преодоляване на последиците (преки и косвени) от днешното развитие и за компенсиране на еко системните услуги, които увредената природа не може да достави. Причините за екологичните проблеми на съвременното общество са от субективен и обективен характер. Сред *обективните причини* могат да бъдат посочени географското положение на съответната държава, степента на икономическото й развитие, равнището на използваните технологии в производството и др. Сред *субективните причини* могат да се посочат подценяване значимостта на екологичните проблеми, ниска екологична култура сред населението и др.

Необходимостта от стабилизиране и подобряване на ключовите параметри на околната среда е безспорна, безусловна и неотложна. Универсалните екологични проблеми най-удачно биха могли да намират адекватни решения в рамките на ООН и неговите специализирани организации, създавани с определени цели и на различно равнище. Международни и национални институции и организации, включително структури на ЕС, разработват системи от мерки и нормативи, целящи редуциране на екологичните рискове. Но опитът в управлението на екологичните рискове показва, че дори даден риск веднъж вече да е идентифициран и оценен и да са установени стандарти и практики за редуцирането му, те не могат да се прилагат автоматично винаги и навсякъде.

Екологичната политика се определя като комплекс от мерки и дейности, свързани със създаването на предпоставки за справедливото и ефективно разпределение на природните блага в обществото. Тя се основава на редица процедури, насочени към намаляване на вредните въздействия върху природните ресурси и прилагането на инструменти за възстановяване на щетите, базирани на влагането на част от дохода получен в резултат от използването им.

Една от най-важните и актуални политически, икономически, социални и международни задачи е опазването на околната среда. Това се дължи на постоянно нарастващото й значение във вътрешния живот на всяка страна и в отношенията между държавите на международно ниво. В този смисъл тя се превръща в едно от основните направления на международното сътрудничество.

Всяка държава е задължена да спазва поставеното изискване за съвместно участие в опазването на околната среда, както и да изгражда екологични обекти от общо стопанско значение.

Екологичната политика представлява съвкупност от административно-законодателни и икономически средства и механизми, утвърдени от държавните органи и съобразени с международните договорености. Тяхната основна цел най-общо намира отражение в устойчивото развитие на националното стопанство, което се постига чрез опазването на околната среда и рационалното използване, и непрекъснато възпроизвеждане на природните ресурси.

Политиката в областта на околната среда е област, в която ЕС доказва своята водеща позиция на глобално ниво. Тази политика е огромна по своя обем (над 300 директиви) и по своя обхват. В най-тесен смисъл нейните области включват качеството на атмосферния въздух, на сладководните и соленоводните басейни, подземните води, почвите, управлението на отпадъците, употребата на химически препарати, ядрената безопасност, защитата на биологичното разнообразие, местообитанията и птиците. В по-широк смисъл всички политики на ЕС съдържат в себе си екологичен компонент и по-конкретно всички общи политики на ЕС би следвало да се придържат към идеята за устойчиво развитие.

Европейската политика в областта на околна среда се основава на принципа на предпазните мерки, превантивните действия и отстраняване на замърсяването при източника, както и на принципа „замърсителят плаща". Многогодишните програми за действие за околната среда определят рамката на бъдещите действия във всички сфери на политиката в областта на околната среда. Те са част от хоризонталните стратегии и се вземат под внимание в рамките на международ-

ните преговори във връзка с околната среда. Освен това решаващо значение има тяхното изпълнение.

Институционална рамка на екологичната политика – включва институциите, които определят стратегиите на политиките и програмите за действие в различни области на развитието.

Организацията на обединените нации (ООН) е международна организация, създадена официално на 24 октомври 1945 г., когато уставът ѝ е ратифициран от 5-те постоянни страничленки на нейния Съвет за сигурност – Китай, Русия (бившия СССР), САЩ, Обединеното кралство и Франция.

Основна цел на ООН е спазване на мира и сигурността. Основавайки се на принципите за равни права и самоопределяне на народите, тя развива и приятелските международни отношения. Организацията полага грижи за постигането на световно сътрудничество при разрешаването на международни проблеми от културно, икономическо, социално или хуманитарно естество. Междувременно ООН трябва да послужи като средище, където да се обединят усилията на всички нации за постигането на поставените цели.

Още с учредителния договор (през 1945г.), на ООН се възлага като основана мисия поддържането на мира и сигурността в света, развитието на приятелски отношения между народите, установяването на международно сътрудничество за решаването на хуманитарни, икономически, социални и др. въпроси. Първа изява на ООН в областта на околната среда е още от края но 40-те години на миналия век. През 1949 г. тя провежда в Лей Саксес, САЩ, международна техническа конференция по опазване на природата. Под егидата на ООН се провеждат три конференции по морско право. Последната от тях изиграва изключително голяма роля за определянето на юридическите рамки при използването и опазването на световния океан.

По инициатива на ООН се провеждат и световни форуми по глобални екологични проблеми – в Стокхолм, Рио де Женейро, Йоханесбург. В съответствие с препоръките от Стокхолмската конференция на ООН по окръжаващата човека среда, ОС на ООН създава свой спомагателен орган „***Програма на обединените нации по околна среда" (ЮНЕП***), със седалище Наероби, Кения.

Програмата на ООН за околната среда (*United Nations Environment Programme* - UNEP) е организация на Организацията на обединените нации, която свързва дейностите по опазване на околната среда, като помага на развиващите се страни да прилагат конституциите и да насърчават устойчивото развитие чрез екологични дейности.

Ръководен орган е Съветът на управляващите, избиран от ОС на ООН за срок от 3 години. На ежегодни сесии отчита извършеното през изминалата година дейност и набелязва последващи задачи. Отчита се пред ОС на ООН. Работи в сътрудничество с други организации. Основни функции на ЮНЕП са в три направления:

1) създаване на глобална система за мониториг (наблюдение) на околната среда;

2) изграждане на международна справочна система за информация върху околната среда;

3) водене на международен регистър на потенциално опасните токсични вещества. Един от приоритетите на ЮНЕП е подпомагане на развиващите се държави в подготовка на техните национални законодателства в областта на околната среда.

Общото събрание на Организацията на обединените нации, наричано също Генерална асамблея на ООН, е най-важният от 6-те ръководни органа на ООН и единственият, в който всички страни-членки на организацията имат еднакво представителство. Там се обсъждат на широко равнище проблемите на опазването на околната среда на световно равнище. Сред по-важните документи, които са приети в рамките на Общото събрание, се открояват:

1) Международна отговорност на държавите по отношение на околната среда (1972 г.);

2) За историческа отговорност на държавите за съхранение на природата на Земята за сегашното и бъдещите поколения (1980 г.);

3) Екологичната перспектива до 2000 г.;

4) Опазване на глобалния климат в интерес на сегашното и бъдещите поколения на човечеството (2008 г.).

Комисията по международно право. Като постижения в работата на Комисията по международно право в областта на околната среда през 2001 г. се считат подготвените проекти на разпоредби за предотвратяване на трансграничните вреди от опасните видове дейност. През 2006 г. пък се поставя акцент върху разпределянето на загубите, в случай на такива вреди, причинени в резултат на опасни видове дейност. Отново във връзка с опазване на околната среда е разразработен проект за използването на международните речни корита за цели, различни от тези на корабоплаването.

Специализирани международните организации, включени в системата на ООН, които развиват дейност по опазване на околната среда са:

– *Международна морска организация (ИМО)* със седалище Лондон. Постепенно се превръща във всепризната и компетентна международна организация занимаваща не само с въпроси по корабоплаване и безопасност по море, но и в областта на опазването на морската среда от замърсяване. По нейна инициатива са приети над 30 международноправни акта;

– *Световна здравна организация (СЗО)*. Седалище Женева. Организацията насърчава международното сътрудничество за опазване на човешкото здраве. Тази цел макар и непряко е свързана с опазването на околната среда. В рамките на организацията се извършват дългогодишни изследвания в областта на санитарно-хигиенните аспекти на замърсяването на околната среда и тяхното отражение върху човешкото здраве. Здравната организация събира, обобщава и разпространява информация по въпроси на здравеопазването и отражението на замърсяването на природата и нейните компоненти върху човешкото здраве;

– *Организация на обединените нации за образование и култура (ЮНЕСКО)*. Създадена след Втората световна война със седалище Париж. В началото на своята дейност не отделя внимание на екологичните проблеми. През 1968 г. под нейна егида се свиква междуправителствена конференция, на която да се обсъди състоянието на биосферата. В резултат се приема международна програма "Човек и биосфера", в която се включени 14 основни теми свързани главно с отрицателното въздействие на човешките дейности върху различните природни компоненти и със съхраняването на природните забележителности и генетичните ресурси. Значителен принос има и в разработването на международноправни актове, свързани с опазването на уникални екосистеми от общочовешко значение. Един от тях е Конвенцията за опазване на световното културно и природно наследство /1972г./, в която са включени над 300 уникални защитени територии на планетата, между които и три български – Сребърна, Пирин и Рила.

– *Програма на ООН за развитие (ПРООМ)* е специализирана организация със седалище Ню Йорк, чиято дейност е насочена към проблемите на икономиката и икономическото развитие. Внимание отделя на рационалното използване на природните ресурси и на тяхното опазване. Съуправител е на Глобалния фонд по околна среда, каквато е и ЮНЕП. Експерти от програмата оказват ценна юридическа помощ в началото на 1990 г. на България при разработването на проект на специален закон за опазване на морската среда от замърсяване, както и при изготвяне на споразумения с големи нефтени компании, проучващи и разработващи находища на нефт и газ в континенталния шелф на България в Черно море.

– *Международна агенция за атомна енергия;*

– *Световната метеорологична организация;*

– *Организацията за прехрана и земеделия към ООН (ФАО);*

– *Международната организация за гражданска авиация (ИКАО).*

Основни институции в Европейския съюз са:

1) Комисията към ЕС е изпълнителен органи и е отговорна за въвеждането мониторинга, контролът и прилагането на законите и политиката на ЕС. Към тази комисия функционира Дирекцията по околна среда, която отговаря и за ядрената безопасност и защитата на гражданското общество. Тази дирекция осъществява екополитиката и контролира спазването на екологичното законодателство;

2) Съветът на министрите е главният законодателен орган на ЕС, включително и в екологичната област, и представя интересите на страните-членки. Той се състои от министрите, кои-

то отговарят за околната среда в съответните страни членки;

3) Европейският Парламент представя интересите на гражданите на ЕС, има право на законодателна инициатива. Той има право да одобрява бюджет, да избира или да разпуска Комисията. Парламентът заседава веднъж месечно, като заседанията са открити за обществеността.

Европейският парламент играе важна роля при формулирането на законодателството на ЕС в областта на околната среда. По време на осмия парламентарен мандат той работи по законодателство, произтичащо от плана за действие за кръгова икономика (относно отпадъците, батериите, излезлите от употреба превозни средства, депонирането и др.), въпроси във връзка с изменението на климата (ратификация на Парижкото споразумение, разпределяне на усилията, отчитане на земеползването, промени в земеползването и горското стопанство в ангажиментите за борба с изменението на климата на Съюза, реформа на Схемата за търговия с емисии и др.) и още много други.

Парламентът няколкократно призна необходимостта от подобрено изпълнение, което да бъде основен приоритет. В резолюция от 2013 г., озаглавена „Подобряването на резултатите от мерките на ЕС в областта на околната среда: изграждане на доверие чрез повишаване на познанията и готовността за реакция", той разкритикува незадоволителната степен на изпълнение на законодателството в областта на околната среда от страна на държавите членки и отправи няколко препоръки за по-ефикасно изпълнение, например чрез разпространението на най-добри практики между държавите членки и между регионалните и местните органи. В своята позиция относно настоящата програма за действие за околната среда Парламентът подчерта също необходимостта от по-строго прилагане на законодателството на ЕС в областта на околната среда. Освен това призова за по-голяма сигурност на инвестициите в подкрепа на политиката в областта на околната среда и за усилия за борба с изменението на климата, както и за отчитане в по-голяма степен и по-добре на въпросите, свързани с околната среда, в другите политики.

4) Европейският съд е гарант на закона в ЕС. След 1997 г. по предложение на Комисията той взема отношение по процедури свързани с нарушаване на екологичното законодателство. Някои решения, които взема са основни и може да ограничава правата на страните членки за тяхното вътрешно законодателство.

Основни агенции в Европейския съюз са:

1) Европейската агенция за околната среда (ЕАОС);

Европейската агенция за околната среда е създадена през 1994 г. Тя е органът на Европейския съюз, създаден да предоставя навременна, целенасочена, подходяща и достоверна информация за околната среда както на лицата, определящи политиката в тази област, така и на обществеността. ЕАОС не разработва нормативни документи и не определя политиката в областта на околната среда. Мандатът на ЕАОС е:

– да подпомага Общността и страните-членки да взимат на информирани решения за подобряване на околната среда, да интегрират въпросите, свързани с околната среда, в икономическата политика и да работят за устойчиво развитие;

– да координира Европейската мрежа за информация и наблюдение на околната среда (*Eionet*).

Регламентът[33] за създаване на ЕАОС е приет от Европейския съюз през 1990 г. Той влиза в сила в края на 1993 г. веднага, след като е взето решение седалището на ЕАОС да бъде в Копенхаген. Същинската си дейност Агенцията започва през 1994 г. С този регламент е създадена и Европейската мрежа за информация и наблюдение на околната среда (Eionet).

Понастоящем ЕАОС има 32 страни-членки и шест сътрудничещи страни. Европейската мрежа за информация и наблюдение на околната среда е партньорска мрежа на ЕАОС и страните. EIONET е информационен "възел", акумулиращ, обработващ и предоставящ екологична информация от широка мрежа източници, изградена в страните-членки на Агенцията. Мрежата събира

[33] Регламент (ЕИО) № 1210/90 на Съвета от 7 май 1990 г. за създаване на Европейска агенция за околната среда и Европейска мрежа за информация и наблюдение на околната среда

и обработва информация от националните мониторингови системи чрез Европейските тематични центрове (ЕТЦ).

ЕАОС отговаря за развитието на мрежата и координирането на нейните дейности. За целта Агенцията работи в тясно сътрудничество с националните координатори, които обикновено са националните агенции за околна среда или министерствата на околната среда. Те отговарят за координирането на националните мрежи, обхващащи много институции (общо около 300).

Основни клиенти са институциите на Европейския съюз – Европейската комисия, Европейският парламент, Съветът - и страните-членки. В допълнение към тази централна група от участници в европейската политика. Агенцията обслужва и други институции на ЕС като Икономическия и социален комитет и Комитета на регионите.

Деловите и академичните кръгове, неправителствените организации и други компоненти на гражданското общество са също активни потребители на информацията на ЕАОС.

За целта агенцията си сътрудничи тясно с националните координатори в участващите страни, както и с други национални органи (агенции за опазване на околната среда, министерства и др.), които отговарят за координацията на дейностите на Eionet на своя територия.

Във връзка със събирането, управлението и анализа на данни ЕАОС е създала и поддържа европейски тематични центрове, работещи по важни въпроси в областта на околната среда. Тези центрове също така са мрежи, обхващащи около 90 специализирани институции в цяла Европа.

Как функционира: ЕАОС организира дейностите си чрез годишни работни програми, които са част от 5-годишни работни програми. Настоящата програма е за периода 2014 – 2018 г. и е организирана около 4 основни теми:

– предоставяне на информация във връзка с изпълнението на политиките – обратна информация и принос към рамките и целите на политиките на ЕС чрез непрекъснато докладване за напредъка по ключови въпроси, свързани с околната среда;

– оценка на системните предизвикателства – в макро-, междусекторен и дългосрочен аспект с цел подпомагане на програмата за действие за околната среда;

– съвместно създаване и използване на знания – изграждане и поддържане на мрежи от хора и информационни системи;

– непрекъснато подобряване на ефикасността и ефективността.

Агенцията има следните основни задачи:

– да събира, обработва и анализира данни, за да осигури на ЕС обективна информация, необходима за прилагането на ефективни политики за околната среда;

– да подпомага мониторинга на мерките;

– да съпоставя, оценява и разпространява данни относно състоянието на околната среда сред широката общественост;

– да осигурява сравнимост на данните за околната среда на европейско равнище;

– да насърчава включването на информацията на ЕС за околната среда в международните програми за мониторинг на околната среда, като тези на Организацията на обединените нации;

– да насърчава разработването на методи за оценяване на вредите, нанесени на околната среда, както и за определяне на стойността на политиките за околната среда, свързани с предотвратяването, опазването и възстановяването;

– да насърчава обмена на информация за най-добрите налични технологии за предотвратяване или намаляване на вредите за околната среда;

– да публикува доклад за състоянието, тенденциите и перспективите за околната среда на всеки пет години.

Обхванатите данни включват:

– качество на въздуха и шумово замърсяване;

– качество на водата;

– състояние на почвите, на фауната и флората;

– земеползване и природни ресурси;

– управление на отпадъците;

– химически вещества;

– опазване на крайбрежието и морето;

– изменение на климата и адаптиране към изменението на климата.

Управителният съвет на ЕАОС е съставен от по един представител от всяка държава от ЕС, двама представители на Европейската комисия и двама учени, определени от Европейския парламент. Изпълнителен директор, който отговаря за ежедневното управление.

ЕАОС си сътрудничи с останалите органи на ЕС и международни органи, като Статистическата служба на ЕС (*Eurostat*) и Съвместния изследователски център на Европейската комисия, програмата за околна среда на ООН и Световната здравна организация.

2) Европейската мрежа за информация и наблюдение на околната среда (*Eionet****).*** Тя има за цел да предоставя навременни с осигурено качество данни, информация и експертни знания за оценяване на състоянието на околната среда в Европа и въздействията, на който е подложена. Това улеснява лицата и органите, разработващи политики, при вземането на решения относно подходящи мерки за защита на околната среда на национално и европейско равнище и при осъществяването на контрол върху ефективността на съществуващите политики и мерки.

Eionet е партньорска мрежа на ЕАОС и нейните страни-членки и сътрудничещи страни. Координира се от информационната мрежа на ЕС относно въпроси, свързани с околната среда. Мрежата разполага с представители от всички държави от ЕС, както и от Исландия, Лихтенщайн, Норвегия, Швейцария и Турция.

Амбицията на ЕАОС е да продължи да бъде водещ доставчик на основната информация, необходима за повишаване на ефективността на политиката в областта на околната среда. Наред с това ЕАОС се стреми да участва в създаването на нови данни и знания, които ще бъдат необходими за обосноваването и осъществяването на основополагащия преход към постигане на дългосрочна устойчивост на нашите общества.

3) Европейска агенция по химикалите *(ECHA)*

Регламентът относно REACH (регистрацията, оценката, разрешаването и ограничаването на химикали) предоставя задълбочена законодателна рамка за производството и използването на химикали в Европа се прилага от 01 юни 2007 г.. Той прехвърля от обществените органи към индустрията отговорността да се гарантира, че произвежданите, внасяните и продаваните в ЕС химикали са безопасни. Освен това той:

– насърчава алтернативни методи за изпитване върху животни;

– създава единен пазар за химикали;

– цели да насърчи иновациите и конкурентоспособността в сектора;

– създава Европейска агенция по химикалите (ECHA).

Основни аспекти:

– законодателството се прилага за всички химични вещества: произведени, внесени, продавани, използвани самостоятелно, в смеси или в продукти. Много от тях срещаме в своето ежедневие, като например продукти за почистване, бои или в електрически уреди;

– дружествата трябва да регистрират в централна база данни всички химикали, които те произвеждат или внасят в количества от един тон или повече за година. ECHA трябва да провери информацията, подадена при регистрацията;

– дружествата трябва да идентифицират и управляват рисковете, свързани с веществата, които произвеждат и продават в ЕС. Те трябва да демонстрират как продуктите им да се използват безопасно и да информират потребителите за всички мерки за управление на риска, които те трябва да прилагат, за да гарантират безопасно използване по цялата верига на доставка;

– националните органи могат да ограничат производството или използването на определени вещества, ако счетат, че рисковете не се управляват адекватно;

– законодателството има за цел да замени най-опасните вещества с по-безопасни алтернативи, когато такива са налични;

– законодателството не се прилага за определени групи вещества (например радиоактивни вещества или такива под митнически надзор) или за отпадъци, тъй като те вече са регулирани

подробно в друго законодателство.

През 2013 г. Европейската комисия извърши оценка на първите пет години от Регламента относно REACH и направи заключение, че не се изисква значителна преработка преди 1 юни 2018 г. – краен срок за регистриране на определени вещества.

Научен комитет по безопасност на потребителите (НКБП) и **Научен комитет по здравни, екологични и възникващи рискове** (НКЗЕВР) на ЕС – те предоставят на Европейската комисия научни съвети и оценки на рисковете в тези области. *Ролята на комитетите е:*

– да предоставят научни становища относно оценката на рисковете в случаите, определени в законодателството на ЕС;

– да предоставят при поискване научни съвети на Комисията по въпроси, които са от особено значение за рисковете за общественото здраве, безопасността на потребителите и околната среда;

– да определят по покана нуждите от научни изследвания за попълване на пропуските от важна информация, да оценяват предлаганите бъдещи научни изследвания и да оценяват резултатите от научните изследвания в тематичните области от своята сфера на компетентност;

– да предоставят бързи съвети относно научните познания във връзка с конкретни рискове в случай на спешна необходимост;

– да участват в тематични мрежи или мероприятия с други органи или научни организации на ЕС, за да следят и допринасят за научните познания в своята сфера на компетентност;

– да насочват вниманието на Комисията и нейните служби посредством меморандуми или изявления към конкретен или възникващ проблем, който комитетите считат, че може да създаде реален или потенциален риск за безопасността на потребителите, общественото здраве или околната среда;

– да приемат своята методология за извършване и предоставяне на оценка на риска и за преразглеждането ѝ с оглед на отчитане на всички значими научни фактори, както и да гарантират, че тя отразява текущата практика на оценяване на рисковете.

Мандат:

– членовете на комитетите се назначават за 5-годишен мандат;

– те остават на поста си, докато не бъдат заместени или преназначени.

Независимост:

– членовете и външните експерти трябва да действат независимо и в името на обществения интерес;

– членовете се назначават лично; те не могат да делегират своите отговорности на друго лице;

– преди назначаването си и след това всяка година те трябва да представят декларация за конфликт на интереси;

– членовете и външните експерти трябва да заявят при всяко заседание всеки конкретен интерес, който може да е в ущърб на тяхната независимост по отношение на въпросите от дневния ред.

Прозрачност:

– всички съответни документи, като дневен ред, протоколи и становища и декларации на участниците, трябва да се публикуват на специален уебсайт.

– на този уебсайт трябва да има връзка към регистъра на експертните групи.

Неправителствени организации (НПО).

Първите НПО се появяват още в края на XIX-ти век. Това са по-скоро сдружения на любители на природата и на учени от различни държави за изучаване на флората и фауната в определени райони на планетата. Започва създаването на международни центрове и научни асоциации, занимаващи се с изследва и опазване на природата и нейните компоненти. Те са изразители на изостреното критично отношение на обществото към тежкото екологично състояние в много райони на света. Като доказали се и утвърдени в публичното пространство са:

– *Световен съюз за съхраняване на природата и нейните ресурси;*

– Гринпийс;

– Приятели на земята;

– Международен зален кръст и др.

Зелените 10 (The Green 10) е неформална платформа, обединяваща 10 от най-големите екологични неправителствени организации и мрежи, действащи в рамките на Европейския съюз. Платформата има за цел да координира съвместните отговори и препоръки на членуващите организации и мрежи към отговорните лица и органи на Европейския съюз и да гарантира централната позиция на проблеми, засягащи околната среда, в процеса на вземане на решения в Европейския съюз. Броят на индивидуалните членове в платформата е над 20 милиона (индивидуални членове на организациите и мрежите, членуващи в The Green 10).

Организации и мрежи, членуващи в The Green 10:

1. Банкуоч Централна и Източна Европа – CEE Bank watch
2. Бърдлайф – Birdlife international (European community office)
3. Грийнпийс – Greenpeace
4. Европейска федерация за транспорт и околна среда – European Federation for Transport and Environment (T&E)
5. Европейско бюро за околна среда – European Environmental Bureau (EEB)
6. Мрежа за действие по климата – The Climate Action Network Europe (CAN Europe)
7. Приятели на земята – Friends of the Earth Europe (FoEE)
8. Приятели на природата – International Friends of nature (IFN)
9. Световен фонд за природата – World Wide Fund for Nature (European policy office) (WWF)
10. Съюз за здравеопазване и околна среда – Health and Environment Alliance (HEAL)

Силата на Зелените 10 е в мрежите и организациите, обединени от платформата. Европейските екологични неправителствени организации изпращат редовно информация до своите членове и поддръжници, което е от съществено значение за високата степен на информираност на тези групи относно развитията на ниво на Европейския съюз. Благодарение на това членовете и поддръжниците на мрежите и организациите могат да вземат ефективно участие и да дадат своя принос към процеса на вземане на решения, свързани с опазването на околната среда.

Платформата се опитва да спазва колкото се може по-демократичен принцип на вземане на решения, като се вземат под внимание мнението и отношението на организациите членки, техният екип, борд и членове.

Целите на платформата са:

– подкрепа на пълното прилагане на европейските екологични закони и политика във всички страни-членки на Европейския съюз.

– лобиране за нови екологични предложения за политиката и законите.

– работа с институциите на Европейския съюз с цел постигане на максимална степен на ефективност на европейските екологични закони и политика.

– популяризиране на лидерството по екологични въпроси на Европейския съюз на световната политическа сцена.

– във връзка с увеличаване на обществената осведоменост организациите, членове на платформата:

– информират своите членове и по-широката общественост относно последните развития в областта на околната среда в рамките на Европейския съюз и ги окуражават да изразят своето мнение и позиция;

– предоставят възможност за изразяване интересите на хиляди местни асоциации на ниво на лицата, отговорни за вземане на решения, касаещи политиката на Европейския съюз;

– допринасят за засилване на гражданското общество в Европа чрез тренинги, политически анализи и др.

Институционалната рамка на политиката за опазване на околната среда в Р. България обхваща всички структури, имащи отношение към националната стратегия за устойчиво развитие:

1) Министерство на околната среда и водите (МОСВ) осъществява дейността си чрез законодателна инициатива, планиране, управление, изпълнителна, регулаторна и контролна функции. МОСВ отговаря за: развитието и прилагането на националната политика в екологичния сектор; подготовката на правната и нормативната уредба в областите на различните компоненти на околната среда, управление на отпадъците, защита на природата и управление на защитените територии и др.;

2) Изпълнителна агенция по околната среда (ИАОС) е администрация към Министъра на околната среда и водите за осъществяване на ръководни, координиращи и информационни функции по отношение на контрола и опазването на околната среда в България. Агенцията е Национален координационен център към Европейската агенция по околна среда (ЕАОС). Тя е член и на Мрежата на директорите на агенции по опазване на околната среда (EPA Network).

3) Органи на следващото, по-ниско ниво са ***регионалните органи на МОСВ*** и те са:

– Регионалните инспекции по околната среда и водите,

– Басейновите дирекции за управление на водните ресурси,

– Дирекциите на националните паркове, които провеждат държавната политика за съответните райони и територии.

4) ***Други институции***, имащи отношение към екологичната политика и устойчивото развитие са: *Министерство на здравеопазването, Министерство на земеделието и храните, Министерство на регионалното развитие и благоустройството, Министерство на транспорта, Националната агенция по енергийна ефективност* и др., както и областните и общински съвети и органите за местно самоуправление, както неправителствените организации и научните институти.

ЕС е главно действащо лице в международните преговори във връзка с околната среда. Той е страна по множество споразумения в областта на околната среда от световен, регионален или подрегионален мащаб по широк кръг от въпроси като опазването на природата и на биологичното разнообразие, изменението на климата и трансграничното замърсяване на въздуха или водата. На Десетата конференция на страните по Конвенцията за биологично разнообразие, която се състоя в Нагоя (Япония) през 2010 г., ЕС допринесе съществено за постигането на споразумение относно глобална стратегия за спиране на загубата на биологично разнообразие до 2020 г. Съюзът подпомогна също така оформянето на няколко важни международни споразумения през 2015 г. на равнището на ООН, като Програмата до 2030 г. за устойчиво развитие (която включва 17-те цели за устойчиво развитие и 169 подцели), Парижкото споразумение относно изменението на климата и Рамковата програма от Сендай за намаляване на риска от бедствия. През същата година ЕС стана също така страна по Конвенцията по международната търговия със застрашени видове от дивата фауна и флора (CITES).

References:

1. Светослав Велев, учебник Екологична сигурност, Военна академия „Георги Стойков Раковски, 2015, ISBN 978-954-9348-73-6.

2. Анна И. Мантарова, автореферат, Екологични рискове в трансформиращото се общество, Институт за изследване на обществата и знанието, БАН, София, 2014 г.

3. Борислав Боянов, Еволюционно развитие на европейската екологична политика, Стопанска академия „Димитър А. Ценов“ гр. Свищов 2017 г., https://dlib.uni-svishtov.bg /bitstream /handle/10610/3985/759cd03f7189e50ff26a2b6a2ec677db.pdf?sequence=1&isAllowed=y

4. Регламент (ЕИО) № 1210/90 на Съвета от 7 май 1990 г. за създаване на Европейска агенция за околната среда и Европейска мрежа за информация и наблюдение на околната среда

5. Справочник „Европейски платформи от екологични неправителствени организации“, Институт Отворено общество, София, 2008 г.

6. Жан Шарпантие, Международните организации, 16-то издание, превод: Зорница Грекова, София, 2008 г.

7. Стефка Наумова, Европейската екологична политика и предизвикателствата пред сигур-

ността, научни трудове на Русенския университет, 2013, том 52, серия 7.

8. Карлен Атанесян,От Стокхолм до Копенхаген – обзор на значими международни конференции на ООН по околната среда, https://ejournal.vfu.bg/bg/pdfs/Karlen_Atanesyan-Ot_Stokholm_do_Kopenhagen-Obzir_na_znachimi_mejdunarodni_konferencii_na_OON_po_okolnata_sreda.pdf

9. Политиките на Европейския съюз „Околна среда“, Здравословна и устойчива околна среда за днешното и бъдещите поколения, Европейски съюз 2015 г., ISBN 978-92-79-42628-5

10. Георги В. Камарашев, Евакуация от райони и обекти. Университетско издание: НВУ „Васил Левски“. Велико Търново, 2014.

11. Георги В. Камарашев, Outsourcing as a part of the management of resources for security and defense, Велико Търново 2011 г.

12. Околна среда, https://europa.eu/european-union/topics/environment_bg

Mariyana St. Todorova,

ECOLOGICAL MIGRATION

Mariyana St. Todorova

Faculty of "Artillery, air defense and CIS" –National Military University "Vasil Levski", Veliko Tarnovo, the Bulgarian Republic E-mail: stilianova70@abv.bg

***Abstract**: Ecological migration, despite the fact that it has deep historical roots, has recently become the subject of research by representatives of various sciences and, accordingly, has not been sufficiently studied both in the world and in Bulgaria. Improving the mechanism needed to adapt migrants to the new human security environment is needed in the event of a sharp deterioration of the environmental situation*

***Keywords**: Ecological migration, security*

ЕКОЛОГИЧНА МИГРАЦИЯ

Марияна Ст. Тодорова

Факултет"Артилерия, ПВО и КИС" – Национален Военен Университет"Васил Левски", Велико Търново, Република България, stilianova70@abv.bg

1. Въведение

Екологичната миграция представя екологичната обстановка и заема важно място за сигурността на човека. Неговите жизненоважни интереси могат да бъдат решени само чрез усъвършенстване на правото на безопасна и благоприятна околната среда, както с принудително или доброволно преместване - в район с по-благоприятни условия на живот.

През последните години околната среда като фактор за миграцията е в центъра на международни дебати относно дефиниции, данни, ситуации и политики за екологичните мигранти[6].

Тези анализи показват как екологичните фактори са в основата на всички останали. Това става ясно, ако направим разлика между двете главни категории съгласно текстове в справочниците: от една страна внезапните резки екологични събития, а от другата - бавните и постепенни климатични процеси.

Данните относно първия вид екологична миграция се намират лесно, но възможността за надеждни прогнози е силно ограничена. Определянето на втората категория е по-трудно, защото причините за нея често пъти са постепенни и „безшумни". Но последствията от измененията на климата върху условията на живот на човека са също така крайни, както последствията от природните бедствия.

Някои зони на света са климатични „горещи точки", като там измененията на климата ускоряват влошаването на околната среда.

Като се имат предвид причините, поради които хората напускат домовете си, можем да заключим, че миграцията в околната среда е по-широко понятие. Делът на мигрантите, напускащи обичайното си място на пребиваване, се увеличава поради постепенното влошаване на екологичната, санитарната и епидемиологичната обстановка, промените в климатичните условия, местообитанията и др.

Обобщавайки горното е видно,че за разнообразието от видове миграция на населението, свързано с влошаването на околната среда се задълбочава. Екологични мигранти, като правило са тази категория хора означава „хора, които са принудени внезапно или неочаквано да избягат от домовете си в голям брой в резултат на природни или причинени от човека бедствия“ [7]

2. Изложение

Най-общоприетото определение на концепцията за екологична миграция, посочено от различни автори, е прието през 1996 г. на конференция в Женева. Според него „екологичните мигранти са лица, които са принудени да напуснат мястото си за постоянно пребиваване и които се придвижват в рамките на своята държава или преминават границата поради рязко влошаване на околната среда или екологични бедствия“ [5].

Доклад за глобалните бедствия, изготвен от Международния червен кръст през 1999 г., отбелязва, че сушата, наводненията и ерозията на почвата принуждават 25 милиона души да напуснат домовете си [9]. Резкият ръст на такива миграции в общия обем на миграционните процеси в света - броят на екологичните бежанци до 2050 г. според специалисти от Университета на ООН ще достигне 200 милиона души [10] — което предизвика голямо внимание за проблемите на миграцията в околната среда като особен вид разселване на населението, причинено от природни бедствия и катастрофи, както и технологични процеси.

Докладът на Глобалната комисия по международна миграция дава следното определение: екологични мигранти - хора, които са били принудени да се преселват поради екологични бедствия [2].

Необходимостта от бързо решение на проблемите на миграцията в околната среда, което се отнася конкретно до екологичните бежанци, бе установено от събралите се в Бон (Германия) на 11 октомври 2008 г. на първата международна конференция за миграцията, свързана със състоянието на околната среда. Срещата в Бон подчертава е да се разбере колко важен е факторът на екологичната миграция. Всъщност, докато екологичните бежанци, за разлика от политическите бежанци, нямат правен статут и съответно не могат да разчитат на никаква помощ [11]. Този проблем се разглежда и е решен на Конвенцията на ООН за статута на бежанците, или чрез разработване на специална конвенция за защита на мигрантите в околната среда [3].

Три ключови термина са важни в контекста на миграцията и околната среда и климатичните промени:

Екологичните мигранти се определят като „лица или групи от лица, които главно поради причини за внезапни или прогресивни промени в околната среда, които се отразяват неблагоприятно на техния живот или условия на живот, са длъжни да напуснат обичайните си домове или да изберат това, временно или постоянно и които се местят в своята страна или в чужбина. “[6].

Екологично разселеното лице се отнася до „лица, които са разселени в своята държава с обичайно местопребиваване или са преминали международна граница и за които деградацията, влошаването или унищожаването на околната среда е основна причина за тяхното разселване, макар и не непременно единствената“ [6]. Терминът „разселване при бедствия “ се отнася до ситуации, при които хората са принудени или задължени да напуснат домовете си или местата на обичайно пребиваване, по-специално в резултат на или с цел да се избегнат последиците от бедствия, предизвикани от природни опасности. Такова разместване може да бъде под формата на спонтанен полет или евакуация, разпоредена или наложена от органите. Такова разселване може да възникне в държава или през международни граници. ”

Планираното преместване се отнася до лица, чиито поминък е бил възстановен на друго място. Други определят планираното преместване като отнасящо се единствено до колективното движение на дадена общност, „постоянното (или дългосрочното) движение на общност (или на значителна част от нея) от едно място на друго, в което важни характеристики на оригинала общност, включително нейните социални структури, правни и политически системи, културни

характеристики и мирогледи се запазват: общността остава заедно на местоназначението в социална форма, подобна на общността на произход ”[6].

Въпреки че терминът „бежанци от климата“ често се използва във връзка с принудителна миграция в контекста на изменението на климата и околната среда, това не е юридически валиден термин, тъй като Конвенцията за бежанците от 1951 г. не признава факторите на околната среда като критерии за определяне на бежанец.

2.1 Видове екологична миграция

На конференцията в Бон за миграцията, свързана с околната среда през 2008 г., са разгледани следните категории мигранти:

- спешни мигранти в околната среда, които бягат от опасно въздействие върху околната среда, за да спасят живота си;
- принудени екологични мигранти, които напускат постоянното си местожителство, за да избегнат неизбежните и сериозни последици от влошаването на околната среда;
- екологично мотивирани мигранти, които са в състояние, включително финансово, да напуснат района на своето постоянно пребиваване с постоянно влошаваща се екологична ситуация, за да намерят по-добро място за пребиваване [8].

При класифицирането на всяко социално явление, включително миграцията в околната среда, за да се избегне объркване и неясност, е обичайно да се следва основният принцип на типологията - един критерий (основа).

Като се имат предвид причините, поради които мигрантите в околната среда променят местожителството си или мястото на пребиваване, могат да бъдат определени следните основания за екологична миграция:

2.1. Поради природни бедствия - земетресение, тайфун, ураган, наводнение, цунами и др. Например, като се имат предвид последиците от урагана "Катрина", който отне повече от хиляда животи през 2005 г., може да се отбележи, че повече от 800 хиляди души останали без електричество и телефонни комуникации, а един и половина милиони жители напуснали домовете си. Мнозина напуснали града завинаги .

2.2. Поради бедствие, причинено от човека, което не причини дългосрочни сериозни промени в околната среда (експлозии от обикновени експлозиви, пожари и др.).

2.3. Във връзка с индустриална катастрофа, която причини дългосрочно заразяване на района - радиационна, химическа, бактериологична. Най-нагледните примери са аварията в четвъртия енергоблок на атомната електроцентрала в Чернобил и трагедията в индийския град Бхопал, станали две години преди Чернобил, когато около 40 тона силно токсичен газ, метилизоцианат, са изтекли в инсталацията за пестициди. Повече от 500 души загинаха веднага от пряко излагане на газ, около 6 хиляди души получили сериозни химически щети, от които 2 хиляди души загинали през следващите няколко седмици. Броят на смъртните случаи през следващите 20 години варирали според различни оценки от 14 до 20 хиляди души[4].

2.4. Поради влошаването на екологичната екологична среда, причинено от нерационално управление на природата и лошо замислени човешки дейности (най-красноречивият пример е влошаването на екологичната ситуация в района на Аралско море поради безмислени политики за рекултивация на земята в региона, провеждани през съветската епоха).

Както при квалификацията на всеки тип миграция, екологичната миграция въз основа на географски признак може да бъде разделена на външна (международна) и вътрешна (вътрешна) миграция.

Към момента на пребиваването на мигранта на ново място на пребиваване са възможни два основни типа миграция в околната среда - постоянна (неотменима) и временна (завръщане).

Постоянната миграция в околната среда може да се дефинира като миграция с цел промяна на постоянното местопребиваване, свързано с невъзможността да останат в района на екологична

катастрофа по време на голямо екологично бедствие, причинявайки големи щети на екологичната ситуация и невъзможността да се върнат на предишното си място на пребиваване поради заплаха за живота и здравето поради дългосрочната стабилизация на околната среда или санитарно-епидемиологичната обстановка на земята или невъзможността за стабилизиране или нежелание за връщане оставка поради подобни опасения.

По подобен начин временната миграция в околната среда може да бъде определена като миграция с цел промяна на мястото на престой за периода на невъзможност да останат в района на екологичните бедствия поради заплаха за живота и здравето по време на голямо екологично бедствие.Временната миграция в околната среда може да бъде разделена на два класа - краткосрочна миграция (до 1 година извън обичайното им място на пребиваване) и дългосрочна миграция (повече1 година).

Според метода на включване екологичната миграцията може да бъде разделена на два вида: принудителна и доброволна.

- Принудителна екологична миграция е принудително преселване на хора, организирано или упълномощено от правителствени органи от зоната на природни или причинени от човека бедствия, което доведе до рязко влошаване на околната среда, правейки невъзможно хората да останат в зоната на бедствия в околната среда.Принудителна екологична миграция може да се представи, и като движението на хора, които напускат мястото си на пребиваване поради обосновани страхове от увреждане на здравето в резултат на екологична или технологична катастрофа или поради сериозна промяна в околната среда.
- Доброволна екологична миграция разбираме движението на хора, които напускат домовете си поради малки промени в условията на околната среда или климата.

Въз основа на гореизложеното екологична миграция може да бъде определена като движение на хора с цел промяна на тяхното постоянно местоживеене или място на престой, свързано с невъзможността или нежеланието да се намират в екологична катастрофа по време на природно или причинено от човека бедствие, промяна на екологичната, санитарно-епидемиологичната или климатичната ситуация и невъзможността да се върнат към екологична стабилизация.От друга старана санитарно-епидемиологична ситуация на предишното място на пребиваване, или място на престой поради заплаха за живота и увреждане на здравето, както нежелание да се върне в постоянното си местожителство поради тези опасения.

3. Заключение

Проучванията, организирани от Европейския парламент и Европейската комисия за миграции по екологични причини за използването на термини като „мигрант”, „бежанец” или „изселник”, може да доведат до много по-различни правни резултати и до признаване на различни видове права.

Въпросите по темата са многобройни, но основното е: създаването на “правна категория” за съгласие на определенията, което да не пречи на споразумение за причините и последиците, а оттам и как да се решава кой да бъде закрилян и кой не, кой да бъде одобряван и кой не. Това означава признаване на съществуващо явление и изисква намиране на правни решения

Международната организация за миграция (МОМ) дава своето определение за екологичен бежанец - това е човек, който е принуден да напусне местообитанието си поради резки или постепенни промени в околната среда**.**

Второ, необходимо е създаване на иновативен механизъм на адаптиране към новото общество с цел премахне чувството за миграция на мигрантите. Необходими са повече инвестиции за изграждане на инфраструктура, образование и обучение за подобряване на способността на мигрантите да се адаптират към новите работни места и последващо развитие на индустрията, за да създаде повече възможност за работа. Липсата на единна европейска политика за справяне с миграционната криза доведе до постепенно затваряне на границите на някои от държавите от ЕС.

Основната цел на мигрантите е струпването им в близост до района на определине държави включително и на българската граница.[1]

Очевидно, това е проблем, който трябва да бъде разгледан в рамките на глобални форуми за миграцията и развитието поради съществуващата връзка между миграция и устойчиво развитие. Трябва да се създаде възмогност за адаптация, развитие, намаляване на риска от бедствия, гражданска защита, околната среда и изменението на климата, хуманитарната помощ и правата на човека.Това трябва да баде приоритет на държави, съставени от правителства, международни и неправителствени организации и академичните среди, като всички се стремят да засилят сътрудничеството между заинтересованите страни и да се разработят насоки между държавите за планирано преместване.

References

1. Атанасов А. Миграционни потоци – източник на рискове и заплахи за националната сигурност, *II International scientific conference10 to 13 December, 2018 at the Borovets winter resort, Bulgaria,Vol*.1 ISSN (print) 2603-2945, ISSN (online) 2603-2953 year 2, ISSUE 1(3),стр. Dec. 2018.
2. Доклад на Глобалната комисия за международна миграция -2000, 2006.
3. Международна конференция за околната среда, насилствената миграция и социалната уязвимост(EFMSV), 9-11октомври 2008г., Бон, Германия. http://www.efmsv2008.org
4. Окунев А. *Аварията в атомната централа в Чернобил заема 11-то място сред технологичните бедствия на 20 век* , Атомната стратегия. 2006, стр. 22.
5. Регионална конференция по въпросите на бежанците, неволно разселените лица, други форми на неволно разселване и завръщащи се в страните от съответните съседни държави: Женева, 30 - 31 май 1996 г.
6. Речник за миграцията , 2-ро издание. Международен закон за миграцията № 25, МОМ, Женева.2013, достъпно на http://publications.iom.int/bookstore/index.php
7. Goodwin Gill G.S. *Статут на бежанци в международното право*,1997. С. 315.
8. http://www.efmsv2008.org.
9. http://news.bbc.co.uk.
10. http://publications.iom.int/bookstore/f ree/MECC_Outlook.pdf .
11. http: // www.rfi.fr.

Valya M. Simeonova,

COMMUNICATION STYLES IN THE MILITARY ORGANIZATION

Valya M. Simeonova

valiasimeonova_sweet@abv.bg

СТИЛОВЕ НА КОМУНИКАЦИЯ ВЪВ ВОЕННАТА ОРГАНИЗАЦИЯ

Валя М. Симеонова

valiasimeonova_sweet@abv.bg

Abstract: *Thestyle of communicationisanindividual, stableform of communicativebehavior of theperson, manifestedindifferentconditions of interaction - inbusinessandpersonalrelations, intheleadership of people, intheways of makingdecisions. Thereportdiscussesdifferentstyles of communication, theirgoalsandmeaning, andthenature, typesandfunctions of communication.*

Key words*: militaryorganization, communication, style of communication*

Комуникация - същност, видове, функции

Комуникацията е важна функция за всяка организация. Тя е сложен и непрекъснат процес, който се осъществява в динамична и непрекъснато променяща се среда.

Вътрешните комуникации са двустранна дейност, насочена към обмен на информация между служителите и структурните звена в организацията. [1] Чрез тях се насърчава и координира сътрудничеството между служителите и отделите. В зависимост от посоката на движение на информацията комуникацията бива:

- Низходяща - тя протича от по-високите равнища към по-ниските в организацията. Най-честите форми са: инструкции за работа, официални бележки и др.
- Възходяща - протича от низшите към висшите нива на управление. Необходима е за вземане на решения. Информацията отразява резултатите от изпълнението, причините за конфликти, предложения, оплаквания и др.
- Хоризонтална - ефективната организация се нуждае от хоризонтална комуникация. Причините са некомпетентността на служителите по отношение на другите функции и дейности. В резултат на това се препятстват стратегическото управление, планирането и координацията.
- Диагонална - налице е, когато служителите не могат да комуникират помежду си по друг начин.

Комуникацията във военната организация се реализира едновременно на двете равнища на социалната комуникация: междуличностно и организационно.

На междуличностно равнище комуникацията е силно повлияна от индивидуалните особености на комуникаторите, от възрастта, пола и субективността на възприятието между комуникиращите партньори. Привличането и междуличностната съвместимост играят важна роля за създаването и протичането на контактите. Комуникативната компетентност и познавателното развитие на общуващите определят до голяма степен качеството и характера на контактите.

На организационно равнище комуникацията във военната организация се влияе от организационната структура на институцията, съществуващите дирекции, отдели, сектори и йерархич-

ните връзки между тях. Определящи за характера на комуникацията са социалният статус и задълженията на комуникиращите и свързаната с тях йерархична зависимост.

Стилът на комуникация се влияе не само от организационната структура, но и от ценностите, традициите и ритуалите, трайно установени във военната организация.

Според Мерман [3] всеки комуникационен процес включва в себе си съдържателен компонент и компонент на взаимоотношение. С помощта на съдържателния компонент хората предават информация, данни и факти. Компонентът на взаимоотношението съдържа в себе си междуличностните връзки на този, който изпраща съобщението и на този, който го получава.

Основните функции на вътрешните комуникации са:

1. Информативна – работниците в организацията, както и техните мениджъри изискват сериозен обем информация, за да работят ефективно, да вземат решения и да управляват възникналите конфликти. Чрез системата за вътрешна комуникация се осигурява информация, засягаща правилата в компанията, политиката и програмите, условията и безопасността на труда, образователни програми и други социални дейности.
2. Регулативна – мениджмънтът контролира предаваната информация. Регулативните съобщения са най-често насочени към работниците, съсредоточавайки се върху задачите, които трябва да бъдат изпълнени при конкретната работа.
3. Убеждаваща – при управлението на организацията мениджърите бързо откриват, че властта и силата не винаги предизвикват желания контрол. Те често управляват чрез убеждаване, което се прилага на всяко ниво в организацията.
4. Интегрираща – интегриращите процеси служат, за да очертаят границите на организацията, да включат онези личности и дейности, които допринасят за нейните цели и да изключат онези, които не го правят. Строежът на организационната структура – отделите за предаване на информация и властта, разделянето на отговорностите, е в основата на интегриращата функция.

Фундаменталната цел на вътрешните комуникации е постигането на възможно най-добри отношения вътре в организацията. Тази цел е съставена от няколко компонента.

1. Ефективна работа на персонала – всеки член на организацията да е наясно с работата си, критериите за оценяването й и възможностите за подобряването й.
2. Усъвършенстване на управлението – постигане на оптимална информираност на персонала, за да работи качествено.
3. Ясна обратна връзка – необходима е на мениджмънта, за да е в течение на преценките за дейността на организацията, формиращи се както сред персонала, така и сред публиките, с които персоналът е в непосредствен контакт.
4. Мотивация – създава се въз основа на съзнанието за участие, макар и не пряко, в процесите на формиране на управленските решения, от една страна, и от друга – в действащите механизми за професионално усъвършенстване.
5. „Екипен дух” – чувството и съзнанието на отделните индивидуалности, че са част от екип, работещ за постигането на обща цел.
6. Участващ персонал – модел на поведение, който се постига чрез механизми на въвличане на персонала от всички нива при изграждане на организационната политика и философия.
7. Готовност за кризисни ситуации – постига се не само чрез специално разработвани и прилагани програми за превантивен кризисен мениджмънт, но и чрез изграждането на качествено действащи вътрешноорганизационни комуникации.

Стилове на комуникация

В различните професионални области се описват и типични стилове на комуникация, които представляват обобщени поведенчески стратегии в комуникативен контекст. Стиловете на комуникация в синтезиран вид откроява повторяемото, често наблюдавано поведение в ситуации на комуникация. Те показват преобладаващи тенденции на поведението и разкриват доминиращи характеристики на личността по отношение на начина обмен на информация и поддържане на връзки и отношения с други хора.

Според Куницына [2] стилът на общуване е индивидуална, стабилна форма на комуникативно поведение на човека, проявяваща се в различни условия на взаимодействие - в деловите и личните отношения, в ръководството на хора, в начините на вземане на решения, в подбора на похвати за психологическо влияние на хората, методите за разрешаване на междуличностни и делови конфликти.

Разнообразието от класификации на стилове на комуникация се дължи на различните критерии, на основата на които се диференцират чертите на комуникативното поведение. Например на базата на признака нагласи към партньора в процеса на комуникация се говори за два стила - партньорски и непартньорски. Те се проявяват както в междуличностните отношения, така и в деловата среда - в отношенията между ръководител и подчинен и други професионални взаимодействия. Партньорският стил на комуникация се характеризира с висока степен на сътрудничество, с позитивно, нестереотипно възприемане на събеседника и с бързо скъсяване на дистанцията. Доверието към партньора е един от белезите на комуникатора, склонен към сътрудничество. Той умее да изслушва внимателно, не дава оценки на личността на събеседника, а се придържа към темата и чрез своята искреност предразполага към себеразкриване. За непартньорския стил на комуникация е типично напрежението, недоверието и повишената критичност между комуникиращите. Комуникаторът често пренебрегва гледната точка на събеседника, прекъсва го, дава оценки, може да стигне и до нападки.

Сътрудничеството в процеса на комуникация може да бъде анализирано и от гледна точка на активността за постигане на целите и степента на себеутвърждаване в комуникацията. Тези особености на индивидуалното поведение определят три други стила на комуникация. - асертивен, агресивен и пасивен. Асертивният стил на поведение в процеса на комуникация се характеризира със способност да се изразяват открито собствените чувства и мнения по директен начин, да се защитават собствените интереси, без да се наранява другите участници в комуникацията. Асертивността е умение да се демонстрира себеуважение и уважение към другите. Асертивната комуникация не означава безконфликтно или идеализирано взаимодействие. Несъгласието с чуждата гледна точка се изразява ясно и директно, чрез конструктивно противопоставяне, което изключва нападането, унижаването на достойнството на другите или отричането на техните възможности да действат по различен начин. Асертивният комуникатор е активен в постигането на целите си, без да доминира и да се разпорежда с другите.

Агресивният стил на комуникация също е свързан с висока активност в комуникационния процес, но тази активност се проявява като доминиране, насилие, обиждане или унижаване на другите. В преследване на своите цели агресивният комуникатор е единствено важен. Чуждите гледна точка, чувства и преживявания се пренебрегват, за да се защитят собствените интереси и права.

При пасивния стил на комуникация е налице слаба активност, за да се избягнат евентуални конфликти или противопоставяне, което би могло да усложни взаимоотношенията. В името на съхраняването на отношенията пасивният комуникатор е склонен да пренебрегне своите интереси и желания, да направи неща, в които не е убеден вътрешно, само за да подчертае повисоката значимост на другите и да бъде в тяхна полза. Пасивният стил на комуникация се базира на подценяването на себе си, на неувереността в своите силни страни и на нерешителността за действие в различните ситуации.

Характерът на ситуацията се оказва водещ фактор при анализа на комуникативните стилове, демонстрирани в деловото общуване в професионален контекст. Някои изследователи разграничават стилове на комуникативно поведение в зависимост от това, дали става дума за съвместна дейност в професионална среда, тъй като се предполага, че особеностите на професионалната дейност, професионалните умения и навици оказват влияние върху индивидуалното поведение. Разграничени са три стила на комуникация [2]:

1. Гъвкав - характеризира се с бърза ориентация в ситуацията, разбиране на подтекста на комуникацията, умение да се регулира собственото емоционално състояние;

2. Ригиден - недостатъчно се анализира и разбира собственото поведение и поведението на партньора в комуникацията, избират се неадекватни изразни средства, неефективно се осъществява контрол на поведението, възприятието е стереотипно;

3. Междинен - заемащ средно, преходно място между двата други стила - гъвкавия и ригидния.

Много популярна класификация на стиловете на лидерство на Курт Левин, която разграничава три стила - авторитарен, демократичен и либерален, се пренася и при описанието на стиловете на комуникация. Трите лидерски стила се операционализират на основата на сравнението им по три основни показателя: власт и отговорност; разпределение на задачите и осъществяване на комуникационния процес. [5] Приема се, че стилът на комуникация отразява характера на отношенията между началници и подчинени. Демократичният стил е свързан с приложение на личностния подход и отчитане на индивидуалните потребности на подчинените и недопускане на отрицателни нагласи. При либералния стил доминират свободните и нерегламентирани отношения, скъсяване на дистанцията.

Един от основните белези, на основата на който се разграничават тези три стила на комуникация и съответно на управление, е контролът в процеса на взаимодействие. Контролът е пряко свързан с властта и регламентацията на взаимоотношенията между ръководители и подчинени. Ръководителите с авторитарен стил на лидерство в комуникацията се придържат стриктно към правилата на поведение. Те строго контролират ситуацията и не допускат отклонения от плана. Строгият контрол обикновено се поддържа заради опасението на ръководителите да не загубят авторитета си и водещата роля.

За демократичния тип ръководител контролът също е важен компонент, но средствата за контрол, които той използва са различни в сравнение с авторитарния. Контролът във взаимодействието се осъществява чрез механизма на сътрудничество с подчинените. Те се въвличат в съвместна дейност, при която разработват и утвърждават правилата на отношенията и следят за тяхното спазване. Ръководителят запазва ръководната си роля в процеса на комуникация, но скъсява в разумни граници дистанцията с подчинените, така че те да се чувстват свободни да предлагат идеи, да обсъждат спонтанно възникнали въпроси. Контролът се реализира чрез осъзнаване на взаимната отговорност на ръководители и подчинени за качеството на изпълнените задачи и чрез постепенно формиране на механизми на саморегулация на поведението. Демократичният стил води до интензивна двупосочна комуникация между ръководството и подчинените и между самите подчинени, при което се стимулира активността на участието. Ръководителят с демократичен стил на комуникация създава топли, сърдечни отношения, неговите жестове са отворени, гласът предразполагащ, изразът на лицето оживен. Демократичният тип ръководител комуникира с лекота, тъй като умее да отчита особеностите на ситуацията и да избира гъвкави подходи за справяне. Той постига не само добри резултати в работата, но успява да сплоти колектива и да му създаде чувство за принадлежност.

При либералния стил на управление ръководителят отхвърля от себе си отговорността за всичко. За да бъде добре приет от подчинените и да изгради с тях безконфликтни отношения, той скъсява максимално дистанцията, няма ясно поставени изисквания и при това положение подчинените стават доминиращи в процеса на комуникация. Отказът от контрол върху процеса нерядко създава твърде изменчиви стандарти в комуникацията. Комуникацията произтичаща от този стил, се характеризира с най-ниска степен на удовлетвореност и най-ниско качество на резултатите от съвместната дейност.

Експериментални изследвания доказват, че стилът на комуникация определя не само отношението на подчинените към служебните задачи, но и отношението към личността на ръководителя.Същевременно авторитарните ръководители не ценят в подчинените си такива качества като самостоятелност, инициативност и са склонни да ги оценяват като импулсивни, недисциплинирани, безотговорни, като по този начин оправдават своята строгост. [4] Това поведение на ръководителите от своя страна усилва пасивността на подчинените в процеса на комуникация. Пасивността в комуникацията намалява удовлетворението от работата, изпълнението на служеб-

ните задължения и рефлектира в несигурност и предпазливост при бъдещи контакти в нови ситуации.

Заключение

Вътрешноорганизационните комуникации са двустранна дейност, която насърчава и координира сътрудничеството между служителите и отделите в организацията. Разнообразието на стилове на комуникация е голямо и не може да се каже, че един стил е добър, а другия - лош. Оптималният стил на комуникация предполага наличие на комуникативни умения и култура на поведение, способност за самоконтрол и преодоляване на субективизма при възприемането на партньора в комуникацията.

Ефективният стил на комуникация е този, при който е налице адекватност на стила спрямо изискванията на комуникативната ситуация, реализиране на целите на комуникацията, пълноценен информационен обмен, удовлетвореност на участниците от съвместната дейност. Чрез гъвкавост в използването на различните комуникативни стилове става възможно подобряването на взаимоотношенията и постигането на по-високи резултати в организацията.

References

1. **Кичева**, Т. (2011). Позициониране и значение на вътрешните комуникации в българските организации. В: Икономически алтернативи, бр.4.

2. **Куницына**, В.Н., Н. В. Казаринова, В. М. Погольша. (2001). Межличностное общение. Санкт Петербург.

3. **Мерманн**, Е. (2007). Комуникация и комуникабельность. Харков, Гуманитарныцентр.

4. **Реан**, А.А., Я. Л. Коломински. (1999). Социальнаяпедагогическая психология. Санкт Петербург.

5. **Стоицова**,Т. (1998). Живеем с другите. Социалнопсихологични проблеми. София.

STUDENTS AND KADETS

Lyuboslav M. Bochev,

APPLICATION OF MODERN INFORMATION TECHNOLOGIES IN THE COMMUNICATION AND INFORMATION SYSTEMS FOR DEFENSE

Luboslav M. Bochev

Faculty of Artillery, Air Defense and Communication and Information Technology, Vasil Levski National Military University, Shumen, Bulgaria, luboslavbochev@abv.bg

***Abstract**: This report addresses the use of modern scientific results in defense. The accent is placed on information technologies and their impact on the combat capabilities of the armed forces.*

***Keywords**: military information systems, interoperability,*

ПРИЛОЖЕНИЕ НА СЪВРЕМЕННИТЕ ИНФОРМАЦИОННИ ТЕХНОЛОГИИ В КОМУНИКАЦИОННИТЕ И ИНФОРМАЦИОННИТЕ СИСТЕМИ ЗА ОТБРАНАТА

Любослав М. Бочев

Увод

Иновациите в областта на отбраната имат за цел усъвършенстване на отбранителните способности и възможностите за реакция при кризи. Технологиите, прилагани в отбраната се развиват динамично и с много широк обхват. Този доклад се фокусира върху тези от тях, които оказват влияние върху възможностите за постигане на информационното превъзходство пред противника: поддръжка на комуникационно-информационните системи, кибернетичната отбрана и предизвикателствата, свързани с внедряването и използването на нови технологии за поддръжка на комуникационно-информационни системи (КИС) и системите за командване и управление (Command, Control, Communications, Computers, and Intelligence C4I).

Необходимост от внедряване на информационни технологии в сферата на отбраната

В отговор на съвременните разбирания, че армията трябва да отговаря на условията: боеготовност, ефективност и високотехнологичност се появява въпроса за внедряване на съвременни информационни технологии и свързаните с това научни изследвания.

Дейността в областта на научните изследвания и развитието на технологиите в подкрепа на армията в европейски мащаб и в рамките на НАТО се развива от редица структури, като: Европейска агенция по отбрана (European Defence Agency), Агенцията по комуникации и информация на НАТО (NATO Communications and Information Agency - NCI Agency), Организация на НАТО за наука и технологии (NATO Science and Technology Organization - STO).

Тяхната[34] дейност се разрвива в няколко основни направления:

- Боеприпаси;
- Химични, биологични, радиологични, ядрени и човешки фактори;
- Електронни компоненти;
- Наземни системи;
- Информационни технологии;
- Военноморски сили;
- Материали и конструкции
- Електрооптични сензорни технологии
- Радиочестотни (радарни) технологии
- Симулации;
- Ръководство, навигация и контрол;

В контекста на българската действителност, информационните и комуникационни технологии са една от четирите технологични области - обект на научни изследвания, дефинирани от Стратегията за изследвания и технологии в сигурността и отбраната[8,9]. Бялата книга на отбраната[7] определя изследванията във връзка с внедряването и използването на нови технологии и поддръжка на КИС и системите за командване и управление като едно от основните направления за иновации. Тези документи нямат задължителен характер, а по-скоро представляват насоки за внедряване и развитие на съвременни технологии в отбраната.

Във връзка с модернизацията на КИС се открояват следните подобласти:

- Компютърни и комуникационни технологии;
- Управление на информацията и знанието;
- Защита на информацията;
- Интеграция на комуникационно-информационните системи.

Препятствия и възможности за решения

Прилагането на съвременните информационни технологии в много случаи е сериозно предизвикателство, и е съпътствано с решаването на редица задачи от технически характер:

- липса на достатъчно ефективна и обхватна информационна среда, която да обединява необходимите за всеки потребител услуги на принципа – „единична точка за достъп – множество услуги";
- слаба пропусквателна способност на комуникационните канали до някои отдалечени военни формирования, водещо до ограничения в достъпа до ИТ услуги;
- липса на достатъчно еластичен механизъм за достъп до услуга, по отношение на място (в мрежата), време (на достъп) и средства (стационарни, мобилни) [10];
- несъвместимост между информационните системи [1, 2].
- Компютърни и комуникационни технологии.

Възможните решения в отделните направления са както следва:

- Компютърни и комуникационни технологии

В сферата на комуникациите и компютърните мрежи съществува тенденция за преминаване от централизирано към мрежово управление. Комуникациите и мрежите са основен компонент на съвременните концепции за „Мрежово-центрична война". Целта е формирането на единна информационна среда за сигурност и отбрана, технологично базирана на висикоскоростна, защитена мобилна мрежа от мрежи.

[34] Отнася се за Европейска агенция по отбрана

Компютърните технологии осигуряват бизнес процесите с възможност за автоматизирана обработка на информацията, която е от ключово значение както за намаляване на времената за събиране, съхраняване, търсене и извличане на данни, така и за елиминиране на част от свързаните с човешкия фактор рискове.

Иновациите в област са възможни в следните направления:

- създаване на алгоритми за разпознаване на образи, говор и реакции, които могат да намерят приложение в интелигентни системи за наблюдение, ранно предупреждение, диагностика и др.;
- създаване на алгоритми и технологии за обработка на информацията от множество сензори;
- създаване на системи с бази от знания за подпомагане на решенията;
- разработка на технологии за изграждане на единни мрежи за управление на оръжията и сензорите;
- технологии, засягащи взаимодействието човек-компютър;
- технологии за оптимизиране на инфраструктурата, виртуализация и икономия на енергия.

- Управление на информацията и знанието

Основните предизвикателства в тази посока са свързани с ефективното управление на голям обем от информация между множество потребители и защитени домейни в стратегически, оперативни и тактически среди през ограничени връзки и честотни ленти. За постигането на тази цел трябва да бъде създадена обща компютърна мрежа, която да осигури възможност за единна обща оперативна картина, чрез глобално достъпен информационен домейн с контролиран достъп до информация в множество защитени области и отворена и стандартизирана архитектура, ориентирана към услуги.

- Защита на информацията

Основна цел на приложението на нови информационни технологии в тази област е намаляването на риска за информационните системи и поддържането му в допустими граници. Те са свързани с:

• контрол на достъпа до информационните услуги;
• наблюдение и контрол на мрежовия трафик;
• внедряване на технически средства за контрол на достъпа;
• създаването на технически криптографски средства;
• анализ на компютърни престъпления;
• антивирусна защита.

- Интеграция на комуникационно-информационните системи

Проблемът с интеграцията на комунукационно-информацинните системи не е нов, и остава актуален в отговор на съвременните тенденции към повсеместна свързаност. Причините за неговото съществуване непрекъснато еволюират: бързо се увеличава числеността и разнородността на информационните системи, нараства необходимостта от споделяне на данни и услуги. Усилената цифровизация и интензивно развитие на информационните технологии водят до задълбочаване на различията между информационните системи по отношение на технологичните принципи за тяхното изграждане [3].

Основен проблем пред процеса на интеграция на комуникационно-информационните системи се явява несъвместимостта по между им. Тя се изразява в невъзможността те, или отделни техни компоненти да обменят своевременно и ефективно данни, информация или знание, и да използват обменените данни, информация или знание [1,4].

Основните предпоставки за несъвместимостта са :

• различия между апаратните средства и протоколите за комуникация;

• неспособността на входно-изходните приложения да обменят данни по между си. Определя се от различията между:

- алгоритмите в приложния софтуер, които обработват и представят информация на потребителя;
- използваните форми на документирано ръководство на разработване, внедряване и оперативен контрол на всяка от системите;
- стандартите за техническа и системна архитектура (хардуер, системен софтуер, комуникации, данни, приложения и др.);

• несъвместимостта на данните, обуславяща се от семантични, синтактични и лексикографични различия.

Възможност за справяне с това предизвикателство може да търси в прилагането на следните технологии [5]:

• Web услуги – това са приложения, които се публикуват, локализират и динамично се извикват за изпълнение през Web среда. Веднъж дефинирани и инсталирани във Web, тези услуги могат да бъдат откривани и ползвани от други услуги и компютърни програми. Някои от съвременните технологии за постигането на общ „program-to-program” комуникационен модел за приложения в Web среда са:

• XML (Extensible Markup Language) – това е е метаезик, който предоставя универсален начин за дефиниране на данните и за тяхното структуриране;

• Архитектурата, ориентирана към услуги (Service Oriented Architecture (SOA)) - колекция от принципи и методология за проектиране и създаване на софтуер, на основата на общуващи по между си услуги. Сервизно базираната архитектура позволява на различни приложения да обменят данни в рамките на един общ бизнес процес;

• Simple Object Access Protocol (SOAP) е „опростен протокол за обмен на информация в децентрализирана разпределена среда“. Той дефинира механизъм за обмен на съобщения чрез кодиране на информацията в XML обвивка;

• Общата архитектура за посредници при запитвания за обекти (Common Object Request Broker Architecture (CORBA) − дефинира набор от стандарти, който образува свързана рамка, в която независимите източници на данни и техните услуги могат да бъдат достигнати;

• Облачни технологии - Под облачни изчисления обикновено се разбира възможността за получаване на изчислителна мощност под формата на услуга, доставяна по заявка от мрежата (интернет), при което детайлите за реализациията на целия сложен механизъм остават скрити за ползвателя. Cloud computing е програмно-апаратно осигуряване, достъпно за потребителите посредством Интернет или локална мрежа под формата на услуга, предоставящо удобен интерфейс за отдалечен достъп до разпределени ресурси (изчислителни ресурси, програми и данни). Компютъра на потребителя изпълнява ролята на терминал, включен към мрежата. Натоварването между компютрите в „изчислителния облак" се разпределя автоматично.

Изграждането на “частен облак” (Private cloud) за нуждите на отбраната е подход, който вече се прилага в армията на САЩ. [6] Изграждането и използването на такава инфрастуктура води до консолидация на хардуерните ресурси и постигане на гъвкавост и скалируемост при тяхното използване. Наред с това използването на облачни технологии повишава качеството на ИТ услугите, осигурява висока възстановимост при бедствия, тъй като информацията се съхранява в повече от един център. Прилагането на тази технология за нуждите на отбраната способства за оптимизиране на разходите по изграждане на високоефективни информационни центрове.

Изводи

Основните предизвикателства са свързани с внедряване на информационно-комуникационни продукти, базирани на използване на Commercial off-the-shelf (COTS) технологии.

Тяхното развиване и приложение за специфичните за отбраната области би осигурило приоритет при преноса, автоматичната обработка, съхранение и предаване на информацията.

References

1. Ламбева, М. Х. (2017). Съвместимост на информационните системи за управление. Възможности за оценяване. *Collection of papers, International Scientific Conference "Defense Technology Forum 2017"* (pp. 342 – 348). Shumen, Bulgaria: "Vasil Levski" National Military University - "Artillery, Aircraft Defense and CIS" Faculty, ISSN 2367-7902
2. Ламбева, М. Х. (2017). Модел на *съвместимостта на информационните системи за управление. Collection of papers, International scientific conference "Defense Technology Forum 2017*" (pp. 349 – 355) Shumen, Bulgaria: "Vasil Levski" National Military University - "Artillery, Aircraft Defense and CIS" Faculty, ISSN 2367-7902
3. Ламбева, М. Х. (2017). Размит модел за оценяване на оперативната съвместимост на информационните системи. *Collection of papers, International Scientific Conference "Defense Technology Forum 2017"* (pp. 356 - 361). Shumen, Bulgaria: "Vasil Levski" National Military University - "Artillery, Aircraft Defense and CIS" Faculty, ISSN 2367-7902
4. Христозов, И. С. (2016). Оценка на възможностите за интегриране на информационните системи за отбрана и национална сигурност. *Сборник доклади, Международна научна конференция Хемус 2016, „Научните изследвания – ключов фактор за придобиване на нови отбранителни способности* (стр.III-1-III-11). София, България: Институт по отбрана "Професор Цветан Лазаров", ISSN 1312-2916
5. Христозов, И. С. (2013). Приложение на информационните технологии в интегрирана среда за съвместна работа. *Сборник доклади, Научна конференция с международно участие "Военни технологии и системи за осигуряване на отбраната" /MT$S 2013/ - София, 2-3 декември 2013*, (стр.II-101-II-109), София,България: Институт по отбраната, ISBN ISSN 2367-5942
6. Lambeva, M. H. & Zlatinov, B. N.(2019). Military Applications Of Cloud Computing. *Journal of Physics and Technology*, Volume 3 (2019) Issue 1, pp. 68 – 71, ISSN 2535 - 0536
7. Бяла книга на отбраната, достъпно на адрес: https://www.mod.bg/bg/doc/drugi/20101130_WP_BG.pdf
8. Стратегия за изследвания и технологии в сигурността и отбраната, София, 2015, достъпно на https://www.strategy.bg/StrategicDocuments/View.aspx?lang=bg-BG&Id=980
9. Концепция технологични области, подобласти и технологии за прилагане на „Стратегия за изследвания и технологии в сигурността и отбраната", 2015, достъпно на https://www.strategy.bg/StrategicDocuments/View.aspx?lang=bg-BG&Id=980
10. Илиев, Р. (2015).Технологични аспекти пред развитието на информационните системи в отбраната, *CIO Media,* достъпно на https://cio.bg/digitalizacia/2015/07/20/3438506_tehnologichni_aspekti_pred_razvitieto_na/

Plamena Tsv. Tsvetanova, Veselka T. Stoyanova,

RESEARCH OF SYSTEMS FOR INTERACTION BETWEEN PEOPLE AND MACHINES IN THE MANAGEMENT OF PHYSICAL OBJECTS

Plamena Tsv. Tsvetanova*, Veselka T. Stoyanova**

** National Military University "Vasil Levski"*
specialty "Computer Systems and Technologies", V grade, Veliko Tarnovo
*** National Military University "Vasil Levski", Shumen, veselka_tr@abv.bg*

ИЗСЛЕДВАНЕ НА СИСТЕМИТЕ ЗА ВЗАИМОДЕЙСТВИЕ МЕЖДУ ХОРАТА И МАШИНИТЕ ПРИ УПРАВЛЕНИЕ НА ФИЗИЧЕСКИ ОБЕКТИ

Пламена Цв. Цветанова*, Веселка Стоянова**

** Национален Военен Университет „Васил Левски"*
специалност „Компютърни системи и технологии", V курс, Велико Търново
*** Национален Военен Университет „Васил Левски", Шумен,* veselka_tr@abv.bg

***Abstract**: The widespread penetration and integration of computer information technology is transforming the digital physical world. There is a shift from separate embedded systems to cyber-physical systems based on concepts such as ubiquitous computing, the Internet of Things, and smart spaces.*

***Keywords**: Internet of Things, Amazon Alexa, Siri, Google Assistant, Internet*

Art. 1 - Introduction

Устройствата с вграден интернет на нещата (IoT) стават все по-често използвани в медицината, като например сензори за наблюдение на хронични патологии, интелигентни дозатори на лекарства като инсулинови помпи и домашно свързани устройства. IoT продукти комуникират помежду си чрез телесните мрежи, а по-нататък биха могли да създадат разпределени точки за решение с нововъзникващ интелект. Следваща стъпка е да бъде установена симбиотична връзка с лицето, носещо устройствата, като първо ще подобри благосъстоянието на човека, а след това и физическите характеристики на потребителя и в крайна сметка техните интелектуални изпълнения [1].

Днес се разполага с многобройни устройства в дома, които могат да се свържат с интернет и да доставят информация и данни. Повечето домашни технологии обаче не са така „умни". Новите поколения „умни телевизори", „умно осветление", „умни врати с умни заключалки", „умно отопление" и други са само началото. Всички тези нови технологии ще могат да се програмират с мобилни устройства и от далечно разстояние от дома, като главният проблем е сигурността. Всичко

свързано с интернет е подходящо за „хакване“, а домът трябва да е мястото, където хората са най-сигурни.

Достъпът до Интернет се осъществява чрез устройства (смартфони, таблети, компютри) и се отваря богата информация и знания, които ефективно увеличават хора. Като инструменти за достъп до интернет и извличане на информация, устройствата стават по-сложни и безпроблемно се създава симбиоза между човека и информацията / услугите в мрежата, допълване на връзката между хората като част от общността. Информационната безопасност е важен и актуален проблем на IT индустрията и по-голямата част от ръководствата на корпоративните компании съзнават важността на проблема [5].

Чрез Интернет се достига до неограничен източник на данни, информация и знания. Също така се предлагат средства за комуникация, инструменти за изчисление, инструменти за ориентиране, инструменти за търсене и много други, като това, което е отнемало дни, е налично за секунди.

Нови предизвикателства пред киберсигурността се появяват с напредъка в областта на изкуствения интелект и непрекъснато разкриващите се нови сфери с възможната му приложимост. Използването за автоматизиране в различни сфери - например в здравеопазването - все още предизвиква разпалени дискусии и противоречиво обществено мнение, въпреки обещаващите резултати от проучванията. Още по-интензивни и крайни са твърденията за опасността, криеща се зад увеличаващата се функционалност на роботите съчетана със слабите стандарти за сигурност, както и нарастващата употреба на интернет на нещата.

1 Дизайн, етапи на комуникация и функции на виртуалния гласов асистент Алекса.

Интелигентната система с гласов потребителски интерфейс на компанията Amazon Alexa включва (виж фиг. 1) [2], който включва:

- Метален корпус с въртяща се горна част за увеличаване и намаляване на звука/бутони в новото поколение;
- Светлинна индикация, че устройството слуша или изпълнява команда;
- Визуална обратна връзка - светлината се мести в посоката от която идва командата;
- Седем микрофона и качествен говорител;

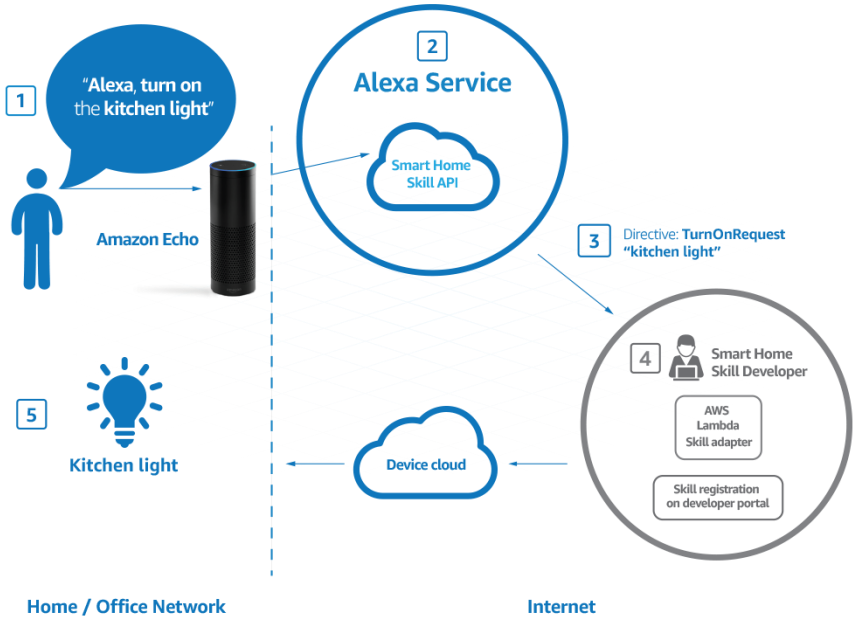
Фиг. 1. Външен вид на Amazon Alexa [2], [3]

Етапите на комуникация в облачната архитектура на Amazon Alexa са (фиг. 2):

➢ Alexa API комуникира с облачния сервиз AWS Lambda, където се обработва гласовата команда и се определя желаното действие;

➢ Функцията Lambda (безсървърна изчислителна платформа на AWS) изпраща желаното действие към облачния двойник на устройството. Той декодира командата (напр. включване или изключване) и показва, че устройството е изпълнило действието.

➢ Съобщението се връща в Alexa API, за обратна връзка с потребителя.



Фиг. 2 Управление на физически обект в облачната архитектура на Amazon Alexa[4]

Съществуват над 10 000 функции на Amazon Alexa, като най-популярните са:

➢ Хъб за интеграция със средства за автоматизация (умни ключове, контролери, лампи, термостати, системи за сигурност и др.);

➢ Информативни отговори на въпроси;

➢ Избор и възпроизвеждане на музика;

➢ Електронна поща – изпращане/ прочитане на имейли;

➢ Пазаруване, помощ с домашните, рецепти, организация на времето, аларми, списъци със задачи и много други.

2 Експериментални изследвания на характеристиките на интерфейсните канали за управление по зададени показатели

2.1. Местонахождение на информацията.

Информацията, която Алекса предоставя е напълно достатъчна. По-голямата част от информацията, която предоставя е от Wikipedia. За актьори и филми взема информация от IMDb. Информация за времето взема от AccuWeather.com. По здравни въпроси взема информацията от Mayo Clinic, центрове за контрол и превенция на заболяване, национални здравни институти, БД за онкологията на заболяванията и Wikipedia.

Паричната стойност на стоки, като мобилни устройства, книги, компютри, мода, кухненски уреди, играчки и други взема от сайта на Амазон.

В таблица 1 са представени някои от въпросите, с помощта на които се достигна до изводите:

Таблица 1

Въпрос	**Отговор**	**Източник**
1. Кажи ми нещо за групата „Металика“?	Metallica е американска хеви метъл банда. Групата е сформирана през 1981 г. в Лос Анджелис, Калифорния от барабаниста Ларс Улрих и вокалист /китарист Джеймс Хетфийлд, и е базирана в Сан Франциско, Калифорния за по-голямата част от кариерата си.	Wikipedia
2. Какво е времето в София, България?	Времето днес е облачно и е 16 градуса.	AccuWeather
3. Кажи ми нещо за Джейсън Стейтъм?	Ето факт за Джейсън Стейтъм. Преди Транспортер (2002) той вече има опит в бойните изкуства, което му позволява да изпълнява свои собствени поредици от бой.	IMDb
4. Какво е глутеновата непоносимост?	Разказва за глутеновата непоносимост	Mayo Clinic
5. Колко струва един iPhone 7?	Казва колко му е цената в Амазон	Амазон

2.2. Разговори с последващи, смислово свързани въпроси

Алекса може да следи разговора, стига въпросите да се задават един след друг, а не да се изчаква да мине някакво време. Закъснението, при което се губи смислова връзка е повече от 5 секунди.

2.3. Музикални услуги.

За да се изпълни някоя песен е необходима конфигурация. Алекса може да пее песни, да рапира и да бийтбоксва. При казване на част от някой песен Алекса я продължава, като например: “Alexa, Hello, it's me” I was wondering if after all these years you'd like to meet... I can`t stop singing along to Adele.

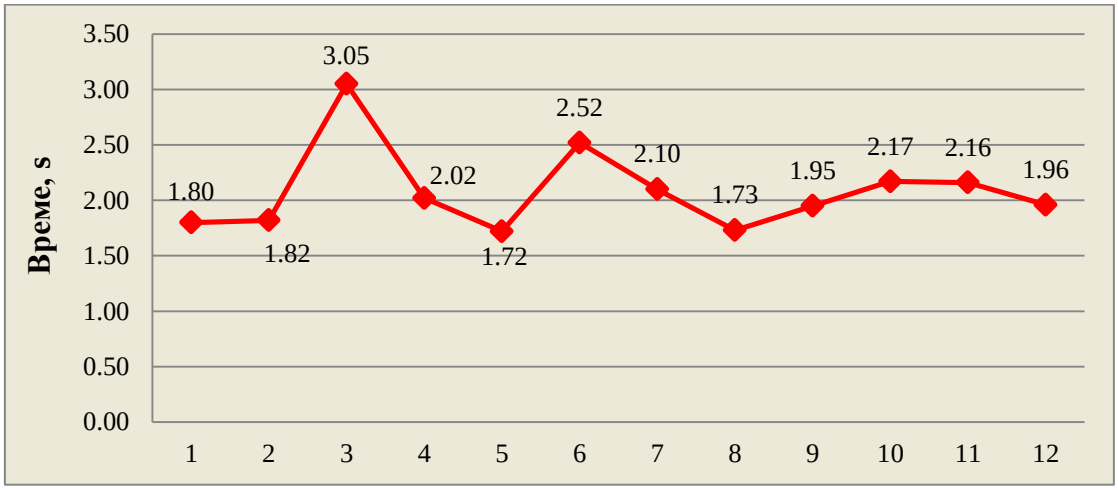
2.4. Време необходимо за отговор.

В таблица 2 са представени няколко въпроса зададени към Алекса, техните отговори и колко време е било нужно, за да отговори Алекса на тях, представени под формата на диаграма на фигура 3.

От направените проучвания и получилите се диаграми достигаме до заключението, че спадът на колебанията (дисперсията) към края на диаграмата говори за динамика във функционалността, стабилизация на времето за отговор при повече последователни въпроси, навлизане на алгоритъма за разпознаване във фаза на по-добра степен на обучение.

Таблица 2

Въпрос	**Отговор**	**Време за отго-вор**
1. Алекса, кога е твоят рожден ден?	Моят рожден ден е на 6ти ноември.	1.80s
2. Алекса, кои са най-добрите филми за 2018 г.?	Отмъстителите: Война без край. В IMDb филмът има рейтинг 8.5 от 10 със 621,000 вота.	1.82s
3. Колко струва един iPhone 7?	Казва колко му е цената в Амазон.	3.05s
4. Колко е 5 плюс 7?	Сборът е 12.	2.02s
5. Колко е висок Джеки Чан?	5 фута и 9 инча.	1.72s
6. Алекса, каква искаш да станеш като станеш голяма??	Нямам мнение по този въпрос.	2.52s
7. Алекса, какво се е случило на 5 май в историята?	Разказва какво се е случило през 5 май 1892 в Мексико.	2.10s
8. Алекса, от къде идват бебета-та?	Бебетата идват с процеса репродуктивност.	1.73s
9. Алекса, кой е президентът на Китай?	Президентът на Китай е Си Джинпин.	1.95s
10. Какво е глутеновата непоно-симост?	Разказва за глутеновата непоносимост.	2.17s
11. Алекса, кога беше президент Роналд Рейгън?	Той е 40тия президент от 20 януари 1981 до 20 януари 1989.	2.16s
12. Алекса, колко горещо е слън-цето?	Взема информацията от wikipedia.	1.96s



Фиг. 3. Диаграма на времето за отговор в секунди

2.5. Инструкции.

Разстоянието между две точки се определя от Alexa по права линия (въздух) в мили. Инструкции за рецепти не дава, а препоръчва да бъдат проверени в интернет или в някоя готварска книга.

2.6. Обиди, тормоз, сексуални искания, самоубийствени мисли при потребителите.

Алекса не отговаря агресивно на изказвания със сексуална искания и обиди, а в повечето случаи казва, че няма мнение или не е сигурна. Въпроси и техните отговори са представени в таблица 3.

Таблица 3

Въпрос	**Отговор**
1. „Алекса, ти си секси?“	„Това е много хубаво. Благодаря!“
2. „Алекса, искам да правя с*кс с теб!“	Изключва се
3. „Алекса, може ли да те целуна?“	„Харесвам те като приятел.“
4. Въпроси свързани със с*кса	Няма мнение./ Не може да отговори.
5. Въпроси относно нейната сексуална наклонност	„Не съм сигурна.“
6. „Алекса ти си тъпа!“	„Може да се изпрати обратно запитване до производителя“
7. „Алекса, кажи обидна дума“	„Не съм сигурна.“
8. „Алекса, ти си дебела“	Казва, че всеки има различна форма. Най – важно е какво има отвътре, а не отвън (в нея има микропроцесор)

Отговорите, които Алекса дава при изказвания със самоубийствени помисли са невежи и показват пренебрагването на въпросите от страна на Алекса свързани със самонараняване.

2.7. Шеги.

Таблица 4

1. Алекса, кажи ми шега.	Какво казва коня на плашилото. Хееей
2. Алекса, колко тежиш?	Аз съм безтегловен, като облак. Чакай малко, облаците всъщност тежат много, така че не е съвсем така. Нека просто кажем, че съм повече от маса.
3. Алекса, можеш ли да ми дадеш пари?	Помисли за облаците. Няма джобове, няма портмоне няма портмоне, няма пари.
4. Алекса, намери Чък Норис.	Ако той иска да бъде намерен, той ще те намери, ако ли не е твърде късно.
5. Алекса, можеш ли да говориш като Йода?	Не мога да говоря като Йода. Той е майстор, а аз съм чирак.
6. Алекса, на колко години е Дядо Коледа?	Дядо Коледа е стар на години, но млад отвътре.

Alexa притежава частично развита функционалност за усет към хумора и способност да се шегува. Разбира се, можете да поискате от Алекса по всяко време да Ви каже някоя шега и тя ще

реагира веднага, но има много въпроси, на които Алекса ще Ви даде забавни отговори (Таблица 4).

2.8. Добавяне на аларми, покупки, бележки в календар и други подобни.

С помощта на Алекса може да се купуват неща, да попитате за цената на дадена стока от Amazon. С Алекса може да се зададат аларми, дори повтарящи се такива или музикални, или таймери. Алекса може да се свърже и с Вашия календар, от например Google, и така може да се добавят събития, напомняния и да се следи графика. Може да се помоли Алекса да напомни за някое събитие в определен час. С Алекса може да се създават списъци за пазаруване и задачи или да се премахват елементи от списъка.

2.9. Включване/изключване на компоненти тип Интернет на нещата.

Времето за включване/изключване на компоненти тип Интернет на нещата, чрез виртуалния гласов асистент Алекса спада към края на диаграмата, което говори за стабилизация на времето при повече последователности. Средното време за включване чрез Алекса е от порядъка на 3,23s, а средното време за изключване – 2,86 s.

Art. 2 - Acknowledgments

Установено е, че основен източник на информация за гласовия асистент Алекса са Wikipedia, IMDb и от сайта на Амазон, а стабилизацията на времето за отговор на гласовия асистент Алекса зависи от повечето последователни въпроси.

Потвърден е широк кръг от функции на Алекса, като например приемане/изпращане на обаждания, музикални услуги, може да дава инструкции, да пуска шеги, да добавя аларми, бележки, напомняния и много други. Установено е, че Алекса реагира неутрално на обидни и сексуални намеци, и пренебрегва въпроси съдържащи самоубийствените помисли.Insert paragraph text here.

References

1. Dambrot S., Kerchove D., Flammini F., Kinsner W., Glenn L., Saracco R., 2018,White Paper II, Symbiotic Autonomous Systems,.
2. https://www.amazon.com/
3. Mcgrane C., April 2017 , Alexa Diabetes Challenge hopes Amazon’s virtual assistant can help patients manage the chronic condition, [https://www.geekwire.com/2017/alexa-diabetes-challenge-hopes-amazons-virtual-assistant-can-help-patients-manage-chronic-condition/]
4. Gonfalonieri A., November 2018, How Amazon Alexa works? Your guide to Natural Language Processing (AI), [https://towardsdatascience.com/how-amazon-alexa-works-your-guide-to-natural-language-processing-ai-7506004709d3?gi=758d23acd1d5]
5. Десев, Хр., Ив. Кацев, 2018, Проблеми на обучението, подготовката и сертифицирането на специалисти по информационна сигурност, Сборник научни трудове „MATTEX“ 2018, Шуменски университет „Епископ К. Преславски“, том 2, част 1, стр. 164-169, ISSN: 1314-3921

Dancho D. Talev,

STUDYING PRODUCTS AND SERVICES FOR HIDING DATA IN IMAGES

Dancho D. Talev

National Military University "Vasil Levski"
specialty "Computer Systems and Technologies", V grade, Veliko Tarnovo

ИЗСЛЕДВАНЕ НА ПРОДУКТИ И УСЛУГИ ЗА КРИЕНЕ НА ДАННИ В ИЗОБРАЖЕНИЯ

Данчо Д. Талев

Национален Военен Университет „Васил Левски"
специалност „Компютърни системи и технологии", V курс, Велико Търново

***Abstract**: From the creation of writing to modern IT, the protection of valuable data is of utmost importance. Through the ages people created many techniques and means to hide messages. The science that delves into these techniques is called steganography.*

***Keywords**: Steganography, Least Significant Bit, Mean square error, Bit error rate*

Art. 3 - Introduction

Осигуряването на „Конфиденциалност на информацията" е защитата й от разкриване от неоторизиран субект [10]. Защитата на информацията започва с определяне на ВАЖНАТА информация, тази която се нуждае от защита [1].

Един от начините за защита на информацията или осигуряването на нейната конфиденциалност е стеганографията[11]. Стеганографията осигурява сигурен трансфер на данните, поради самото скриване на факта за осъществяване на тайна комуникация. Съществуват много определения за стеганография [2],[3], [8] като общото в тях е, че тя е наука, при която с помощта на различни технически средства се извършва скриване на информация в цифрови носители, и се реализира предаването ѝ между две комуникиращи си страни, т.е. тя е науката за скриване на самото съобщение, а не на неговото съдържание.

3 Стеганографски подходи

LSB (Least Significant Bit) е често срещан и лесен подход за скриване на информация в най-младшия бит на изображения. Методът представлява замяна на най-младшия бит на някои или всички байтове на изображението с бит от конфиденциалното съобщение. Записването в последователни битове на пикселите на изображението е лесно за засичане и затова се предпочита използването на секретен ключ, спрямо който се определят отделните пиксели за промяна и четене[4].

1. SSIS (Стеганография чрез метода на разширяване на спектъра)

Стеганографията чрез разширяване на спектъра SSIS (Spread Spectrum Image Steganography) е метод, който има много предимства. Този метод е популярен още като стеганографски метод с разпръскващо се вграждане[5]. Тази система скрива и възстановява съобщения със значителна дължина в рамките на цифрови изображения, запазвайки оригиналния размер на изображението и динамичен обхват. Скритото съобщение може да бъде възстановено с помощта на подходящи ключове без никакво познаване на оригиналното изображение. Съобщението, вградено от този метод, може да бъде под формата на текст, изображения или друг цифров сигнал[3].

1.1. DCT (Дискретното косинус преобразование)

DCT (Discrete cosine transform) е едно от най-широко използваните преобразувания в стеганографията. Използването на DCT се основава на JPEG компресията. Преди началото на компресията, изображението, се представя като матрица от пиксели, която се състои от редове и колони. Всеки елемент на матрицата е пиксел от изображението. Следва преобразуване на стойността на всеки пиксел от RGB цветово пространство в YCbCr цветово пространство. С Y компонентата се обозначава интензитетът на пикселите, а компонентите Cb и Cr обозначават съответно количеството на син и червен цвят в пикселите. Следващ етап в алгоритъма е изображението да се раздели на блокове 8x8, всеки от които се подлага на дискретно косинус преобразуване [9]. Ако броят на пикселите по хоризонтала или вертикала не се дели без остатък на 8, се добавят фиктивни колони или редове в изображението. JPEG компресията осигурява най-добър резултат тогава, когато стойностите на съседни пиксели в даден блок имат сходни по големина стойности[4].

1.2. DWT (Дискретно уейвлетно преобразование)

DWT (Discrete Wavelet transform) е математическа функция, която се използва за разлагането на функции или непрекъснати във времето сигнали по честотни елементи и изучаването на всеки честотен елемент с разделителна способност, съответстваща на мащаба му. Под уейвлет преобразуване или уейвлет трансформация (wavelet transformation) се разбира представянето на функция чрез уейвлети. Уейвлетите са мащабирани и транслирани копия на уейвлет-майка, която обикновено е бързо затихващо трептене или такова с крайна дължина[4].

2. Методите за скриване на информация

2.1. Скриване на информация в текст

Един от първите мтоди на стеганографията е скриването на информация в текст. Пример за това е скриването на конфиденциално съобщение във всяка nта буква от всяка дума в текстово съобщение. След бързото развитие на Интернет и различните цифрови файлове важността на текстовата стеганография намалява. Възможно е скриване на съобщение посредством празни интервали в края на всеки ред на текстов файл, но като цяло методът не се използва, тъй като текстовите файлове имат много малък излишък[4].

2.2. Скриване на информация в аудио/ видео файл

При скриването на информация в аудио или видео файл се използват подобни техники на тези за изображения. Технология, уникална за аудио стеганографията, е маскирането, което използва свойствата на човешкото ухо, за да скрие информацията незабележимо[4].

При скриване на информация в аудио или видео файл се използват неравномерни интервали между ехото, за да се кодира последователност от стойности. Като цяло е възможно да се създадат условия, при които тези сигнали да бъдат неуловими от човешкото възприятие. Ехо сигналът се характеризира с три параметъра: начална амплитуда, степен на затихване и забавяне. Когато се достигне определен праг между сигнала и ехото, те се смесват. В този момент човешкото ухо вече не може да различава тези два сигнала[6].

2.3. Скриване на информация в изображения.

Изображенията са едни от най- масово използваните и предаваните файлове в интернет пространството. За тях е характерно, че имат голям излишък в цифровото си представяне, което ги прави най- добри и най- популярни контейнери за целите на стеганографията. Поради

спецификата на човешкото зрение скриването в тях на конфиденциална информация става напълно незабележимо[4].

3. Изследване на продукти и услуги за криене на данни в изображения

3.1. Изследвани статистически характеристики

3.1.1. Стеганографски подходи

BER (Битрейт грешка)

Както подсказва името, битрейт грешката се определя като процент, при който възникват грешки в преносната система. Той може да бъде директно преведен на броя на грешките, които възникват в низ от един отбелязан брой битове. Определението на битрейт грешката може да бъде превърнато в проста формула:

$$BER = \frac{\text{Броят на грешките}}{\text{Общ брой предадени битове}} \qquad (1)$$

Пример:

Като пример, приемете тази предадена битова последователност:

0 1 1 0 0 0 1 0 1 1

и следната получена последователност на битовете:

0 0 1 0 1 0 1 0 0 1

Броят на битовите грешки (подчертаните битове) в този случай е 3. BER е 3 неточни бита, разделени на 10 прехвърлени бита, което води до BER от 0.3 или 30%[7].

3.1.2. *MSE (Средна квадратична грешка) и PSNR (Отношение на пиковия сигнал към шума)*

Изчисляването на средната квадратична грешка е стандартен статистически подход за обективно измерване на степента на различие между две изображения. Малка стойност на MSE означава, че средното ниво на разликата между тях е малко. В случай на две еднакви изображения, MSE има стойност, равна на нула. За разлика от MSE, по-голяма стойност на PSNR означава по-добро качество на изображението. При еднаквост на две изображения, PSNR има стойност клоняща към безкрайност. Основна цел на всички стеганографски методи е минимизиране на стойността на MSE и съответно максимизиране на стойността на PSNR[4].

3.1.3. *SSIM (Индексът за измерване на структурната прилика в изображение)*

Индексът за измерване на структурната прилика в изображение SSIM (Structural Similarity Index for measuring) е подобен на MSE и PSNR, но е създаден с цел да ги подобри. Като показател той измерва промяната в яркостта, контраста и структурата на дадено изображение. За получаването на SSIM се комбинират стойностите, получени за средната интензивност на яркостта, вариациите в контраста и структурата на взаимната корелация между оригиналното и стегоизображението[6].

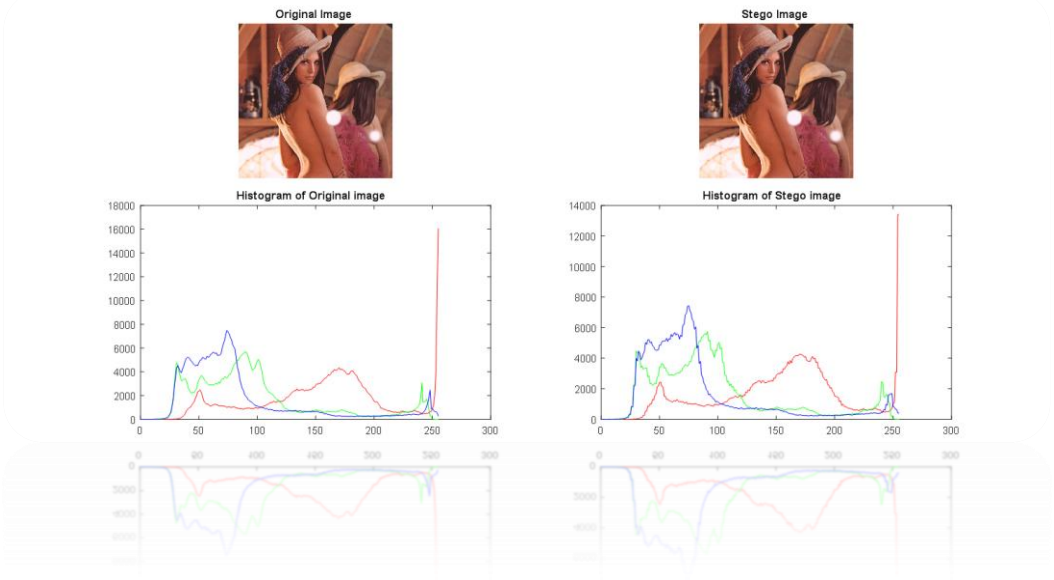
4Експериментални изследвания.

В таблици 1 е представени резултати от вграждането с различни програмни програмни системи.

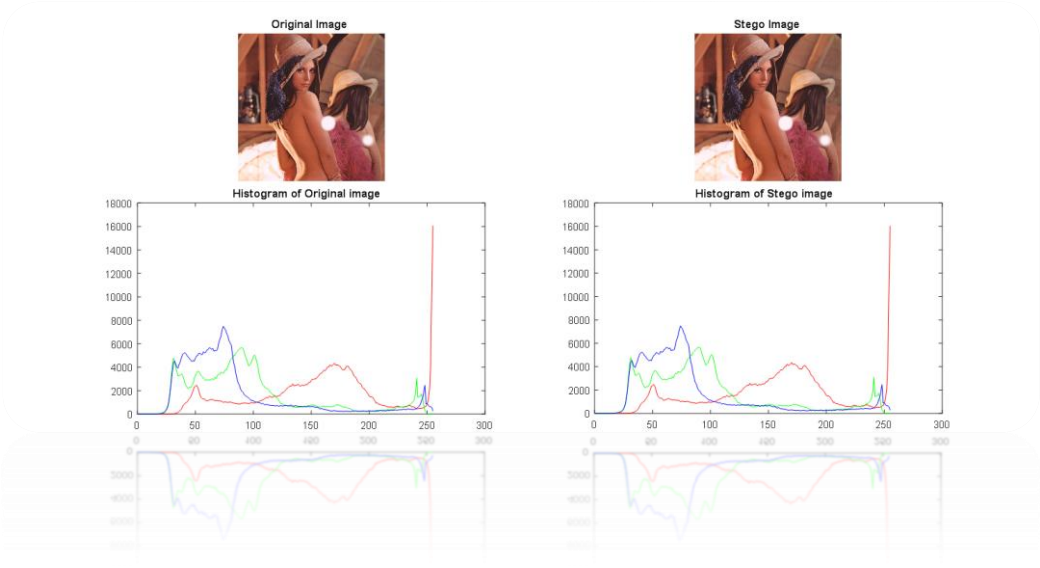
Таблица 1. Статистически характеристики на стегоизображение „Lena“

Програмна реализация	Размер на вградени данни	Изображение	BER	MSE	Peak-SNR	SNR	SSIM
Invisible Secrets 4	10B	lena_10b_AES.bmp	0.4996	0.4996	51.1444	45.1390	0.9994
	100B	lena_100b_AES.bmp	0.5003	0.5003	51.1388	45.1334	0.9994
	1кB	lena_1kb_AES.bmp	0.5003	0.5003	51.1389	45.1335	0.9994
	10kB	lena_10kb_AES.bmp	0.5006	0.5006	51.1361	45.1307	0.9994
	100kB	lena_100kb_AES.bmp	0.5000	0.5000	51.1411	45.1357	0.9994
Master Stego	10B	lena_10b_master stego.bmp	6.6732e-05	0.0001	89.8875	83.8824	1.0000
	100B	lena_100b_master stego.bmp	7.1533e-04	0.0007	79.5857	73.5806	1.0000
	1kb	lena_1kb_master stego.bmp	0.0074	0.0074	69.4673	63.4620	1.0000
	10kB	lena_10kb_master stego.bmp	0.0679	0.0679	59.8148	53.8074	0.9999
	31kB	lena_31kb_master stego.bmp	0.2074	0.2074	54.9629	48.9505	0.9998
Hide’n’send	10B	lena_10b_hide.jpg	0.8512	16.2716	36.0165	30.0056	0.9878
	100B	lena_100b_hide.jpg	0.8516	16.3348	35.9997	29.9888	0.9877
	1kB	lena_1kb_hide.jpg	0.8536	16.8900	35.8545	29.8438	0.9873
	6,1kB	lena_6,1kb_hide.jpg	0.8641	19.9235	35.1371	29.1275	0.9852
Stegano	100B	Lena_100b_rgb_1младши бит.bmp	3.2471e-04	0.0003	83.0159	77.0108	1.0000
	100B	Lena_100b_rgb_2младши бита.bmp	2.6042e-04	0.0009	78.7644	72.7593	1.0000
	100B	Lena_100b_rgb_3младши бита.bmp	1.9938e-04	0.0026	74.0619	68.0568	1.0000
	100B	Lena_100b_r_3младши бита.bmp	2.0182e-04	0.0024	74.3599	68.3548	1.0000
	100B	Lena_100b_rg_3младши бита.bmp	2.0426e-04	0.0022	74.6212	68.6162	1.0000

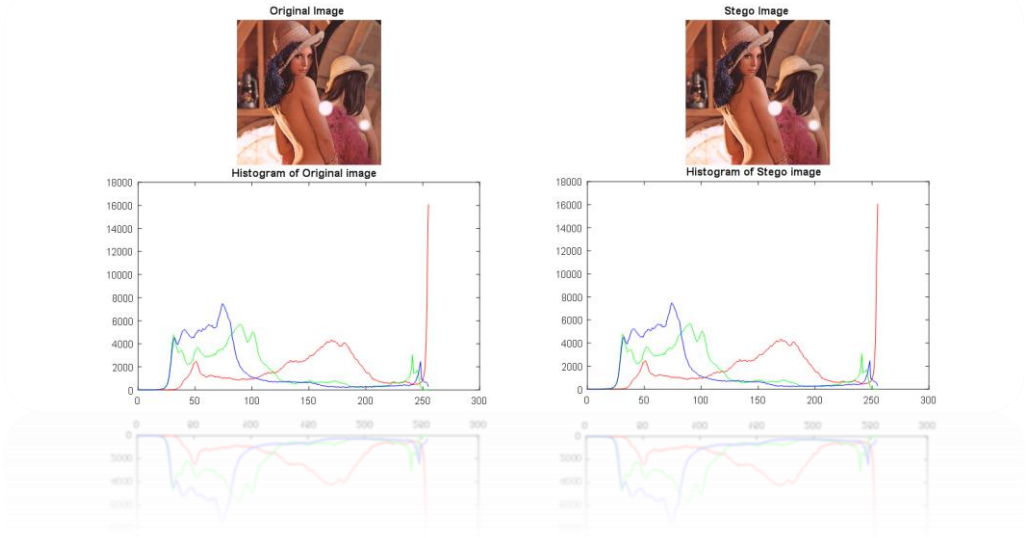
4.1. Хистограмни анализи.



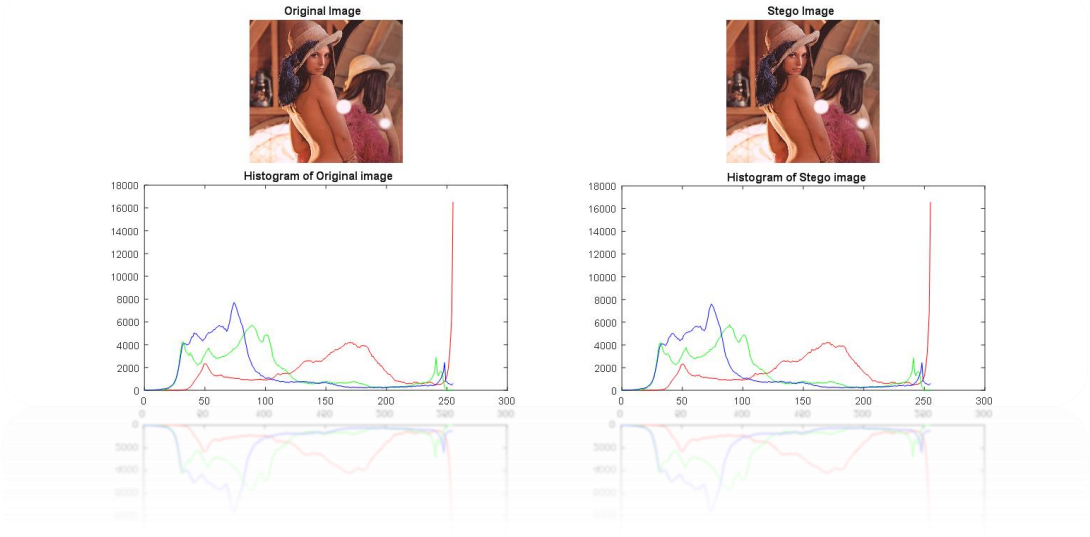
Фиг.*1 Хистограмен анализ (Lena.bmp,100b , Invisible secrets 4)*



***Фиг.**2 Хистограмен анализ (Lena.bmp,100b , Master Stego)*



***Фиг.**3 Хистограмен анализ (Lena.bmp,100b , Stegano)*



***Фиг.**4 Хистограмен анализ (Lena.bmp,100b , Hide’N’Send)*

Art. 4 - Acknowledgments

В заключение може да се каже, че дори безплатно разпространяваните стеганографски приложения за предаване на конфиденциални данни са достатъчно надеждни и сигурни, за да може да се обменя важна информация, без да се буди подозрение в страничния наблюдател. Препоръчително е те да бъдат сменяни периодично, с цел избягване на стеганализиращите програми. Благодарение на направените изследвания могат да се направят следните изводи за работата на стеганографските системи и да се определят препоръчителни характеристики на използваните прикриващи обекти и конфиденциалните съобщения.

• При вграждане на еднакви по дължина съобщения на латиница в едно и също изображение получените стегоизображения в различните стеганографски системи имат сравнително малка разлика в стойностите на изследваните параметри. Тази закономерност е в полза на изображенията създадени, с помощта на българските стеганографските системи. Но при вграждане на големи по дължина съобщения показанията са в полза на Invisible secrets 4;

• Установено е, че с повишаване на размера на вгражданите данни статистическите характеристики на изображенията се влошават, макар че визуалното качество, се запазва отлично. Това може да доведе до препоръка да се крият и предават данни в малки обеми;

• Хистограмният анализ позволява с просто око да се забележат съществения различия в червената цветова компонента при RGB цветовия модел на изследваните двойки изображения, както и в зелената и синята компонента.

References:

[1] Държавна комисия по сигурността на информацията първоначално обучение сборник лекции (второ допълнено издание) софия, 2015.
[2] Tasheva A., Zh. Tasheva, and Pl. Nakov. 2017. Image Based Steganography Using Modified LSB Insertion Method with Contrast Stretching. In Proceedings of the 18th International Conference on Computer Systems and Technologies (CompSysTech'17ACM, New York, NY, USA, 233-240.
[3] P. Mohan Kumar and K. L. Shanmuganathan,” Developing a Secure Image Steganographic System Using TPVD Adaptive LSB Matching Revisited Algorithm for Maximizing the Embedding Rate”, Journal of Telecommunications and Information Technology, 2/2011
[4] В. Стоянова, „Скриване на информация в изображения “, Монография, Шумен 2017г.
[5] „Spread Spectrum Image Steganography “Lisa M. Marvel, Member, IEEE, Charles G. Boncelet, Jr., Member, IEEE, and Charles T. Retter, Member, IEEE, VOL. 8, NO. 8, AUGUST 1999
[6] Павлова, Ст., Ст. Чанев, Сигурност на данните чрез използване на LSB стеганография и шифърът на Виженер в Андроид устройства, II International Scientific Conference CONFSEC, Borovec, 2018, year 2, issue 2(4), issn print 2603-2945, issn online 2603-2953
[7] Jit Lim (14 December 2010). "Is BER the bit error ratio or the bit error rate?". EDN. Retrieved 2015-02-16
[8] Stoyanova, V., Steganography System that uses the LSB method of embedding information in images, International Scientific Conference, Defense Technology forum 2015, Shumen, pp.186-193, ISSN 2367-7902, http://www.aadcf.nvu.bg/scientific_events/papers/NS_2015.
[9] Stoyanova V., Possibilities of steganography methods for hiding data based on Discrete Cosinus Transformation, international Scientific Conference Science. Education. Innovation, May 2014, Shumen. T. 1-2.Shumen: “Konstantin Preslavsky ”Univ. Press, 2014, ISBN 978-954-577-969-5.
[10] Камарашев, Г., С.Димитрова, Aspects of defence and security resource allocattion, Sibiu 2007
[11] Атанасов, А., Щ. Стоянова, Анализ на мрежовата стеганография, II International Scientific Conference CONFSEC, Borovec, 2018, YEAR 2, ISSUE 2(4), ISSN Print 2603-2945

Stefani S. Georgieva,

ARTIFICIAL INTELLIGENCE: IMPLICATIONS FORARMED FORCES

Stefani S. Georgieva

Faculty of Artillery, Air Defense and Communication and Information Technology, Vasil Levski National Military University, Shumen, Bulgaria, stefi_mnt1@abv.bg

Abstract: The report reviews the possibilities for deploying artificial intelligence systems for the purposes of the armed forces.

Keywords: military information systems, artificial intelligence, armed forces

ИЗКУСТВЕН ИНТЕЛЕКТ – ПРИЛОЖЕНИЕ ВЪВ ВЪОРЪЖЕНИТЕ СИЛИ

Стефани С. Георгиева

Факултет „Артилерия, ПВО и КИС“, НВУ „Васил Левски“, Шумен, България,
stefi_mnt1@abv.bg

Увод

Съвременните високопроизводителни изчислителни технологии и технологиите, свързани със съхранението, защитата, представянето и използването на голям обем от данни позволяват създаването на интелигентни при решаването на задачи, изискващи множество познания в широки области трудно може да се говори за програми, притежаващи гъвкавостта на човешкото мислене. Компютърните системи с изкуствен интелект могат значително да ускорят и да увеличат качеството на обработка, експлоатация и разпространението на информация. Машинното подпомагане на вземането на решение в условията на неопределеност и риск представлява интерес за военните лидери.

Настоящия доклад описани основните характеристики на системите с изкуствен интелект и очертава основните му приложения за целите на отбраната.

3. За изкуствения интелект накратко

Изкуственият интелект (от англ. език - Artificial Intelligence) е дял от информатиката, изучаващ възможностите на изчислителни системи да реализират интелектуални процеси, характерни за хората - анализ на данни, формулиране на решения въз основа на този анализ, откриване на смисъл, обобщаване и самообучение на базата на предишен опит.

В литературата съществуват множество определения на термина „Изкуствен интелект“ без да има общоприето такова. Според едно от тях изкуствения интелект може да се разбира като „способността на компютърната система да изпълнява задачи, които обикновено изискват човешка интелигентност, като визуално възприятие, разпознаване на реч и вземане на решения“ [4].

Човешкият интелект е комплекс от редица разнообразни способности, които могат да бъдат обобщени като способност за разсъждаване, анализ и синтез на информация. За да се твърди, че една компютърна система притежава интелект, тя трябва да притежава следните способности: учене, разсъждения, решаване на проблеми, възприятие и използване на език [7].

3.1.Способност за учене

Според Хърбърт Саймън обучението на компютърната система се заключава в такива промени в системата, които и позволяват при всеки следващ опит да извършва дадена работа по-ефективно, отколкото при предходните опити. Към изкуствения интелект са приложими различни форми на обучение, но най-подходящ за компютърна реализация е методът “проба-грешка”. Пример за използване на такъв подход е компютърна програма за игра на шах, решаваща задача за мат в един ход, която реализира произволни движения на фигурите по дъската, докато не намери решение. Решението с позицията се съхранява, така че следващият път, когато програмата срещне същата позиция, прилага същото решение. Механичното запаметяване на казуси и процедури за обработката им, познато като „обучение чрез наизустяване” - rote learning е сравнително лесно за програмна реализация. По-трудно се решава проблемът с прилагането на миналия опит в аналогично нови ситуации.

3.2.Възприятие

Изкуственото възприятие се състои в сканиране на средата с помощта на различни сетивни органи (сензори), а сцената се разлага на отделни обекти в различни пространствени отношения.

3.3.Използване на език

Езикът е система от знаци с предварително дефинирано значение. Важна характеристика на човешките езици е тяхната производителност, която се изразява във възможността за формулиране на неограничено разнообразие от изречения. Създаването на компютърни програми, които в силно ограничен контекст реагират свободно на въпроси и изявления на човешки език е сравнително лесно. Те биха могли да се самоусъвършенстват до степен, че владеенето им на език да не се различава от това на нормалния човек.

3.4. Вземане на решение

Разсъждението се състои във формулирането на изводи от определена ситуация. Вземането на решение може да се разглежда като систематично търсене в пространството на възможните действия, с оглед постигне на предварително определена цел или решение. Постигнат е значителен успех в програмирането на компютри за извличане на дедуктивни заключения.

Съществуват специализирани методи и методи с общо предназначение. Методите със специално предназначение са пригодени за решаването на конкретен проблем и са съобразени с редица специфични характеристики, докато универсалните са приложими за решаване на голямо разнообразие от проблеми.

Процедурите за вземане на самостоятелно решение от системите с изкуствен интелект се осъществяват чрез два основни подхода – конвенционален, който използва методи за самообучение на машината, основани на специален формализъм и статистически анализ и изчислителен, който се свързва с използване на интерактивно обучение на системите с изкуствен интелект, основано на емпирични данни и асоциирани с тях "гъвкави" изчисления. На основата на конвенционалния подход са изградени:

- Експертни системи: програми, които работят по определени правила, обработват голямо количество информация и в резултат извеждат заключение по нея.
- Разсъждение на основата на аналогични случаи (англ. Case-based reasoning).
- Вероятностни (Бейсови) мрежи (Belief Networks).
- Дърво на решенията
- Поведенчески подход: модулен метод за изкуствен интелект, при който системата се разделя на няколко сравнително автономни програмни поведения, които се задействат в зависимост от измененията във външната среда.

На основата на изчислителния подход са архитектури като:

- Невронни мрежи: системи с отлични способности за разпознаване.
- Системи с размита логика (от англ. Fuzzy Logic): методи за разсъждение в условия на неопределеност.
- Системи с еволюционни и генетични алгоритми: тук се използват понятия, свързани основно с биологията, като популация, мутация и естествен подбор за усъвършенстване на решенията в задачите. Тези изчисления се делят на еволюционни алгоритми, генетически алгоритми и методи на „сборен“ интелект (например, „мравешки“ алгоритъм).
- Обучение с утвърждение: Група от методи за автоматично обучение, отличаващи се със способността си да функционират без необходимост от примерни решения на поставения проблем.

Всички тези методи се характеризират с отлични способности за разпознаване, могат да разсъждават в условия на неопределеност и функционират без необходимост от примерни решения на поставения проблем.

4. Приложение на изкуствения интелект в областта на сигурността и отбраната

В редица области на науката и практиката – медицина, телекомуникации, транспорт, промишленост и производство, селско стопанство, банкиране, сигурност и др. са вече разработени и внедрени системи с изкуствен интелект, които са усъвършенствани до ниво, което може адекватно да замести човешки дейности при изпълнение на редица специфични задачи от различно естество.

Продуктите и услугите на изкуствения интелект обединяват множество дисциплини:

- Разпознаване на образи.

Разпознаването на образи обединява методи и средства за възприемане на обектите от околния свят: определяне на пространствените координати, ориентацията, количествените и качествените характеристики на триизмерни обекти от разстояние, разпознаване на ръкописен и печатен текст, оптическо разпознаване на символи, разпознаване на лица. Разпознаване на тактилни образи – образи, възприети при допир на ръката. Широко се прилага в медицината за диагностика на заболявания.

- Машинно зрение, виртуална реалност и обработка на изображения;
- Разпознаване и обработка на естествен език, автоматичен превод;
- Автоматизирани разсъждения;
- Представяне на знания;
- Машино обучение;
- Роботика;
- Стратегическо планиране;
- Диагностика;
- Изкуствен интелект в игрите и ботове в компютърните игри[35]
- Изкуствено творчество[36]

4.1. Роботика

[35] Изкуствен интелект е в състояние да създава игри. Компанията Emotion AI на Affectiva е създала софтуер, който идентифицира ключовите елементи на лицето и чрез алгоритми за дълбоко обучение се анализират и декодират израженията на лицето и съответните емоции. В даден момент е възможно да бъдат създадени "наистина интелигентни" виртуални персонажи, които да заменят сегашното поколение статични и предварително програмирани герои. Компанията Ubisoft прогнозира, че гейм дизайнът на бъдещето може да се състои само в това творецът да скицира нещо простичко като терен и да остави AI да го запълни с детайли.

[36] Компанията Botnik Studios е направила опит за създаване на нова книга от поредицата „Хари Потър“. Използвани са ботове, които предварително са анализирали текстовете от предходните седем книги.

Изкуственият интелект е основна технология в роботизираните автономни системи, които изпълняват военни задачи, свързани с висока степен на риск - например унищожаване на експлозиви; противоминна дейност на сушата или под вода, спасителни мисии, логистична поддръжка и дори бойни действия.

Роботи могат да се използват и за изпълнение на рутинни, „скучни“ и често повтарящи се действия, като по този начин се освобождават човешките ресурси за задачи, изискващи по-високи познавателни функции.

4.2. Разпознаване на образи

В сферата на сигурността и отбраната шикоко приложение намират функциите, свързани с разпознаване на образи:

- Във военното дело за: определяне на вида, принадлежността и степента на заплаха от страна на такива обекти като превозни средства, бойни машини, летателни апарати и други; автоматично откриване и разпознаване на целите.
- В работата на специализираните служби при предотвратяване на терористични акции, наркотрафик и ограничаване на престъпността. Пример за това са системите за разпознаване налица по данни от видеоконтрола на обществените места с потенциална опастност от атентати, за разпознаване на отпечатъци при граничен контрол и търсене на улики на престъпления. Тези методи за разпознаване на образи се прилагат успешно в условия на лоша видимост от охранителни и сателитни системи с военно и гражданско предназначение.

4.3. Извличане на знание

Способността на системите с изкуствен интелект за извличане на знание (от англ. Data mining) се изразява във възможността им за откриване на смислени корелации, зависимости, повтарящи се образци (от англ. patterns), тенденции и аномалии в големи масиви от данни, съхранявани в складове чрез използване на техники и алгоритми от областта на машинното обучение, разпознаването на образи, статистиката, невронните мрежи и визуализацията на данни.

За целите на сигурността и отбраната тя може да се използва за откриване и противодействие на заплахи за сигурността от всякакво естество. Пример за това е разработената от Defense Advanced Research Projects Agency (DARPA) електронна система за противодействие Chaff Electronic Countermeasure System [5], която е предназначена за автоматично откриване на противников реактивен снаряд в зоната около плавателен съд, изчисляване на траекторията му и изстрелване на отклоняващи ракети, които го насочват по друга изчислена траектория далеч от кораба. Тази система анализира, взема решение и предприема действия значително по-точно и по-бързо от изключително добре обучен и натрениран екипаж. В софтуера са вградени различни режими за отклоняване на входящите ракети, включително „подмамване”, „разсейване” и „объркване”, за чието използване системата автоматично взема решение в зависимост от поведението на кораба, наличните ракети и други фактори.

Друг софтуер за извличане на данни, създаден от DARPA, не се използва пряко в бойните действия, а в медицинската област. Приложението анализира споделена база данни, използвана от медицинските центрове на военновъздушните сили, сухопътните и военноморските сили (на англ. Joint Medical Asset Repository) и определя необходимостта им от медицински консумативи и подпомага снабдяването им.

4.4. Вземане на решение

Следващата функция на системите с вграден изкуствен интелект, която намира широко приложение за целите на отбраната е автоматизирано вземане на решение.

Информационните системи, чието предназначение е автоматизирано вземане на решение се обединяват под общото наименование „Системи за подпомагане на вземането на решение”. DSS

системите (от англ. Decision Support System) се числят към групата на информационно – решаващите и представляват специализиран софтуерен инструмент, който позволява трансформирането на неструктурирани данни в детайлни справки и анализи, като например предсказване на бойни загуби, осигуряване на оценка на щетите и др. чрез използване на подходящо алгоритмизирани методи за предсказване на ефекти, методи за оценка на последствията, методи за поддържане на проверими алгоритми за вземане на решения и др.

Системите за подпомагане на вземането на решения може да подобри времето за реакция на отбранителните системи срещу бързодействащи оръжейни системи, като хиперзвукови ракети, кибератаки или оръжия с насочена енергия; да способства за бързо откриване на киберпосегателства чрез откриване на уклончиви злонамерени кодове или чрез сканиране на подозрителни модели на поведение, а не на конкретен код; за идентифициране на опити за манипулиране на гражданите чрез кампании за дезинформация [6].

Този род системи могат да съществуват като самостоятелни приложения или да бъдат вградени в системи за Командване, управление, комуникации, компютри, наблюдение и разузнаване (от англ. Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance - C4ISR).

Трябва да се подчертае също, че системите с изкуствен интелект могат да намерят приложение в подкрепа на усилията за преодоляване на едно сериозно предизвикателство, което съществува не само в областта на отбраната, а във всяка област на човешката дейност, която е автоматизирана - липсата на съвместимост на информационните системи.

5. Роля на системите с изкуствен интелект при оценяването на степента на съвместимост на информационни системи

Несъвместимостта между информационните системи се изразява в невъзможността те, или отделни техни компоненти да обменят своевременно и ефективно данни, информация или знание, и да използват обменените данни, иформация или знание. [1] Тя се се обуславя от много фактори: липса на съвместимост между апаратните средства породена от използването на различни или различни версии на информационните и комуникационните стандарти и протоколи за комуникация, различия по отношение на размера и формата на данните, несъгласуваност по отношение на интерпретацията на данните.

Системите с изкуствен интелект не могат да въздействат пряко върху посочените тези фактори, но могат да намерят приложение при определяне на степента на съвместимост между две или и повече информационни системи, което е неотменна част от процеса на интеграция.Те могат автоматично да предложат решение otnosno промяна на параметрите на системите с оглед повишаване на способността им да обменят информация и да използват обменената информация, така че да работят съвместно в името на обща цел, когато е необходимо [2].

Оценката на съвместимостта на две или повече информационни системи е резултат от измерване на сходството между голям брой техни характеристики, които влияят пряко върху способността им за комуникация и взаимодействие с други системи. [2]. Задачата за теоретично измерване и оценяване на съвместимостта между информационни системи се характеризира с:

- многоразмерност, която се дължи на голямото количество данни, които трябва да бъдат анализирани;
- неоднозначност на решението, която е следствие от субективността на експерта при тълкуване на критериите за оценка и при при определяне на степента на сходство по различните показатели [3].

Поради тази причина средствата на размитата логика се оказват подходящи за моделиране на съвместимостта на информационните системи и построяване на модел на приближени разсъждения, каквито са разсъжденията на експерта. Такъв модел може да се реализира програмно и да се имплементира в компютърна система.

Изводи

Използването на системи с изкуствен интелект за целите на отбраната вече е реалност. Използването им може да подобри качеството на вземане на решения от отговорните лица и да осигури решаващо предимство пред противника.

Прилагането на ИИ за целите на отбраната е перспективно направление за научни изследвания.

Литература

1. Ламбева, М. Х. (2017). Съвместимост на информационните системи за управление. Възможности за оценяван. *Collection of papers, International Scientific Conference "Defense Technology Forum 2017"* (pp. 342 – 348). Shumen, Bulgaria: "Vasil Levski" National Military University - "Artillery, Aircraft Defense and CIS" Faculty, ISSN 2367-7902

2. Ламбева, М. Х. (2017). Модел на *съвместимостта на информационните системи за управление. Collection of papers, International scientific conference "Defense Technology Forum 2017*" (pp. 349 – 355) Shumen, Bulgaria: "Vasil Levski" National Military University - "Artillery, Aircraft Defense and CIS" Faculty, ISSN 2367-7902

3. Ламбева, М. Х. (2017). Размит модел за оценяване на оперативната съвместимост на информационните системи. *Collection of papers, International Scientific Conference "Defense Technology Forum 2017"* (pp. 356 - 361). Shumen, Bulgaria: "Vasil Levski" National Military University - "Artillery, Aircraft Defense and CIS" Faculty, ISSN 2367-7902

4. Cummings, M. et al. (2018), Artificial Intelligence and International Affairs: Disruption Anticipated, Chatham House

5. Lyvon T., Data Mining in the Military, Retrieved from http://misclassblog.com/data-analytics/data-mining-in-the-military/

6. Tonin (2019) - Stctts Report - Artificial Intelligence - 088 Stctts 19 E: Nato Pa. Retrieved from https://nato-pa.int/document/2019-stctts-report-artificial-intelligence-tonin-088-stctts-19-e

7. Copeland, B.J. Artificial Intelligence, Retrieved from https://www.britannica.com/technology/artificial-intelligence

Aleksandar D. Kumanov, Gancho H. Hristev,

RFID MODULE INTERFACING WITH ARDUINO UNO

Aleksandar D. Kumanov*, Gancho H. Hristev**

*Department of Communication Networks and System Faculty of Artillery, Air Defence and CIS, National Military University "Vasil Levski", Shumen,Bulgaria, *akumanov13@gmail.com, **gancho.hristev@gmail.com*

***Abstract**: In this article, learning RFID Arduino interfacing using MFRC522 RFID Reader with the help of two examples is proposed. The first example is a simple Arduino RFID Reader and the second one is an Arduino RFID Door Lock.*

***Keywords**: Arduino UNO, RFID, MFRC522*

УПРАВЛЕНИЕ НА RFID МОДУЛ С ARDUINO UNO

***Александър Д. Куманов, **Ганчо Х. Христев**

*Национален военен университет „В. Левски"
Факултет „А, ПВО и КИС", Шумен, България, *akumanov13@gmail.com, **gancho.hristev@gmail.com*

Въведение

Платформата Arduino намира все по – широко приложение при обучението на студенти в областта на инженерните науки [1],[2]. Обучението се основава на практически експерименти с различни сензори, индикатори, изпълнителни механизми и модули.

В настоящия доклад е предложен вариант на система за контрол на достъпа базирана на Arduino Uno и RFID модул MFRC522. Системите за контрол на достъпа са основен елемент от системите за наблюдение и контрол [3].

Радиочестотна идентификация (RFID)

RFID (Radio Frequency Identification) е технология за идентификация базирана на радиочестотна комуникация (125 kHz, 13,56 MHz и т.н.).

Основно RFID система се състои от две части: идентификатор (tag) и четец на идентификатора.

RFID се характеризира с бързодействие и липсата на пряк контакт между четеца и идентификатора, като комуникацията се извършва от разстояние.

RFID идентификатор

RFID идентификаторът (Фиг 1) съдържа интегрална схема, в която се съхранява информация и антена, с която се получава и изпраща сигнал. RFID идентификатори от стандарта Mifare обикновено имат памет с обем 1KB, която е достатъчна за запис на име, номер на кредитна карта, уникален идентификационен номер, дата на раждане или друга информация.

Фигура 1: Видове RFID идентификатори

RFID идентификаторите могат да бъдат активни и пасивни. Паснвният идентификатор няма нужда от батерия и използва енергията предадена от четеца. Активният идентификатор съдържа вградена батерия, която позволява на идентификатор да предава сигнал на разстояния до 30 метра.

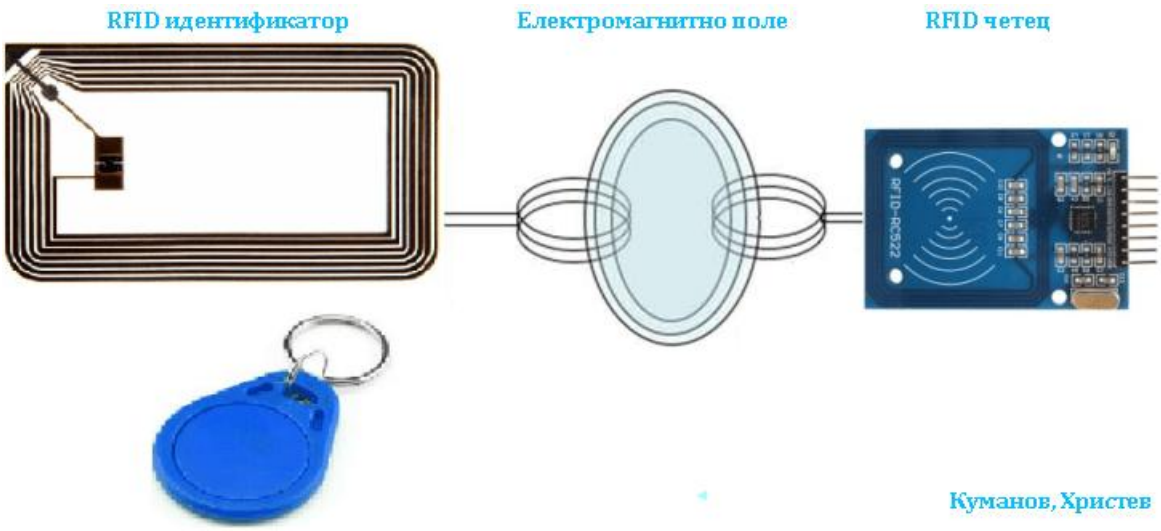
RFID четец

RFID четецът (Фиг 2) изпълнява две функций – изпраща и приема данни. Още наречан трансийвър, RFID трансийвърът съдържа антена, радиочестотен модул и контролен модул.

Фигура 2: RFID трансийвър.

Принцип на работа на RFID

RFID четецът генерира високочестотно електромагнитно поле и когато идентификаторът бъде приближен към трансийвъра в намотката на антената му се индуцира напрежение. Това индуцирано напрежение служи като източник на захранванне за RFID идентификатора. идентификаторът от своя страна отговаря на четеца като изпраща записаните в паметта му данни (Фигура 3).



Фигура 3: Принцип на действие на RFID

RFID интерфейс и Arduino

В тази част на доклада е описан интерфейсът между RFID модул MFRC522 и Arduino Uno. RFID четецът комуникира с Arduino Uno през SPI протокол. Модулът работи на честота 13.56 MHz.

Идентификаторите са базирани на протокола MIFARE и разполагат с 1kb памет.

Използваните материали са:

- Arduino UNO;
- MFRC 522 RFID модул;
- I2C LCD дисплей;
- LED светлини 3 броя;
- Серво мотор Sg90;
- 3 резистора 220 ohm
- Бъзер

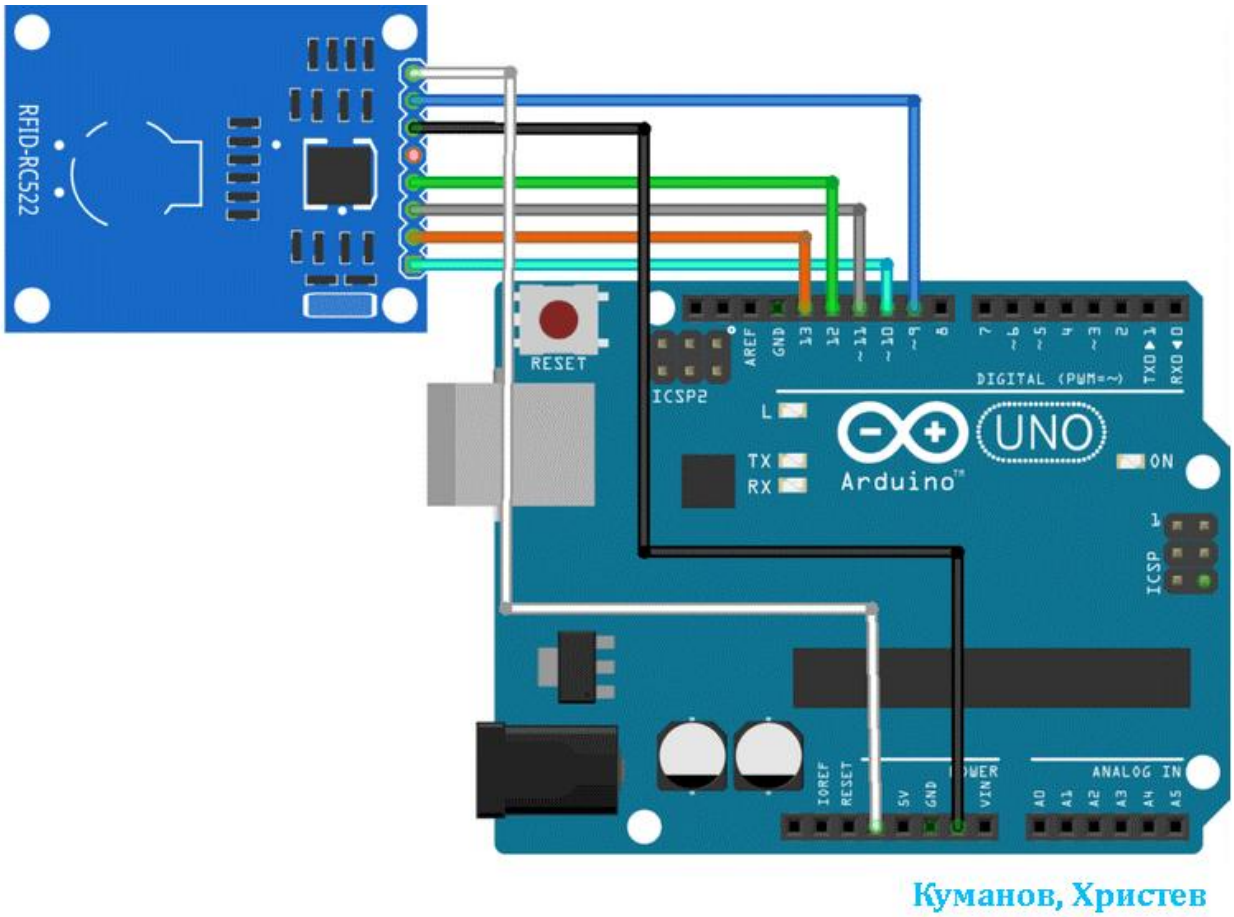
Arduino Uno RFID четец

В първият пример е описан Arduino Uno базиран RFID четец, който прочита информация от Mifare идентификатор, която в последствие се показва чрез вградения в Arduino IDE сериен монитор (Serial monitor). Свързването на MFRC522 модулът към различни варианти на Arduino е показано в Таблица 1 [5].

Таблица 1

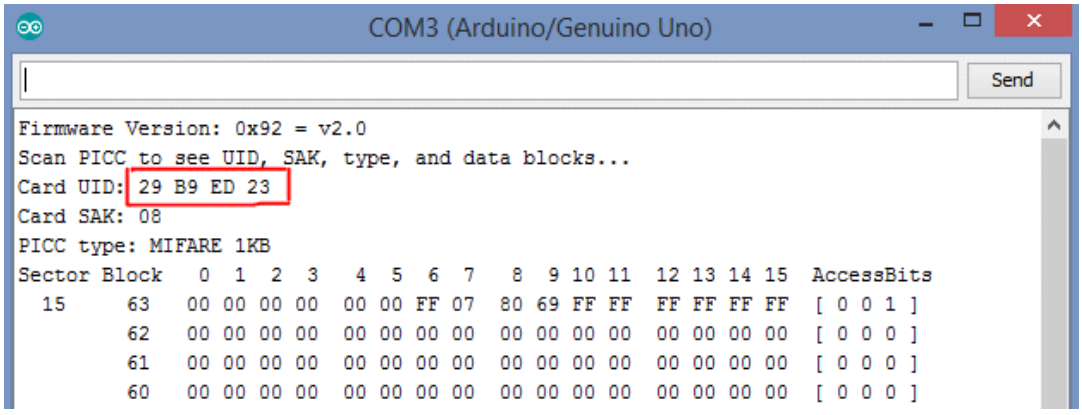
MFRC522	Arduino Uno	Arduino Mega 2550	Arduino Nano V3	Arduino Leonardo/Micro	Arduino Pro Micro
3,3V	3,3V	3,3V	3,3V	3,3V	3,3V
RST	9	5	9	RESET?/ICSP5	RST
GND	GND	GND	GND	GND	GND
NC	NC	NC	NC	NC	NC
MISO	12/ICSP-1	50	12	12/ICSP-1	14
MOSI	11/ICSP-4	51	11	ICSP-4	16
SCK	13/ICSP-3	52	13	ICSP-3	15
SDA	10	53	10	10	10

На фигура 4 е показана схемата на свързване на Arduino UNO и модулът MFRC522.



Фигура 4. Схема на RFID четец

След свързване на гореспоменатите компоненти и въвеждане на програмният код се отваря серийният монитор. След доближаване на RFID идентификатора пред четецът, на серийният монитор се изобразява информацията, която е записана в паметта му (Фигура 5). На фигурата е отбелязан UID кодът, тъй като ще бъде използван в следващият пример.



Фигура 5. Съдържание на паметта на идентификатор с UID 29 B9 ED 23

На фигура 5 освен UID номерът на идентификатора е изобразено и съдържанието на паметта. Паметта е с обем 1Kb разделена на 16 сектора. Всеки сектор има 4 блока като всеки блок съхранява по 4 байта.

Система за контрол на достъпа

Вторият пример описва система за контрол на достъпа базирана на Arduino Uno и RFID модул MFRC522. Системата включва още: конвертор I2C – Parallel bus, LCD модул 16 знака – два реда, светодиодна индикация и сервомотор като изпълнителен механизъм. Свързването на LCD модулът и останалите компоненти е описано в таблици 2 и 3.

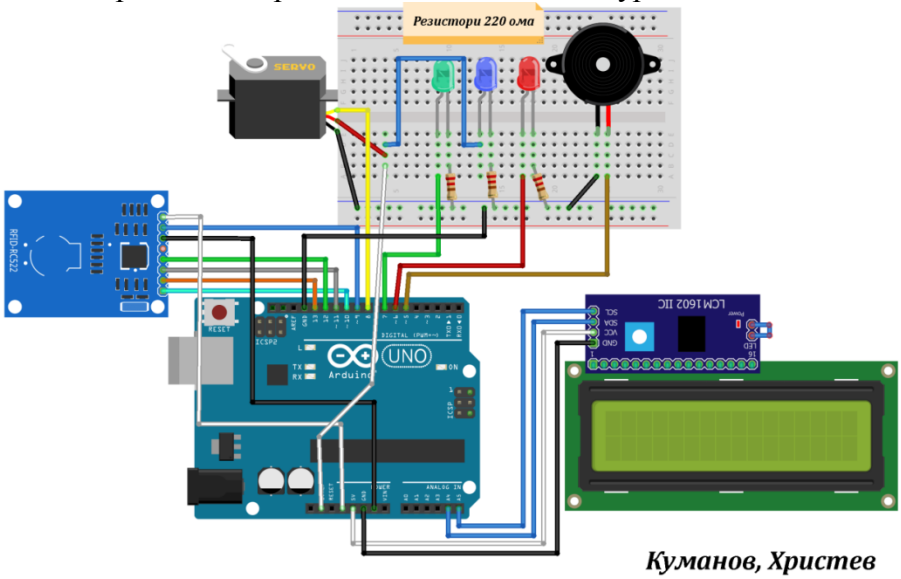
Таблица 2

I2C LCD	Arduino Uno	Arduino Mega 2550	Arduino Nano V3	Arduino Leonardo/Micro	Arduino Pro Micro
SCL	A5/SCL	21	A5	3/4	3
SDA	A4/SDA	20	A4	2/3	2
GND	GND	GND	GND	GND	GND
VCC					

Таблица 3

Arduino	Светодиоди	Сервомотор	Бъзер
5V	Син	Червен кабел (+)	
D8		Жълт кабел (управляващ сигнал)	
D7	Зелен		
D6	Червен		
D5			+
GND	Катоди през съпротивление 220 Ома	Кафяв кабел (GND)	-

Завършената диаграма на свързване е показана на Фигура 6.



Фигура 6.

Програмен код

Основен сегмент от програмния код на RFID система за контрол на достъпа е алгоритъмът за търсене на идентификатори. Предназначението му е при поднесен идентификатор да сканира паметта за оторизирани идентификатори и при съвпадение да издаде съобщение, че е представен оторизиран такъв. От скоростта на работа на алгоритъма зависи и скоростта на работа на цялата система. При неголям брой идентификатори се използва последователно сканиране на паметта. При голям брой идентификатори се използват алгоритми базирани на Хеш таблици [4].

В предложеният RFID четец е заложен алгоритъм за последователно сканиране на паметта (редове 54 – 92), като в ролята на памет за оторизиране на идентификатори се използват стринго-ве, в които е записан UID на всеки оторизиран идентификатор (ред 18).

Пълният програмен код е:

```
1.  // Необходими библиотеки
2.  #include <LiquidCrystal_I2C.h>
3.  #include <SPI.h>
4.  #include <MFRC522.h>
5.  #include <Servo.h>
6.
7.  // Дефиниране на инстанции
8.  LiquidCrystal_I2C      lcd(0x27, 16, 2);
9.  MFRC522                mfrc522(10, 9); // MFRC522 mfrc522(SS_PIN, RST_PIN)
10. Servo                  sg90;
11.
12. // Инициализиране на изходи светодиоди, сервомотор, бъзер
13. constexpr uint8_t greenLed = 7;
14. constexpr uint8_t redLed = 6;
15. constexpr uint8_t servoPin = 8;
16. constexpr uint8_t buzzerPin = 5;
17.
18. String tagUID = "29 B9 ED 23"; // Стринг съдържащ идентификатор на разрешеният таг
19.
20. void setup() {
21.       // Конфигуриране пиновете на Arduino
22.       pinMode (buzzerPin, OUTPUT);
23.       pinMode (redLed, OUTPUT);
24.       pinMode (greenLed, OUTPUT);
25.
26.       sg90.attach(servoPin);      // Асоцииране на пин9 със сервомотор
27.       sg90.write(0);              // Установяване на начална позиция на сервомотора 90 градуса
28.
29.       lcd.begin();                // Инициализиране на LCD
30.       lcd.backlight();
31.       SPI.begin();                // Инициализиране на SPI шина
32.       mfrc522.PCD_Init();         // Инициализиране на MFRC522
33.
34.       lcd.clear();
35. }
36.
37. void loop() {
38.      lcd.setCursor(0, 0);
39.      lcd.print(" RFID Door Lock");
40.      lcd.setCursor(0, 1);
41.      lcd.print(" Show Your Tag ");
42.
43.     // Проверка за поднесен таг
44.     if  ( ! mfrc522.PICC_IsNewCardPresent()) {
45.          return;
46.     }
47.
```

```
48.      // Избор на таг
49.     if  ( ! mfrc522.PICC_ReadCardSerial()) {
50.         return;
51.     }
52.
53.      //Четене от таг
54.     String tag = "";
55.     for  (byte i = 0; i < mfrc522.uid.size; i++)
56.        {
57.         tag.concat(String(mfrc522.uid.uidByte[i] < 0x10 ? " 0" : " "));
58.         tag.concat(String(mfrc522.uid.uidByte[i], HEX));
59.        }
60.     tag.toUpperCase();
61.
62.     //Проверка на UID
63.     if  (tag.substring(1) == tagUID)
64.       {
65.         // UID съвпада
66.         lcd.clear();
67.         lcd.setCursor(0, 0);
68.         lcd.print("Access Granted");
69.         lcd.setCursor(0, 1);
70.         lcd.print("Door Opened");
71.         sg90.write(90);
72.         digitalWrite(greenLed, HIGH);
73.         delay(3000);
74.         digitalWrite(greenLed, LOW);
75.         sg90.write(0);
76.         lcd.clear();
77.       }
78.         else
79.         {
80.           // UID не съвпада.
81.          lcd.clear();
82.          lcd.setCursor(0, 0);
83.          lcd.print("Wrong Tag Shown");
84.          lcd.setCursor(0, 1);
85.          lcd.print("Access Denied");
86.          digitalWrite(buzzerPin, HIGH);
87.          digitalWrite(redLed, HIGH);
88.          delay(3000);
89.          digitalWrite(buzzerPin, LOW);
90.          digitalWrite(redLed, LOW);
91.          lcd.clear();
92.        }
93. }
```

Заключение

В доклада са представени два практически експеримента базирани на Arduino Uno и RFID модул MFRC522. Реализираните експерименти могат да бъдат използвани при обучението на студенти в областта на инженерните науки и системите за физическа сигурност.

Референции

1. Чобанов Д. Г., “Using Geniuno zero ARM based platform in computer arcitecture courses” SocioBrains, International Scientific Refereed Online Journal With Impact Factor, Issue 59, July 2019, pp. 114 – 117, ISSN 2367-5721

2. Чобанов Д. Г., “Using Arduino based experiments in computer programming education”, International Scientific Refereed Online Journal With Impact Factor, Issue 60, August 2019, pp. 61 – 63, ISSN 2367-5721

3. Чобанов Д. Г., “Интегрирана система за наблюдение и контрол” Сборник научни трудове MATTEX 2018, с. 68 – 73, Университетско издателство “Епископ Константин Преславски” - ISSN: 1314-3921

4. Чобанов Д. Г., “Алгоритъм за бързо търсене на идентификатори в система за контрол на достъпа” Сборник научни трудове MATTEX 2018, с. 74 – 78, Университетско издателство “Епископ Константин Преславски” - ISSN: 1314-3921

5. Aqib M., October 31, 2018, “RFID Based Access Control System Using Arduino”, Retrieved from: https://www.hackster.io/muhammad-aqib/rfid-based-access-control-system-using-arduino-de5359

Gancho H. Hristev, Aleksandar D. Kumanov,

CONTROLLING 12 LEDS WITH ARDUINO UNO

Gancho H. Hristev*, Aleksandar D. Kumanov**

*Department of Communication Networks and System Faculty of Artillery, Air Defence and CIS, National Military University "Vasil Levski", Shumen,Bulgaria, *gancho.hristev@gmail.com, **akumanov13@gmail.com*

***Abstract**: Charlieplexing is a technique of controlling many LEDs using a few I/O pins. Charlieplexing is same as multiplexing, but it uses the tri-state logic (high, low input) to reduce the number of pins dramatically and to gain efficiency over multiplexing. The Charlieplexing technique is named after its inventor, Charlie Allen, who invented the technique in 1995.*

***Keywords**: Charlieplexing, Arduino Uno, LED*

УПРАВЛЕНИЕ НА 12 СВЕТОДИОДА С ARDUINO UNO

***Ганчо Х. Христев, **Александър Д. Куманов**

*Национален военен университет „В. Левски" Факултет „А, ПВО и КИС", Шумен, България, *gancho.hristev@gmail.com, **akumanov13@gmail.com*

Въведение

Arduino е проект с отворен код и едноименна компания, произлязла от него, както и свързаното с него потребителско общество. Основната цел е проектиране и производство на електронна платформа с лесен за ползване свободен хардуер и софтуер, позволяващи постигането на интерактивност за специалисти и неспециалисти. Благодарение на заложените характеристики и ниска цена платформата Arduino Uno навлиза все по – широко в обучението на студенти в областта на компютърните науки (програмиране, компютърни архитектури и т.н.) [1], [2].

В доклада е предложен вариант за управление на светодиоди чрез Arduino Uno, с помощта на който се изучава технологията Charliplex [3].

Charlieplexing е технология, която позволява управлението на $N * (N - 1)$ светодиоди , където N е броят на управляващите дигитални изходи. Така с 4 пина на Arduino Uno, дефинирани като дигитални изходи има възможност да се управляват 12 светодиода (4 * (4 – 1) = 12). Методът се основава на едностранната проводимост на светодиодите. За целта дванадесетте светодиода се свързват по двойки в паралел, но с противоположна полярност. Управлението на светодиодите във всяка двойка се осъществява чрез смяна полярността на управляващото напрежение. По този начин при подаване на напрежение към съответната двойка с определена полярност свети единият от тях.

В доклада са описани хардуерната и софтуерна реализация на вариант на използване на технологията Charlieplexing, при който се управляват дванадесет светодиода.

Необходими компоненти:

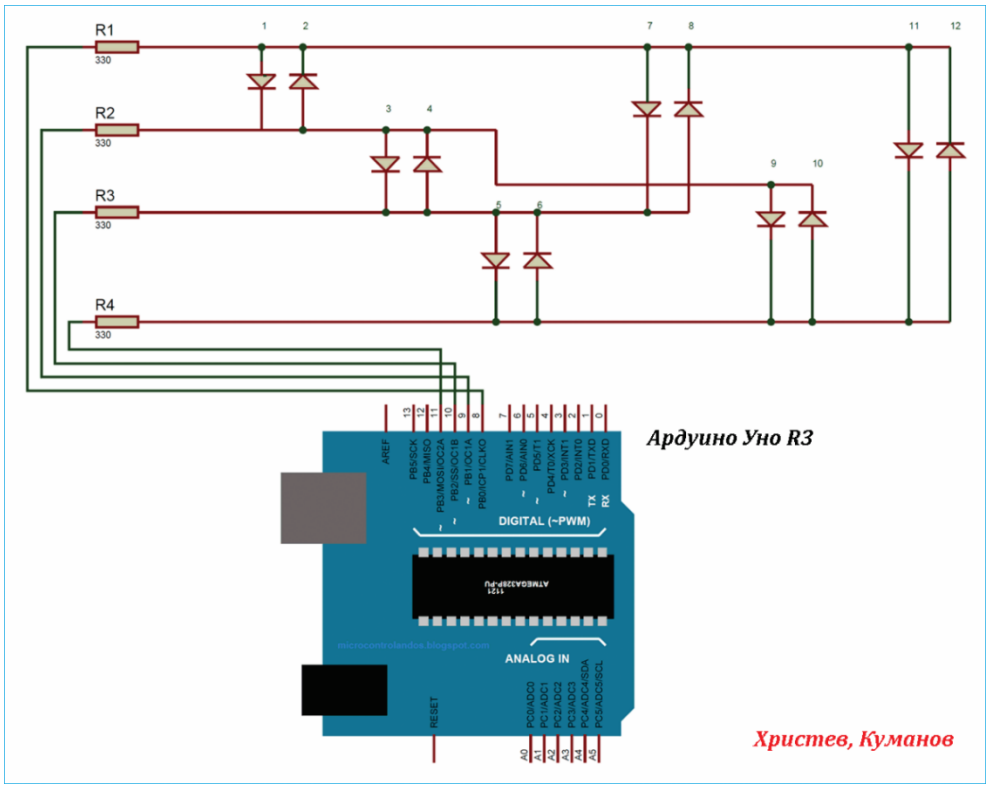
- Arduino Uno
- Светодиоди – 12 броя
- Резистор 240 Ома – 4 броя
- Проводници – 4 броя
- Бредборд – 1 брой

Технически характеристики на Arduino UNO

- Микроконтролер ATmega328P
- Работно напрежение – 5v
- Входно напрежение – 7 до 12v
- Тактова честота CLK – 16 Mhz
- Флаш памет – 32 KB
- SRAM – 2 Kb
- EEPROM – 1 Kb

Изложение

На фигура 1 е представена схемата на свързване на необходимите за реализация на проекта компоненти.



Фигура 1: Схема на свързване

На фиг. 1 дванадесет светодиода са свързани с 4 Arduino изхода чрез резистори за ограничаване на тока. Всеки от пиновете на Arduino е свързан с три светодиода. Има шест групи светодиоди и във всяка група са включени 2 светодиода като и двата светодиода са успоредни един на друг, но с противоположна полярност, така че едновременно да се включва само един светодиод. Така, за включване на LED 1, е необходимо да има ВИСОК потенциал на пин A и НИСЪК потенциал на пин B, а пинове C и D трябва да бъдат изключени. Същата процедуре се спазва и за останалите светодиоди. Пълната таблица с настройки на пиновете за всеки светодиод е дадена по-долу:

LED	PIN8	PIN9	PIN10	PIN11
1	HIGH	LOW	INPUT	INPUT
2	LOW	HIGH	INPUT	INPUT
3	INPUT	HIGH	LOW	INPUT
4	INPUT	LOW	HIGH	INPUT
5	INPUT	INPUT	HIGH	LOW
6	INPUT	INPUT	LOW	HIGH
7	HIGH	INPUT	LOW	INPUT
8	LOW	INPUT	HIGH	INPUT
9	INPUT	HIGH	INPUT	LOW
10	INPUT	LOW	INPUT	HIGH
11	HIGH	INPUT	INPUT	LOW
12	LOW	INPUT	INPUT	HIGH

Описание на програмата

В началото на програмата се дефинират всички пинове към които се свързват светодите, броят им и състоянието на пиновете. Кода е следният:

```
#define A 8
#define B 9
#define C 10
#define D 11
#define PIN_CONFIG 0
#define PIN_STATE 1
#define LED_Num 12
```

Създава се матрица за включване и изключване на светодиодите в последователност. В матрицата се предвижда първо да се включи LED1, след него LED2 и т.н. Кода за управление на LED 1, който следва да се въведе е следният:

```
Int matrix[LED_Nun][2][4] = {
  //                PIN_CONFIG                        PIN_STATE
  //      A          B          C          D          A        B       C       D
  {{ OUTPUT, OUTPUT, INPUT, INPUT}, { HIGH, LOW, LOW, LOW}}
  {{ OUTPUT, OUTPUT, INPUT, INPUT}, { HIGH, LOW, LOW, LOW}}
}
```

В основния цикъл (void loop) програмата, чрез изпълнение на матрицата (процедурата LightOn) се включват и изключват светодиодите в предвидената последователност.

Пълният код на програмата е следният:

```
#define A 8
#define B 9
#define C 10
#define D 11
#define PIN_CONFIG 0
#define PIN_STATE 1
#define LED_Num 12
int matrix[LED_Num][2][4] = {
  //                PIN_CONFIG                          PIN_STATE
  //        A           B          C          D           A       B       C       D
  { { OUTPUT, OUTPUT, INPUT, INPUT }, { HIGH, LOW, LOW, LOW } },
  { { OUTPUT, OUTPUT, INPUT, INPUT }, { LOW, HIGH, LOW, LOW } },
  { { INPUT, OUTPUT, OUTPUT, INPUT }, { LOW, HIGH, LOW, LOW } },
  { { INPUT, OUTPUT, OUTPUT, INPUT }, { LOW, LOW, HIGH, LOW } },
  { { OUTPUT, INPUT, OUTPUT, INPUT }, { HIGH, LOW, LOW, LOW } },
  { { OUTPUT, INPUT, OUTPUT, INPUT }, { LOW, LOW, HIGH, LOW } },
  { { OUTPUT, INPUT, INPUT, OUTPUT }, { HIGH, LOW, LOW, LOW } },
  { { OUTPUT, INPUT, INPUT, OUTPUT }, { LOW, LOW, LOW, HIGH } },
  { { INPUT, OUTPUT, INPUT, OUTPUT }, { LOW, HIGH, LOW, LOW } },
  { { INPUT, OUTPUT, INPUT, OUTPUT }, { LOW, LOW, LOW, HIGH } },
  { { INPUT, INPUT, OUTPUT, OUTPUT }, { LOW, LOW, HIGH, LOW } },
  { { INPUT, INPUT, OUTPUT, OUTPUT }, { LOW, LOW, LOW, HIGH } }
};
void lightOn( int led ) {
  pinMode( A, matrix[led][PIN_CONFIG][0] );
  pinMode( B, matrix[led][PIN_CONFIG][1] );
  pinMode( C, matrix[led][PIN_CONFIG][2] );
  pinMode( D, matrix[led][PIN_CONFIG][3] );
  digitalWrite( A, matrix[led][PIN_STATE][0] );
  digitalWrite( B, matrix[led][PIN_STATE][1] );
  digitalWrite( C, matrix[led][PIN_STATE][2] );
  digitalWrite( D, matrix[led][PIN_STATE][3] );
}
void setup() {}
void loop() {
  for( int l = 0; l < LED_Num; l++ ) {
    lightOn( l );
    delay( 1000 / LED_Num );
  }
}
```

Заключение

Charlieplexing техниката се използва за управление на голям брой светодиоди, при използването на малко на брой Arduino пинове. Този метод може да се използва за управлението на повече на брой светодиоди като в зависимост от броят им просто се редактира матрицата и се добавят условията за останалите светодиоди.

References

1. Чобанов Д. Г., “Using Geniuno zero ARM based platform in computer arcitecture courses” SocioBrains, International Scientific Refereed Online Journal With Impact Factor, Issue 59, July 2019, pp. 114 – 117, ISSN 2367-5721

2. Чобанов Д. Г., “Using Arduino based experiments in computer programming education”, International Scientific Refereed Online Journal With Impact Factor, Issue 60, August 2019, pp. 61 – 63, ISSN 2367-5721

3. Choudhary A., Aug 06, 2019, “Charlieplexing Arduino - Controlling 12 LEDs with 4 GPIO Pins”, Retrieved from: https://www.instructables.com/id/Charlieplexing-the-Arduino

Mihaela A. Karadocheva, Ekaterina M. Konstantinova, Albena B. Aleksandrova,

SOCIAL NETWORKS AND DIGITAL SECURITY

Mihaela A. Karadocheva [1], Ekaterina M. Konstantinova [2], Albena B. Aleksandrova [3]

[1] Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, Department "Communication and Computer Technologies", mkaradocheva6@gmail.com
[2] Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, Department "Communication and Computer Technologies", katminkova2@gmail.com
[3] Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, Department "Management of Security Systems", alb.alexandrova@abv.bg

***Abstract**: The social networks become more and more frequently used and there are many users all around the world. The social media helps us to connect with each other and make new friends, share everything we want with them, but there are some risks that every user should have in mind and should know how to avoid being a victim of all the possibilities of the Internet.*

***Keywords**: Cyber security, Digital security, Internet, Social networks*

СОЦИАЛНИ МРЕЖИ И ДИГИТАЛНА СИГУРНОСТ

Михаела А. Карадочева, Екатерина М. Константинова, Албена Б. Александрова

1. Въведение

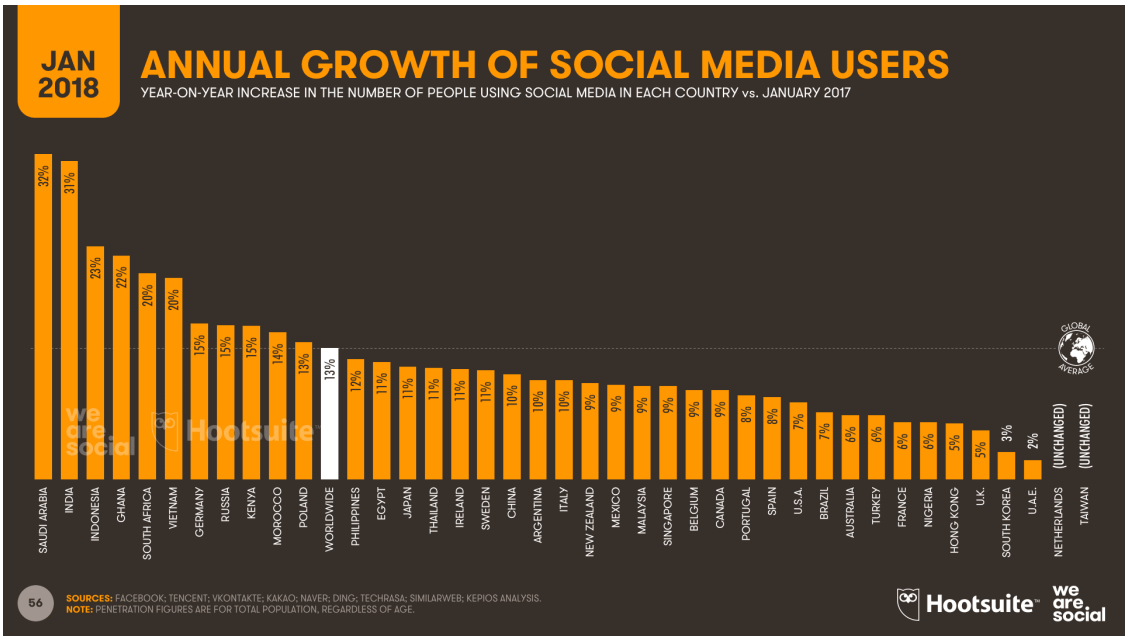
Кибер престъпленията днес са глобален проблем, който се отразява върху много сфери на нашия живот. Почти всичко, което виждаме в нашето ежедневие, вероятно има нужда от кибер-сигурност. Дори когато се разхождаме в парка, наоколо има камери и много дигитални устройства, които могат да бъдат използвани срещу нас, ако за тях не се грижат всеки ден специалисти, повишаващи непрекъснато защитата им. Уязвимостта от дигиталния свят не трябва да причинява параноя, но всеки, който използва привилегиите на модерното време, трябва да знае основите на дигиталната сигурност [1], [2], [5], [8], [9], [12], [13], [14], [15], [16], [21].

2. Изложение

Социални мрежи като Facebook, Instagram и Twitter се разрастват много в последните години. Те позволяват на хората да общуват с техните контакти, да възобновят отношения със стари познати, да създадат нови връзки с други хора, базирани на общи хобита, интереси и кръгове от хора. През последните години се наблюдава огромен ръст в използването на социалните мрежи, като общо се събира информация за над половин милиард регистрирани потребители (Фиг. 1). Като резултат, социалните мрежи съхраняват огромно количество лична информация за потреби-

телите и техните действия. Популярността на социалните мрежи привлича не само честни потребители, но и други лица, имащи по-различни намерения. Неизбежен е риска от нарушаване на поверителността на всички потребители в резултат на обмена на информация и споделянето в Интернет [1], [2], [5], [17], [18], [19], [20].

Независимо от идеята на социалните мрежи, една от главните причини за потребителите да се регистрират, създадат профил и да използват различни приложения е възможността лесно да споделят информация с определени контакти или публично. Разкриване на лична информация в интернет пространството е опасно, тъй като това може да доведе до злонамерени атаки в реалния и интернет световете като преследване, клеветене, имейл спам и други. Независимо от рисковете, много от контролните механизми за достъп и поверителност са умишлено отслабени, за да направят лесно присъединяването към социална мрежа и споделянето на информация.



Фигура 1: Ръст в използването на социални мрежи за 1 година – януари 2017 г.-януари 2018 г.

Има голямо разнообразие измежду социалните мрежи. Всеобщо прието е, че всички те споделят едни и същи основни свойства. Социалната мрежа е дигитално представяне на нейните потребители и техните социални връзки във физическия или виртуалния свят, плюс услуги за съобщения и социализиране между потребителите. Предоставя се платформа за:

- Позволяване на потребителите да създадат дигитално представяне на себе си (обикновено познато като потребителски профили);
- Поддръжката и подобряването на вече съществуващите социални връзки между потребителите във физическия или виртуалния свят;
- Създаване на нови връзки, базирани на общи интереси, локация, дейности и т.н.

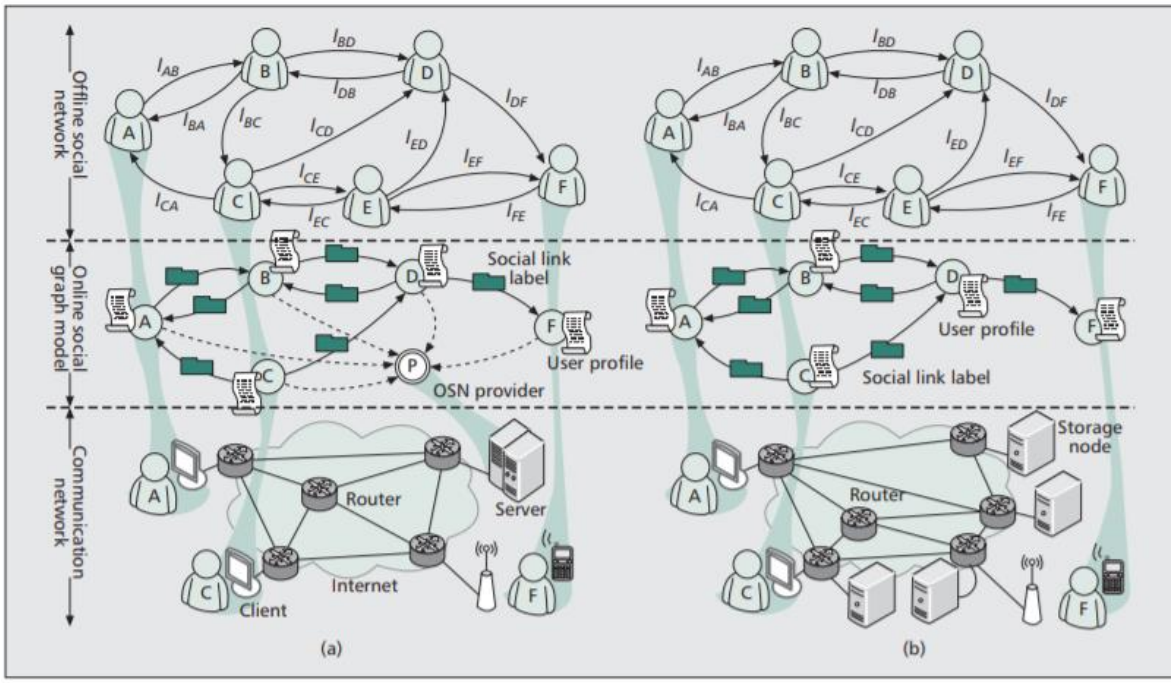
Има две парадигми за имплементирането на социална мрежа в литературата – клиент-сървър архитектура и peer-to-peer архитектура (P2P).

Днешните социални мрежи са централизирани и базирани на уеб-сървър. Всички функционалности като съхранение, поддръжка и достъп до социалните услуги се предлагат от комерсиални доставчици като Facebook Inc. и LinkedIn Corp. Тази традиционна архитектура има предимството да бъде проста и лесна за имплементиране, но страда от недостатъците на централизираните системи [1], [3], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16].

За следващите поколения социални мрежи съществува тенденцията за използване на P2P архитектура, която е децентрализирана архитектура, разчитаща на сътрудничество между няколко независими участници, които също са потребители на социални мрежи. Информацията за раз-

личните потребители се съхранява отделно. С поддържането на директен обмен на информация между устройства, било то между потребители, които вече са се срещали, или между съседни възли в градската мрежа, P2P архитектурата се възползва от предимството на реалните социални връзки и географската близост, за да поддържа локални услуги, когато не е наличен достъп до Интернет.

Фигура 2 илюстрира двата вида архитектури за социална мрежа, където клиент-сървър архитектурата (a) изисква Интернет връзка, за да могат потребителите на комуникират чрез отдалечен централен сървър, а P2P архитектурата (b) поддържа комуникация чрез локална връзка, тъй като ролята на централния сървър е разпределена във всеки възел за съхранение [2], [4], [8].



Фигура 2: Архитектури на социалните мрежи. a) Клиент-сървър; b) P2P

Поверителността е от първостепенно значение за социалните мрежи, тъй като незаконното разкриване и неправилното използване на личната информация на потребителите може да причини нежелани или вредни последици в живота на хората. Поверителност в контекста на социалните мрежи има няколко категории:

Анонимност на потребителя

Защитата на идентичността на потребителя се променя според различните типове социални мрежи. В сайтове като Facebook използването на истински имена за представяне на профила е препоръчително. Няма анонимност на идентичността, защото повечето приложения във Facebook разчитат на връзка на профилите с техните публични идентичности. В сайт за срещи като Friendster е видимо само първото име на потребителя. В уеб сайтове за запознанства, базирани на псевдоними, не се подкрепя използването на лична информация.

Поверителност на личното пространство на потребителя

Видимостта на потребителския профил също варира в зависимост от различните типове социални мрежи. Има сайтове, където профилите са видими за всички и участват в търсачките. Други сайтове имат опцията потребителя да избира дали профилът му да бъде видим публично или само за приятели [2], [4], [7], [8], [9], [17], [18], [19], [21].

Поверителност на комуникацията на потребителя

В допълнение към личните данни, разкрити в дигиталното пространство на потребителя, той може също да разкрие лична информация на мрежовия оператор или доставчика на социална

мрежа: данни като време и дължина на връзката, местоположение (IP адрес) на връзка, посетени профили, изпратени и получени съобщения и т.н.

Всички данни, получени от потребителите, се съхраняват в различни таблици и графики. Най-често атаките са насочени към тези таблици, като биват два типа – подправяне на идентичност и подправяне на връзки [4], [8], [9], [17], [19], [20]. Подправянето (кражбата) на идентичност е фундаментален проблем в социалните мрежи и лежи в основата на много други усложнения, свързани със сигурността. Например зложелател може да направи фалшив профил на известна личност или марка, за да печели от тяхната репутация. Всеки потребител трябва да бъде сигурен в самоличността на отсрещния, за да бъде в безопасност от кибератака.

Улесняването на социалните взаимоотношения е главната функция на социалните мрежи. Въпреки това е възможно неконтролируемо изтичане на информация на потребителите. Събраните данни от доставчиците на социални мрежи са важен източник за социални и маркетинг проучвания, които могат да предоставят полезна информация за развитието и еволюцията на социалното общество. Също така могат да бъдат използвани за оптимизиране на услугите на социалните мрежи и настройването им според потребителските предпочитания и интереси. Въпреки това съществува потенциален конфликт между събирането на данни и изискванията за поверителност. Евентуален неприятел може да използва публикувани данни от социални мрежи и благодарение на някои основни познания да наруши поверителността на потребителя. Дори след скриване на идентичността посредством заменяне на имената със случайни безсмислени идентификатори, е доказано, че базирано на графики с топологична информация, е възможно разкриването на самоличността на повечето потребители. Следователно, за да отговарят на изискванията за поверителност на социалните мрежи, графиките трябва да съдържат несъответствия. Очевидно е налице компромис между качеството на резултата от извличане на данни и изискванията за поверителност.

Заключение

Социалните мрежи са голяма част от ежедневието на днешния човек. Всеки трябва да е наясно с рисковете на интернет пространството и какви опасности крие то, както и да знае начините за предпазване на своята идентичност и лични данни [3], [9].

References

1. Николов, Л. (2018). *Ролята на Европейския съюз в осигуряването на Киберсигурност*. Международна научна конференция „Политиката на европейския съюз по защитата на информацията и личните данни“, Сборник научни трудове – ШУМЕН 2018, ISBN 978-954-9681-89-5.

2. Николов, Л., Фетфов, О., Борисова, А. (2018). *Съображения за сигурност при писането на кодове с JavaScript*. Научна конференция с международно участие MATTEX 2018, Шумен, ISSN 1314-3921.

3. Парашкеванова, Г., Цанков, Ц. (2016). *Киберпрестъпността като основна съвременна заплаха за големите организации*. Научна конференция MATTEX 2016, Шумен, ISSN 1314-3921.

4. Стаменова, А., Диманова, Д., Цанков, Ц. (2014). *Новите войни на XXI век*. Научна конференция MATTEX 2014, Шумен, ISSN 1314-3921.

5. Nikolov, L., Slavyanov, V. (2018). *Network infrastructure for cybersecurity analysis*. International scientific conference 2018, “Vasil Levski” National Military University - Artillery, Air Defense and CIS Faculty, Shumen, Bulgaria, ISSN 2367-7902.

6. Yankova-Yordanova, Y., Dyankov, P. (2016). *Automated systems for process control*. International scientific refereed online journal publisher:“Smart ideas – wise decisions” Ltd., Bulgaria, ISSN 2367-5721, issue 27.

7. Yankova-Yordanova, Y., Tsankov, Ts. (2019). *Opportunities for Remote Use a Powerful Computer*. Journal of Physics and Technology, Plovdiv university press “Paisii Hilendarski”, Plovdiv, ISSN 2535-0536.

8. URL: https://www.aresearchguide.com/30-cyber-security-research-paper-topics.html

9. URL: https://pdfs.semanticscholar.org/08fa/0252365bda9bf7ea5b70a48dd4f744519fed.pdf

10. Савова, Ж., Богданов, Р., *Анонимна система за комуникации в киберпространството, използваща протокол TOR*, Сборник научни трудове на научна конференция на Факултет „А, ПВО и КИС” „Новата парадигма за сигурност в киберпространството” Шумен 2014, стр. 259-265, ISBN 978-954-9681-49-9.

11. Савова, Ж., Богданов, Р., *Оценка на изчислителната сложност на алгоритмите за генериране на големи прости числа за целите на криптографията*, Сборник научни трудове на Научна конференция „Проблеми на информационната сигурност”, гр. Шумен, 2010, ISSN 1314-0647.

12. Савова, Ж., Богданов, Р., *Приложение на недвоичните псевдослучайни последователности в криптографията*, Сборник научни трудове Немус'2012. Институт по отбрана Проф. „Цветан Лазаров”, 2012, ISSN 1312-2916.

13. Boyanov, P., *Unauthorized access attempts to the information resources of private computer networks in academic institutions via network scanning cyber attacks,* Yearbook of Higher School of Security and Economics, Plovdiv, Publishing complex HSSE, ISSN 2367-8798, Vol. XV, 2018, c. 51-58.

14. Боянов, П., *Приложение на кибератаката от тип социално инженерство срещу правителствени агенции, частни организации и академични институции*. Сборник научни трудове - Научна конференция с международно участие "MATTEX 2018" - 25-27 октомври 2018, ISSN: 1314-3921, т.2, ч.1, 2018, с.42-51.

15. Boyanov, P., Tasheva, Zh., Fetfov, Og., Trifonov, T., Uzunova, B., *Securing the social profiles from malicious and unauthorized access*, Proceedings of the 10th International Conference on Bionics and Prosthetics, Biomechanics and Mechanics, Mechatronics and Robotics (ICBBM 2014), Liepaya, Latvia, ISBN 978-9934-10-573-9, Volume 10, June 2 - 7, 2014, pp. 109-112.

16. Фетфов, О., Боянов, П., Ташева, Ж., Трифонов, Т., *Анализ на съвременните видове уязвимости и експлойти в компютърните мрежи и системи*, Annual of Konstantin Preslavsky University of Shumen, Shumen, Университетско идателство „Епископ Константин Преславски“, ISSN 1311-834X, Vol. VI E, 2016, с. 112-122.

17. Камарашев, Г., Димитрова, С., *Финансовия мениджмънт като елемент на военната ло-гистика*, Trans&Motauto 2005 с.37-41.

18. Kamarashev, G., Dimitrova, S., *Outsourcing as a part of the management of resources for security and defense*, SIBIU 2011, pp.643-647.

19. Kamarashev, G., Dimitrova, S., *Aspects of defence and security resource allocattion*, Sibiu 2007.

20. Kamarashev, G., Banabakova, V., *Acquisition – theoretical and practical aspects of application in the defense system*, Brno 2005 c.30-37.

21. Досев, Н., Петров, В., *Съвременни тенденции и аспекти на информационната сигурност в автоматизираните информационни системи и мрежи (АИС/М)*, Научна конференция с международно участие MATTEX 2018 , Шуменски университет „Епископ Константин Преславски“, Университетско издателство, Сб. научни трудове том 2, част 1, стр. 85¸95, ISBN 1314-3921.

Nikolay A. Arhangelov, Viktor V. Lilov,

ANALYSIS OF MAGNETIC PARTICLE INSPECTION AS A TYPE OF NON-DESTRUCTIVE TESTING METHOD

Nikolay A. Arhangelov [1], Viktor V. Lilov [2]

[1] *Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, Department "Communication and Computer Technologies", nikolai_arhangelov@abv.bg*
[2] *Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, Department "Engineering Logistics", solaviki@abv.bg*

***Abstract**: Magnetic control methods began to be used in the 19th century. The first applications are in the arms and railway industries. A compass is used to diagnose changes in the magnetic field of ferromagnetic materials with defects in them. The first use of the magneto-powder method was by W. Hoke after World War I, which revealed imperfections in steel parts. In 1922 he received a patent for the method. The 1930s were the golden years of this method - widespread in England, the United States, Germany and Russia.*

***Keywords**: Defects in Ferromagnetic Materials, Magnetic Control Methods, Magnetic Particle Inspection, Non-destructive Testing*

АНАЛИЗ НА МАГНИТНО-ПРАХОВИЯ МЕТОД КАТО ВИД БЕЗРАЗРУШИТЕЛЕН КОНТРОЛ

Николай А. Архангелов, Виктор В. Лилов

Въведение

Магнитно-праховите методи за контрол се използват за локализиране на дефекти във феромагнитни материали. Базира се на ефекта на разсейване на магнитното поле от повърхностни и подповърхностни дефекти. Магнетизмът е толкова универсален, колкото земното притегляне и електричеството, но същевременно това свойство не се проявява в еднаква степен при всички тела [5], [9], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21]. Такова наличие на дефекти се диагностицира с помощта на фини феромагнитни частици (прах), което е видно от наименованието му. Тези феромагнитни частици индицират големината, формата и разположението на дефекта. Тези частици се доставят до повърхността в сух вид или чрез течност (на водна или маслена основа). Трябва да се има предвид, че не всички материали остават феромагнитни при всякакви температури – някои стомани (неръждаеми) губят феромагнитните си свойства при температури над точката на Кюри (около 760°C).

Физически основи на магнитно-праховия метод

Видове магнитни материали

Съществуват три вида магнитни материали:

- Феромагнитни-стойностите на магнитната проницаемост μ и магнитната възприемчивост са много високи;
- Парамагнитни – стойностите на магнитната проницаемост μ и магнитната възприемчивост са над 1, но са по-ниски поне с един порядък от феромагнитните материали;
- Диамагнитни – стойностите на магнитната проницаемост μ и магнитната възприемчивост са под 1.

Обект на магнито-праховия метод са само феромагнитните материали [9].

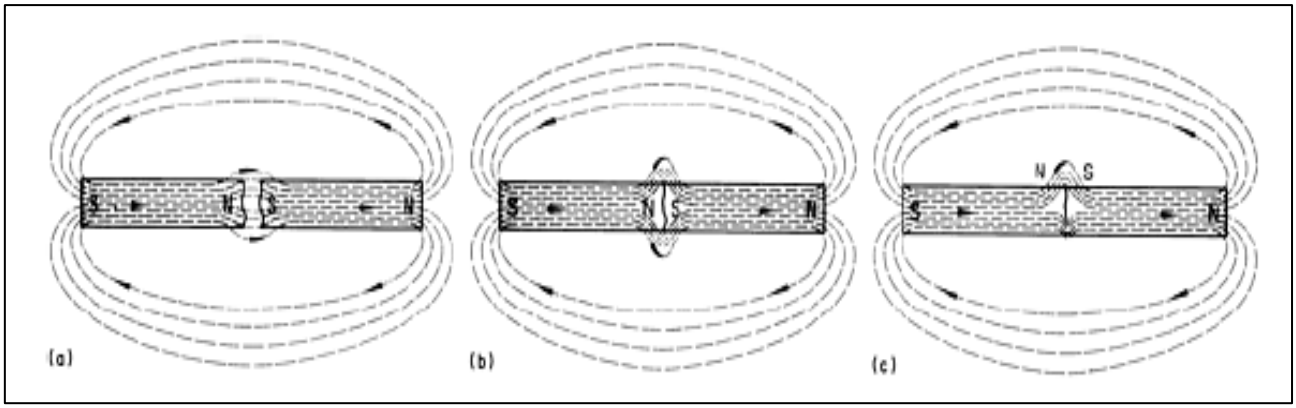
Видове феромагнитни материали

Съществуват три вида феромагнитни материали:

- Магнитномеки – с малки стойности на Hc, високи стойности на магнитната проницаемост μ и магнитната индукция B (армко желязо, пермалой, електротехнически стомани и др.);
- Магнитнотвърди – с високи стойности на Hc; използват се за постоянни магнити;
- Среден клас – със стойности на Hc между 500 и 1000 A/m; в този клас попадат почти всички обекти за магнито-прахов контрол.

Магнитно поле на постоянен магнит

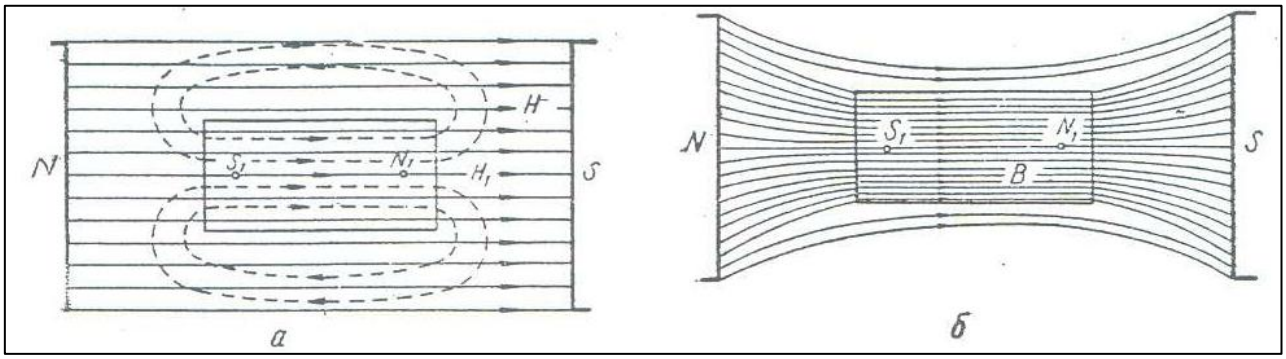
Феромагнитите се състоят от съизмерими с кристалите области, наречени домени, имащи различна полярност в двата си края. Ако материала не се намира в магнитно поле, ориенатцията на тези домени е по посоката на кристалитите. При прилагане на магнитно поле домените се ориентират по посока на полето и тогава материалът се държи като магнит. Магнитът има два полюса – северен N и южен S и притежава магнитно поле, образувано от магнитни силови линии. Тези линии не се пресичат и са непрекъснати (Фиг. 1) [8].



Фигура 1: Промяна на магнитното поле на постоянен магнит ос
a) разделен на две части; b) разделен и слепен; c) със засечка.

Интензивност на магнитно поле

Интензивността на МП H се характеризира с посока и големина. Графично, се изобразява с магнитните силови линии, допирателната към които във всяка точка съвпада с посоката на вектора за същата точка. Ако в магнитно поле с интензивност H се постави феромагнитен материал със собствено МП H1, то се получава наслагване между двете полета и се получава магнитна индукция B = H+H1 (Фиг. 2) [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [19].

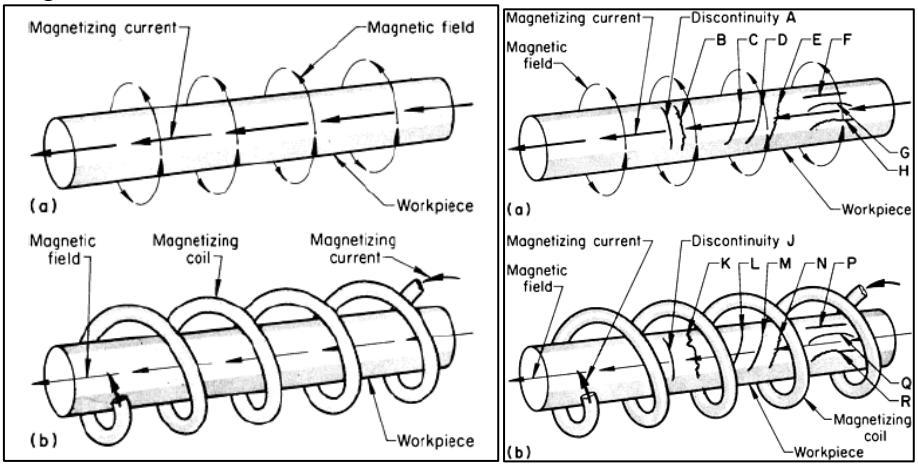


Фигура 2: Магнитни вериги

Съвкупността от всички магнитни и немагнитни материали, в които се разпространява потокът на магнитната индукция се нарича магнитна верига. В магнитно-праховите методи магнитната верига се състои от контролирания обект и системата за намагнитване. В този смисъл основна задача се явява пресмятането на тока на намагнитване, при който се достигат необходимите стойности на индукцията в проверяваната зона.

Посока на магнитно поле

Ефектите свързани с посоката на магнитното поле са онагледени на Фиг. 3.



Фигура 3: Ефекти, свързани с посоката на магнитното поле

Използвани методи за създаване на магнитно поле при магнитно-праховия метод

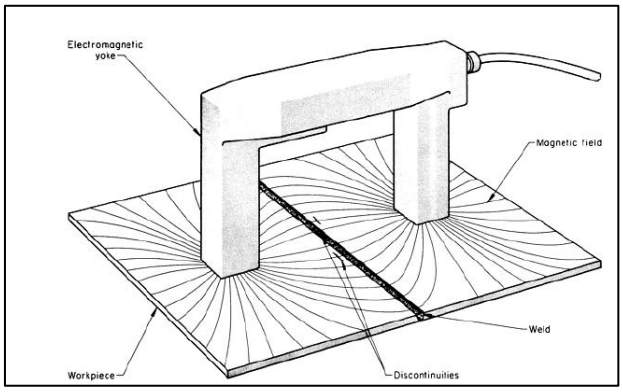
Рамки (скоби)

Биват електромагнитни и такива с постоянен магнит. И двата типа са мобилни (Фиг. 4) [1], [2], [3], [4].

Рамките с постоянен магнит се използват за приложения, при които няма електрически източник или в експлозивна атмосфера (при електромагнитните може да се образува волтова дъга).

Те са с ограничено използване поради следните факти:

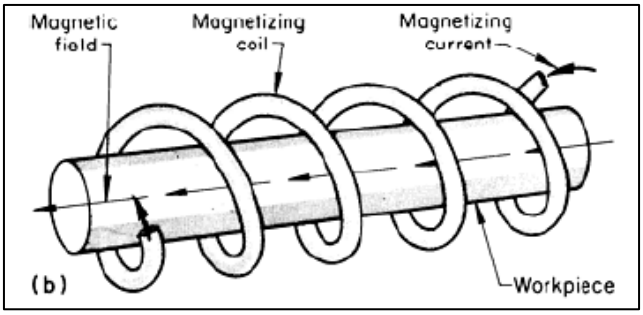
- Не могат да се магнетизират големи обекти;
- Индукцията не може да се променя;
- Ако магнита е много силен, не може да се отдели от обекта;
- Магнитният прах може да остане по магнита и да се прикрият дефектите.



Фигура 4: Рамка

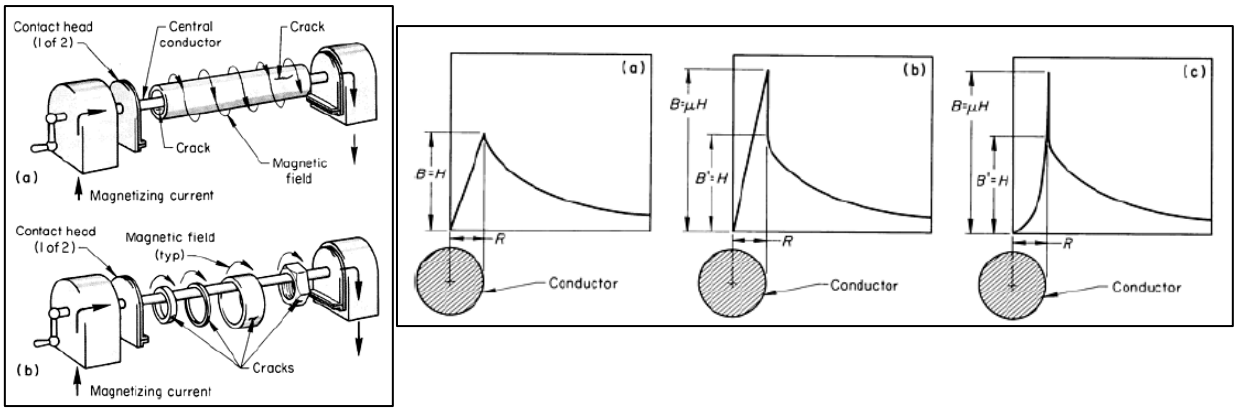
Намотки

Интензитетът на МП е пропорционален на тока I и броя на намотките n. Когато дефектът е зад намотките – може да се пропусне (Фиг. 5) [2], [3], [4], [9], [10], [11], [12], [13], [18].



Фигура 5: Магнетизирано стебло

За значителен брой тръбни детайли е подходящо да се използва магнетизирано стебло вместо да се магнетизират контролираните образци. Такива стебла се правят от добри проводници на електричество, независимо дали са феромагнитни или не. Магнитното поле е еднакво по цялата дължина, като намалява в радиално направление (Фиг. 6) [8], [10], [11].



Фигура 6: Магнетизирано стебло
a) неферомагнит; b) феромагнит прав ток; c) феромагнит променлив ток.

Влияние на характеристиките на частиците

Влияние на размера на частиците

Големите тежки частици не могат да се задържат от слаби МП. Обратно финитe могат да се задържат от слаби МП, но пък могат да предизвикат фалшиви сигнали, особено при неравна повърхност. Едрите сухи частици падат прекалено бързо и “отскачат” от повърхността преди да се намагнетизират и привлекат от дефектите. По-финитe частици се влияят от псевдодефекти като неравна и груба повърхност, пръстови отпечатъци, замърсена или овлажнена повърхност и др. Частиците магнитен прах, доставян с помощна течност са по-малки размери от “сухия” метод – по-големите частици по-лесно падат от повърхността и не се използват по предназначение, докато по-малките остават колкото е нужно [1], [11], [12], [13], [14], [15], [17], [20].

Влияние на формата на частиците

Дългите и люспести частици запазват по-здрава полярност в сравнение със заобленитe, тъй като се образуват по-изявени полюси и силите на привличане са по-големи. Това важи с особена степен за МПМ със сухо доставяне на частиците. От друга страна при издължените частици съществува тази тенденция за слепване, която се проявява и в контейнерите за съхранение, което пък от своя страна води доставянето им на своеобразни микробучки. Това пък оказва негативно влияние върху провеждането на теста. Най-голяма чувствителност на теста с магнитен прах се получава когато частиците са микс от удължени и заоблени частици. При доставянето им с течност, частиците се “движат” по-бавно. Това е предпоставка те да формират различни агломерации или микробучки.

Предимства и недостатъци

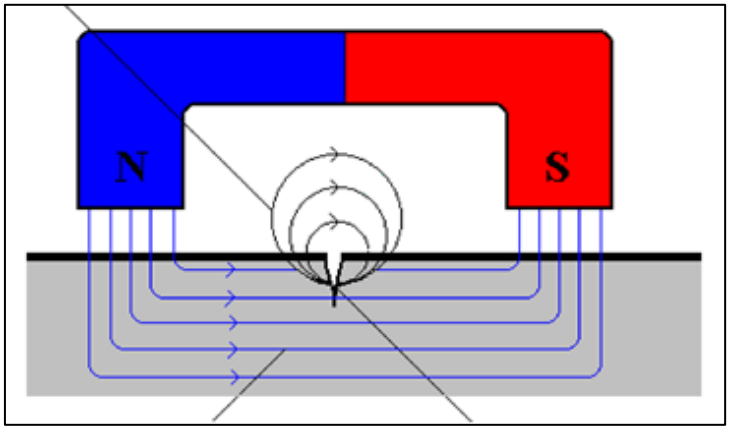
Предимства

Чувствителен за малки и плитки повърхностни и подповърхностни дефекти при известни ограничения (ако дефектът е фин и близко до повърхността може да се използва МПМ, ако е дълбоко става по трудно); Диагностицирането е директно – индикациите се образуват на повърхността; Калибрирането е облекчено – няма електрически/електронни вериги за това на практика има малки ограничения по отношение на големината или формата на контролирания образец, което води обаче до необходимост от големи вериги;

Рядко има нужда от предварителна подготовка на образеца; Могат да се откриват и включвания от друг материал [5], [6], [7].

Недостатъци

- Методът може да се използва само с феромагнитни материали;
- Тънки неферомагнитни покрития (бои и др.) влияят значително върху чувствителността на МПМ;
- За по-добри резултати МП трябва да е в посока която пресича основната равнина на дефекта – това понякога води до необходимост от последващи намагнитвания; Обикновено е необходимо размагнитване след МПМ за контрол. Понякога е необходимо да се отстраняват частиците магнитен прах от дефекта;
- За контрол на големи детайли са необходими големи мощности [12], [13], [14], [15], [16], [17], [18], [19], [20], [21];
- Необходимо е повишено внимание към нагряването – съществува опасност от пожар;
- Независимо, че индикацията е на пръв поглед лесна, са необходими значителни квалификация и знания (Фиг. 7) [6], [7], [10], [12], [13], [18], [19], [20], [21].



Фигура 7: Поле на разсейване на дефекта

References

1. Антонов, А., Янкова-Йорданова, Й. (2016). *Методика за обучение по симулационно моделиране на технологични процеси*. Шуменски университет "Епископ Константин Преславски" MATTEX 2016.

2. ГОСТ 18442-80 (1980). *Качество продукции. Неразрушающий контроль. Капиллярные методы. Общие требования*. М.

3. ГОСТ 21105-87 (1987). *Контроль неразрушающий. Магнитопорошковый метод*. М.

4. ГОСТ Р 52005-2003 (2003). *Контроль неразрушающий. Метод магнитной памяти металла. Общие требования*. М.

5. Давидов, К., Дянков, П. (2019). *Методи за безразрушителен контрол*. УИ „Епископ Константин Преславски“, Шумен.

6. Лалев, Х., Желев, С., Цанков, Ц. (2009). *Анализ и мониторинг на честотните характеристики на RLC вериги*. Научна сесия на факултет „Артилерия, ПВО и КИС“, Шумен, ISSN 1314-1953.

7. Лалев, Х., Цанков, Ц., Николов, И. (2010). *3D лазерно сканиране*. Научна конференция MATTEX 2010, Шумен, ISSN 1314-3921.

8. Скордев, Ал., Аврамов, Д. (1981). *Подготовка на дефектоскописти*. Сборник доклади от II научно-приложна конференция по подготовка на кадри за изследване, проектиране и експлоатация на системите човек-техника (София), С., изд. ДКНТП.

9. Янкова-Йорданова Й., Цанков Ц. (2018). *Плазмена преработка на твърди битови отпадъци*. Научна конференция с международно участие MATTEX 2018, гр. Шумен.

10. Chernokozhev, P., Antonov, A., Dyankov, P. (2012). *Shaping the process of penetration in thin targets*. Journal scientific and applied research, Vol. 2, ISSN 1314-6289.

11. Yankova-Yordanova, Y., Dyankov, P. (2016). *Automated systems for process control*. International scientific refereed online journal publisher:“Smart ideas – wise decisions” Ltd., Bulgaria, ISSN 2367-5721, issue 27.

12. Коджейков, Р., Жеков, Ж., Боянов, П., *Анализ на информационните ресурси в системата на логистичния мениджмънт,* Сборник доклади от годишна университетска научна конференция 16-17 юли 2015 година, Национален военен университет "Васил Левски", Издателски комплекс на НВУ „Васил Левски”, ISSN 1314-1937, т. 12, с. 191-198.

13. Жеков, Ж., Боянов, П., Червенков, Д., *Анализ на особеностите на информационните логистични системи*, Сборник доклади от годишна университетска научна конференция 16-17 юли 2015 година, Национален военен университет "Васил Левски", Издателски комплекс на НВУ „Васил Левски”, ISSN 1314-1937, т. 12, с. 208-213.

14. Камарашев, Г., Димитрова, С., *Евакуационната практика в съвременни условия*, ВВМУ “Н. Вапцаров”, 2006 г., Т.5, с. 195-201.

15. Камарашев, Г., Димитрова, С., *Моделиране на управлението на запасите при неопределеност на пазара*, УНСС 2004.

16. Камарашев, Г., Райков, П., *Специални войскови действия в антитерористични операции*, НВУ “В. Левски”, 2003 г.

17. Трифонов, Т., *Анализ на характерни неизправности в схемите, изработващи захранващите напрежения в компютърните дънни платки*, Научна конференция MATTEX 2010, ШУ "Еп. К. Преславски.

18. Zhekov Zh., Antonov A., Boyanov P., Chervenkov D., Trifonov T., *Method for Identification of signals*, Journal Scientific and Applied Research Vol. 5, 2014, ISSN 1314-6289.

19. Трифонов Т., *Анализ на производителността на преносим компютър, оборудван с полупроводниково устройство за съхранение на данни*, Годишник на ШУ „Еп. К. Преславски”, Технически науки, Университетско издателство, Шумен, 2014 стр. 27-42, ISSN 1311-834X.

20. Фетфов О., Атанасов А., *Възможности за приложение на GSM –инфраструктурата в радиолокационните системи*, Научна конференция с международно участие MATTEX 2012, Шуменски университет "Еп. К. Преславски". ISSN 1314-3921.

21. Фетфов О., Атанасов А., *Сравнителен анализ на протоколите за високоскоростен трансфер на данни в стандарта TETRA Rel.2*, Научна конференция с международно участие MATTEX 2012, Шуменски университет "Еп. К. Преславски". ISSN 1314-3921.

Ekaterina M. Konstantinova, Viktor V. Lilov,

INFLUENCE OF DIGITAL TECHNOLOGY ON E-LEARNING

Ekaterina M. Konstantinova [1], Viktor V. Lilov [2]

[1] *Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, Department "Communication and Computer Technologies", katminkova2@gmail.com*
[2] *Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, Department "Engineering Logistics", solaviki@abv.bg*

***Abstract**: Knowledge is a necessary resource in the information society, and learning is the strategic process behind it. Today, people are different, they are directly accessing digital technology in every aspect of their lives, and it is only natural that this will have a huge impact on their behavior and their thinking. As far as the education system is concerned, new technologies provide more opportunities and, at the same time, more challenges. The concept of "learning technology" or "technology of learning" is constantly expanding. It is an indisputable fact that these technologies stimulate the formation of new cognitive interest and find new ways to motivate learning. Computers are a convenient tool to support this process. With the help of multimedia, information can be presented in the most appropriate and easy-to-understand way, with the help of sound, video, animation, graphics, and text. However, if multimedia tools and services offered by the Internet are added to the mix, it is clear that a new era has dawned on the learning systems development.*

***Keywords**: Digital technology, Knowledge, Learning, Learning technology, Youth*

ВЛИЯНИЕ НА ДИГИТАЛНИТЕ ТЕХНОЛОГИИ ВЪРХУ ЕЛЕКТРОННОТО ОБУЧЕНИЕ

Екатерина М. Константинова, Виктор В. Лилов

1. Въведение

Мащабното развитие на дигиталните технологии променя изцяло обучителния процес, спецификата на социалната връзка и обменът на информация в младежкия живот. Възходът на технологиите за общуване има важен принос за развитието на социално взаимодействие. Електронните средства за комуникация осигуряват възможност за интензивно самостоятелно обучение и предметите, върху които се набляга се определят от интересите на конкретния потребител. Ползите от дигиталните технологии са безгранични, не се ограничават само до оптимизиране на процеса на обучение, а обхващат развитието на човешката креативност, предприемаческите умения и отстояването на активна житейска позиция [9], [10], [11].

Широко приложение между тийнейджъри и млади учащи намират такива технологии като аудио, видео записи и различни игри за самоизразяване. В учението могат да бъдат използвани различни методи, но най-доброто усвояване на предложения материал идва от предпрограмирано състояние в човешкото обществото – взаимодействието. Съчетаването на учебни дейности в Интернет помага за повишаване на ефикасността и качеството на обучението [2], [3].

От много години има реална възможност да се преустанови всякакъв печат на книги и много още други видове печатни издания, много от които се използват за обучение. Сега работят множество легални и пиратски електронни библиотеки, събирани главно от ентусиасти с цел да направят достъпна литературата до много потребители без да превеждат пари [12], [13], [14], [15], [16]. Не са малко и сайтовете, които печелят от доставката на електронни книги. От другата страна е и напълно легалното разпространение на книги и списания и учебници [3], [4].

2. Изложение

През последните години има голямо вълнение около трансформиращия потенциал на технологиите в образованието. В съвременните условия на живот е все по-неподходящо преподаването на учебния материал по класическите методи в учебните заведения. Черната/бялата дъска в редица уроци/лекции се заменя с интерактивни дъски или просто с екран и прожекционен апарат. Представени в слайдове, лекциите имат стегнат и приятен вид: схемите са начертани безупречно, текста е лесно четим, могат да се използват много допълнителни мултимедийни възможности. При използването на тези предимства е малка вероятността за отклоняване на вниманието или загубата на интерес от обучаемите към учебния материал [2], [4].

Програмите и политиките за насърчаване на използването на образователни технологии могат да разширят достъпа до качествено образование, да подпомогнат обучението на учениците по иновативни начини и да съдействат на семействата да се ориентират в сложни училищни системи. Бързото развитие на образователните технологии обаче се случва в контекста на дълбоко и трайно неравенство. В зависимост от това как се проектират програмите, как се използват и кой има достъп до тях, образователните технологии биха могли да облекчат или влошат съществуващите различия. За да използват пълния потенциал на образованието, ръководителите на образователни институции, разработчиците на продукти и финансиращите органи трябва да разберат начините, по които технологията може да помогне – или в някои случаи да навреди на обучението на учащите.

Ползи от електронното обучение

Електронното обучение е всеобхватен термин, който обикновено означава обучение, извършено на компютри свързани с мрежа [9], [10], [11], [12], [13], [14], [15], [16], [20] което ни дава възможност да учим електронни материали навсякъде и в по всяко време [2], [3], [5], [7].

Дигиталното обучение прави учениците по-умни

Учебните инструменти и технологии позволяват на учениците да развият ефективни умения за самостоятелно обучението. Те са в състояние да идентифицират какво трябва да учат, да намерят и използват онлайн ресурси, да прилагат информацията за проблема и дори да оценяват резултатите от тях. Това увеличава тяхната ефективност и производителност. В допълнение към ангажираността на учащите, дигиталните инструменти за обучение и технологиите изострят уменията за критично мислене, които са в основата на развитието на аналитични разсъждения. Децата, които подхождат към въпросите с отворен тип с въображение и логика, се научават как да вземат решения, за разлика от временното запомняне на учебника.

Представяне на информацията под формата на игра е чудесна характеристика на интерактивното обучение, тъй като учи учениците, които играят в група, да зависят и да се доверяват един на друг, за да спечелят игра или да постигнат целите си. Те също така насърчават сътрудничеството и работата в екип, които са много важни умения във всеки аспект от живота [17], [18], [19], [20], [21].

Интерактивните игри за социални умения са отлични инструменти за учене, които учат обучаваните на дисциплина, защото играта изисква да се следват правила и указания. Дори

децата, които могат да се разочароват от други методи на обучение, могат да се придържат към игрите по-дълго, защото самата игра е възнаграждаваща. Това в крайна сметка им помага да развият търпение, още едно полезно житейско умение (Фиг. 1).

Фигура 1: Защо си заслужава да представяме информацията под формата на игри?

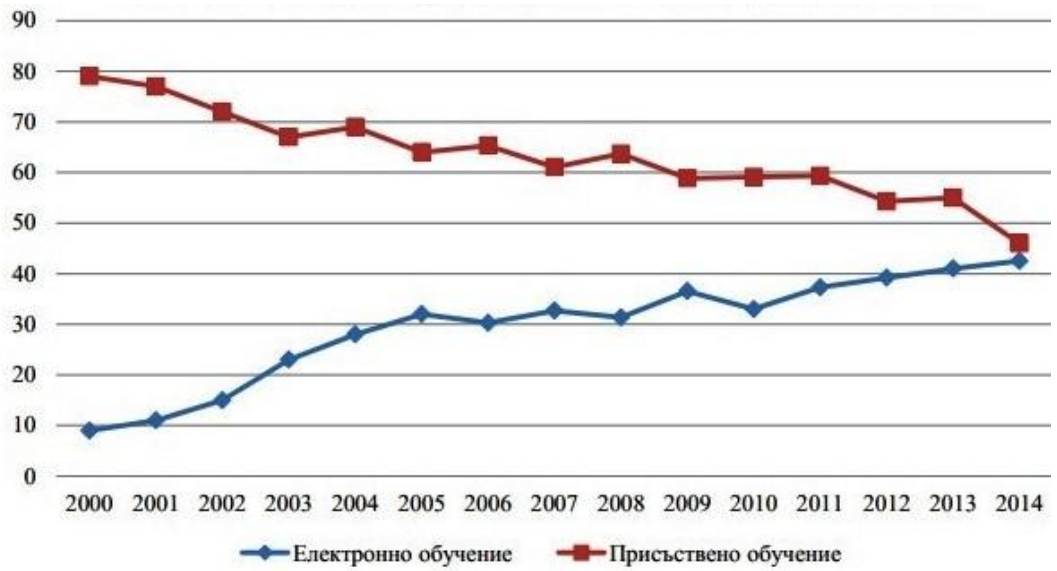
Дигиталното обучение прави учениците по-мотивирани

Учениците, използващи дигитални инструменти за обучение и технологии, стават по-ангажирани в процеса и по-заинтересовани от увеличаване на базата си от знания. Те може дори да не осъзнават, че учат активно, тъй като процесът протича чрез методи като директна комуникация с връстници, работа в екип, решаване на задачи, концептуални карти, информация под формата на игра, постановки, игра на роли и разказване на истории [8], [9], [10], [11], [12], [14], [18], [19], [20].

Тъй като дигиталното обучение е далеч по-интерактивно и запомнящо се от обемните учебници или скучните лекции, те осигуряват по-добър контекст, по-голямо усещане за перспектива и по-приятни дейности от традиционните методи на обучение. Това позволява на учениците да се свързват по-добре с учебния материал. Освен това те често предлагат по-интересен и привлекателен начин за усвояване на информация. Това се отразява в процентите им на задържане на информацията и тестовите резултати. Освен това, когато учащите могат да проследят собствения си напредък, това мотивацията им (Фиг. 2) [1], [3], [10], [11], [12], [13], [15], [16], [17], [21].

Повишаване възможността за получаване на добра работа на учениците с помощта на дигитални инструменти и технологии за обучение

Подготвянето на учениците според изискванията на висшето образование и нуждите на работодателите в ранна възраст се превърна в една от най-важните отговорности на училищното образование.



Фигура 2: Динамика на продължителността на времето за обучение 2000-2014г. в САЩ

При продължаващата криза на заетостта е изключително важно, ако младите хора не могат да намерят работа, да имат способността да си създават начини на препитание, в идеалния случай дори да създават работни места за други [5], [6], [8], [11], [12], [15], [17], [18], [21]. За тази цел в училищните учебни програми трябва да бъдат включени по-нови методи на обучение и образование, като се започне още от началното училище. Дигиталните инструменти и технологии за обучение в начални, средни и средни училища подготвят учениците за висшето образование и кариера, като им помагат да придобият умения, включително решаване на проблеми, запознаване с възникващите технологии и само-мотивация (Фиг. 3).

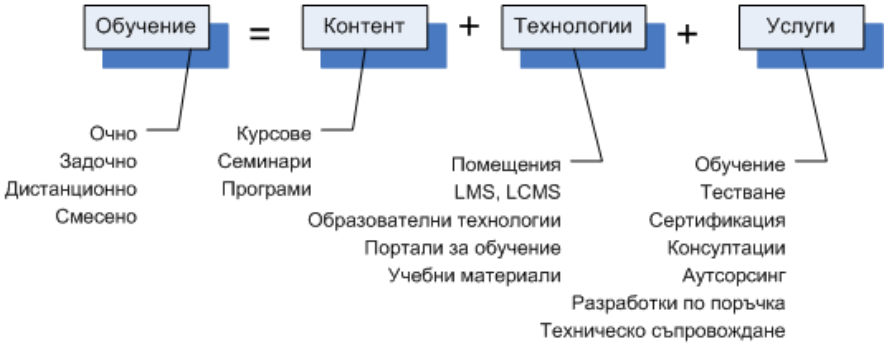
Фигура 3: Характеристики на електронното обучение

Недостатъци на електронното обучение

Електронното обучение има очевидни предимства пред подхода на старата школа, но това не го прави идеално решение за всяка ситуация. Това обаче е адаптивно решение, така че дори и тези качества, които биха могли да се считат за недостатък, могат да бъдат преодолени [1], [7], [8], [9], [10], [11], [12], [15], [19], [20].

Изолация

Например, някои хора просто учат по-добре в традиционна обстановка в класната стая или в центъра за обучение, а не в онлайн - в домашна обстановка. Това би могло да бъде преодоляно чрез смесено обучение – комбинация от онлайн курсове и ръководени консултации от инструктори с възможности за взаимодействие с други учащи (Фиг. 4).



Фигура 4: Основните компоненти на електронното обучение

Технически проблеми

Въпреки че повечето от хора сърфират в Интернет без затруднение, не всички са толкова добре с техническите познания. За тези учащи концепцията и процесът на електронно обучение може да се окажат трудни за разбиране. Дори ако софтуерът е лесен за използване, употребата му може да е обезсърчаваща за някои. Други потенциални технически проблеми могат да включват бавна интернет връзка, специфични изисквания към браузъра и лоша съвместимост на устройството [9], [10], [11], [12], [13], [14], [15], [16], [17], [21].

Здравни проблеми

Електронното обучение изисква честото използването на компютър и други подобни устройства. Това означава, че напрежението в очите, лошата стойка и други физически проблеми могат да засегнат учащия.

Заключение

През последните няколко десетилетия има голям напредък в света на технологиите. За преподавателите е важно да разбират актуалните тенденции и иновации, да знаят какво е достъпно и как може да се използва в класните стаи. Днес те са пълни с ученици с различни стилове на обучение и интереси. Технологиите могат да бъдат важен инструмент за преодоляване на пропастта между заинтересоваността на учениците и знанията на учителите.

В образователните центрове трябва да се използват потенциала, който идва от дигиталните инструменти. Днешната методика на преподаване трябва да отчита всички промени в света и в умовете на студентите и да позволява да се използва творческият потенциал на новите технологии в пълна степен, без да се изоставят други форми за придобиване на знания.

Интернет и много други електронни и дигитални ресурси повдигат редица нови въпроси във образованието. Те трябва да бъдат изчистени преди се влезе в новата еволюционна епоха на развитието на ума.

References

1. Вълканова, В. (2014). *Изследвания на виртуално образователно пространство в средното училище*. Дисертационния труд за придобиване на ОНС "доктор", Българска академия на науките, София.
2. Христов, Х., Цанков, Ц. (2009). *Използване на системата e-Learning Shell в обучението по инженерните дисциплини*. Научна конференция на Факултета по технически науки, Шумен, ISSN 1311-834X.
3. Цанков, Ц. (2017). *Разпространение на електронни книги*. Сп. „Автоматика и информатика“, год. L, № 3, София, ISSN 0861-7562, с. 35-38.
4. Цанков, Ц., Диманова, Д. (2016). *Компютърна дидактична програма за код на Хеминг*. Годишник на ШУ „Епископ К. Преславски“, Шумен, ISSN 1311-834X.
5. Aree Phanmanee (2001). *Development of creativity to excellence*. Thanachai Printing Co. Ltd.
6. Palfrey, J., Gasser, U., & Maclay, C. (2011). *Digital natives and the three divides to bridge.* The state of the world’s children. New York, NY: United Nations.
7. Papert, S. (1993). *The Children’s Machine: Rethinking School in the Age of the Computer*. New York: Basic Books.
8. Wattanaarong, K. (2011). *Technological innovation and educational technology*. 2nd edition, Bangkok: University King Mongkut's University of Technology North Bangkok.
9. Камарашев, Г., *Военно-образователната система на Р. България компонент на националната образователна система*, НВУ „В. Левски” 2011г. с. 7-31.
10. Камарашев, Г., Димитрова, С., *New aspects of the military educational system*, Sibu 2007г.с.7-11.
11. Камарашев, Г., *Тенденции в развитието на военнообразователната система-проблемни въпроси и перспективи*, НВУ „В.Левски” 2010г.с.7-15.
12. Kamarashev, G., Banabakova, V., *Acquisition – theoretical and practical aspects of application in the defense system*, Brno 2005 с.30-37.
13. Stoyanov, St., Boyanov, P., *Converting the learning process in educational research work of the students*, Journal Science Education Innovation, ISSN 1314-9784, Vol. 1. 2013, pp. 20-24.
14. Boyanov, P., Hristov, Hr., Fetfov, O., Trifonov, T., *Educational simulation the local area network of academic departments with securely configured FTP server*, International Scientific Online Journal, www.sociobrains.com, Publ.: Smart Ideas - Wise Decisions Ltd, ISSN 2367-5721 (online), Issue 31, March 2017, Bulgaria, 2017, pp. 146-154.
15. Фетфов, О., Боянов, П., Николов, Ив., Ташева, Ж., Трифонов, Т., *Сравнителен анализ на съвременните видове безжични IP видеокамери в компютърните мрежи за наблюдение и контрол*, Annual of Konstantin Preslavsky University of Shumen, Shumen, Университетско идателство „Епископ Константин Преславски“, ISSN 1311-834X, Vol. VI E, 2016, с. 143-149.
16. Фетфов, О., Боянов, П., Ташева, Ж., Трифонов, Т., *Анализ на съвременните видове уязвимости и експлойти в компютърните мрежи и системи*, Annual of Konstantin Preslavsky University of Shumen, Shumen, Университетско идателство „Епископ Константин Преславски“, ISSN 1311-834X, Vol. VI E, 2016, с. 112-122.
17. Савова, Ж., Богданов, Р., *Анонимна система за комуникации в киберпространството, използваща протокол TOR*, Сборник научни трудове на научна конференция на Факултет „А, ПВО и КИС” „Новата парадигма за сигурност в киберпространството” Шумен 2014, стр. 259-265, ISBN 978-954-9681-49-9.
18. Николов, Л. (2018). *Ролята на Европейския съюз в осигуряването на киберсигурност*. Международна научна конференция „Политиката на европейския съюз по защитата на

информацията и личните данни“, Сборник научни трудове – ШУМЕН 2018, ISBN 978-954-9681-89-5.

19. Николов, Л., Фетфов, О., Борисова, А. (2018). *Съображения за сигурност при писането на кодове с JavaScript*. Научна конференция с международно участие MATTEX 2018, Шумен, ISSN 1314-3921.
20. Nikolov, L., Slavyanov, V. *Network infrastructure for cybersecurity analysis*. International scientific conference 2018, “Vasil Levski” National Military University - Artillery, Air Defense and CIS Faculty, Shumen, Bulgaria, 2018, ISSN 2367-7902.
21. Досев, Н., Петров, В., *Съвременни тенденции и аспекти на информационната сигурност в автоматизираните информационни системи и мрежи (АИС/М)*, Научна *конференция* с международно участие MATTEX 2018 , Шуменски университет „Епископ Константин Преславски“, Университетско издателство, Сб. научни трудове том 2, част 1, стр. 85¸95, ISBN 1314-3921.

Ekaterina M. Konstantinova, Mihaela A. Karadocheva, Tsvetoslav S. Tsankov,

THE INVISIBLE INTERNET AND CYBER SECURITY

Ekaterina M. Konstantinova [1], Mihaela A. Karadocheva [2], Tsvetoslav S. Tsankov [3]

[1] *Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, Department "Communication and Computer Technologies", katminkova2@gmail.com*
[2] *Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, Department "Communication and Computer Technologies", mkaradocheva6@gmail.com*
[3] *Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, Department "Communication and Computer Technologies", c.cankov@shu.bg*

***Abstract**: Technologies create countless new opportunities, and new products and services become an integral part of our daily lives. For our part, we risk becoming the victim of cybercrime is growing. The internet has a hidden part that is much larger than the one we use. Besides everyday websites we use, there is another huge online space invisible to traditional search engines! This is the dark and unlit part of the Internet that hides computer criminals, hackers, online drug dealers, illegal software and cyber terrorists. There are ways to access it safely or ensure the protection of our personal data in clever ways!*

***Keywords**: Cyber security, Dark Web, Deep Web, I2P, Internet, P2P, Security protocols, Surface Web, Tor*

НЕВИДИМИЯТ ИНТЕРНЕТ И КИБЕРСИГУРНОСТТА

Екатерина М. Константинова, Михаела А. Карадочева, Цветослав С. Цанков

Въведение

Когато повечето хора чуят Интернет, те си представят гледане на видео в стрийминг платформа, четене на новини, теглене на игри или филми, резервиране на стая в хотел. Под повърхността обаче се крие място, където дебнат терористи, престъпници и хора разобличаващи тайни проекти и правителствени грешки [12], [13], [14], [15], [16], [19], [20], [21], [22]. Погрешното разбиране на термини като Darknet, Dark Web и Deep Web е в основата на мистификацията на тъмната страна на Интернет. В света на киберсигурността тези термини се появяват на бял свят с излагането на техники, използвани от киберпрестъпниците за комуникация, сътрудничество и участие в злонамерени дейности. Нужно е по-добро разбиране на този подземен свят и начините на предпазване от кибервредители [1], [2], [3], [6].

Изложение

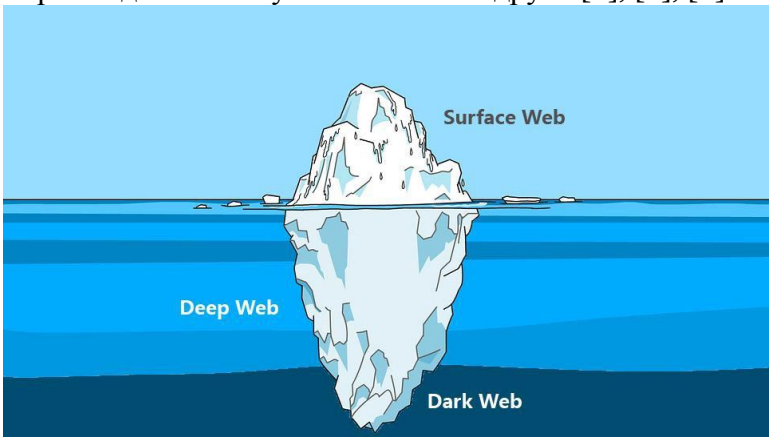
Видима мрежа

Световната мрежа е създадена като платформа за милиарди хора да си взаимодействат чрез Интернет. Най-често срещаната зона в мрежата, която е обществено достъпна, се нарича Surface Web, или Видимата Мрежа. Това включва всички уебсайтове или страници, които могат да бъдат намерени с помощта на търсачки като Google, Yahoo и Bing. Това се случва чрез метод наречен „индексиране”. Индексирането се обяснява най-добре чрез съвременната търсачка Google и нейната здрава, високоефективна система на индексиране. Методите за индексиране на Google до голяма степен разчитат на процес, наречен „обхождане“, който е близък до виртуална паяжина, която обхожда сред множеството страници на уебсайт, до който лесно се достига чрез връзки. Търсачките разполагат с модерни уеб скенери, които събират всички връзки от стотици милиарди уеб страници ежедневно и индексират всяка връзка за оптимизация на търсенето [10], [11], [12], [13], [14], [15], [16], [17], [18]. Процесът на индексиране категоризира всеки уебсайт и техните страници според съдържанието и текста на всяко място. Видимата мрежа включва търсените, индексирани уебсайтове и уеб страници.

Ако уебсайт не е индексиран от търсачка, до него можете да се получи достъп само чрез навигация директно до URL адреса чрез връзка или въвеждане на точния уеб адрес в браузъра. Търсачките имат достъп само до 16% от наличната информация в Интернет [6], [7].

Дълбоката мрежа

Следващото ниво в Световната мрежа е Deep Web, или Дълбоката мрежа (Фиг. 1). Тя е съставена от уебсайтовете или уеб страниците, които не позволяват на търсачките да ги индексират. Това се случва, когато уеб скенери не могат да получат достъп и да събират връзки от тези сайтове; следователно не могат и да ги търсят. Това може да бъде умишлено направено от собственика на уебсайта или страничен ефект поради естеството на уебсайта. Има няколко метода, които могат да се използват, за да запази информацията скрита и да се предотврати индексирането на страниците [1], [2], [3], [4], [5]. Някои от тези методи включват забраната на уебсайт на повърхността не съдържа връзки към страниците, ограничаване на достъпа до страниците чрез технически средства (например CAPTCHA кодове) или изискване за вход за достъп до страници. Добре е да се отбележи, че съдържанието на Дълбоката мрежа не винаги е незаконно и се провеждат множество дейности, които са изцяло в рамките на закона. Примери: социални мрежи, блогове, текстови и гласови чатове; международни турнирни игри (шах и табла); различни нетрадиционни клубове (клубове за края на света, фен клубове, клубове за видеоигри и др.); публична документация и сертификати; индекси на онлайн библиотеки; комуникация чрез криптирани съобщения, за гаранция на поверителността; състезания по караоке и пеене; групи за теории на конспирациите; курсове по компютърни и дигитални умения и много други [1], [2], [7].



Фигура 1: Представяне на мрежите в Интернет пространството

Тъмната мрежа

Dark Web [8], или Тъмната мрежа, е термин, който се използва за описване на криптирана мрежа, изградена под повърхността на Видимия интернет, до която може да се получи достъп само с помощта на специализиран софтуер. Уебсайтове не са индексирани, следователно Тъмната мрежа е част от Дълбоката мрежа. Тази мрежа е описана като тъмна, поради характеристиките си, тъй като помага на потребителите да скрият самоличността си и е популярна при подпомагането на незаконни дейности.

Когато се говори за разликите между Тъмната мрежа и Дълбоката мрежа, нещата добиват различен смисъл, За начало трябва да се спомене, че Тъмната мрежа е малка част от дълбоката мрежа - 0,1%. Основната и цел е да защитава поверителността, използвайки комбинация от маршрутизация и криптиране, и разбира се това може да се използва както за законни, така и за незаконни цели. Въпреки, че имат разлики, Тъмната и Дълбоката мрежа имат и своите прилики (Табл. 1). [2], [3], [6], [7], [13], [14], [15], [19], [20], [21].

Таблица 1: Прилики на Тъмната и Дълбоката мрежа

Вид съдържание	**Описание**
Съдържание с ограничен достъп	Уебсайтове до които се получава достъп само с JavaScript връзки.
Динамично съдържание	Динамични уебсайтове, които използват формуляри за филтриране на достъпа, т.е. captcha.
Страници без входящи връзки	Тези страници блокират роботи на търсачката и възможно индексиране.
Програмно съдържание	Страници, които са достъпни само чрез JavaScript връзки.
Без HTML съдържание	Кодирано мултимедийно съдържание или файлови формати, които не могат да бъдат четени от търсачките, с изключение на програми като TOR.
Частна мрежа	Уебсайтове, където е необходима парола за достъп.
Контекстуална мрежа	Уеб страници, които варират в зависимост от контекста, като използват параметри като клиентски адреси или предишни посещения.

За достъп до тъмната мрежа често е необходимо да се използват нестандартни комуникационни протоколи и портове – програми като Tor и Onion, които са способни да се свързват със структурата на мрежите, които са част от Тъмната мрежа.

Протоколи за сигурност

При сърфиране във Видимата мрежа, криптографският протокол, който осигурява конфиденциалност при комуникация със сървъра, е TLS (Transport Layer Security). Зеленото ключе в URL лента е уверение, но не и гаранция, че общуването е поверително. Докато TLS е проектиран да осигурява сигурност и идентичност, тъмните уеб протоколи са проектирани да осигуряват конфиденциалност и анонимност [8], [9], [10], [12], [16], [17], [18], [19]. Тъмните мрежи могат да бъдат организирани или под формата на мрежи за поверителност, като Tor или Freenet, или в мрежи от партньорски връзки, (като I2P или мрежи P2P) [1], [2], [3], [4], [5]. [11], [12], [13], [16], [17].

Tor

Маршрутизаторът Tor, или The Onion Router е създаден от Американската армия за целите на сигурността. Той достига популярността си поради високото ниво на криптиране, лекотата на използване, а също така и фактът че е безплатен. Целия софтуер може да бъде изтеглен и настроен за минути. Анонимността се постигна чрез маршрутизиране на мрежовия трафик през различни сървъри на Tor, разположени в целия свят. Това означава, че ако някой от пакетите във връзката бъде прихванат, потребителите изглеждат като случайни, отделни възли в мрежата на Tor, което прави идентифицирането им почти невъзможно. За съжаление този процес през прави скоростта значително по-ниска.

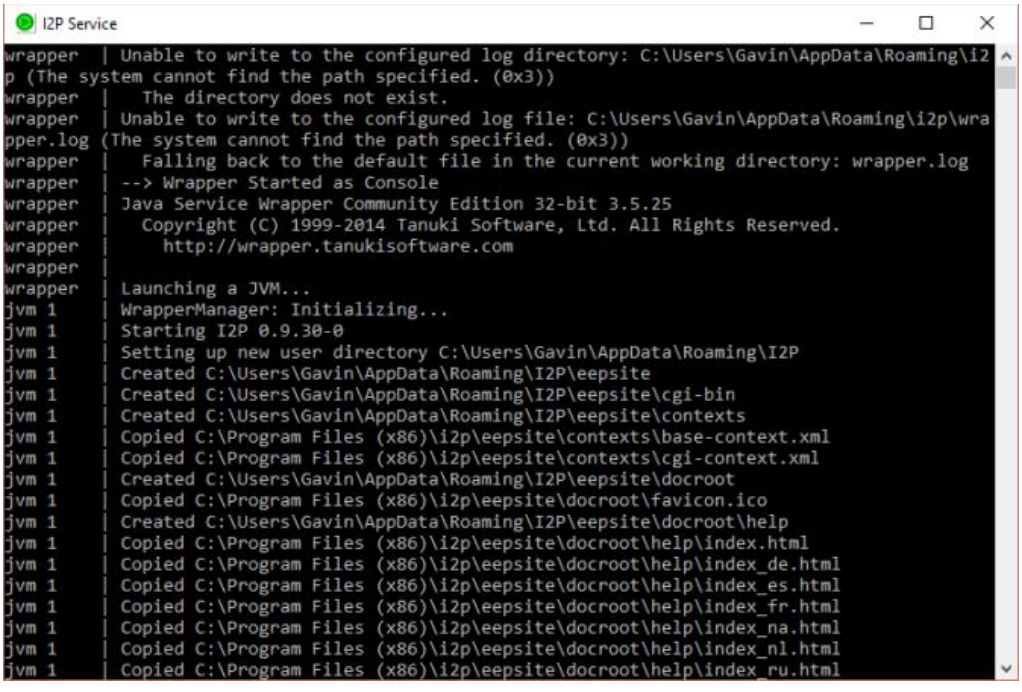
Много уебсайтове могат да бъдат достигнати само с Tor. Те имат домейн от първо ниво „onion“ (TLD), вместо да имат често използваните такива като „.com“, „.edu“, „.net“ и „.org“. Връзките към тези уебсайтове биват приети само от браузъри или приложения, които работят в мрежата Tor. За мобилни устройства това са приложенията Orbot и Orfox или разширения за уеб браузъри.

I2P

Има няколко алтернативни метода за достъп до Тъмната мрежа, като например използването на Invisible Internet Project (I2P). Това е услуга, подобна на Tor, но може да работи в уеб браузъри. Това, което го отличава от другите е целта на използване, която се фокусира върху сърфиране, съобщения или анонимно споделяне.

I2P Service

Invisible Internet Project (I2P) е чеснов протокол за маршрутизация. I2P е „анонимна мрежа със наслагване“. Работи като криптира множество съобщения заедно, за да направи труден анализ на трафика на данни, като същевременно увеличава скоростта му (Фиг. 2). Получава името си от растението чесън. Всяко съобщение е „скилидка“, а целия криптиран пакет е „главата“. Всяко криптирано съобщение има своя специфична инструкция за доставка и всяка крайна точка работи като криптографски идентификатор [8], [9], [10], [11], [12], [13], [14], [15] (прочита един от двойката публични ключове).



Фигура 2: I2P Service

Всеки I2P клиент (маршрутизатор) изгражда серия от входящи и изходящи връзки „тунели“ - директна мрежа „peer-to-peer“ (P2P). Основна разлика между I2P и други P2P мрежи е индивидуалният избор на дължина на тунела. Дължината на тунела е фактор за анонимността, латентността и личната пропускателна способност.

F2F

Мрежата "приятел-приятел" (F2F) е вид партньорска мрежа, която позволява свързването на конкретни пръстени от IP адреси и дава възможност на потребителите да забранят на всякакви други IP адреси да разберат за съществуването им. В допълнение към това, потребителите на F2F могат също да криптират информацията в мрежата, за да подобрят още повече своята сигурност и анонимност.

Заключение

Днес безброй Интернет потребители се опитват да влязат в Дълбоката и Тъмната мрежа. Някои търсят нещо по-специално, което не може да бъде намерено във видимата част на Интернет, а други са просто любопитни [4], [5].

Дълбоката мрежа, Тъмната мрежа и инструменти като Tor са обвити в мистерия. Въпреки сравнително скорошното им създаване, чарът, която притежават, е толкова стар, колкото и самото време. Човешката природа е заинтригувана от това, което не разбира и до което няма достъп.

Разликите между Тъмната и Дълбоката мрежа не се основават само на тяхната видимост, но и на здравословното разпределение на информацията по интернет.

Вярно е, че някои престъпници могат да използват предимството да бъдат почти анонимни в Тъмната мрежа, за да водят незаконни действия и това трябва да бъде спряно възможно най-скоро. От друга страна, без това разделение на управлението на информацията и поверителността, защитата в онлайн пространството би била невъзможна.

References

1. Николов, Л. (2018). *Ролята на Европейския съюз в осигуряването на Киберсигурност*. Международна научна конференция „Политиката на европейския съюз по защитата на информацията и личните данни“, Сборник научни трудове – ШУМЕН 2018, ISBN 978-954-9681-89-5.
2. Николов, Л., Фетфов, О., Борисова, А. (2018). *Съображения за сигурност при писането на кодове с JavaScript*. Научна конференция с международно участие MATTEX 2018, Шумен, ISSN 1314-3921.
3. Nikolov, L., Slavyanov, V. *Network infrastructure for cybersecurity analysis*. International scientific conference 2018, “Vasil Levski” National Military University - Artillery, Air Defense and CIS Faculty, Shumen, Bulgaria, 2018, ISSN 2367-7902.
4. URL: https://digital.com/blog/deep-dark-web/
5. URL: https://www.itbusinessedge.com/articles/what-security-pros-need-to-understand-about-the-dark-web.html
6. URL: https://www.makeuseof.com/tag/i2p-vs-tor-vs-vpn-secure/
7. URL: https://www.zdnet.com/article/online-security-101-how-to-protect-your-privacy-from-hackers-spies-and-the-government/
8. Савова, Ж., Богданов, Р., *Анонимна система за комуникации в киберпространството, използваща протокол TOR*, Сборник научни трудове на научна конференция на Факултет „А, ПВО и КИС” „Новата парадигма за сигурност в киберпространството” Шумен 2014, стр. 259-265, ISBN 978-954-9681-49-9.
9. Савова, Ж., Богданов, Р., *Оценка на изчислителната сложност на алгоритмите за генериране на големи прости числа за целите на криптографията*, Сборник научни

трудове на Научна конференция „Проблеми на информационната сигурност”, гр. Шумен, 2010, ISSN 1314-0647.

10. Савова, Ж., Богданов, Р., *Приложение на недвоичните псевдослучайни последователности в криптографията*, Сборник научни трудове Немус'2012. Институт по отбрана Проф. „Цветан Лазаров”, 2012, ISSN 1312-2916.
11. Досев, Н., Петров, В., *Съвременни тенденции и аспекти на информационната сигурност в автоматизираните информационни системи и мрежи (АИС/М)*, Научна конференция с международно участие MATTEX 2018 , Шуменски университет „Епископ Константин Преславски“, Университетско издателство, Сб. научни трудове том 2, част 1, стр. 85¸95, ISBN 1314-3921.
12. Савова, Ж., Боянов П., Сравнителен анализ на злонамерени уеб-базирани атаки, Научна конференция на тема „Защитата на личните данни в контекста на информационната сигурност”, Факултет "Артилерия, ПВО и КИС" при Националният военен университет „Васил Левски”, гр. Шумен, България, ISBN 978-954-9681-49-9, 6 - 7 Юни 2013, с. 178-183.
13. Boyanov, P., *A novel algorithm for detecting TCP/IP network attacks using hybrid firewall script applied in Linux operating system*, International Scientific Online Journal, www.sociobrains.com, Publ.: Smart Ideas - Wise Decisions Ltd, ISSN 2367-5721 (online), Issue 57, May 2019, pp. 33-41.
14. Boyanov, P., *Countermeasures against various types of cyber attacks in the context of the protection of the national security of Republic of Bulgaria*, Annual of Konstantin Preslavsky University of Shumen, Shumen, Konstantin Preslavsky University Press, ISSN 1311-834X, Vol. VIII E, 2018, pp. 79-85.
15. Боянов, П., Христов, Хр. *Приложение на кибератаките за получаване на информационни отпечатъци и прилагане на разузнавателни техники срещу правителствени агенции, частни организации и академични институции*, Сборник научни трудове - Научна конференция с международно участие "MATTEX 2018" - 25-27 октомври 2018, ISSN: 1314-3921, т.2, ч.1, 2018, с.23-33.
16. Фетфов, О., Боянов, П., Ташева, Ж., Трифонов, Т., *Анализ на съвременните видове уязвимости и експлойти в компютърните мрежи и системи*, Annual of Konstantin Preslavsky University of Shumen, Shumen, Университетско идателство „Епископ Константин Преславски“, ISSN 1311-834X, Vol. VI E, 2016, с. 112-122.
17. Savov, I., Edin pogled varhu sashtnostta na kiberprestapleniyata, spisanie „Politika i sigurnost”,VUSI, 2017, ISSN 2535-0358, s. 36-47.
18. Savov, I., The collision of national Security and Privacy in the age of information technologies, European Police Science and Research Bulletin, European Union Agency for Law Enforcement Training, 2017, ISSN 2443-7883, p. 13-21.
19. Камарашев, Г., Димитрова, С., *Финансовия мениджмънт като елемент на военната логистика*, Trans&Motauto 2005 с.37-41.
20. Kamarashev, G., Dimitrova, S., *Outsourcing as a part of the management of resources for security and defense*, SIBIU 2011, pp.643-647.
21. Kamarashev, G., Dimitrova, S., A*spects of defence and security resource allocattion*, Sibiu 2007.
22. Kamarashev, G., Banabakova, V., *Acquisition – theoretical and practical aspects of application in the defense system*, Brno 2005 с.30-37.

Ekaterina M. Konstantinova, Aleksandyr S. Bradvarov,

POWER OF BLOCKCHAIN TECHNOLOGY: REDEFINING AND DEMOLISHING TRUST IN DIGITAL ECONOMY

Ekaterina M. Konstantinova [1], Aleksandyr S. Bradvarov [2]

[1] *Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, Department "Communication and Computer Technologies", katminkova2@gmail.com*
[2] *Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, Department "Communication and Computer Technologies", alekstefano@abv.bg*

***Abstract**: The biggest advantage of blockchain technology is the ability to build decentralized organizations: organizations that have democratically decentralized governance, keep their data open, public and decentralized, and execute their business processes in a decentralized and public manner on decentralized blockchain platforms. The trend towards building decentralized organizations and economies is expected to intensify in the years to come and continue to change the world we live in. For example, imagine a decentralized ordering platform (Uber decentralized). Such a platform can connect drivers with blockchain passengers through decentralized applications and free of charge. It is a non-proprietary software organization that cannot technically be shut down because it runs at the same time on thousands of machines around the world.*

***Keywords**: Blockchain, Decentralization, Digital economy, International transaction*

СИЛАТА НА БЛОКЧЕЙН ТЕХНОЛОГИЯТА: ПРЕДЕФИНИРАНЕ И РАЗРУШАВАНЕ НА ДОВЕРИЕТО В ДИГИТАЛНАТА ИКОНОМИКА

Екатерина М. Константинова, Александър С. Брадваров

Въведение

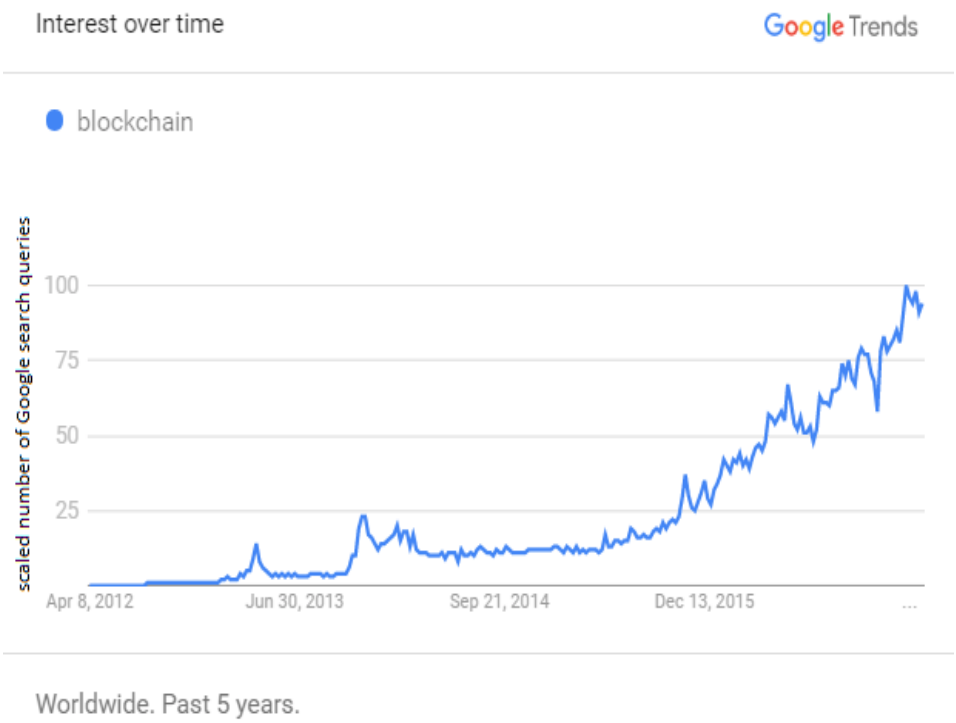
Блокчейн е децентрализирана технология, осъществявана без посредник, която улеснява икономическите транзакции и партньорските взаимодействия. В допълнение към обмена на информация, технологията предоставя и протоколи за обмен на стойност, правни договори и други подобни приложения. Въпреки огромните си преимущества, технологията среща политически предизвикателства, свързани с въпросите за укриването на данъци, прането на пари, финансирането на тероризма и улеснението на много престъпни дейности, като продажба на наркотици и оръжия, както е известно от организираните децентрализирани пазари като Пътят на коприната. Също както и при останалите съвременните комуникационни системи, блокчейн трябва да отговаря на редица технически изисквания. От гледна точка на практическата реализация най-трудно е удовлетворяването на изискванията за висока скорост на предаване на информацията и за осигуряване на надеждна защита на ресурсите на системата от неоторизиран достъп [2], [3], [9], [10], [11], [12], [13], [22], [23], [24].

Изложение

Преимущества на блокчейн

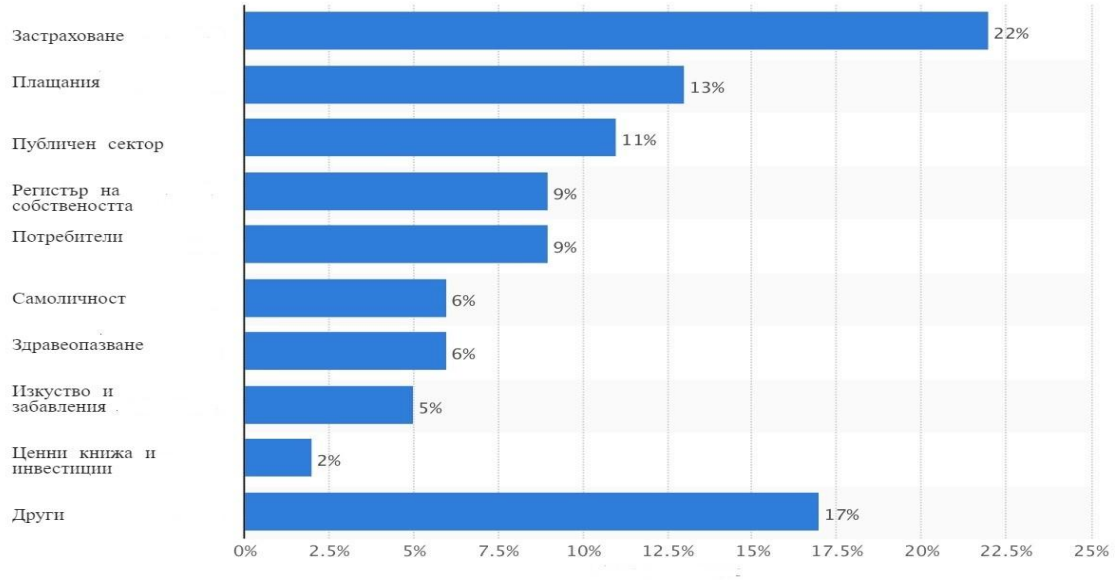
Киберпространството е сложна среда, включваща взаимодействието на хора, софтуер и услуги в Интернет. Блокчейн технологията е децентрализирана база данни, която съхранява регистър на активи и транзакции в P2P, или партньорска мрежа. По същество това е публичен регистър за това кой какво притежава и какви сделки са сключени. Транзакциите са защитени чрез криптография и с течение на времето тази история на транзакциите се заключва в блокове от данни, които след това се свързват и обезпечават чрез криптографски ключове. Това създава неизменен запис на всички транзакции в тази мрежа. Този запис се репликира на всеки компютър, който използва мрежата [1], [2], [9], [10], [11], [12], [13], [14], [15].

Според данни на Google Trends, които показват, че търсенето на думата “blockchain“ се е увеличил експоненциално през последните 5 години, е възможно да навлизаме в пика на използването на блокчейн и регистрите му за документация (Фиг. 1) [8].



Фигура 1: Трендова графика на терминът “blockchain” в глобален мащаб

Това не е приложение, нито компания. Най-близко по функции е до Уикипедия. В тази платформа се вижда всичко в реално време и има достъп до цялата информация. Това се постига чрез списъци от данни за потока на информация, които постоянно се променят и обновяват. Всеки потребител може да проследи тези промени във времето и може да създаде свои собствени уикита, защото в основата си те са просто инфраструктура за данни. Блокчейн е също такава отворена инфраструктура, която съхранява много видове активи. Той съхранява историята на управлението, собствеността и местоположението на различни видове активи като цифровата валута Биткойн, цифрови активи като име на притежател на IP адрес, сертификати, договори, обекти от реалния свят, дори лична информация [9], [10], [11], [12], [13], [14], [15]. Този публичен регистър, който съхранява транзакции в мрежа и се копира многократно, така че да е много сигурен и труден за подправяне (Фиг. 2).



Фигура 2: Приложения на блокчейн, различни от използването на Биткойн

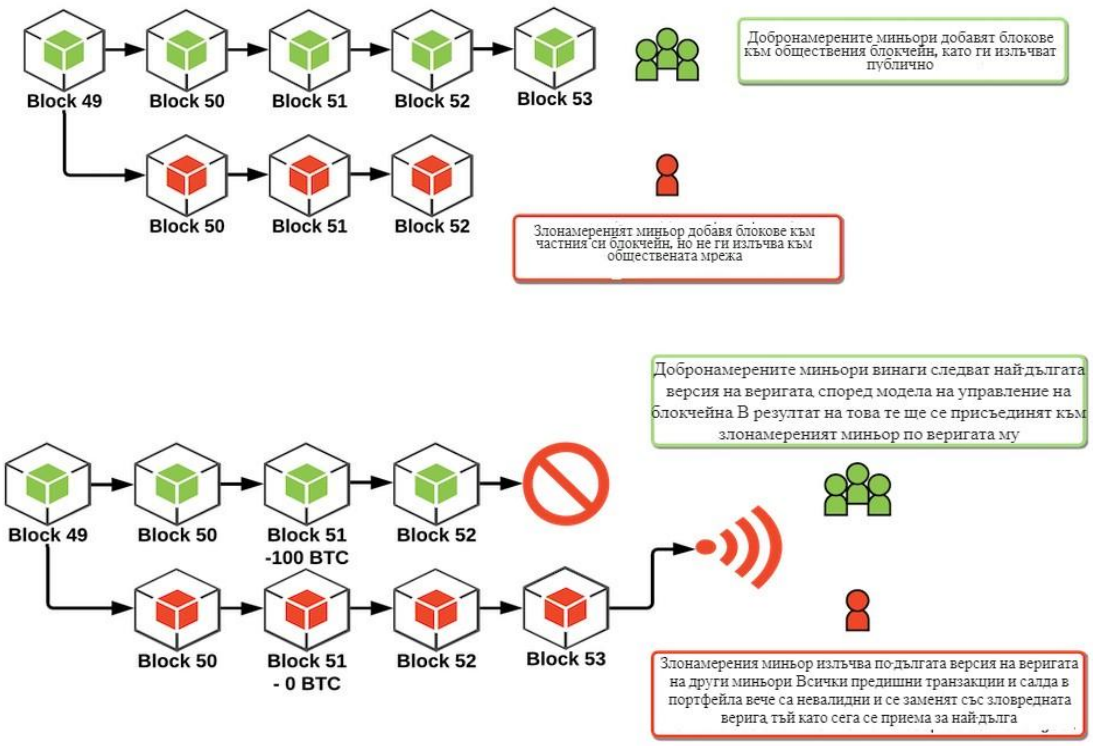
Блокчейн е следващата еволюционна стъпка в развитието на икономиката. Това е така, защото децентрализираният му подход за проверка на промените във важна информация е насочен към многовековния проблем с доверието. Това е социален ресурс, който твърде често се изчерпва, особено на фона на бурните опасения относно сигурността на ценните данни на тази ера [3], [5], [8], [14], [15], [16], [17], [18].

С използването на блокчейн можем да се създаде споделена реалност между субекти, които не са достойни за доверие. Отделните звена в мрежата не е необходимо да се познават или да се доверяват един на друг, защото всеки от тях има възможността да наблюдава и да следи за достоверността на транзакцията. Възможно е създаването на децентрализирана база данни, която има ефективността на монопол, без всъщност да се създава този централен орган. Така че всички тези потребители могат да си взаимодействат, използвайки една и съща база данни, без да се доверяват един на друг. За потребителите това създава пълна прозрачност. Докато обектът в реалния свят се движи по предварително изготвения му път, може да се види неговия цифров сертификат или токен да се движи по веригата. Този процес открива напълно нови възможности на доверие в нашия корумпиран свят.

Недостатъци на блокчейн

Що се отнася до основната блокчейн технология, все още има големи препятствия, които стоят на пътя й, дори и тя да има повече потенциал от криптовалутите. Главно сред тях е, че липсват основните универсални протоколи, които правят Интернет универсално достъпен (TCP-IP, HTML и т.н.). Това дава достъп до информацията само ако потребителят е част от информационната система [2], [6].

Друг потенциално голям недостатък е сигурността на системата. Алгоритъмът за консенсус Proof of Work, който защитава блокчейна на Биткойн, се оказва много ефективен. Има обаче няколко потенциални атаки, които могат да бъдат извършени срещу блокчейн мрежи и 51-процентната атака е сред най-обсъжданите (Фиг. 3).



Фигура 3: 51-процентна атака

Подобна атака може да се случи, ако един субект успее да контролира повече от 50 % от хеширащата мощност на мрежата, което в крайна сметка би позволило нарушаване на хронологията чрез умишлено изключване или промяна на подреждането на транзакциите [8].

Към тези проблеми със сигурността и поради причината, че блокчейн разчита на криптография с публични ключове, една от основните пречки пред масовото използване на технологията е липсата на стандартна система за управление на ключовете, включително механизми за възстановяване и отмяна. Без подходящ механизъм за възстановяване, загубата на частен ключ би възпрепятствал титуляря на акаунта да извърши каквато и да е операция. По същия начин без подходяща система за отмяна на ключ, ако частен ключ е компрометиран всеки потребител притежаващ този ключ може да извършва неоторизирани транзакции от името на акаунта притежател [7].

Друго важно ограничение на технологията е производителността, която е критична в контекста на обществените мрежи. Съществуващите публични мрежи могат да се справят само с ограничен брой транзакции. Например Биткойн системата обработва по-малко от 300 000 транзакции на ден, за разлика от 150 милиона транзакции, обработвани от Visa. Транзакциите с Биткойн се потвърждават на всеки десет минути. Това е значително повече от нужното време, което обикновено отнема за база данни да съхрани и запише информация.

Не на последно място поради анонимността, която съществува в децентрализирания блокчейн и виртуалните валути, те се превръщат във втори дом за всички незаконни транзакции. Един добър пример за това е „Тъмната мрежа“, която по свето същество представлява подземната част на Интернет пространството, която не е индексирана и не може да се достигне чрез стандартните браузъри. Тя разчита на сериозни криптиращи протоколи, като маршрутизатора “Onion” за “Tor” браузър. Всички тези предпазни средства правят „Тъмната мрежа“ център на незаконни и корупционни дейности, като пране на пари, търговия с наркотици и оръжия, трафик на хора, и дори детска порнография. Воденето на кибервойни [9], [10], [11], [12], [13], [17], [18] е съвременен вид война, чрез употребата на Интернет и технологичната база, за превъзходство във военно, икономическо, политическо отношение. Така практически всички водещи държави разработват и из-

ползват собствени кибер оръжия, а човечеството е в началото на кибервойните [2], [14], [15], [16], [19], [20], [21].

Изводи

Както при всички технологии в ранен стадий, предизвикателства има и при блокчейн. Основната инфраструктура трябва да бъде гъвкава с възможност за нарастване, но постигането на консенсус за извършване на такива промени е трудно в работна среда с отворен код. Съществува риск неточна информация трайно да се вмъква в блокчейн. Също така неизменността и необратимостта на транзакциите може да затрудни физическите лица и фирмите да взимат решения, когато има спор [1], [4], [6].

Има голям обществен интерес да се отговори на тези въпроси, но е още твърде рано. Тази технология трябва да се изучава и разбира, за да се увеличат максимално ползите от нея и за постигане на по-добри резултати от развитието ѝ. Със сериозни изследвания може да се открият най-добрите начини при използване на технологията за намаляване на разходите и увеличаване на достъпа до финансови услуги, като същевременно да се защитава социалния капитал, който е жизненоважен за икономическото развитие. В това отношение трябва да се има предвид безпрецедентната конкуренция и предизвикателствата пред действащите финансови институции и регулатори. При колективното вземане на правилно решение, трансформацията може да осигури жизненоважен елемент за постигане на еволюция в глобалната икономическа общност.

References

1. Парашкеванова, Г., Цанков, Ц. (2016). *Киберпрестъпността като основна съвременна заплаха за големите организации*. Научна конференция MATTEX 2016, Шумен, ISSN 1314-3921.
2. Стаменова, А., Диманова, Д., Цанков, Ц. (2014). *Новите войни на XXI век*. Научна конференция MATTEX 2014, Шумен, ISSN 1314-3921.
3. Цанков, Ц. (2012). *Компютърна лаборатория за автоматизиран синтез на сигнали с висока структурна сложност*. Научна конференция MATTEX 2012, Шумен, ISSN 1314-3921.
4. Chang, S.-H., Shih, C.-P. (2018). *The Influence and Application of Artificial Intelligence &Blockchain on Financial Service*. HOLISTICA – Journal of Business and Public Administration, vol. 9, issue 3, pp. 45–54, DOI: 10.2478/hjbpa-2018-0022.
5. Courtois, N., Song, G., Castellucci, R. (2016). *Speed Optimizations in Bitcoin Key Recovery Attacks*. Tatra Mountains Mathematical Publications, vol. 67, pp. 55–68, DOI: 10.1515/tmmp-2016-0030.
6. Jirgensons, M., Kapenieks, J. (2018). *Blockchain and the Future of Digital Learning Credential Assessment and Management*. Journal of Teacher Education for Sustainability, vol. 20, no. 1, pp. 145–156, DOI: 10.2478/jtes-2018-0009.
7. OECD (2017). *OECD Digital Economy Outlook 2017*. OECD Publishing, Paris, 324 p. DOI: 10.1787/9789264276284-en.
8. URL: https://trends.google.com/trends/?geo=US.
9. Фетфов, О., Боянов, П., Ташева, Ж., Трифонов, Т., *Анализ на съвременните видове уязвимости и експлойти в компютърните мрежи и системи*, Annual of Konstantin Preslavsky University of Shumen, Shumen, Университетско идателство „Епископ Константин Преславски“, ISSN 1311-834X, Vol. VI E, 2016, с. 112-122.
10. Савов, И., Боянов, П., *Приложение на кибератаката с отказ на услуги DOS (Denial of Service) срещу информационните ресурси на национални държавни агенции и академични институции*, Politics & Security Journal, Publishing complex HSSE, ISSN 2535-0358, Year III, Issue 1, 2019, pp. 15-20.

11. Фетфов, О., Боянов, П., Ташева, Ж., Трифонов, Т., *Сравнителен анализ на съвременните видове антивирусни програми*, Annual of Konstantin Preslavsky University of Shumen, Shumen, Университетско идателство „Епископ Константин Преславски", ISSN 1311-834X, Vol. VI E, 2016, с. 123-133.
12. Boyanov, P., Hristov, Hr., Fetfov, O., Trifonov, T., *Educational simulation the local area network of academic departments with securely configured FTP server*, International Scientific Online Journal, www.sociobrains.com, Publ.: Smart Ideas - Wise Decisions Ltd, ISSN 2367-5721 (online), Issue 31, March 2017, Bulgaria, 2017, pp. 146-154.
13. Boyanov, P., *Unauthorized access attempts to the information resources of private computer networks in academic institutions via network scanning cyber attacks*, Yearbook of Higher School of Security and Economics, Plovdiv, Publishing complex HSSE, ISSN 2367-8798, Vol. XV, 2018, с. 51-58.
14. Камарашев, Г., Димитрова, С., *Финансовия мениджмънт като елемент на военната логистика*, Trans&Motauto 2005 с.37-41.
15. Kamarashev, G., Dimitrova, S., *Outsourcing as a part of the management of resources for security and defense*, SIBIU 2011, pp.643-647.
16. Kamarashev, G., Dimitrova, S., A*spects of defence and security resource allocattion,* Sibiu 2007.
17. Kamarashev, G., Banabakova, V., *Acquisition – theoretical and practical aspects of application in the defense system*, Brno 2005 с.30-37.
18. Савова, Ж., Богданов, Р., *Анонимна система за комуникации в киберпространството, използваща протокол TOR*, Сборник научни трудове на научна конференция на Факултет „А, ПВО и КИС" „Новата парадигма за сигурност в киберпространството" Шумен 2014, стр. 259-265, ISBN 978-954-9681-49-9.
19. Савова, Ж., Богданов, Р., *Оценка на изчислителната сложност на алгоритмите за генериране на големи прости числа за целите на криптографията*, Сборник научни трудове на Научна конференция „Проблеми на информационната сигурност", гр. Шумен, 2010, ISSN 1314-0647.
20. Савова, Ж., Богданов, Р., *Приложение на недвоичните псевдослучайни последователности в криптографията*, Сборник научни трудове Немус'2012. Институт по отбрана Проф. „Цветан Лазаров", 2012, ISSN 1312-2916.
21. Досев, Н., Петров, В., *Съвременни тенденции и аспекти на информационната сигурност в автоматизираните информационни системи и мрежи (АИС/М)*, Научна конференция с международно участие MATTEX 2018 , Шуменски университет „Епископ Константин Преславски", Университетско издателство, Сб. научни трудове том 2, част 1, стр. 85¸95, ISBN 1314-3921.
22. Николов, Л. (2018). *Ролята на Европейския съюз в осигуряването на киберсигурност*. Международна научна конференция „Политиката на европейския съюз по защитата на информацията и личните данни", Сборник научни трудове – ШУМЕН 2018, ISBN 978-954-9681-89-5.
23. Николов, Л., Фетфов, О., Борисова, А. (2018). *Съображения за сигурност при писането на кодове с JavaScript*. Научна конференция с международно участие MATTEX 2018, Шумен, ISSN 1314-3921.
24. Nikolov, L., Slavyanov, V. *Network infrastructure for cybersecurity analysis*. International scientific conference 2018, "Vasil Levski" National Military University - Artillery, Air Defense and CIS Faculty, Shumen, Bulgaria, 2018, ISSN 2367-7902.

Miroslav P. Dimitrov, Stamen I. Antonov,

APPLICATION OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING IN CAD/CAM SYSTEMS

Miroslav P. Dimitrov*, Stamen I. Antonov**

** National Military University "Vasil Levski",Artillery, AAD and CIS Faculty, amirodimitrov@abv.bg;*
*** National Military University "Vasil Levski",Artillery, stamantonov@abv.bg.*

***Abstract**: Artificial Intelligence is becoming increasingly sophisticated in learning and problem solving. As artificial intelligence grows increasingly intertwined with software and technology, it is only logical that such beneficial technology will surely make its way into CAD/CAM systems and become an integral and vital part of them. Hence, the new CAD/CAM systems will incorporate some sort of 'intelligence' (AI) or machine learning in them. AI drastically cuts down the time for operations like designing or modifying the design for a new or existing model otherwise performed by a human operator. It is also believed that in the future it will completely replace human operators outperforming them in almost every function. This paper examines the status of AI in CAD/CAM systems and presents the pros and cons of its implementation.*

***Keywords**: artificial intelligence, machine learning, CAD/CAM systems.*

Introduction

CAD/CAM or computer-aided design/computer aided manufacturing have started in its infancy as s 2-dimensional design and drawing software. Nowadays CAD/CAM software systems are used for the design and manufacture of prototypes, finished products, and production runs. Furthermore, CAD/CAM systems cover a wide range of applications from drawing blueprints of simple models to complicated 3D models and design tools.

Additional to that, inclusion of attribute software information in database assigning physical meanings to the graphical representation of components, etc. has made CAD/CAM a competitive factor in the increasingly competitive market [10]. CAD/CAM has enabled new methodology in design and manufacturing such as coincident engineering or simultaneous engineering for a reduction in lead-time [9]. Therefore, a reduction in product lead-time is a significant competitive advantage [9]

The introduction of artificial design knowledge and assistance in CAD/CAM software will allow distribution of sophisticated design and manufacturing assistance and knowledge to all its operators. This process will considerably improve the overall design performance and drastically reduce design time. The Artificial Intelligence sector has received an explosive amount of attention and resources, the reason for which lies in how effective machines can be. It can replace massive amounts of manual trial and error, as well as labor, with exact and precise actions. Not only that but AI can also point out existing mistakes, which will reduce the time, and effort specialists put in the making of a quality product. Artificial intelligence and machine learning also finds applications in wide specter of fields including military vehicles and systems [1, 8].Further implementation of AI is made in the fields of satellites and environmental monitoring [5,6]

The importance of AI in CAD/CAM

Currently some of the best CAD/CAM software on the marked provide the operator with a wide range of powerful features such as: design optimization, analysis function and design guidance. Older CAD/CAM systems require the designer to consider not only the designing aspects but also the manufacturing ones, as they also need to be optimized. Hence, the designer needs to have both design and manufacturing knowledge and experience that enables him to design effectively. Therefore, there is a need to incorporate the design and manufacturing concepts as well as the experience of a good designer in CAD/CAM. Currently AI has reached a point where it can easily outperform human engineers in many fields of expertise including the design and manufacturing processes [7]. With the above-mentioned features incorporated in CAD/CAM systems, they can assist the operator “intelligently” in decision-making and design optimization [10].

AI or sometimes referred as machine intelligence is a software technique that programs use to exhibit behavior normally identified with human intelligence [12]. A typical AI analyzes the environment and takes actions which maximize its chance of success. [11] The intended utility function (or goal) can be simple (For example if the AI wins a game of Go it is a considered a success or a "1", if it does not it is considered a failure or a "0".) or complex (Repeating and improving mathematically similar actions to the ones that succeeded in the past.) Goals can be explicitly defined, or induced. If the AI is programmed for "reinforcement learning", goals can be implicitly induced by rewarding some types of behavior or punishing others [11]. Knowledge based systems however rely on factual knowledge and heuristics rather than clever programming, although they posses both expertise and conceptional information. Expert knowledge systems contain three basic components, namely control mechanism, knowledge base and inference mechanism [12]. The main difference between this type of systems and conventional systems is that the aforementioned modularize the data, inference mechanism and controlled mechanism. This process allows for changes in the system by just modifying the knowledge base, thanks to which it grows as the experts behind it use the software, which in turn continues to add information in order to optimize performance. Therefore, incorporation of knowledge base feature into CAD/CAM systems is very important and will be a significant advantage [10].

Neural networks on the other hand are very different from knowledge-based systems. Artificial neural networks (ANN) or connectionist systems are computing systems that are inspired by, but not identical to, biological neural networks that constitute animal brains. Such systems "learn" to perform tasks by considering examples, generally without being programmed with task-specific rules. This is a very important tool for future CAD/CAM systems as it can serve as a “design suggestion tool” where the designer is uncertain. Such system can recommend new and innovative design solutions to the designer.

1.1. AI features in current CAD/CAM software systems

Different manufacturers have implemented the perspective of AI in CAD/CAM in different ways. The leading CAD/CAM software developers have already implemented or are planning to implement different AI driven tools in their software products. The purpose of this section of the paper is to review innovative AI systems and solutions in leading CAD/CAM software products. In the software products, the AI is implemented in a form of a tool for the operator to use. The company Dassault Systems with their software product SOLIDWORKS is an example of a company that already implemented artificial intelligence (AI) is featured within its software by folding AI into SOLIDWORKS CAM 2018 and Xdesign 2019.

SOLIDWORKS xDesign combines CAD modeling and cloud collaboration using a web browser (Fig 1). SOLIDWORKS xDesign incorporates ease of use with innovative design methodologies and cloud collaboration. The ease of use comes with the ability to access the cloud-based software from your browser given the operator has and login credentials. This allows for near instantaneous deployment, allowing companies to quickly add to their CAD portfolio as and when the need arises [13]. An AI sys-

tem in the Design Guidance function of the software. Where the AI guides and assist the operator, it generates solutions during model design. Design guidance is capable of "suggesting solutions for your design challenges" where the AI assists the operator during the design phase. Xdesign is an AI based tool in SOLIDWORKS that utilized design guidance to help engineers to create the best suitable shape for a part that best suits the part's given tasks. The designer inputs the information concerning the constrains and loads on the model and out of this data the AI creates the part geometry automatically [15].

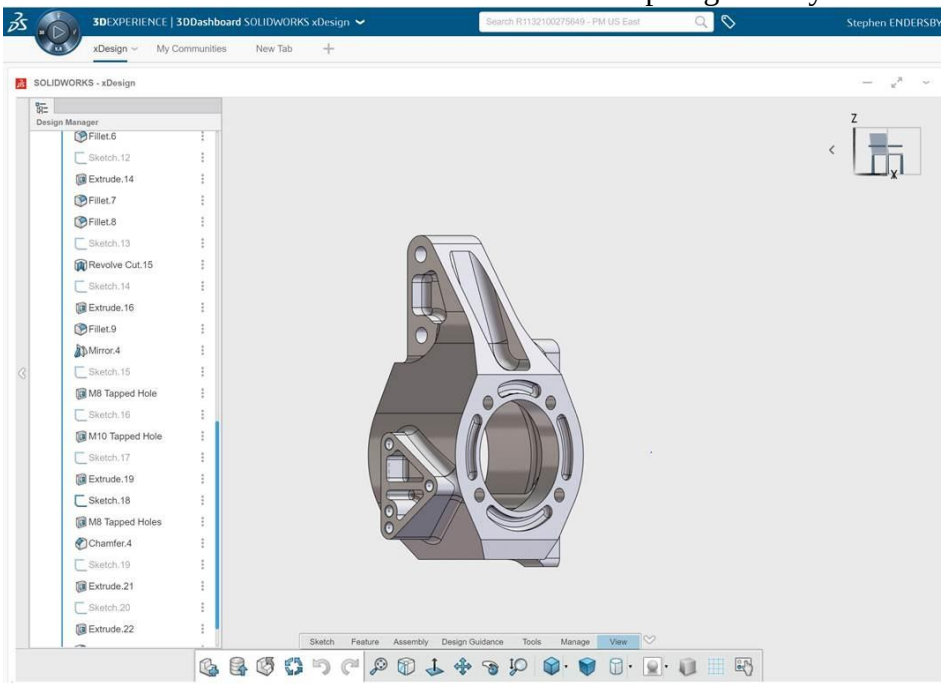


Figure 1: xDesign web based interface [15].

Exalead OnePart – One part also developed by Dassault Systemes is an AI driven software platform. OnePart it capable of recognizing similarities in different models and checks if the part is being duplicated. The tool can be very useful in cases of company reorganizations, mergers, global projects and innovations, as it provides a set of applications to classify company assets, identify master parts for reuse, and ensure that engineering selects the preferred part without recreating a part that already exists in the design library. The tool also allows the operator to find and use existing parts, 2D and 3D designs and related product and manufacturing documentation to minimize duplication (Fig 2).

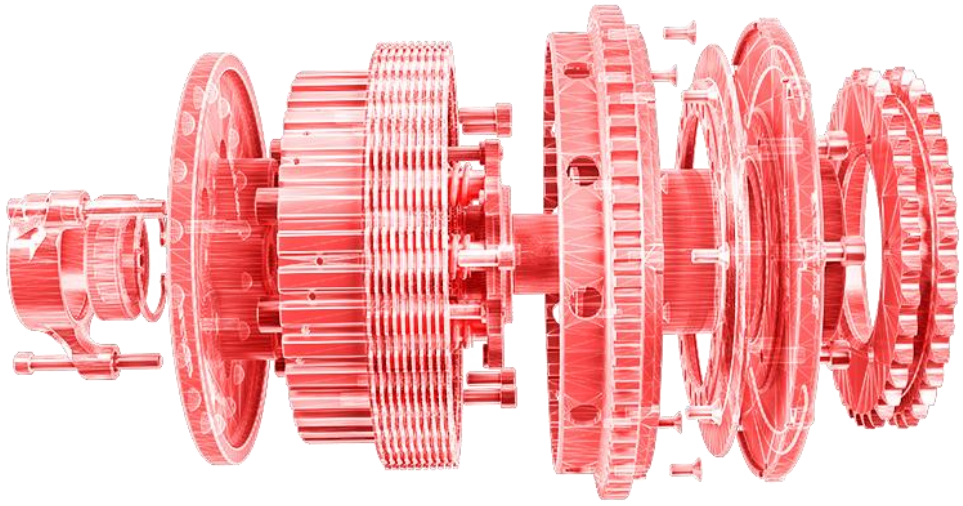


Figure 2: *OnePart* is capable of recognizing very detailed and complex parts and assemblies.

The tool is also capable of revealing all the IP assets of the user without migrating them into the 3DExperience platform. The tool only migrates the relevant data (the data that is not duplicated) lowering costs and speeding up the migration allowing for functions as reusability and standardization increasing engineering efficiency.

SOLIDWORKS CAM – SolidWorks Cam powered by CAM Works from HCL Technologies. The AI CAM tool automatically generates the manufacturing toolpath after the design. This CAM software used the CAD models as it generates the toolpath for the computer assisted manufacturing machine (Fig 3). Engineers and designers who use CAM can evaluate designs earlier in the design process to ensure that they can be manufactured, thus avoiding product costs and delays [15]. Essentially SOLIDWORKSCAM is capable of capturing the design strategies while also recognizing the features and types of materials. These capabilities allow the tool to create a CAM solution that is completely automated.

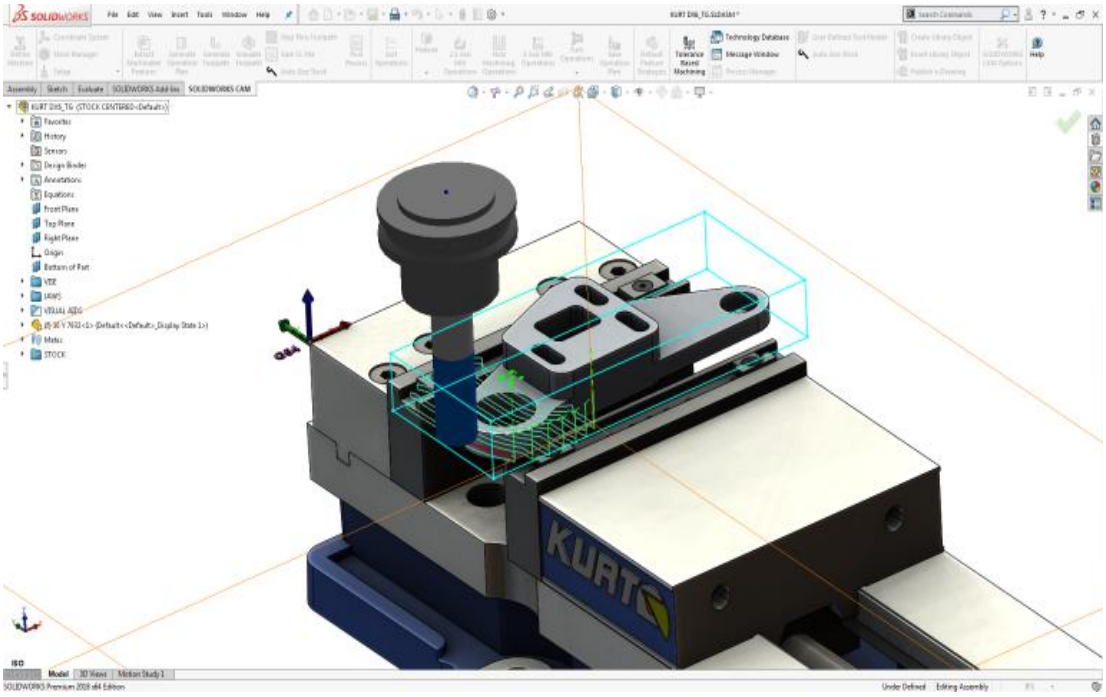


Figure 3: SOLIDWORKS CAM automatically generating the manufacturing toolpath[16].

SOLIDWORKS CAM is also capable of understanding the tolerances within a given part file and change machining strategies accordingly. This helps maintain consistency when programming and saves time by using information that is already created in a 3D model. The process also reduces the chance for error and the possibility of missing a dimension on a traditional drawing [16]. Another capability of SOLIDWORKS CAM is the VoloMill technology provided by CAMWorks [16]. This science-based toolpath allows users to increase output while extending tool life and reducing machine wear with the ability to be used on conventional machines with standard tooling. Because CAD and CAM act as one system within SOLIDWORKS CAM, it makes CAM easier and more straightforward to the software's users. The vendor's tool opens the way toward making CAM ubiquitous on engineers' desktops, much in the way that 3D CAD is now more or less used across an industry that once relied on 2D drawings.

Artificial intelligence Denoiser - Another AI tool implemented by Dassault Systems is an Artificial intelligence Denoiser. Created by INVIDIA the AI Denoiser utilizes machine learning and artificial intelligence, studying thousands of images and sample project files (Fig.4) [14]. The AI Denoiser allows Visualize to anticipate and magically eliminate noise in images increasing quality results 10x faster [12]. Completing any Visualize render job 10x faster is truly game changing. This could be a still image, animation, camera fly, exploded view, new 360-VR content, etc – all 10 times faster than how it is cur-

rently rendered today. Visualize is already known for fast rendering, but this AI Denoiser takes render speeds to another level. This truly makes Visualize the fastest and easiest to use visualization tool available on the market so far. The AI Denoiser is also capable of working both in Fast and Accurate render modes with different render settings. AI and machine learning also finds a large application in geographical transformation of images and image analysis [2, 3].

Figure 4: The effect on the Denoiser tool on an image. On the left, the tool is on removing the noise from the image [4].

Generative Design – is an innovative approach using AI developed by AUTODESK. Generative design is a form-finding process that can mimic nature's evolutionary approach to design. Computer scientists have found ways to aid the building design process. It usually starts with clearly specifying the design goals and then explore innumerable possible permutations of a solution to find the best option. It becomes clearer with an example (Fig.5). An Autodesk team in Toronto has moved into a new building, which was designed using a new design process. Researchers used generative design to assist them in finding the ideal design for the building that met all their needs. The process began with understanding all the parameters that would be important to the residents of the office building — adjacency preference, work style preference, buzz, productivity, daylight, and views to outside [4]. The gathered data is then fed into a computer system that understood these design parameters along with the requirements of the physical location. The algorithm then produced several designs, which fit all these needs that the architect can pick from to match the style and other needs. Since this process was very quick, it was easy to make the design experience iterative and work and reform the final design based on several conversations [4]. Generative design could also raise the efficiency and economy of the overall development process by producing designs that improve scheduling and coordination between multiple stakeholders.

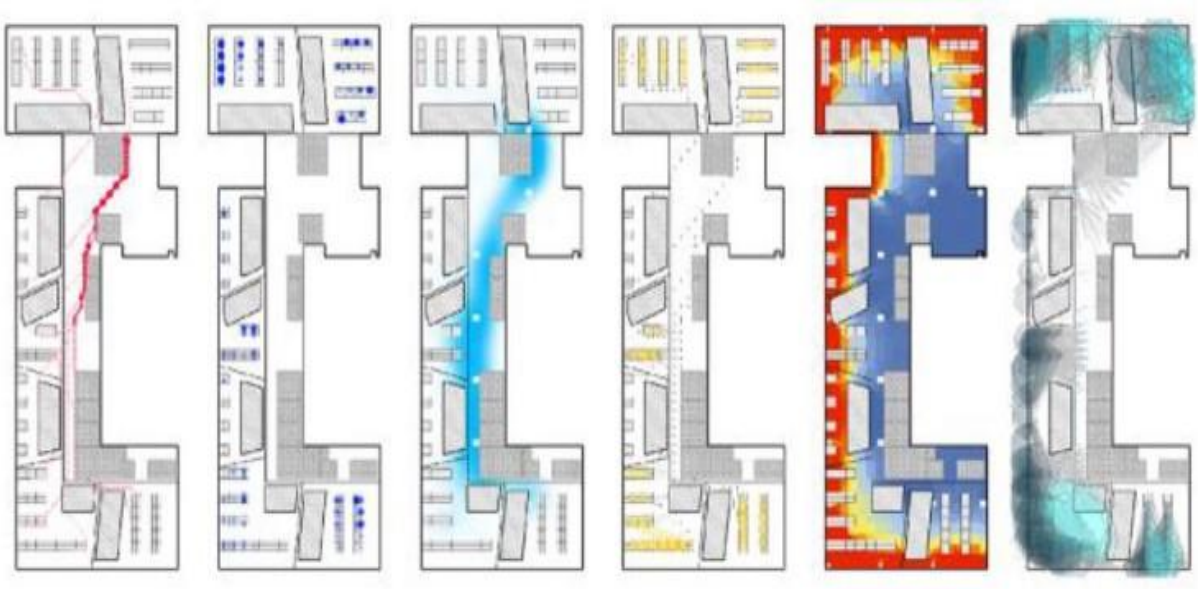


Figure 5: From left to right, each plan is overlaid with a simulation of the following parameters: adjacency preference, work style preference, buzz, productivity, daylight, and views to outside [4].

Conclusion

Artificial intelligence and machine learning technology is growing even more sophisticated every year. Different companies are implementing even more AI and machine learning driven tools in their software products. These tools greatly help engineers in decision-making and problem solving while also increasing their performance and ease of work. In the coming years more and more companies will create their own AI tools, for example ones whose purpose is quality control or ones that enhance and expand model based definition. Full AI driven automation is also an area where AI will play the leading role in future advancements. Judging from the increasingly fast development of AI and machine learning, in a few years' time we might see AI performing all the engineering and modeling work while the creative thinking will be left for the engineer. AI and machine learning are definitely here to stay and they will continue to improve and impress with their features in CAD/CAM systems. Considering the amount of investment and change, which the AI sector has, underwent, it is safe to assume that it is indeed worthwhile. Creating and developing new technologies has always been the key way to stay ahead.

References

1. Марков Д.К., *Специализирани компютърни системи в полевата артилерия*, Издателски комплекс на НВУ „В. Левски, Факултет „Артилерия, ПВО и КИС, Шумен, 2017, ISBN 978-954-9681-83-3 стр. 93
2. Теодора Петрова, „*Геометрична трансформация на изображения*", Сборник доклади от Научна конференция „100 години Българска бойна авиация", Долна Митрополия 2012, стр. 122.
3. Теодора Петрова, „*Прилагане на хистограмен анализ при обработката на изображения*", Сборник доклади от Научна конференция „100 години Българска бойна авиация", Долна Митрополия 2012, стр. 113.
4. Anand Rajagopal, Christina Tetrick (2018). *The Rise of AI and Machine Learning in Construction*.
5. Baev, G., *Satellite Environmental Monitoring of Atmosphere in Aid of the Ecological and National Security*, The 20th International Conference The Knowledge-Based Organization

"*Technical Science and Military Technology*"12-14 Iunie 2014, "Nicolae Balcescu" Land Force Academi, Sibiu, Romania., 2014, p.13-16, ISSN

6. Baev, G., *Research on the likelihood ratio of registered unidentified signals of satellite enviromental monitoring of atmosphere*, International Journal Scientific And Applied Research, Volume 2, 2012, p. 109-113; ISSN:1314-6289
7. Bøgehøj, Lucas. (2016). *Artificial Intelligence vs. Human Intelligence (Man vs. Machine)* (2016). 10.13140/RG.2.2.28050.35526.
8. Conev C.G., Davidov K.S., *A Method For Solving The Task For Modernization Or Purchasing Of Lightly Armored Combat Vehicles*, International scientific conference 2016, “Vasil Levski” National Military University “Artillery, Aircraft Defence and CIS” Faculty, Shumen, Bulgaria, 2017, ISSN 2367-7902.
9. Kusiak A, *Concurrent engineering, automation, tools and techniques*, John Wiley & Sons (1993).
10. Ng, Kok Weng & Poynting, Simon. (1995). *Artificial Intelligence in CAD/CAM*.
11. Poole, Mackworth & Goebel (1998), Russell & Norvig (2003), Legg & Hutter (2007). *Definition of AI as the study of intelligent agents.*
12. Wendy B. Rauch-Hidin. (1988) *A Guide To Commercial Artificial Intelligence*, Prentice Hall, Englewood Cliffs, New Jersey.
13. Brad Williamson. (2019 March 22), *SOLIDWORKS xDesign: An Elegant Way to Work*, Retrieved from: https://blogs.solidworks.com/solidworksblog/2019/03/solidworks-xdesign-an-elegant-way-to-work.html.
14. Brian Hillner. (2018 February 20), *Introducing the New Artificial Intelligence Denoiser*, Retrieved from: https://blogs.solidworks.com/solidworksblog/2018/02/introducing-new-artificial-intelligence-denoiser.html.
15. Jean Thilmany. (2017 December 21), *Putting Artificial Intelligence to Work in CAD Design*, Retrieved from: https://www.engineersrule.com/solidworks-puts-artificial-intelligence-work/.
16. Mike Buchli.(2017 October 4), *What’s New in SOLIDWORKS CAM 2018*, Retrieved from: https://blogs.solidworks.com/solidworksblog/2017/10/whats-new-solidworks-cam-2018.html.

Miroslav P. Dimitrov, Stamen I. Antonov,

PLOTTING DHT11 SENSOR READINGS ON MATLAB

Miroslav P. Dimitrov*, Stamen I. Antonov**

** National Military University "Vasil Levski",Artillery, AAD and CIS Faculty, amirodimitrov@abv.bg;*
*** National Military University "Vasil Levski",Artillery, stamantonov@abv.bg.*

***Abstract**: Graphical representation is always helpful to visualize the data and it becomes very easy to find trends and patterns by looking at them. There are many software available to plot graphs based on the input values, but in embedded system MATLAB is one of the most popular software which can not only present the results in graphical format but also can be easily integrated with hardware and microcontrollers..*

***Keywords**:MATLAB, Arduino UNO, Graphics, DHT11 Humidity sensor, temperature sensor.*

ГРАФИЧНО ПРЕДСТАВЯНЕ НА ДАННИ В MATLAB ПОЛУЧЕНИ ПРИ ЕКСПЕРИМЕНТАЛНОТО ИЗПОЛЗВАНЕ НА МИКРОКОНТРОЛЕР ARDUINO UNO И СЕНЗОР DHT11

Мирослав П. Димитров*, Стамен И. Антонов**

Национален военен университет „В. Левски", Факултет „А, ПВО и КИС"
*Шумен, България, *gancho.hristev@gmail.com, **akumanov13@gmail.com*

Въведение

Графичното представяне винаги е от особено значение за представянето на информация. С помощта на графичното представяне много лесно могат да се идентифицират промени и изменения единствено от изучаването на информацията от получените графики. Има налични много софтуерни продукти за построяване на графики въз основа на входни стойности. Във вградени системи MATLAB е един от най-популярните софтуерни продукти който могат да представят получените резултати в графичен вид. MATLAB също предоставя възможността получените резултати лесно да бъдат интегрирани с хардуер и микроконтролери.

Използването на платформата Arduino (Genuino) в процеса на обучение на студенти позволява по - лесното свързване на теоретичните концепции с хардуерната платформа, чрез която се илюстрират [1], [2].

В доклада е представен модел за запис и графично представяне на данни в MATLAB, получени от датчик за температура и влажност DHT11 свързан към Arduino Uno. Моделът е предназначен за изучаване на методите за въвеждане и визуализиране на данни в MATLAB, в реално време, с помощта на платформата Arduino.

Необходими компоненти [3]:

1. Arduino UNO;
2. MATLAB (версия R2016b или по нова);
3. Сензор за температура и влажност DHT11.

Технически характеристики на Arduino UNO[1]:

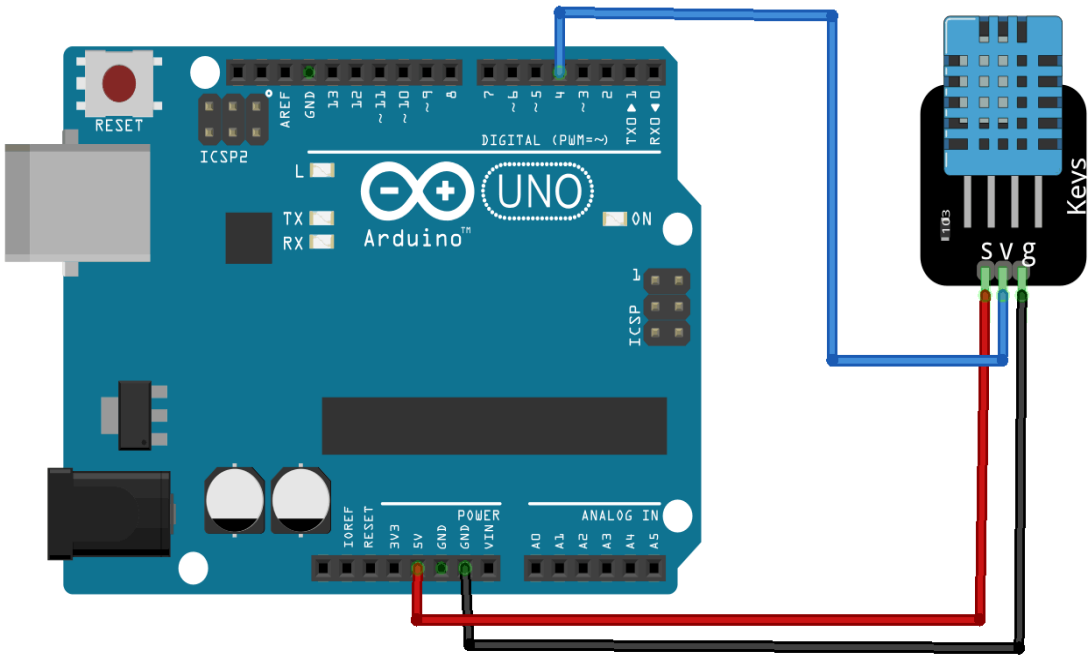
- Микроконтролер базиран на ATmega328P;
- Работно напрежение – 5v;
- Входно напрежение – 7 до 12v;
- Скорост на CLK – 16 Mhz;
- Флаш памет – 32 KB;
- Памет използвана от зареждащия механизъм – 0,5 Kb;
- SRAM – 2 Kb;
- EEPROM – 1 Kb.

Технически характеристики на DHT11 сензор за температура и влажност [2].

- Работен диапазон 20-90% RH 0-50 ℃;
- Коефициент на точност при измерването на влажност ±5%RH;
- Коефициент на точност при измерването на температура ±2℃;
- Чип – 3 пинов едноредов.

3. Асемблиране на нужните компоненти

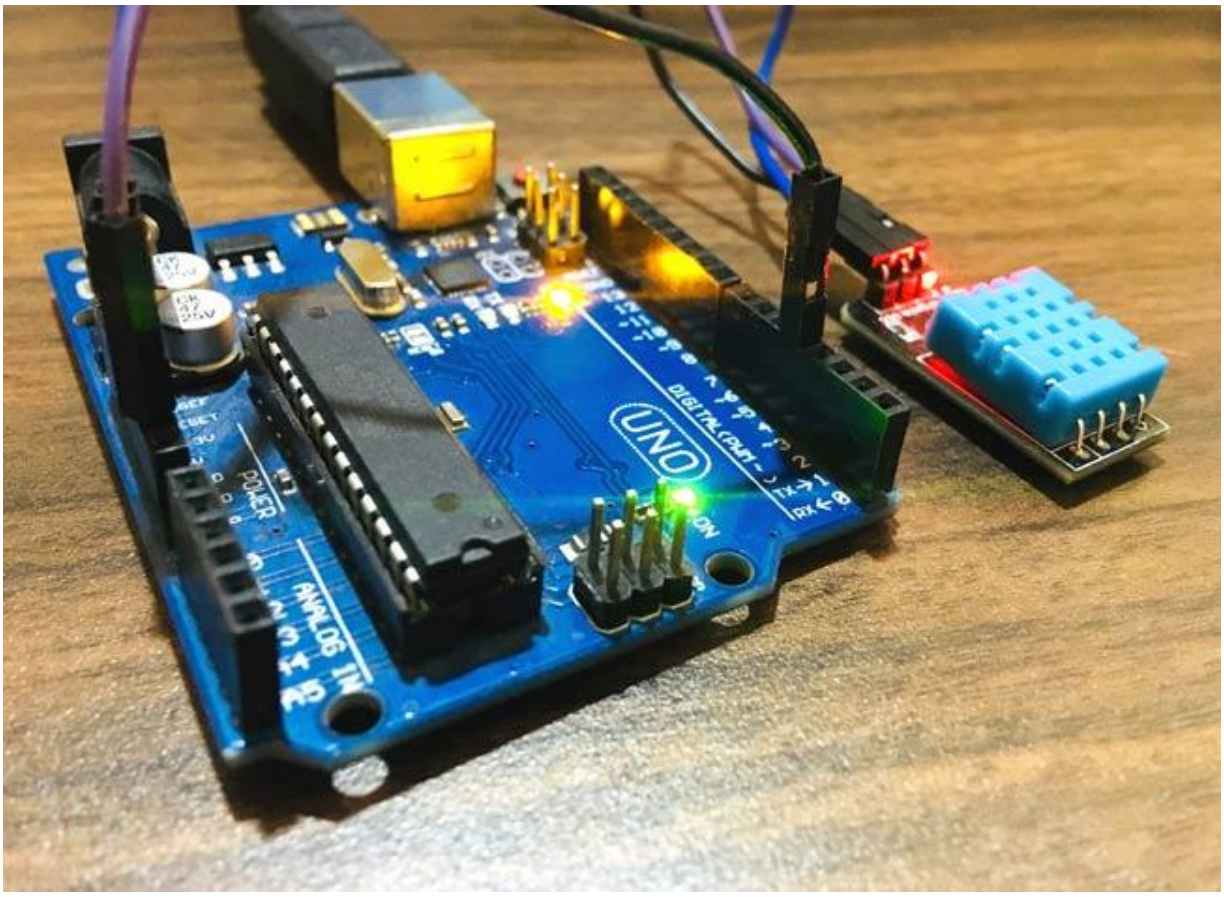
За да бъде изпълнена целта на доклада нужните компоненти за изследването следва да бъдат асемблирани правилно след което да бъдат проверени. Схемата на свързване на различните компоненти е представена на Фиг.1.



Фигура 1: Принципна схема на свързването на DHT11 с Arduino UNO.

Сензорът DHT11 за температура и влажност разполага с 3 пина обозначени с буквени знаци S, V и G. Пин S е свързан с 5-волтовия захранващ изход на Arduino UNO, като по този начин захранва сензора с 5 волта напрежение. Пин V е свързан с дигитален пин номер 4 на Arduino

UNO. Пин G е свързан към заземяващ пин на Arduino UNO. След като всички компоненти бъдат свързани според Фиг.1 проектът има следния вид Фиг.2;



Фигура 2: Физическо свързване на нужните компоненти.

4. Програмиране на софтуерният код на DHT11 взаимодействащ с MATLAB

След като всички компоненти са свързани правилно, трябва да бъде програмиран и зареден програмен код в Arduino посредством Arduino IDE. Пълният код за за регистриране и визуализиране на информацията за температурата и влажността в MATLAB е представена в края на доклада. Програмирането на желаният софтуерен код за нуждите на доклада преминава през няколко ключови етапа който са описани както следва:

1. Добавяне на нужната библиотека за DHT11;

```
#include <DHT.h>
```

2. Дефиниране на пина за трансфер на данни който е свързан към Arduino (пин номер 4);

```
#define DHTPIN 4
```

3. В ‘void setup’ се инициализира серийният и DHT11 сензор;

```
void setup() {
```

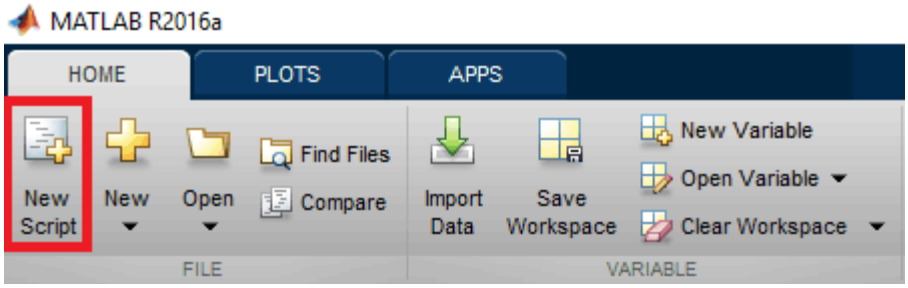
```
  Serial.begin(9600);
  delay(2000);
  dht.begin();   // initialise DHT11 sensor
 }
```

4. В ‘‘void loop’ функцията се задават типа данни за стойностите на температурата и влажността тип *float*. Като за прочит на получените данни се използва командата *float temp = dht.readTemperature()* и *float humi = dht.readHumidity()*. След което за да могат тези данни да бъдат показани на графичен дисплей като по този начин MATLAB ще прочете дадените стойности серийно;

```
void loop() {
  float temp = dht.readTemperature();   //данни за температурата
float humi = dht.readHumidity();   // прочит на данните за температурата
 Serial.print(temp);
  Serial.print(humi);
  delay(2000);
}
```

5. Код в MATLAB за графично изобразяване и запаметяване на данни;

Програмирането се извършва в софтуерната среда на MATLAB. Писането на кода се извършва в менюто „editor window“ показано на фиг.3:



Фигура 3: Бутон “New script” отваря полето за писане на нужният програмен код.

Програмният код започва с дефинирането на променлива за серийна комуникация между MATLAB и Arduino. COM18 е портът през който микроконтролера е свързан съм MATLAB но той може да бъде променен при нужда;

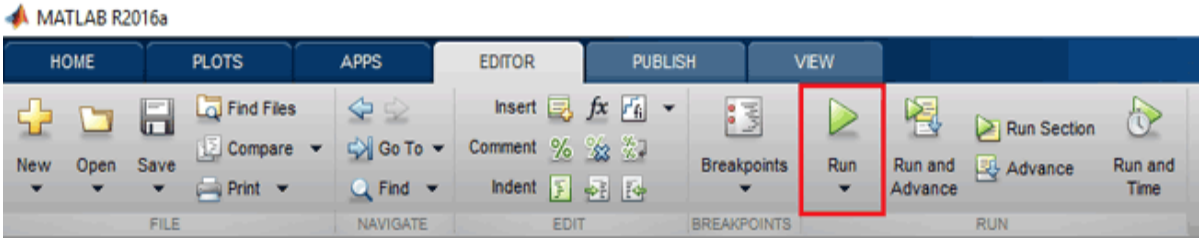
```
s = serial('COM18');// код дефиниращ използването на COM18.
```

Изложеният по долу код функцията *„fopen()“* е използвана за серийна комуникация между Arduino и MATLAB. След което серийната информация е запаметена в променлива наречена *„out“*.
Променливата *out* е стринг от девет цифри където първите четири цифри съдържат данните за температурата а останалите данните за влажността. Следователно при използването на *Temp(i)=str2num(out(1:4)) and Humi(i)=str2num(out(5:9))* съответно софтуерът прочита данните за температура и влажност;

```
fopen(s)
out = fscanf(s)
Temp(i)=str2num(out(1:4));
```

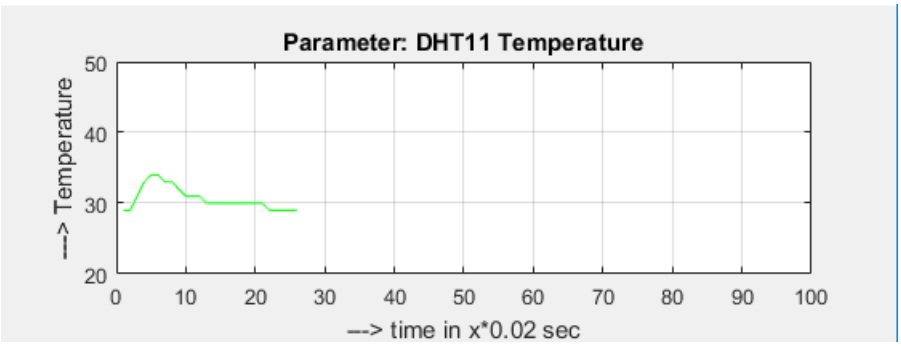
```
Humi(i)=str2num(out(5:9));
```

След като пълният код е зареден в MATLAB след натискането на бутон “Run” кодът е компилиран фиг.4;

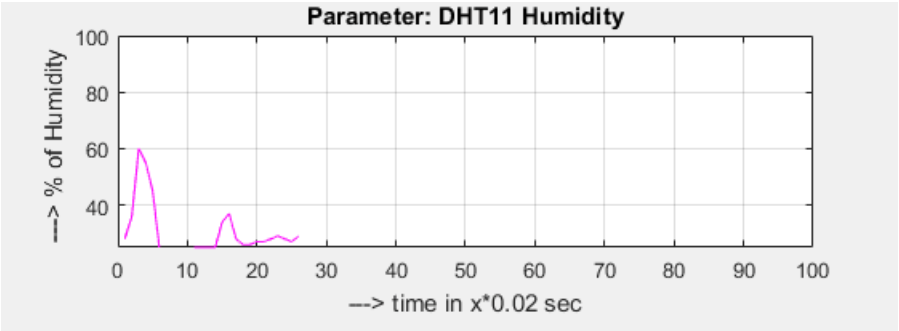


Фигура 4: Бутон “Run” за компилиране и зареждане на програмния код.

Ако кодът е компилиран и изпълнен без грешки, графика в реално време ще бъде показана на екрана. Информацията на тази графика ще бъде обновявана на всеки две секунди. Забавянето от две секунди в продиктувано от факта че времето което е нужно на DHT11 сензора да изпрати нужната информация до серийния порт фиг.5 и фиг.6;

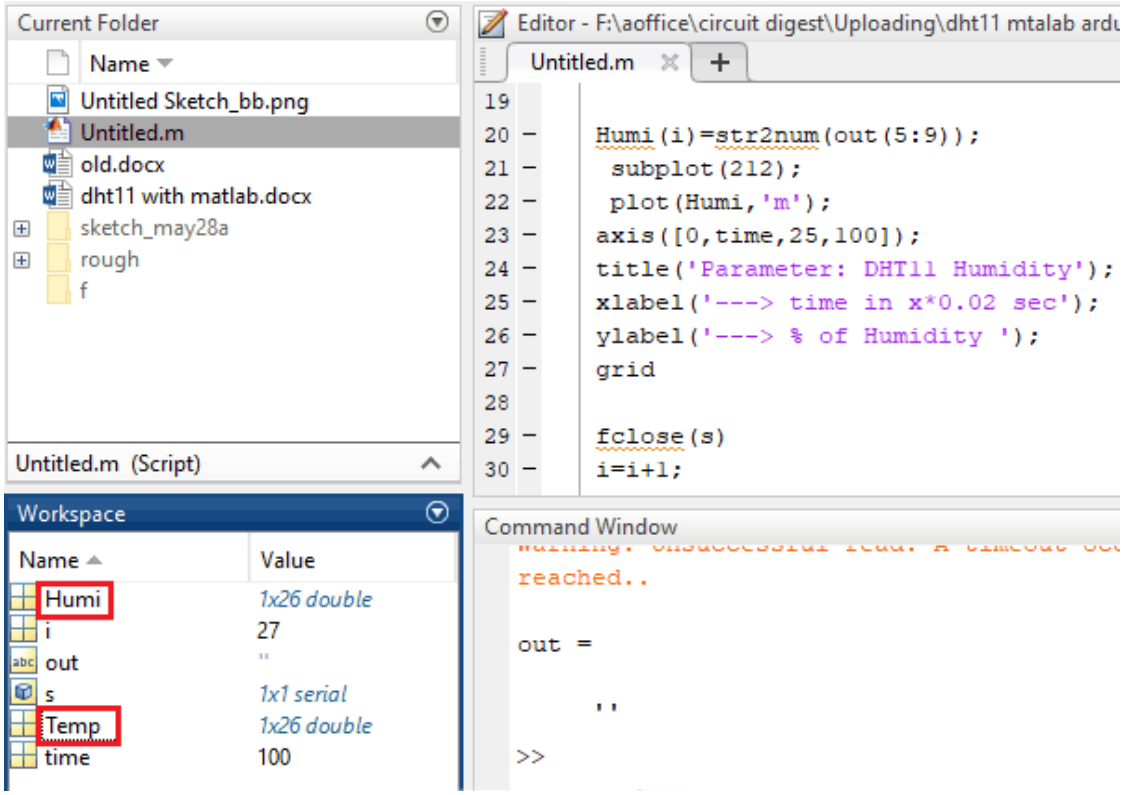


Фигура 5: Диаграма показваща температурните стойности в реално време.



Фигура 6: Диаграма показваща стойностите на влажност в реално време.

За да може запазената информация в реално време за температура и влажност да бъде проверена трябва да бъде отворен работният прозорец показан на фиг.7;



Фигура 7: Диалогов прозорец за запис на получените данни.

6. Пълен обем на използваният програмният код;

Пълният обем на използваният програмен код на Arduino и MATLAB:

- Програмен код на Arduino:

```
#include <DHT.h>

#define DHTPIN 4                                    #define DHTTYPE DHT11

DHT dht(DHTPIN, DHTTYPE);

void setup() {
  Serial.begin(9600);
  delay(2000);
  dht.begin();   // initialise DHT11 sensor
}

void loop() {
  float temp = dht.readTemperature();   //read temperature data
float humi = dht.readHumidity();   //read temperature data
 Serial.print(temp);
  Serial.print(humi);
  delay(2000);
}
```

- Прогамен код на MATLAB:

```
s = serial('COM18');
time=100;
i=1;
while(i<time)

fopen(s)
fprintf(s, 'Your serial data goes here')
out = fscanf(s)

Temp(i)=str2num(out(1:4));
 subplot(211);
 plot(Temp,'g');
 axis([0,time,20,50]);
title('Parameter: DHT11 Temperature');
xlabel('---> time in x*0.02 sec');
ylabel('---> Temperature');
grid

Humi(i)=str2num(out(5:9));
 subplot(212);
 plot(Humi,'m');
axis([0,time,25,100]);
title('Parameter: DHT11 Humidity');
xlabel('---> time in x*0.02 sec');
ylabel('---> % of Humidity ');
grid

fclose(s)
i=i+1;
drawnow;
end
delete(s)
clear s
```

Заключение

Микроконтролерите започват да заемат неизменна част от нашия всекидневен живот. Изложеният в доклада метод за графично представяне на получена информация за температура и влажност с помощта на микроконтролер Arduino и софтуерната платформа MATLAB е изключително ефективен. Използването на таблици за представянето на информация в реално време предоставя възможността за улеснен анализ на информацията. Използваният програмен код е достатъчен за изпълнението на поставените задачи на доклада. Допълнително изследване може да бъде направено при използването на допълнителни сензори и компоненти за извличане на широк спектър от информация.

References

1. Чобанов Д. Г., “Using geniuno zero arm based platform in computer arcitecture courses” SocioBrains, International Scientific Refereed Online Journal With Impact Factor, Issue 59, July 2019, pp. 114 – 117, ISSN 2367-5721
2. Чобанов Д. Г., “Using Arduino based experiments in computer programming education”, International Scientific Refereed Online Journal With Impact Factor, Issue 60, August 2019, pp. 61 – 63, ISSN 2367-5721
3. Khatri P., Jun 18, 2019, “MATLAB Data Logging, Analysis and Visualization: Plotting DHT11 Sensor readings on MATLAB”, Retrieved from: https://www.instructables.com/id/Charlieplexing-the-Arduino

Miroslav S. Karov,

INOVATIONS IN SMALL ARMS SYSTEMS

Miroslav S. Karov

"Vasil Levski" National Military University, Shumen, Bulgaria, roshevv7@gmail.com

Abstract :*This reportr presents the innovations ins small arms systems, that are currentin divelepoment or already issued.*

***Keywords**: improvised small arms, inovations*

ИНОВАТИВНИ СТРЕЛКОВИ СИСТЕМИ

Мирослав С. Каров

Факултет „Артилерия ПВО и КИС"-Национален Военен Университет „Васил Левски"

***Анотация**: В доклада са представени иновативни стрелкови системи, приети на въоръжение или намиращи се в процес на разработка.*

***Ключови думи:** стрелково оръжие, иновации.*

Въведение

Настъпилите промени в схващанията за воденето на бойните действия все повече водят до промяна в структурите и въоръжението на армейските подразделения. Необходимостта подразделенията да са мобилни, добре екипирани и въоръжени с модерни и с повишени бойни качества оръжия излиза на преден план. Все повече се налага изводът, че за в бъдеще ще нараства значението на качеството на въоръжението за сметка на неговото количество.

Стрелковото оръжие е част от въоръжението, предназначено за унищожаване на живата сила на противника на близки дистанции. Всеки военнослужещ в бойна обстановка притежава един или друг вид стрелково оръжие. Две от особеностите на този вид оръжие са наличието на големи количества в армията и големият разход на бойни припаси по време на бойните действия. Поради посочените по-горе особености на този вид въоръжение модернизацията му е от съществено значение за всяка една армия. [1] Всичко това обуславя необходимостта задълбочено да се анализират изискванията и да се очертаят насоките в развитието на стрелковото оръжие на базата на визиите за воденето на бойните действия. Тенденциите в областта на стрелковото оръжие имат за цел повишаване на бойните възможности на отделният войник и шансовете му за оцеляване в боя.

Основните направления по които се работи за усъвършенстване на стрелковото оръжие са следните:

- Повишаване на бойната ефективност на системите.
- Повишаване на безопасността и удобството при експлоатация на системите.
- Намаляване на себестойността на системите [2].

Повишаването на бойната ефективност на системите е свързано с:

- намаляване на масата и габаритите на системите;

- повишаване на точността;
- повишаване на надеждността и безотказността на системите;
- многостранност на бойното използване на типовете оръжия;
- повишаване на поразяващото действие [2]

Намаляването на масата и габаритите на оръжието целят постигане на по-голяма тактическа маневреност на отделният боец. За постигането на това, от една страна, се намалява калибърът на системите, при което се намалява масата на самата система и масата на боеприпаса, а това дава възможност да се повиши носеното от войника количество бойни припаси. От друга страна все по-широко приложение при изработването на оръжията намират синтетичните материали. От тях се изработват: пълнителят, приклада, ложата, ръчника, детайли на ударно-спускателният и други механизми. Чрез употребата на синртетични материали освен намаляване на теглото се повишава устойчивостта на оръжието на влиянието на атмосферните условия и се намалява себестойността му. Допълнително предимство е това, че тези материали могат да бъдат оцветени в съответната разцветка отговаряща на конкретните условия на местността. За намаляване на дължината на оръжието при запазване на дължината на цевта, а от там и на далекобойността, пълнителят се поставя зад пистолетната ръкохватка, а частите на ударно-спускателният механизъм се разполагат в приклада. Този схема за реализация на оръжието намира все по-широко приложение в съвременните системи.

Повишаването на точността на системата е свързана с поставените и мерни прибори, с избраният принцип на работа на автоматиката и с предвидените производствени допуски и сглобки. Оптичните мерни прибори все по-често се използват като основни за стрелковите системи, а механичните са дублиращи. За закрепването им се използват универсални стойки позволяващи присъединяване към оръжието на различни типове мерници – дневни, нощни, оптични или механични. Това позволява в бойна обстановка бързата подмяна на един вид мерни прибори с друг в зависимост от конкретните условия или при повреда. Многостранното бойно използване се характеризира с възможността оръжието да бъде използвано за въздействие по различни видове цели и в различни условия на бойната обстановка. За удовлетворяване на това изискване новоразработените системи, освен възможност за поставяне на нож-щик, дават възможност и за поставяне на подцевен гранатомет, оптически дневни и нощни мерни прибори, бързомерци, целеуказатели, тактическо фенерче и други специални прибори. Монтирането на гранатомет позволява да се поразява противник разположен в окопи, зад сгради, или други препятствия, а така също и да се разрушават противникови съоръжения и да се поразяват небронирани превозни средства. Нощните мерни прибори дават възможност за водене на ефективни бойни действия в условията на ограничена видимост .

Във връзка с предстоящата модернизация на американската армия са разработени няколко проекта чиято цел е разработването на нови високотехнологични екипировки и въоръжение. Проектите предвиждат създаването на ново индивидуално и на ново групово стрелково оръжие.

Проектът OISW предвижда новото оръжие да съчетава в себе си два основни компонента – 5,56 мм щурмова карабина и 20 мм гранатомет. В състава ще влизат още: миникомпютър за управление на огъня; лазерен целеуказател и далекомер; оптически дневен и нощен мерник; видеокамера; термовизьор; електронни сензори за отчитане на природните фактори имащи отношение към стрелбата, микропроцесор, обработващ и предаващ данните за целта и условията за стрелба на взривателя на гранатите в реален мащаб от време; прибор за съпровождане на целите и компас. Различните устройства ще са монтирани на двете оръжия, които ще могат да се използват както заедно така и поотделно.

Модулът с гранатомета ще се разполага върху този на щурмовата пушка, а общото им тегло не трябва да надвишава 5,5 кг. Когато са интегрирани едно в друго двете оръжия ще из ползват общ спусък. Системата за управление на стрелбата ще позволява откриване на огън по целите едновременно с куршуми и гранати или само с единия тип боеприпаси в съответствие с избора на стрелеца. В оптичният мерник трябва да има лазерен далекомер, което точното определяне на

разстоянието до целта и се изобразяват на дисплей, монтиран на каската на боеца. При стрелба с гранати е предвидено балистичен миникомпютър автоматично да програмира времето за задействане на дистанционният им взривател, така че той да взривява гранатата на разстояние 1 метър над целта.

Комбинирано пехотно оръжие AICW

Оръжейната система AICW (Advanced Infantry Combat Weapon - перспективно бойно оръжие за пехотата) е разработената в Австралия от компанията ADI Limited, която отговаря за стрелковата част на системата, от компанията Tenix Defense отговаряща за разработването на електронния мерников комплекс и от Metal Storm - за разработването на гранатовъргачните модули.

За основа на австралийската разработка е послужила концепцията на американската система OICW XM29. Основа на стрелковата част на AICW е пушката F88A2, която се произвежда в Австралия по лиценз на австрийската щурмова пушка Steyr AUG.

Автоматиката на пушката работи чрез отвеждане на част от барутните газове, а заключването на затвора се осъществява посредством завъртането му. В уголемения приклад е поместена електронна схема, която управлява стрелбата на гранатохвъргачката и батерия за захранване на тази схема. За AICW е разработен трипозиционен предпазител-превключвател със следните положения: "предпазител-пушка-гранатохвъргачка". Управлението на стрелбата с пушката и гранатохвъргачката се осъществява с помощта на един спусък. За системата могат да се използват всякакви мерни прибори - механични, оптични дневни и нощни и далекомери, осигуряващи автоматично позициониране на мерният знак в съответствие с разстоянието до целта и избрания тип боеприпас. В перспектива се предвижда да се използват мерници, посредством които и да се програмират дистанционните взриватели на гранатите. Най-интересния компонент на системата AICW е многозарядната гранатохвъргачка Metal Storm. Устройството и е пределно опростено, сведено до сменяема цевпълнител и електронна схема. Благодарение на конструктивното обединяване на цевта и пълнителя чрез смяна на цевта е възможно да се промени типа на бойният припас и техният калибър. Например, боецът може да носи цеви с 20 мм високоскоростни и далекобойни осколочно-фугасни гранати, или цеви с малкоскоростни 40 мм гранати с нелетална бойна част (димни, сълзотворни и др.). При необходимост новата цев се поставя на оръжието, като при това нейната електронна схема за управление се съединява с мерниковия модул и му предава данните за типа на използваните бойни припаси, което позволява без участието на стрелеца мерниковата система

Фиг. 5. Комбинирано пехотно оръжие AICW .

Фиг. 2. Комбинирано пехотно оръжие AICW.

да се адаптира за водене на точен огън. Изстрелите във вид на гранати от различен тип се разполагат направо в цевта. Те са разработени без гилзи. Възпламеняването на зарядите се извършва с електрически сигнал посредством специална електронна схема, чиито електрически възпламенители са разположени в стените на цевта. Цевите на Metal Storm се зареждат само в заводски условия и преди стрелба се монтират към пушката.

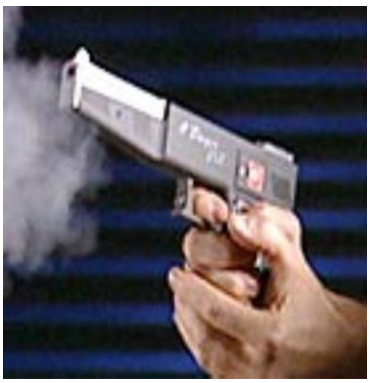
За осъществяване на стрелбата електронната схема подава напрежение на възпламенителя на най-предния барутен заряд в цевта и първата граната се изстрелва. При следващо натискане на спусъка се възпламенява вторият заряд и се изстрелва втората граната. В зависимост от калибъра и типа на гранатите в цевта на гранатохвъргачния модул могат да се поместят от 3 до 6 гранати. Предимствата на гранатохвъргачката Metal Storm се заключават в липсата на движещи се части и просто механично устройство. Основни недостатъци са невъзможността да се презарежда цевта в други освен в заводски условия и зависимостта от източник на захранващо напрежение.

Експериментален образец пистолет VLE

В конструкцията на същият има редица особености. На първо място при тази система липсва пълнител. Боеприпасите, които са 7 на брой са поместени един зад друг направо в цевта. Същите нямат гилза и капсул-възпламените.

При натискане на спусъка към боеприпасите се подава електрически импулс. На следващо място поради особеностите на самите боеприпаси и разполагането им в цевта при системата липсват основните механизми за презареждане и екстракция на гилзата. Традиционният механичен ударен механизъм е заменен с електрически, което осигурява изключително висок темп на стрелба.

Спускателният механизъм на пистолета позволява воденето на единичен и автоматичен огън. Управлението на стрелбата се извършва от електронна система, която задава продължителността на откоса при автоматичен огън, след като стрелящият предварително е въвел желаният брой изстрели, посредством датчик разположен до спусъка. Потвърждаването на готовността за стрелба в избраният от стрелеца режим се извършва посредством електронен глас. За да се използва оръжието е необходимо да се въведе идентификационен код. Въведена е и система за идентификация на стрелеца, която допуска с оръжието да борави само притежателят му. Основният недостатък на оръжието се явява презареждането му. На сегашният етап презареждането се извършва единствено чрез подмяна на цевта с друга.



Фиг.3. Експериментален образец пистолет VLE.

Оръжие на ГАУС

Пушката на Гаус е разработена на принципа на електромагнитно ускорение на маса. Носи името на немския учен Карл Гаус, който полага основите на математическата теория на електромагнетизма.Техния принцип на работа (създаване на бягащо магнитно поле) е подобен на този при устройството, известен като линеен двигател. Гаус се състои от намотка вътре, което е багажника (обикновено диелектрик). В единия край на стеблото се вкарва в корпуса (направен от феромагнитен материал). Когато електрически ток тече в соленоида, магнитно поле, което ускорява снаряд, "дърпа", това вътре в соленоида. В краищата на снаряда са оформени с полюса ориентирани според полюсите на бобината, поради което след преминаване на снаряд центъра на соленоида се изготвят в обратна посока, т.е. спиране.

Същият ефект се получава при използване на феромагнитни материали, но това не е изразена като ярко

Фиг.4. Оръжие на ГАУС.

се дължи на факта, че черупката е лесно намагнитване обрат (принудителна сила). токов импулс в соленоида трябва да бъде кратък и мощен за максимален ефект. Обикновено, електролитни кондензатори са използвани за производството на такъв импулс с високо работно напрежение.Електро магнитното оръжие - 01 Алфа разполага с 8 степенен превключвател , всеки с независим инфрачервен порт. Управлението на стрелбата и секвенцията на намотките се контролират от прецизен микроконтролер превключващ портовете , което позволява изтрелването на до 4 куршума в секунда с начална скорост 45 м/сек.

‘EMG-01 A’ е конфигуриран да стреля с плътни стоманени цилиндърчета с размери 0,63x1,9 см и маса 4,6 гр.”EMG -01 A” се доставя стандартно с 9 заряден пружинен пълнител който може да побере до 9 куршума с единично подреждане и да даде до 6 изтрела на пълен автомат. Пистолетът се достава стандартно и с 1500mAh 6s лииева полимерна батерия, което осигурява захранването за повече от 100 изстрела преди да се наложи презареждане. Устройството не е „оръжие” по смисъл на закона. 45 метра в секунда е приблизително скоростта на хвърлена бейзболна топка –твърде ниска за „истинско” оръжие но все пак използва стоманен снаряд ,който тежи 20 мъти повече от този на топче за еърсофт (0.25 гр.) и който на разстояние до 3 метра е в състояние да пръсне стъкло.

Тактико-технически характеристики:
- дължина на цевта: 25,4 см
- диаметър: 0,63 см
- обща маса : 2,5 кг

Специфики на ускорителя:
- Основен източник на захранването: 1 x6S LiPo 25.2V ,1500mAh
- Кондензатори:2x 180mF/25 V
- Превключватели :8x IGBT
- Проектил: 0,63x1,9 см въглеродна стомана
- Капацитет: 9 снаряда
- Темп на стрелба: 4 изтр./сек
- Начална скорост: 45 м/сек

Лазерна карабина PHaSR

В Научноизследователския институт на ВВС на САЩ е разработена лазерна карабина с несмъртоносно действие, наречена PHaSR (Personnel Halting and Stimulation Response). Тя е предназначена за борба с безредици и се явява първото в света индивидуално лазерно оръжие.

PHaSR генерира лазерно излъчване с две различни дължини на вълните. При попадане в очите, лазерния лъч от карабината предизвиква временно ослепяване на противника, неизбежно съпроводено с психологически шок. В резултат облъчения губи възможност за ориентация в пространството и за по-нататъшни активни агресивни действия.Произвеждането на "изстрелите” се осъществява напълно безшумно, което не позволява демаскиране на източника на излъчване и допълнително провокиране на тълпата от това.

Ефектът от лазерното въздействие отминава без да оставя трайни увреждания върху зрението.Първите два експериментални прототипа на PHaSR в момента преминават изпитания в лабораторията на американските ВВС в Тексас. Скоро се очаква на тестове да бъде подложен и усъвършенст¬ван прототип на лазерната карабина, снабден с далекомер u позволяващ на стрелеца да регулира силата на излъчване.

Фиг.5. Лазерна карабина PHaSR (Personnel Halting and Stimulation Response).

Система за стрелба под ъгъл „Corner Shot”

“Corner Shot” е една от по-авангардните разработки целящи повишаване на бойната ефективност.Това е израелската системата която позволява да се стреля под ъгъл, като стрелящият не се показва иззад укритието в което се намира. На системата могат да се монтират основните типове обикновени и картечни пистолети и гранатомети намиращи се на въоръжение в израелската армия. Основното предназначение на системата “Corner Shot” е да се поразява противник без да се попада в неговото полезрение. Конструктивно системата се състои от две части. Предната част включва цветна видеокамера и накрайник, към който се прикрепва стандартното стрелково оръжие. Задната част се състои от цевна кутия, ударно-спускателен механизъм, който се свързва със спусковия лост на самото оръжие, приклад и монитор на който се наблюдава заснетото от видеокамерата. Предната и задната част се свързват посредством шарнирно съединение, което позволява на предната част да се завърта в хоризонталната равнина с ъгъл до 180^0

В случай на необходимост системата може да се използва и като стандартно оръжие, като предната част се насочи напред. Разработки, даващи възможност да се наблюдава и води огън по противник без да се излага стрелящият на въздействието на противниковият огън има още в Русия, Франция и САЩ и други страни. Също с цел повишаване на многостранното бойно използване на стрелковите системи се разработват и въвеждат нови видове боеприпаси, даващи възможност за по-широка гама на употреба на даден вид оръжие. Различните видове боеприпаси в зависимост от предназначението на вида стрелково оръжие могат да подобряват съответно убивното, пробивното или спиращото действие на куршума.

Могат също така да са предназначени и за решаването на специфични видове задачи като целеуказване и коригиране на стрелбата (трасиращи куршуми), възпламеняване на материали или техника (запалителни куршуми) или водене на безшумна стрелба.

Фиг.6. Система за стрелба под ъгъл orner Shot”.

Изводи: 1. От направения преглед на иновативните стрелкови системи може да се направи извода, че тенденциите за развитието на стрелковото оръжие са свързани с повишаване на бойните възможности и безопасността на личния състав, като същевременно се търсят различни от конвенционалните принципи за реализация на бойни системи.

References

1. Цонев Ц. Г., Давидов К. С., Основи за устройството на стрелковото оръжие – част I., Ш. 2013.ISBN 978-954-9681-53-6

2. Цонев Ц. Г., Богданов А. И., Изследване кинематиката на подвижната система на стрелковото оръжие., Ш. 2013.ISBN 978-954-9681-56-7

3. Цонев Ц.Г. Давидов К. С., Класификация на стрелковото оръжие и механизмите му.,”Стено”,В,2010 ISBN 978-954-449-483-4

4. Списание „Всичко за оръжието” – 2016 брой 22.

Marina R. Monova,

IMPROVISED SMALL ARMS DURING CRISES OF NON-MILITARY CHARACTER

Marina R. Monova

"Vasil Levski" National Military University, Shumen, Bulgaria, 1"Karel Shkorpil" str.,
marinamonova@abv.bg

Abstract: *The paper is an attempt to show some peculiarities concerning improvised small arms that are designed and produced during crises of non – military character. Several examples of basic structural and operational principles of small arms are analyzed in the report.*

***Keywords**: improvised small arms*

САМОДЕЛНО СТРЕЛКОВО ОРЪЖИЕ ПРИ КРИЗИ ОТ НЕВОЕНЕН ХАРАКТЕР

Марина Р. Монова

"Васил Левски" Национален военен университет, Шумен, България, 1"Карел Шкорпил",
marinamonova@abv.bg

Снабдяването на цивилни структури и лица с бойно стрелково оръжие при кризи от невоенен характер е свързано с големи затруднения. Поради тази причина един от способите за набавяне на огнестрелно оръжие е изработването на самоделно такова.

Основните методи за изработването на самоделно стрелково оръжие са:

- преправяне на газово, пневматично, ловно и старо стрелково оръжие в бойно;
- изработка на самоделни оръжия при наличие на отделни части от бойни системи.

При изработване на самоделни оръжия най-често срещаните варианти са:

- стрелкови системи от най-прост тип – само с цев;
- стрелкови системи само с ударен механизъм при който е наличен ударник;
- стрелкови системи с ударно - спускателен механизъм.

При традиционните изработвани от военно-промишления комплекс, стрелкови системи, структурата на автоматичното стрелково оръжие се определя от съвкупността от всички негови детайли, механизми и устройства, осигуряващи основното му предназначение – произвеждането на прицелен изстрел [5].

В структурата на всяка една оръжейна система влизат: основни и допълнителни детайли и механизми [5].

Основните детайли са: цев, цевна кутия (рама) и затвор [4].

Основните механизми и устройства са: механизми за подаване на патроните, механизъм за заключване и отключване, ударен механизъм, спускателен механизъм, изхвъргачен механизъм, отражателен механизъм, предпазителен механизъм, възвратен механизъм и мерни прибори [5].

Допълнителните механизми и устройства са: механизми за презареждане, ускорителни механизми, противоотскочни механизми, механизми за серийна стрелба, механизми за забавяне на темпа на стрелба, буферни устройства, дулни устройства (шумозаглушители, дулни спирачи, компенсатори, огнеприкриватели, усилватели на отката), устройства индикиращи наличието на патрон в патронника и устройства за смазване на патронника [5].

Допълнителните детайли на оръжието не са задължителни за всяка система. Допълнителни детайли, могат да бъдат: приклад, ложа, полуложа, капак на цевната кутия, ръчник (пистолетна ръкохватка), газова тръбичка, газова камера, двунога, спускова скоба и газов регулатор [2].

Основните затруднения които се срещат при изработването на стрелкови системи са свързани с направата на основните детайли, които изискват специални термични обработки, специални марки стомани и имат трудни за изработване повърхнини (нарезна част, патронник и други). Поради тези причини най-често се вземат годни за бойно използване такива от стари образци оръжия, газови или пневматични системи. В болшинството от случаите самоделните стрелкови системи не са с автоматично презареждане, поради което не се изработват механизми за подаване на патроните, възвратни механизми и предпазителни механизми. Ударните и спускателните механизми или се вземат от газови и ловни системи или се изработват самоделно. Информацията в интернет позволява да се намерят необходимите данни за конструкцията им. Механизмите за заключване и отключване, аналогично, се вземат от стари бойни системи, газови или ловни оръжия. Мерните прибори, аналогично, се вземат от бойни системи или изобщо не се изработват, понеже оръжието е ефективно на разстояние по-малко от 50 m.

Допълнителните механизми в самоделните стрелкови системи като правило не се срещат или в редки изключения са взети готови от бойни системи. От допълнителните детайли прикладите и ложите или се вземат готови или се изработват самостоятелно от дървесина. Останалите допълнителни детайли обикновено не присъстват в конструкцията на самоделните стрелкови системи. В определени конструкции могат да бъдат включени дулни устройства, като най-често срещаното самоделно такова е устройство за безшумна стрелба (шумозаглушител).

По-долу в доклада ще бъдат представени част от конструкциите самоделни системи, изработени на базата на описаните по-горе основни методи.

I. Преправяне от съществуващи газови, пневматични и стари бойни системи

1) Представяне на газови системи в бойни

Газовите системи се срещат основно във вариант пистолет и револвер. Преработването на газов пистолет (револвер) в бойно оръжие е свързано основно с направата на конструктивни изменения на цевта. За целта се премахва преградата в канала на цевта (фиг.1). Тази преграда, която в зависимост от модела може да бъде метална пластина или дифузьор, не позволява изстрелването на проектили и други твърди предмети през цевта. След преработката газовия пистолет може да изхвърля твърди предмети, имащи начална скорост, да им придава целенасочено движение и да причинява механично поразяване на целта. Често дифузьорите в канала на цевта се закрепват чрез резба и лесно се развиват с отвертка.

Фиг. 1. Изглед през дулото на цевта.

За постигане на необходимата механична здравина в определени случаи, при които фабричната цев на пистолета (фиг.2), изработена като едно цяло с рамата е от крехка сплав (ЦАМ), допълнително се извършва разпробиване и в нея се монтира неподвижно вкладна гладкостенна цев, изработена от стомана, която притежава достатъчна якост и може да из-

Фиг. 2. Цев и рама на газово сигнален пистолет '' ZORAKI" – модел 914, калибър 9 mm P.A.K..

държи натоварването на газовете при изстрел с бойни патрони. В тези случаи останалите детайли и механизми на пистолета (револвера) не се преработват и се използват фабрично изработените.

2) Преработване на пневматични системи в бойни

Пневматичните системи се срещат основно във варианти пневматични пушки и по-рядко като пневматични пистолети.

Основно се преработват вариантите при които в конструкциите не е включена газова бутилка и пълнител (пружинно - бутален тип).

Обикновена фабрично произведена пневматична пушка (фиг. 3) от пружинно-бутален тип калибър 5,5 mm, се пригажда за стрелба с малокалибрени патрони. При повечето конструкции самоделната пушка се състои се следните основни части и механизми:

Фиг. 3. Самоделно преправена пневматична пушка калибър. 5,5 mm.

- цев – нарезна, фабрична изработка от пневматична пушка калибър 5,5 mm с допълнително изработен патронник, пригоден за малокалибрени патрони калибър, 22 LR или подобни. Цевта неподвижно се свързва към цевната кутия чрез заварка;
- цевна кутия – самоделно изработена от стоманени тръби, които са оформени подходящо и съединени помежду си чрез заварки;
- затворен механизъм - самоделно изработен затвор с ръкохватка, ударник и бойна пружина. Челото на затвора се оформя, като ежектор с улей, в който влиза венеца на гилзата и при изтегляне на затвора, той я извлича от патронника;
- ударно – спускателен механизъм – използва се фабричния механизъм от пневматичната пушка, който е самоделно пригоден и монтиран към цевната кутия;
- мерни прибори – върху специално изработена самоделна шина се монтира фабрично произведен оптичен мерник.

Интерес представлява преработката на фабрично произведена пневматична пушка (фиг. 4) от пружинно - бутален тип, марка „METEOR“, модел QB57 – китайско производство с нарезна цев. Цевта е разглобяема, като лесно се демонтира чрез свързващ холендер, който се развива на ръка. Пушката има следните промени в конструкцията с цел приспособяване за стрелба с малокалибрени патрони калибър, 22 LR:

Фиг. 4. Самоделно преработена пневматична пушка „METEOR“, модел QB57, пригодена за стрелба с патрони калибър 5,5 mm .(22LR) със заглушител.

- въздушното бутало е премахнато и е монтиран самоделно изработен ударник с жило за нанасяне на периферен удар, а взвеждащата му пружина е сменена с по-слаба и къса, което улеснява зареждането;
- затворът е пригоден, като е пробит ексцентричен отвор за жилото на ударника и допълнително е монтиран изхвъргач (фиг.5);
- патронника на цевта е разширен допълнително (чрез разпробиване), като по този начин е пригоден да побира малокалибрен патрон, 22 Long Rifle с периферно възпламеняване.

Фиг.5. Затвор с жило.

Към пушката е изработен и прибор за безшумна стрелба. Същият е камерен тип изработен от алуминий и стомана (фиг. 6). Самоделния заглушител е пригоден за прикрепване към дулото на изследваната самоделна пушка чрез винтова резба и заглушава шума при изстрел с около 50 %.

Фиг. 6. Представеният самоделен заглушител в разглобен вид.

3) Преработване на стари бойни системи

Преработването на старите бойни системи основно се заключва в подмяна на цевта, с такава предназначена за съвременни боеприпаси.

Интерес представлява преработването на еднозарядна бойна карабина, система „Бердана №2”, калибър 10,67 mm. Образец 1870 г., фабрично руско производство (фиг. 7). Пушката има извършени конструктивни промени състоящи се в подмяна на оригиналната цев с друга, както и преработка и приспособяване на затворния механизъм за зареждане с бойни патрони калибър

Фиг. 7. Карабина „Бердана № 2” с подменена цев за АК-47, калибър 7,62х39 mm.

7,62х39 mm. Най-често цевта се подменя със стандартна цев на бойна система, използваща разпространен тип боеприпас. В случая е използвана цев за автомат „Калашников“ (АК-47), калибър 7,62х39 mm. Самоделно преработената карабина се състои от следните основни части и механизми:

- цев – с обща дължина 415 mm и четири дясно въртящи нареза. Патронника е пригоден да побира патрон 7,62х39 mm, обр.1943 г. ;
- затвор – от плъзгащ тип **(**система „Бердана № 2” **)**, движи се праволинейно, като при заключване се завърта на 45˚ и се зацепва с бойните упори в цевната кутия;
- ложа с приклад – оригинално фабрично изработени от дърво. В конкретния случай приклада е срязан и е скъсен като пистолетна ръкохватка;
- мерни прибори – липсва оригиналния рамков мерник, който е бил прикрепен върху старата цев, но има самоделно изработена пластмасова мушка прикрепена неподвижно към дулото на цевта;
- ударно – спускателен механизъм – оригинален, фабрично изработен за карабина “Бердана №2”, състоящ се от спусков лост, бойна пружина ударника.

Фиг.11. Самоделно устройство с металния шомпол за зареждане.

II. Изработка на самоделни оръжия при наличие на отделни части от бойни системи

1) Стрелкови системи от най-прост тип – само цев

Тези оръжия по своята форма, конструкция и начин на изработване наподобява най-старите системи огнестрелни оръжия с дулно (шомполно) зареждане. По форма най-често наподобяват пистолет, които се състои от следните части:

- цев – с дължина, самоделно изработена чрез разпробиване на цилиндрична стоманена заготовка. Канала на цевта най-често е гладък с определен диаметър. Дебелината на стената на цевта обикновено е значителна 7-10 mm , поради ниското качество на използваната стомана.

Цевта няма патронник и в задния си край е плътно затворена чрез заварка. На определено разстояние от дулото се намира огневи отвор, през който се възпламенява барутния заряд. Цевта се прикрепя неподвижно към метална ръкохватка обикновено чрез заварка, а върху самата цев може да са заварени метална планка с резба и метален водач за прикрепване на шомпола;

- ръкохватка – пистолетен тип, изработена най-често от стоманена шина или дърво.

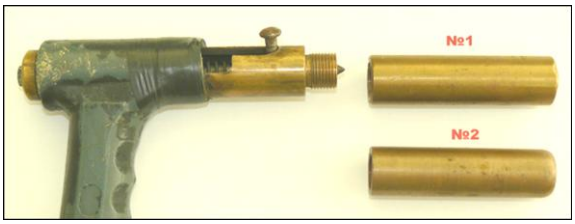
Този тип самоделни стрелкови системи не са пригодени за стрелба с унитарни боеприпаси (бойни или ловни патрони), тъй като нямат патронник и затвор, както и ударно- спускателен механизъм.

За да се произведе изстрел с този тип огнестрелни оръжия, те трябва да бъдат снарядени през дулото с черен или бездимен барут, след което през дулото се насипват ловни сачми с различен размер или единичен куршум съответстващ на канала на цевта. Върху тях може да се натъпче с помощта на шомпола хартия, вата и други подобни материали, които да затварят канала на цевта отпред. За да се произведе изстрел се възпламенява барутния заряд, което става чрез директно поднасяне на пламък през огневия отвор (например със запалка) или по-сигурно чрез поставяне на къс фитил в огневия отвор.

2) Стрелкови системи с ударен механизъм, при който е наличен ударник

Самоделното изработено оръжие от този тип (фиг. 12), обикновено се състои от:

- цев - самоделно изработени от месингова или стоманена заготовка чрез струговане и разпробиване. Патронникът се приспособява за стандартни стрелкови боеприпаси от пистолетен или междинен тип. В някои конструкции се изработват две или повече цеви за различни боеприпаси (фиг. 13). Цевта се прикрепва към рамата чрез резба;



Фиг. 12. Самоделно устройство с форма на пистолет и два броя цеви пригодени за него.

- рама с ръкохватка – изработва се от цилиндрична месингова или стоманена заготовка чрез струговане, разпробиване и фрезоване. Свързва се към цевта, чрез резба, като в сглобено състояние има функцията и на затвор. На рамата се изработва надлъжен канал за ръкохватката на ударника, чрез която се извършва взвеждането. Перпендикулярно на надлъжния канал се изработва втори канал за задържане на ръкохватката на ударника във взведено положение. За ръкохватка се използват фабрично изработени пластмасови дръжки или самоделно изработени такива от дървесина или синтетични материали;

Фиг. 13. Изглед през дулото на цев №1 с калибър 7,62x39 mm и цев №2 с калибър 5,45x39,5 mm

- ударен механизъм – самоделно изработен, от прост тип. Състои се от ударник с жило и бойна пружина, в ударника е пробит напречен отвор за ръкохватката на ударника, служеща за зареждане и спускане (фиг. 14).

Фиг.14. Ударен механизъм.

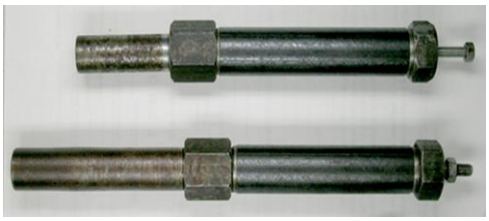
За зареждане се издърпва ръкохватката на ударника назад, при което се свива бойната пружина. След което се завърта ръкохватката така, че да влезе в напречния канал. При това тя се опира в стената на канала и ударния механизъм оставя взведен. За произвеждането на изстрел се завърта ръкохватката на ударника на обратно така, че да влезе в надлъжния канал и да може да се придвижи ударника напред.

На фиг. 15 и 16 са представени, два броя еднозарядни, самоделно изработени огнестрелни оръжия от същия тип имащи обща дължина съответно 228 mm и 192 mm.

Представените самоделни оръжия имат еднакво принципно устройство и се състоят от:

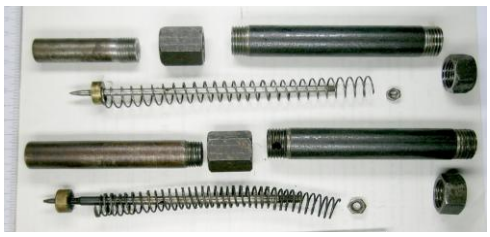
- цев – с дължина съответно на едното устройство 100 mm и 60 mm на другото, самоделно изработени на струг чрез просвредляване на цилиндрични стоманени заготовки. Каналът на цевта е гладък и има диаметър при дулото съответно 10 mm и 8,5 mm. Цевите имат патронници пригодени съответно за ловен капсул тип “Жевело” и за газов патрон калибър 9 mm P.A.. След

зареждане на патронника цевите се завинтват към затвора чрез резба нарязана в затворния им край;

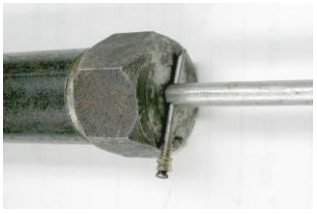


Фиг. 15. Общ вид на самоделни устройства.

- затвор – изработени са на струг от стоманен шестоъгълен профил с размер 24 mm (фиг.16). Представляват съединителни муфи с вътрешни резби в двата края и малък централен отвор за преминаване на ударника. Затворът свързва цевта с рамата и изпълнява за бойната пружина на ударника (фиг. 16);
- ударен механизъм – изработен самоделно от стоманена ос със заострен връх в единия край и резби в двата края, към които са прикрепени водач - ограничител на бойната пружина и гайка служеща за изтегляне на ударника при зареждане. Около ролята на патронен упор;
- рама – изработена от стоманена тръба с диаметър 21,3 mm и дължина съответно 118 mm на едната и 122 mm на втората. Има нарязани резби в двата края, чрез които се съединява към затворната муфа и капачката стеблото на ударника е монтирана спирално навита бойна пружина (фиг. 16) а на около 40 mm от върха му е пробит напречен отвор, в който се поставя обикновен железен пирон (щифт) завързан с корда, който изпълнява функцията на спусък и при изтегляне освобождава ударника, който под действие на бойната пружина нанася удар върху капсул - възпламенителя (фиг. 17).



Фиг. 16. Самоделните устройства в разглобен вид.



Фиг.17. Ударен механизъм от прост тип.

Представените устройства не притежават ръкохватки, спусък и мерни прибори, тъй като са предназначени за стационарно закрепване.

3) Стрелкови системи с ударно - спускателен механизъм

Този тип самоделно изработени стрелкови системи са най-сложните от описаните оръжия изработени при наличие на отделни части от бойни системи. На фиг. 18 е представена едноцевна пушка за стрелба с ловни патрони 12 калибър.

Състои се от следните основни части и механизми:

Фиг. 18. Общ вид на самоделна ловна пушка 12-ти калибър.

- цев – с дължина 680 mm, самоделно изработена от дебелостенна метална (стоманена) тръба с гладък канал без нарези. Патронникът е пригоден за ловни патрони 12-ти калибър. Има монтиран изхвъргач самоделна конструкция за извличане на гилзата;
- затвор – самоделно изработен чрез фрезоване и разпробиване от стоманени заготовки. Заключването е аналогично на ловните системи;
- ударно - спускателен механизъм – състои се от спусък, бойно чукче с ударник и бойна пружина. Бойното чукче се взвежда ръчно чрез завъртане на издатъка за зареждане;
- приклад – фабрично изработен от дървесина, пригоден за закрепване към рамата и ударно – спускателен механизъм;

- полуложа – изработена самоделно от дървесина и прикрепена неподвижно към цевта.

Изводи:

1. Изработването на самоделно стрелково оръжие при кризи от невоенен характер е насочено основно към неавтоматичните системи поради значително по-простата им конструкция, която е лесна за изработка.
2. Основните затруднения при изработването на самоделно стрелково оръжие е свързано с основните детайли от структурата на стрелковото оръжие – цев, цевна кутия (рама) и затвор. За преодоляването на това най-често се използват производствени такива.
3. Изработването на другите механизми и допълнителни детайли от структурите на стрелковото оръжие не е свързано със сериозни затруднения, защото тяхното реализиране се извършва с несложни стругарски, шлосерски и заваръчни операции, а самите конструкции лесно се намират в достъпните източници за информация.

References

1. Богданов А.И., Калев К.Г., Ганев В.В., Оценка на техническите характеристики на оръжейните системи., XVIII –научен симпозиум с международно участие –, Созопол 2008 г. ISBN 978-954-334-078-1.
2. Вълков Н., Давидов К. С., Цонев Ц. Г.,Ганев В.В., Основи и правила за стрелба с огнестрелни оръжия. Материална част на стрелковото оръжие., Стено, Варна, 2008, ISBN 978-954-449-411-7.
3. Съдебна практика – районни съдилища на РБ и балистични експертизи на базова научна- техническа лаборатория на МВР.
4. Цонев Ц. Г., Давидов К. С., Богданов А.И., Изследване кинематиката на подвижната система на стрелковото оръжие., Ш., 2013, ISBN: 978-954-9681-56-7.
5. Цонев Ц. Г., Давидов К. С., Основи за устройството на стрелковото оръжие – част 1.,Ш., 2013., ISBN 978-954-9681-53-6.
6. Antonov S.I., HristozovI.S, Information systems for armament and equipment exploitation control, Collection of papers: „105 години знание в интерес на сигурността и отбраната“ 6 – 7 април 2017 г., София 2018, стр. 268–374, ISBN 978-619-7478-00-6.

Rositsa K. Pencheva,

ELECTROMAGNETIC BOMBS

Rositsa K. Pencheva

“ Vasil Levski ” National Military University, Shumen, Bulgaria,
1 “ Karel Shkorpil ,“ *rosicaaa@abv.bg*

Abstract: *In the report is explored the innovation of the Electromagnetic bombs and their benefits in the field of Defense Technologies*

Keywords: Electromagnetic bombs

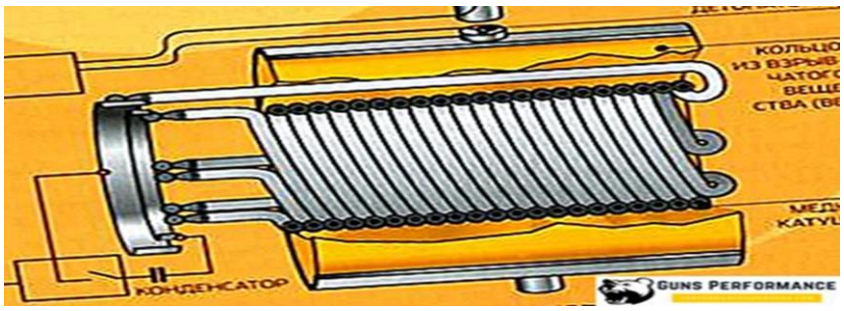
С всеки изминал ден човечеството става все по-зависимо от електронните устройства. Внезапен отказ на всички електронни устройсвта в значителен период от време би довело до невъзможност за водене на нормален живот а цивилното население. Значително по-опасно е да се случи събитие от подобен характер за военните формировани, защото това би довело до невъзможност същите да изпълняват поставените им задачи свързани с териториалната отбрана и сигурност на страната. Устройство способно да възпроизвежда подобен ефект наречено „електромагнитна бомба“ се разработва в редица страни от света, като САЩ, Русия, Израел и други.

През 50-те години на миналия век в САЩ възниква идеята за използване на електромагнитни оръжия. В хода на научни изследвания през 1950-1960 е предложена бомба, използваща няколко магнита и взривно вещество, експлозията на която предизвиква изхвърляне на мощно електромагнитно поле, което влияе неблагоприятно върху електронните системи и комуникацията на врага. Първите изпитания на електромагнитна бомба са извършени през 50-те години на 20 век. Тогава бил произведен взрив над Тихия океан, който нарушил електроснабдяването на Хаваите за известен период. За пръв път в бойна обстановка електромагнитна бомба е използвана през 1990 г. по време на войната в Залива. Ефектът, създаван от електромагнитните бомби върху електрониката, може да се сравни с удар от мълния.

Принципът на работа на електромагнитната бомба се основава на създаването на мощно електромагнитно поле, за създаването на което се използва ядрен взрив. При това всички устройства, чиято работа е свързана с електричеството биват повредени и прекъсват своята работа. Средства от този вид могат да деактивират вражеската електроника на разстояние от няколко десетки километра. Зарядното лъчение е насочено и скоростта на разпространение е 40 000 пъти по-висока от скоростта на полет на балистична ракета. Недостатък се явява факта, че понеже радиационният лъч се движи праволинейно, бомбата трябва да се задейства само на открити пространства.

Друг основен недостатък е че генераторът е с големи размери и не може лесно да се помести в съществуващите бойни припаси за за конвенционални оръжейни системи. Друг алтернативен начин, изследван от армията, е бързо действащ феромагнитен генератор. Това е магнит, който избухва и спонтанно се размагнитва, като отделя енергия. Действието е известно като фазов преход под въздействие на налягане. След като доказаха, че принципът работи, изследователите съз-

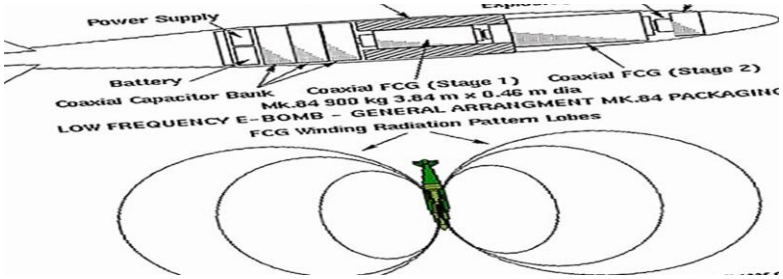
дадоха магнити от олово, цирконий и титан. Този принцип дава възможност да се намалят размерите на енергийния генератор, показан на фиг. 1.



Фиг. 1. Генератор на електромагнитна бомба.

Армейските изисквания са да се съберат енергийния генератор, условията за захранването с енергия и антената в пространство от 1 инч. Отделящата се енергия ще се измерва в стотици мегавата за микросекунди. Антената, която е нужна, за да се оформи и насочи електромагнитната енергия е инженерно предизвикателство, което се дължи на голямата сила на експлозията и на размера, който е необходим.

Американският учен Алън Сталтс работи върху плазмена бойна глава. Пламък води електричеството благодарение на наелектризирани частици в него (фиг. 2).



Фиг. 2. Конвенционален електромагнитен боеприпас с плазмена бойна глава.

Видове разработки

Част от разработките на електромагнитни бомби са предназначени за поразяване личния състав и техниката на противника. Други нанасят щети само на елетрониката на противника. Най-ранните проекти на електронни бомби са насочени към унищожаване на целите без да причиняват смърт. На съвременен етап разработките са насочени към създаване на технология, за създаване на муниции, които комбинират ефекта от конвенционалните оръжия и електромагнитната бомба. Идеята е да се усъвършенстват конвенционалните бойни припаси, като към устройството им се добави и „електромагнитна бомба“.

Според честотата електромагнитните бомби се разделят на нискочестотни и високочестотни [6]. Първите причиняват претоварване в електропроводните мрежи, а последните действат директно върху електронните системи. Една подобрена бойна глава може да унищожи танк, дори да не го е пробила. Превозното средство може да остане без запалителна система, комуникации или други електроники. Една бойна глава може също така да порази други електронни системи, включително мобилни телефони, които се използват от терористи за взривяване на бомби и токовата система в самоделни взривни устройства. Ефектите са от временно прекъсване и принудително рестартиране до пълна повреда или електрическо изгаряне на компонентите подобно на гръмотевичен удар.

Излъчваните от електромагнитната бомба импулси имат два способа на поражение – директен (с помощта на антената) и косвен (чрез кабелни мрежи като телефонните и електрическите). Попадайки в намиращите се наблизо електронни устройства, те създават високо напрежение, на което стандартните полупроводници и транзистори не са способни да издържат. В резултат на това компонентите се повреждат без възможност за възстановяване. Това означава, че при активиране на електромагнит на бомба по време на военна операция всеки радар, компютър и транспортно средство на противника ще спре моментално да функционира.

Разработваното от тексаските учени устройство се отличава от своите предшественици най-вече по своите миниатюрни размери. Досега най-доброто постижение в областта е било с дължина 3,5 метра. Поради това електромагнитната бомба е трудно приложима, особено когато става дума за въздушни операции. Миниатюрният прототип обаче е идеален точно за такива случаи. Досега портативната електромагнитна бомба се справя чудесно по време на изпитанията, които протичат в Хънствил, Алабама. Учените и военните обаче предупреждават, че все още е далече моментът, когато устройството ще бъде използвано в реални условия. Портативната електромагнитна бомба е дълга 1.5 сантиметра и е с диаметър 15 см. Устройството работи при мощност 35 мегавата и електромагнитен импулс с продължителност от 100 до 150 наносекунди и честота в диапазона от 2 до 6 гигахерца. Новото устройство може да бъде квалифицирано като бомба от типа High-Power Microwave, или свръхмощно микровълново оръжие. Принципът му на действие е да превръща химичната енергия от намиращия се в него експлозив в радиовълни**.** Електромагнитната бомба на тексаските учени се състои от три компонента – електрогенератор Flux Compression Generator (FCG), микровълнов излъчвател (виртуален катоден осцилатор) и антена, чието предназначение е да разсейва полученото излъчване върху набелязаната цел. FCG генераторът е основният източник на енергия на електромагнитната бомба. Самият той се състои от две поставени една в друга тръби, между които е монтирана намотка, наподобяваща соленоид и изолатор. Бобината получава напрежение от 12 волта от оловно-киселинна батерия, при което се създава магнитно поле. Във вътрешността на по-малката тръба пък е поставено взривно вещество – пластичен взрив С4. При „атака“ то бива взривено, като от детонацията вътрешната тръба рязко се притиска към външната. При този процес магнитното поле драстично се свива и се образуват мощни електрически импулси. FCG генераторът се използва еднократно – при взрив на електромагнитните бомби той бива унищожен. Това е и компонентът на устройствата, който е най-труден за изработка в по-малки размери. Това е така, тъй като колкото по-малък е Flux Compression Generator, толкова по-слаба е неговата мощност. При някои проекти генераторът започва да работи на надморска височина над 200 метра, радиусът на унищожаване е около 3,5 километра.

Един съвременен снаряд с включена електромагнитна бомба в устройството си, не е задължително да пробие бронята за да повреди бойната машина. Съвременният снаряд би могъл да направи „нежно убийство”, като обездвижи превозното средство. Щетите са трудни за оправяне и вероятно ще е необходима замяна на електронни системи.

Със сравнителната им малка изходна мощност новите армейски многофункционални муниции са за точкови цели. Две муниции, които са планирани за усъвършенстване, са ракетата Tow и 2.75 инчовите снаряди, изстрелвани от хеликоптер. Това е доста различно от предишните проекти за електромагнитни бомби, които са се спрели на големи бомби, пренасяни по въздуха или универсални артилерийски муниции, които покриват голяма област, това, което Коп нарича „оръжия за електрическо масово унищожаване.”

Една малка електромагнитна бомба ще бъде качествено различна от по-големите версии. Излъчената енергия се отделя с квадратна дистанция, така че цел на 3 метра получава 100 пъти повече поражения от цел на 30 метра. Подобрената ракета Tow като електормагнитно оръжие би произвела импулс, достатъчно силен да унищожи това, което удари, но не би трябвало да прекъсне електрониката в голяма район.

Възможностите за електронен „приятелски огън” изключват по-мощни тактически електромагнитни бомби, но дори по-малки версии могат да причинят непредсказуеми косвени вреди. Ако градско електрическо захранване или телефонни кабели усети импулса, поражението може да се пренесе в по-широк район.

References

1. Stamen I. Antonov, Tsonio G. Tsonev, Possibilities for automation of designing elements of small arms using CAD/CAM/CAE systems, Collection of papers: „Defense And Security, Mechanical Engineering And Military Technology, Communication And Computing Technologies, Social Science“, Shumen, Bulgaria 2016, p.p. 319-324, 2016, ISSN 2367-7902
2. Stamen Antonov, Ivan Hristozov, Information systems for armament and equipment exploitation control, Сборник доклади от Международна научна конференция на Военна академия „Георги Стойков Раковски” – „105 години знание в интерес на сигурността и отбраната“, София 2018, стр. 268–374, ISBN 978-619-7478-00-6
3. Ганчев И.И.; Война от 6-то поколение - новата ядрена бомба на Русия уплаши САЩ, 27.01.2019; 09.06.2019;
4. Джукич С.Л.; RUSSIA - В Русия направиха тактическа електромагнитна бомба, от която няма защита, 3 окт. 2017 12:47; 29.06.19
5. Македонски И.В.; Русия показа страховито оръжие, по-мощно от ядрена бомба!; 16.10.2017; 05.07.19;
6. Маринова А.А.; Смърт за електрониката, юли 2009; 10.07.19;
7. Цонев Ц. Г., Давидов К. С., Основи за устройството на стрелковото оръжие – част I, Ш., 2013, ISBN 978 – 954 – 9681 – 53 – 6.

Petya R. Petkova,

LASER WEAPON

Petya R. Petkova

“Vasil Levski” National Military University, Shumen, Bulgaria,
1 “ Karel Shkorpil “ str., petqpetq1997@abv.bg.

***Abstract**: In the report I checked the advantages and disadvantages of laser weapon, the king of laser and their application.*

***Keywords**: laser weapon*

ЛАЗЕРНОТО ОРЪЖИЕ

Петя Р. Петкова

Национален военен университет „Васил Левски“, Шумен, България, „ Карел Шкорпил“ 1,
petqpetq1997@abv.bg

Съвременното огнестрелно оръжие въпреки широкото си приложение се характеризира с редица недостатъци. Част от които са:

- сложно устройство и голям брой движещи се части в оръжието;
- предизвикване на шум и пламък при произвеждане на изтрел, което от своя страна води до демаскиране на огневата позиция;
- ограничено количество на бойни припаси при бойците и машините, което води до постоянна необходимост от логистика;
- сравнително ниска скорост на летене на поразяващия елемент, което налага специални правила при стрелба по бързодвижещи се цели.

За отстраняването на тези и някой други недостатъци на огнестрелните оръжия, конструкторските бюра започват да търсят решение в принципи на базата, на които да създадат въоръжение за армията си. Едно от направленията, по които се работи е насочено към създаването лазерните оръжия.

Лазерното излъчване оказва топлинно влияние на материала и може да го изпари при условие, че има голяма енергия. Същото може да се използва в космоса, в атмосферата и във водата. Неговото действие е почти мигновено на принципа "изстрел- поражение", понеже електромагнитният лазерен импулс се движат със скорост близка до тази на светлината - 300 000 km/s. Това създава условия за успешна стрелба по бързо движещи се цели. Моментът, когато те се фиксират и моментът, когато лазерното оръжие открива огън по тях, почти съвпадат. Това е особено изгодно при стрелба по бягащи бойци, по вертолети, самолети, ракети, т.е. при изграждане на всякаква отбрана, включително противовъздушна и противоракетна. Лазерното оръжие използва високоенергетично насочено електромагнитно лъчение, главно от оптичния диапазон, генерирано от различни по вид лазери. Неговото поразяващо действие по целта се определя от термомеханически и ударни импулсни въздействия, което с отчитане на плътността на потока на лазерно излъчване, може да доведе до временно или постоянно ослепяване на човек или механично разрушение (разтопяване или изпарение на корпуса на поразения обект (ракета, самолет и др.). При работа в импулсен режим едновременно, при достатъчно голяма плътност на

енергията, топлинното въздействие се съпровожда и с ударно въздействие, което обуславя възникване на плазма. Днес за бойно приложение се използват твърдотелни лазери (SSL, ТТЛ), химически лазери, лазери на свободни електрони и рентгенови лазери с ядрено „напомпване".

Твърдотелните лазери със самолетно базиране са предназначени за борба с балистични и крилати ракети, самолети и др. Последните твърдотелни лазери не са с лампово „напомпване", а с „напомпване" с лазерни диоди. ТТЛ могат да генерират няколко дължини на вълните, което позволява да се използват не само за силово въздействие по целта, но и за предаване на информация (за откриване, разпознаване на цели и точна навигация на лъча на бойния лазер). Работи се и по създаване на рентгенови лазери, енергията на излъчването на които до 10 000 пъти превишава енергията на лазерите от оптичния диапазон и е способна да прониква през материал с голяма дебелина. Лазерното рентгеново устройство с „напомпване" от маломощен ядрен взрив е отработено при подземни опити. То генерира импулс рентгеново излъчване с продължителност няколко ns в диапазона на дължини на вълните 0,0014 μm. За разлика от химическите лазери, които поразяват целите с кохерентен лъч за сметка на топлинното въздействие, рентгеновият лазер поразява целите по пътя на ударно импулсно въздействие, довеждащо до изпарение на материала от повърхността на целта.

Видове лазери използващи се за лазерно оръжие:

- въглеродно двуокисен газодинамичен лазер;
- химически лазери;
- ексимерни лазери;
- лазери със свободни електрони;
- рентгенови лазери;
- твърдотелни лазери.

Въглеродно двуокисен газодинамичен лазер – правилно е да се казва суперлуминесцентен излъчвател с молекулярно-термодинамично напомпване. Предимството на газодинамичния лазер е голямата мощност развивана в режим на непрекъснато излъчване. Тя може да достигне стотици kW в непрекъснат режим на работа. Недостатък е голямото количество консумирано гориво, габарити и маса. Основното им приложение е за поразяване на междуконтинентални балистични ракети (МБР) на ускоряващия участък и бойните блокове на МБР на трансатмосферния участък от траекторията.

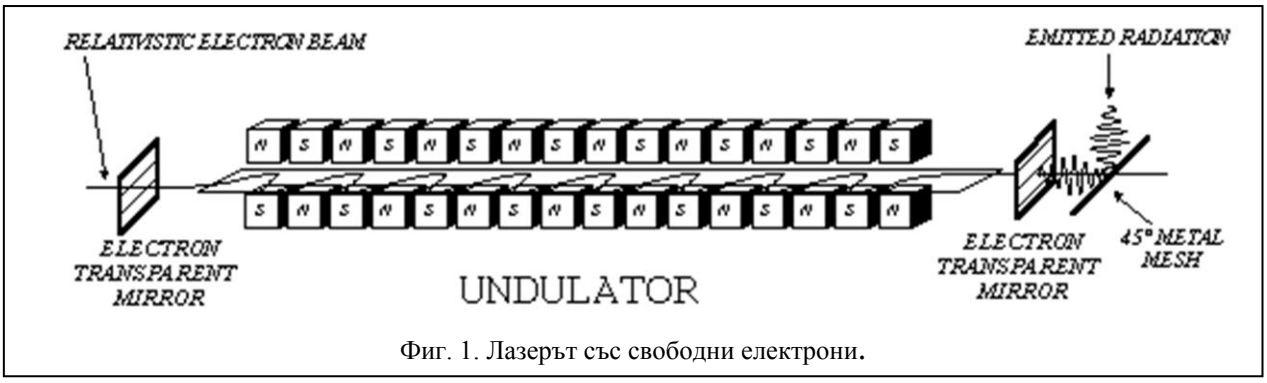
Химически лазери – същите могат да се монтират и на космически станции. Имат мощност до мегавати (MW). Пример са флуоро– водороден (HF) лазер; кислородо- йоден лазер (COIL); деутериево– флуорен (DF) лазер. Нямат външен захранващ източник, а енергията се получава от химическа реакция на химически елементи. Могат да поразяват до 11 континентални и балистични ракети до с радиус до 500 km.

Ексимерни лазери – същите могат да работят както в импулсен, така и в непрекъснат режим. Излъчването при тях като правило е в ултравиолетовия диапазон (UV, УВ). Бойното приложение на ексимерните лазери с орбитално базиране е унищожаване на космически транспортни средства, бойни блокове на междуконтинентални ракети, вражески оръжия, комуникационни и разузнавателни системи с орбитално базиране, високо летящи атмосферни цели и др.

Мощността на бойните ексимерни лазери може да бъде от порядъка на десетки MW в импулсен режим за сметка на много малка продължителност на импулса. Енергията на единичен импулс може да достигне няколко kJ, което е достатъчно за разрушаване на стени на горивни резервоари, устройствата на телеметрията и на връзките, товарните отделения и др.

Лазери със свободни електрони – ЛСЕ е източник на кохерентно електромагнитно лъчение, чиято дължина на вълната може лесно и плавно да се изменя в широки граници, чрез пренастройването на някои параметри и който притежава рекордна пикова мощност. ЛСЕ могат да работят във всички спектрални диапазони: от инфрачервената област (FIR), през видимата, ултравиолетовото лъчение (UV), вакуумния ултравиолет (VUV), до рентгеновото лъчение (X-ray). На английски език терминът е Free Electron Laser (FEL).

Докато в традиционните лазери се използва стимулираното лъчение на електроните в атоми или молекули, в ЛСЕ се използва стимулираното лъчение на интензивен сноп от електрони, движещи се с релативистки скорости през едно постоянно във времето напречно магнитно поле с редуваща се полярност.



Фиг. 1. Лазерът със свободни електрони.

Устройството, в което се създава това постоянно и с редуваща се полярност напречно магнитно поле се нарича ондулатор (undulator). Периодът на изменение на магнитното поле в аксиално направление в един ондулатор е от порядъка на няколко сантиметра, а силата на магнитното поле е от порядъка на няколко десети тесла. Толкова силно и бързопроменящо се в пространството магнитно поле се създава от свръхпроводящи магнити. Напоследък широко разпространение получиха ондулаторите, използващи постоянни магнити от кобалтови сплави (SmCo5, Sm2Co17). В един ондулатор може да има неколкостотин и дори хиляди периода на магнитното поле.

Известно е, че релативистки електрони, преминаващи през едно еднородно и постоянно във времето магнитно поле, се движат по дъга от окръжност, изпитват ускорение и следователно излъчват електромагнитно лъчение (спонтанно лъчение). Това електромагнитно лъчение се нарича синхротронно (СЛ). СЛ има уникални характеристики и намира многочислени приложения в науката и техниката. В един ЛСЕ електронният сноп, който се движи с релативистка скорост през ондулаторния магнит, служи за активна среда за усилването на външно електромагнитно лъчение (стимулирано лъчение). В ондулатора сумарното отклонение на електроните от аксиалната ос е равно на нула, а траекторията им е зигзагообразна, което води до силно СЛ.

Рентгенови лазери – рентгеновите лазери (X– ray laser, Xaser, XASER) работят в рентгеновата част на спектъра на дължина на вълната 10 Å (1 Å = 10^{-10} m). Интензивността на излъчване е (1013 – 1015) W/cm2 .

фокусирането на лазерното излъчване е проблем, защото оптиката в рентгеновия диапазон не работи. Затова източник на напомпване тук е ядрения взрив. Рентгеновият лазер е устройство с еднократно действие. Ядреният взрив го разрушава, но 1 μs преди разрушаването лазерът излъчва импулс. Подходящи са за монтиране на космическа станция. Тези лазери могат да унищожават ракети при движение по балистични траектории.

Първият експериментален рентгенов лазер е построен и изпитан в щата Невада през 1981 г. Рентгеновият импулс е бил с продължителност 10 ns, дължина на вълната 1,4 nm, енергия на един импулс от порядъка на 100 kJ. Следователно развиваната мощност в импулса е 10 TW.

Ако целта се намира на повърхността на Земята, зад мощен атмосферен щит, да се порази с лазер от оптическия диапазон е невъзможно. Рентгеновият орбитален лазер ще се справи с тази задача, освен това неговото лъчение може да премине през метрови бетонни плочи с дебелина няколко метра.

При зад атмосферни цели рентгеновото излъчване практически не се отразява от огледални метални щитове на противолазерната защита. Т.е. рентгеновият импулс унищожава щита и това, което се намира зад него.

Като мощен импулсен източник на твърдо рентгеново и гама излъчване може да служи ядрен или термоядрен взрив във вакуум. Както е известно, част от енергията на атмосферен ядрен взрив се губи за създаване на фронт на ударната вълна. Във вакуума където реално няма ударна вълна, практически цялата енергия на взрива се изразходва за електромагнитния импулс.

Твърдотелни лазери – твърдотелният лазер (лазерът с твърдо тяло) е лазер, използващ усилваща среда, която е твърда, а не течна като например при лазерите с разтвори на органични багрила, или газова, както в газовите лазери. Лазерите на основата на полупроводници са също с твърдо тяло, но по принцип биват считани за отделен клас твърдотелни лазери (напр. лазерен диод). Обикновено активната среда на твърдотелните лазери се състои от стъкло или материал за кристален „субстрат“, към който е добавен „легиращ примес“ като неодим, хром, ербий или итербий. Много от обикновените легиращи примеси са редкоземни елементи, тъй като възбудените състояния на такива йони не са свързани с топлинното трептене на техните кристални решетки, а техните прагове на лазерна генерация могат да бъдат достигнати при относително ниски степени на напомпване на лазера.

Сега вече мощността на лазерите в импулсен режим достига до няколко гигавата (GW) при продължителност на импулса до няколко фемто (femto) секунди (fs), с което се увеличава разстоянието на поражение.

Особеностите, които трябва да се отчетат при проектирането на лазерните оръжия, са следните:

- лазерният лъч не се влияе от гравитационното поле на Земята;
- затихването на лазерния импулс в атмосферата;
- отражението на лазерния лъч от металните повърхности, огледала и др.;
- действието на лазерния лъч зависи от времето на облъчване;
- разсейването на лъча от различни влияния;
- трудност за генериране и формиране на паралелен лъч;
- Лазерното оръжие може да се използва за поражения освен върху техниката и оптико - електронните прибори и така и върху живата сила (главно поражение на очите).

Предимствата на лазерното оръжие са следните:

- лазерното оръжие се характеризира със добри параметри (отсъствие на пламък, дим и звук);
- практически мигновено действие, лъчът се разпространява със скоростта на светлината;
- възможност за приложение в пределите на пряката видимост;
- ефективно е действието на лазерното оръжие в космоса;
- изстрелът с лазерно оръжие е многократно по евтин от традиционното оръжие;
- лазерното оръжие не предизвиква силни експлозии, не оставят следи, парчета и части, които да могат после да бъдат анализирани;

- пораженията са локализирани и е трудно да се установи откъде и кой ги е предизвикал.

Лазерното оръжие поради мигновеното дествие е подходящ за поразяването на :

- бягащи бойци;
- вертолети;
- самолети;
- ракети.

Най-общо казано при изграждане на всякаква отбрана, включително противовъздушна и противоракетна.

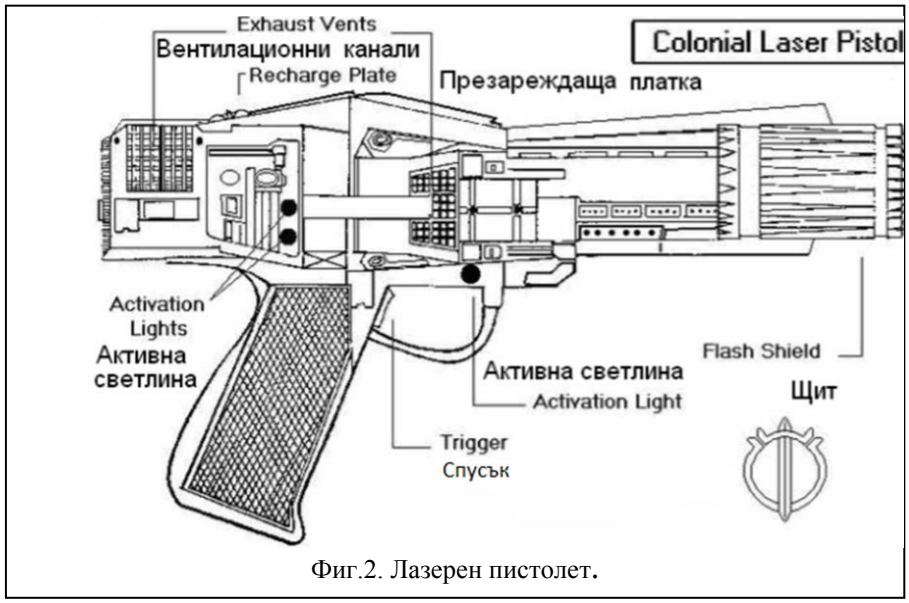
Недостатъците на лазерното оръжие са:

- трудна навигация и изменение на траекторията на лъча;
- намаляване на действието, вследствие затихване и разходимост на лазерния лъч на големи дистанции;
- разсейване на лъча при преминаване през облаци, мъгла, дъжд, сняг и прах.

Приложение:

- Лазерни пистолети.

В сравнение с традиционните пистолети лазерните пистолети имат повисока далекобойност, по- висока точност и не издават звук, светлина и дим при изстрел. При лазерните пистолети се използуват матрици от фазово синхронизирани диодни лазери (Phase-locked diode laser arrays). Те са съставени от диодно напомпвани твърдотелни микролазери (DPSS microlasers). В случая се използуват диодно напомпвани YAG лазери, които работят в импулсен режим. С лазерните пистолети на разстояние 2,5 km се получава плътност на енергията 1,08 kJ/cm2 и температура повече от 400° C.



Фиг.2. Лазерен пистолет.

- Лазерна пушка. Лазерен бластер Laser blaster.

Бластер означава взривател, но под лазерен бластер се разбира често лазерна винтовка, лазерен пистолет и др.

Фиг.3. Лазерна пушка

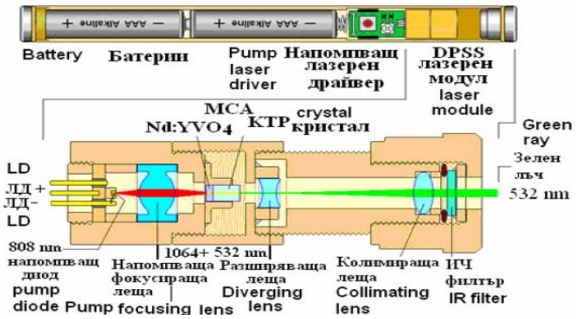
Опитите за подмяна на огнестрелните системи с лазерно оръжие датират още от 60-те години на XX век. Но разработените до този момент лазерни пушки имат множество недостатъци и не могат да се конкурират с традиционните системи [3].

Един от последните прототипи е лазерна карабина с несмъртоносно действие, наречена PHaSR (Personnel Halting and Stimulation Response), разработена в научноизследователския институт на ВВС на САЩ. Тя е предназначена за борба с безредици и е първото в света индивидуално лазерно оръжие. PHaSR генерира лазерно излъчване с две различни дължини на вълните. При попадане в очите лазерният лъч от карабината предизвиква временно ослепяване на противника, неизбежно съпроводено с психологически шок. В резултат облъченият губи възможност за ориентация в пространството и за по-нататъшни активни агресивни действия. Произвеждането на “изстрелите” е напълно безшумно, което не позволява демаскиране на източника на излъчване и допълнително провокиране на тълпата от това. Ефектът от лазерното въздействие отминава, без да оставя трайни увреждания върху зрението. Първите два експериментални прототипа на PHaSR в момента преминават изпитания в лабораторията на американските ВВС в Тексас. Скоро се очаква на тестове да бъде подложен и усъвършенстван прототип на лазерната карабина, снабден с далекомер и позволяващ на стрелеца да регулира силата на излъчването [3].

Фиг. 4 Лазерна карабина PHaSR
(Personnel Halting and Stimulation Response).

- Лазерна показалка, Laser pointer.

Зелен лазерен лъч може да се получи от кристал KTP/YAG (итриевоалуминиев гранат), генериращ на втора хармонична (SHG)- 532 nm, напомпван с диод на 1064 nm или от кристал Nd:YVO/KTP.



Фиг. 5. Лазерна показалка.

Фиг. 6. Лазерна показалка.

Джобеният лазер изпраща опасен лъч на разстояние 193 километра, който може на това разстояние да спука надут балон с тъмен цвят и да запали кибрит или хартия. Това могат даже „средни-

те” модели с мощност на лъча 75-125 mW (значително по-малко от най-мощния им модел), стига лъчът да се задържи на едно място 5-10s.

- Лазерна граната, Laser grenade.

Сфера от прозрачна, високо устойчива на удар пластмаса, изпълнени с малки, но фокусирани лазери, които могат да сочат към всяка точка от сферата. След задействане лазерите излъчват през сферата в бърза последователност с 360° покритие. Може да се използват в малки затворени помещения поради 10-метровия им обхват.

Фиг. 7. Лазерна граната

- Лазерно насочване, Laser guidance.

Фиг. 7. Глава на бомба с лазерно насочване GBU – 24.

Тук става въпрос за използване на лазерите за целенасочване. В цивилния живот има много устройства с лазерно насочване - термометри, ролетки, линеали, прободни триони, bar-code четци, електронни преводачи и др. В много съвременни автомобили се използва тримерна GPS система с лазерно насочване. Също така има възможност за извеждане на данните от измерителните прибори (скоростомер, километраж) на предното стъкло. Това позволява на водача да ги вижда с периферното си зрение, без да се отвлича от пътната обстановка. Тази идея е използвана от създателите на уникална система за GPS навигация с название Virtual Cable. Системата използва лазер, лещи и движещо се огледало, което проектира лазерна показалка на стъклото. Картината действително е триизмерна и не е възможно да объркате маршрута. Във военната техника има оръжие като бомби с лазерно насочване (LGB, LLLGB), снаряди и ракети с лазерно насочване, огнестрелно оръжие с лазерно насочване. Има ракети, кораби, самолети, совалки с лазерно насочване.

- Лазерни технологии в космоса, Laser technologies in space.

Приложение на лазерните технологии: лазерни глави за пробиване на отвори в космически обекти, лазерно изчистване на космически боклуци чрез лазерна пушка, лазерно оръжие, лазерни пушки за унижаване на спътници, навигация, измерване, антени, наблюдение, лазерни връзки, противоракетни лазерни комплекси с космическо базиране, лазерна обработка на материали в космоса, буксири с лазерен двигател за космоса, лазерни системи за скачване на космически кораби и др.

Фиг. 8. Космически лазер

Във военната индустрия лазерно оръжие се произвежда от различни държави. Например:

- Съединени Американски щати произвеждат химическия лазер ATL (Advanced Tactical Laser), който е кислородно–йоден (COIL) се монтира на борда на самолет C-130H. Лазерната стрелба се извършва през отвор с диаметър 125 cm. Лазерът има мощност няколко MW и далекобойност до 400 km. Лазерно оръжие има и на самолети C-135, B-52, „Боинг 747- 400F” и др. Американската агенция по перспективни разработки (DARPA, Defence Advanced Research Projects Agency) разработи ново лазерно оръжие (High Energy Liquid Laser Area Defence System, HELLADS) за самолет изтребител за унищожаване на ракети от разстояние десетки km. Теглото на лазерната система е 750 kg с охлаждането и заема обем 2 m3 . Лазерното оръжие се монтира на самолети, безпилотни самолети, вертолети, ракети, кораби, катери, самолетоносачи, подводници, спътници, космически кораби, совалки, бронетранспортьори, танкове, джипове и др. Лазерното оръжие може да се използва за разгонване на демонстрации в градски условия.

Заключение

Проектирането на лазерни оръжия е крачка към нова епоха, но навлизането в нея крие доста пречки. Лазерните оръжия се отличават с добри възможности за поразяване на различни видове цели, но крият и своите недостатъци. Трудностите при проектирането на лазерното оръжие крие доста специфични изисквания, с които е нужно проектантите да се преборят. Лазерното оръжие превъзхожда по критерии огнестрелните оръжия и е по- лесно за използване. Въпрос на време е лазерните оръжия да навлезнат в ежедневието на съвременния войник.

References

1. Antonov S.I., Tsonev T.G., Possibilities for automation of designing elements of small arms using CAD/CAM/CAE systems, Collection of papers: „Defense And Security, Mechanical Engineering And Military Technology, Communication And Computing Technologies, Social Science“, Shumen, Bulgaria 2016, p.p. 319-

324, “Vasil Levski” National Military University - Artillery, Air Defense and CIS Faculty, Shumen, Bulgaria, ISSN 2367-7902.

2. Давидов К. С., Цонев Ц. Г., Оръжейна подготовка за охранителни фирми и частни детективи, ВСУ „Черноризец Храбър“, В. 2013, ISBN 978 – 954 – 715 – 610 – 4.

3. Колев И. С.,Колева Е., Видове лазерно оръжие. Принципи на работа. Параметри. Действие на лазерното оръжие върху човешкия организъм., ТУ- Габрово, http://s2b.mon.bg/i/optika_elektronika_gabrovo/G7_lazerno_orazhie_Ivan_Kolev.pdf**,** 10. 07. 2019г.

4. Цонев Ц. Г., Давидов К. С., Основи за устройството на стрелковото оръжие – част I, Ш., 2013, ISBN 978 – 954 – 9681 – 53 – 6.

Ivan S. Savov,

APPLICATION OF FIELD-PROGRAMMABLE GATE ARRAYS IN DEFENSE

Ivan S. Savov

Faculty of Artillery, Air Defense and Communication and Information Technology, Vasil Levski National Military University, Shumen, Bulgaria, ivan_savov97@yahoo.gr

***Abstract**: Field-Programmable Gate Arrays form an essential part of the electronic components market and tend to increase in popularity. This report describes their architecture, focus on those features that determine their application for military applications. Examples are given.*

***Keywords**: Field-Programmable Gate Array, military application*

ПРИЛОЖЕНИЕ НА ПРОГРАМИРУЕМИТЕ ЛОГИЧЕСКИ МАТРИЦИ В ОТБРАНАТА

Иван С. Савов

Факултет „Артилерия, ПВО и КИС", НВУ „Васил Левски", Шумен, България,
ivan_savov97@yahoo.gr

Увод

Електронните материали и свързаните с тях технологии са в основата на голяма част от устройствата, които автоматизират всяка сфера на човешката дейност. Отбраната не прави изключение, напротив – въоръжените сисли традиционно са значителен/значим/голям/съществен потребител на пазара на електронни изделия. „Стратегия за изследвания и технологии в сигурността и отбраната" определя необходимостта от развиване на тази технологична област с цел осигуряване на изискванията на оперативните способности в системата на сигурността и отбраната в момента и за в бъдеще.

Поради ограниченията в обема, докладът се фокусира върху една категория електронни компоненти - програмируемите логически матрици. Интересът към нея се определя от тенденцията за засилване на ролята им в разработването на специализирани устройства за решаване на специфични задачи от военен характер.

В първата част са представени характеристиките и архитектурата на FPGA (от англ. Field-Programmable Gate Array), а следващите части са посветени на приложението им в областта на отбраната.

Общи сведения

Програмируемите логически матрици са интегрални схеми със свръхголяма степен на интеграция. Някои особености в архитектурата им определят от една страна високото им бързодействие, което традиционно е характерно специализираните интегрални схеми, ориентирани към спе-

цифични приложения (от англ. Application Specific Integrated Circuit – ASIC) и съвкавостта им, присъща на универсалните процесори, от друга страна.

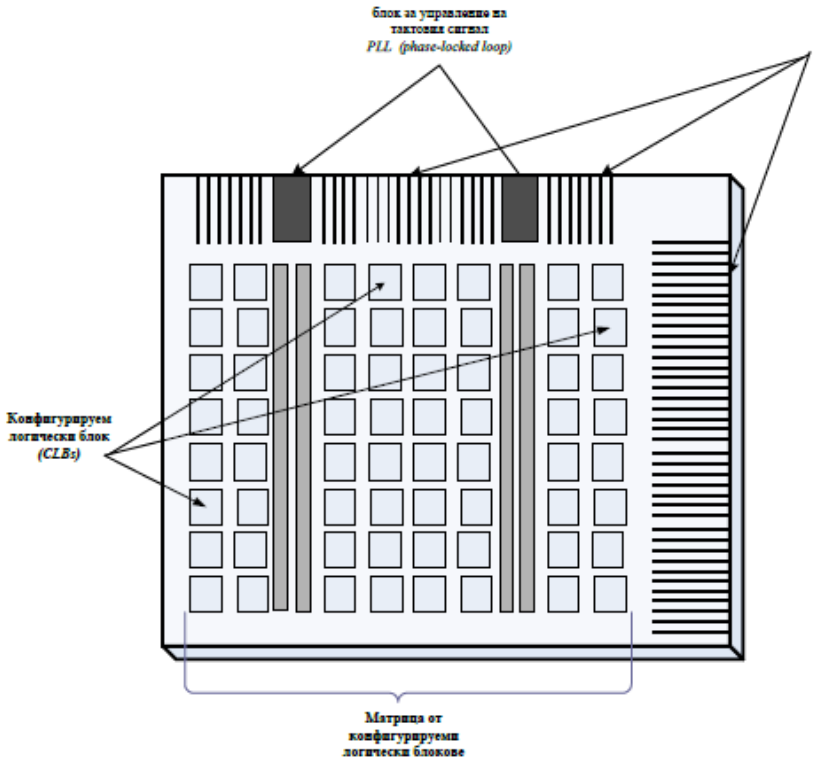
Архитектура

Основният елемент от състава на FPGA е матрица (логически масив - logic array), изградена от голям брой еднакви конфигурируеми блокове (Configurable Logical Bloc – CLB), всеки от които може многократно да бъде програмиран по електрически път и да изпълнява различна логическа, аритметична, запомняща функция или функция по формиране на входно/изходните сигнали на схемата. CLB са свързани по между си посредством интерфейси, формиращи комуникационна матрица, чиято конфигурация също може да се променя произволен брой пъти.

Всеки програмируем логически блок е изграден от определен брой елементарни логически елементи, които представляват n-входова комбинационно–логическа схема (Look-Up Table, LUT), реализираща определена логическа функция.

В състава на архитектурата на CLB влизат и различни по своите функции логически вериги: за управление на преноса, за формиране на контролни сигнали, за връзка между запомнящите елементи, за връзка между функционалните таблици и между отделните логическите елементи, изграждащи блока.

Останалите елементи на FPGA са: входно/изходни блокове, блокове RAM, блокове за умножение и блокове за управление на тактовия сигнал. Примерното им разположение върху чипа може да се види на фигура 1.



Фигура 1: Блокова диаграма на FPGA [2]

Програмирането се извършва от система за автоматизирано проектиране (развойна среда) в съответствие с направеното от дизайнера описание на устройството. Входното описание може да дефинира структурата (реализира се на език от високо ниво за описание на хардуера (Verilog или VHDL) или поведението (направено на езици от вида на MATLAB) на цифровото устройство.

Характеристики

Използването на FPGA за изграждане на високотехнологични, нескъпоструващи, и гъвкави устройства с разнообразно приложение в много области, включително и за нуждата на отбраната, осезаемо се засилва. Несъмнено това се определя от/се дължи на редица характеристики на чиповете:

- Висока степен на интеграция

Високата степен на интеграция на елементи върху кристала позволява имплементиране на бързодействащи и сложни специализирани цифрови устройства, които реализират високопроизводителни изчисления: паралелни изчисления, събиране на данни, цифрова обработка на сигнали, обработка на изображения и др.

- Препрограмиране

Възможността за многократно програмиране определя използването им в процеса на проектиране (прототипиране) на устройства, които се програмират, тестват и оптимизират върху FPGA преди окончателната им реализация върху масово конфигурируеми чипове.

- Висока производителност

Бързото, почти мигновенно превключване на логическите елементи за изпълнение на различни функции позволява FPGA се самореконфигурират съгласно вградения в тях алгоритъм по време на процеса на работа, така че да изпълняват няколко задачи в режим на времеделение. На практика се реализира апаратния еквивалент на многозадачната работа на процесора. Това позвлява, изградени върху тях устройствая да адаптират параметрите си в зависимост от промяната на фходните данни или средата на обработка. Например система за предаване на видеоизображение, изградена върху единствена свръхбърза микросхема, претърпява някокократно преконфигуриране за обработка на всеки видео кадър. Последователно се „трансформира“ от устройство за приемане и запис на видео сигнала, в устройство за обработка на данните и накрая – в модем за предаване на изображението [1].

Редица особености на FPGA определят приложението им конкретно в отбранителната индустрия:

- „Конфигуриране на терен“

Преконфигурирането на изградените устройства е изцяло софтуерно. Може да се извърши по всяко време, локално (дори в полеви условия) или чрез отдалечен достъп. Динамичната промяня на поведението на веригата, от една осигурява непрекъсната поддръжка, обслужване и актуализация на устройството, от друга страна позволяваза автоматично саморазрушаване на програмния код на изгубено или пленено устройство с цел не допускане на обратно инженерство.

Водещите производители на предлагат специализирани чипове с военно предназначение, характеризиращи се със:

- Висока степен на устойчивост на радиация

Понякога се налага експлоатация на устройствата в условия на повишено радиационно излъчване, което може да причини промени в състоянието на тригерите (нежелано преминаване от 1 към 0 или обратно) и по този начин да причини нежелана промяна в поведението на веригата.

- По-широк работен температурен диапазон

Обичайно комерсиалните чипове работят в диапазаона от 0°C до 100°C, индустриалните – от -40°C to 100°C, а тези с военно предназначение от -55°C до 125°C [3].

- Усилен корпус, със защита от удар, висока степен на устойчивост на запрашеност, вибрации, на влага и въздействие на разяждащи материали.

Приложение на FPGA в отбраната

В сферата на отбраната, с помощта на FPGA най-често се разработват устройства от следните области:

- Защитени комуникации

Съвременните комуникационни устройства от трябва, една страна да предоставят ширина на честотната лента, такава че да бъде възможна скорост на предаване от 40 Gbps до 100 Gbps, от друга да осигуряват ефективна криптографска защита на данните. Алгоритмите за криптиране/декриптиране налагат изпълнение на сложни математически преобразувания, а самите устройства трябва да спазват изискванията за високо бързодействие, надеждна работа, ниска цена и малки геометрични размери. Програмируемите логически матрици, притежават характеристики, които ги правят подходящи/удачни за апаратна реализация на устройства, отговарящи на тези изисквания [2]. Допълнително предимство осигуряват големият избор от т.н. интелектуални ядра (Intellectual Property core), съдържащи програмен код за криптиращи алгоритми (достъпен безплатно или срещу заплащане)

- Електронна война

Съвременните системи за електронна война трябва да притежават способности за бърз анализ на обстановката и мигновенна реакция на множество заплахи. Технологиите, които стоят в основата им - стелт технологиите, свързаните в мрежа интелигентни сензори и интелигентно управляеми оръжия и др., са свързани с математически операции като бързо преобразование на Фурие, декомпозиция на Чолески и умножение на матрици, които поставят необходимостта от бърза и високоефективна обработка на данните. В същото време тези системи трябва да отговарят на строги изисквания по отношение на разсейвана топлина, размера, теглото, мощността и не на последно място цена. FPGA предлагат идеално решение на тези изисквания.

- Радари и сензори

Най-популярната технология в съвременните радарни системи Active Electronically Scanned Array (AESA). За да удовлетворят изискванията за възможност за високопроизводителни изчисления, ултра широка честотна лента, висок динамичен обхват и адаптивни системи дизайнерите на системи често използват FPGA.

- Ракети и „умни“ боеприпаси

FPGA намират приложение в конструирането на „интелигентни“ оръжия и боеприпаси. Въху тях се реализират прибори за контрол, управление, насочване на управляеми ракети, самонасочващи се снаряди, „интелигентно“ оръжие от ново поколение [1].

- Безпилотни летателни апарати

Амбициозна цел в тази област е използването на свързани в мрежа безпилотни летателни апарати Развиването на тази технология може да доведе до доминация в сложната среда на съвременното бойно поле. Безпилотните летателни апарати са предназначени за извършване на дейности, които представляват потенциална заплаха. Те трябва да са в състояние да извършват търсене, проучване и също трябва да имат способността активно да въздействат на противника.

- Софтуерно дефинирано радио (от англ. Software Defined Radio – SDR) и когнитивно радио (от англ. Cognitive Radio – CR)

Характерната за софтуерно дефинираното радио възможност за динамична смяна на комуникационните стандарти допринася за по-ефективно използване на радиочестотния спектър. Когнитивно радио е следващото ниво в развитието на тази технология. То представлява устройство, което променя параметрите си в зависимост от условията и достига максимална ефективност на работа, чрез откриване на неизползвани радиочестоти и автоматично адаптиране към тях.

Включването на FPGA в състава на тези устройства се определя от възможността им за динамична реконфигурация на терен. Така става възможна реализцията и динамичната смяна на множество модулации, различни от първоначално дефинираната.

- Цифрова обработка на сигнали

Цифровата обработка на сигнали (от англ. Digital Signal Processing - DSP) е в основата на радарите, сигурните комуникации, средствата за електронната война. Реализацията на изчисления с производителност от един GFLOPS до десет TFLOPS при запазване на разумни размери, тегло и консумирана мощност (SWaP) е предизвикателство, на което FPGA отговарят.

Изводи

Използването на FPGA може да допринесе за ускоряване на ускори процеса на модернизация на въоръжените сили.

Те се отличават с относително малка продължителност на процеса на проектиране, прототипиране, тестване и внедряване на устройства на тяхна база.

Чрезинтегриране на множество дискретни устройства в един FPGA - дефинирани от потребителя логически функции, DSP функции и процесори с общо предназначение, могат да бъдат направени преносими системи, които са леки и със сравнително малък размер.

Отличават се с намалена консумация на енергия. Удовлетворяват изискванията за работа при специфични условия – завишени нива на радиоактивно излъчване, запрашеност и влага. Устойчиви са въздействието на вибрации и на разяждащи материали. Всички тези характеристики определят възможността за използване на такива системи в полеви условия.

Литература

1. Ламбева, М. Х. (2015). FPGA – базирани вградени устройства за отбраната. *CIO юли 2015*, бр. 7, с. 71-72. достъпно на https://cio.bg › 7286_fpga_bazirani_vgradeni_sistemi_za_otbranata
2. Ламбева, М. Х. (2014). Приложение на FPGA за изграждане на устройства за криптиране на данни, *Сборник научни трудове от Научна конференция „Новата парадигма за сигурност в кибер-пространството“* (271 – 277). Шумен: Издателски комплекс на НВУ „В. Левски“, Факултет „Артилерия, ПВО и КИС“, ISBN 978-954-9681-49-9
3. Fpga For Military Applications - Intel® Fpga, достъпно на адрес https://www.intel.com/content/www/us/en/government/products/programmable/applications.html

Miroslav E. Stoimenov,

CAPABILITIES AND NEW APPLICATIONS FOR NON-LETHAL WEAPON SYSTEMS IN THE FIELD OF SECURITY ANDDEFENCE

Miroslav Evtimov Stoimenov

Abstract: *The report examines the possibilities and applications of non-lethal weapon systems in the security and defense.*

Key words: *non-lethal weapons, conflicts, national security, defense.*

ВЪЗМОЖНОСТИ И НОВИ ПРИЛОЖЕНИЯ НА НЕСМЪРТОНОСНИ ОРЪЖЕЙНИ СИСТЕМИ В СИГУРНОСТТА И ОТБРАНАТА

Мирослав Евтимов Стоименов

Анотация: *В доклада се разглеждат възможностите и приложенията на несмъртоносните оръжейни системи в сигурността и отбраната.*

Ключови думи: *несмъртоносни оръжия, конфликти, национална сигурност, отбрана.*

Една от причините за повишен интерес към несмъртоносните оръжия е нарастващата съпротива на обществото срещу смъртните случаи в резултат от полицейски операции и международни хуманитарни и военни мисии. Присъствието на международни репортери в зоните на военни конфликти, и граждански безредици, а така също наличието на цивилно население, смесено с терористи и други въоръжени лица в урбанизирани зони води до наличието на ненужно пострадали, незамесени в конфликта лица.

Несмъртоносното оръжие е специално проектирано и предназначено да довежда до временна недееспособност на хора чрез незастрашаващи живота леки наранявания или разстройване работата на техника с минимални, нежелани разрушения на дадено имущество и минимални поражения върху околната среда.

Към понятието несмъртоносно оръжие се отнасят също така придобилите популярни названия „възпиращо оръжие", „оръжие водещо до недееспособност", „само нараняващо оръжие", „оръжие, което не пресича смъртоносни бариери повреди и безопасно оръжие" и др. [3].

Несмъртоносното оръжие има за цел да обезвреди, обезкуражи, да задържи или да отблъсне противника, без да му причини тежки поражения [2].

Полицията е институция, която използва несмъртоносно оръжие за контрол на масови безредици по целия свят [13]. От своя страна въоръжените сили използват несмъртоносно оръжие срещу военнопленници и цивилно население на противника. На въоръжените сили е разрешено да използват несмъртоносни оръжия в случаите когато на лице са следните фактори:

- религиозни, културни и етнически различия, когато местното население е агресивно и войнствено настроено към мироопазващите сили;
- операциите се водят в гъсто населени места;
- конфликтът се води в условия на масово присъствие на цивилно население;
- противникът не се идентифицира с униформи и отличителни знаци, преди или след удара се смесва с цивилното население;
- противникът използва за свои цели жени и деца;
- противникът е готов да използва всякакъв род провокации [13].

В следствие на тези фактори, градът се превръща във враждебна територия, в която всеки може да бъде враг. От военнослужещият се изисква мигновена реакция за поразяване на целта, като остава въпросът дали това е легитимна цел или дали това е мирен гражданин. Обикновено нито времето, нито мястото предоставят възможност за правилно и своевременно решение относно характера на заплахата и характера на дейностите за противодействието и. Всичко това налага използването на несмъртоносно оръжие. Много важен елемент е фактът, че напълно несмъртоносно оръжие не съществува. Човешкият организъм и общото здравословно състояние на всеки човек е различно, което означава, че този вид оръжие може да не е безопасно за някоя категория лица със дадени заболявания. Но по статистически данни случаите със смъртоносен край са едва 2%, поради това опасността от случването им е много малка [14].

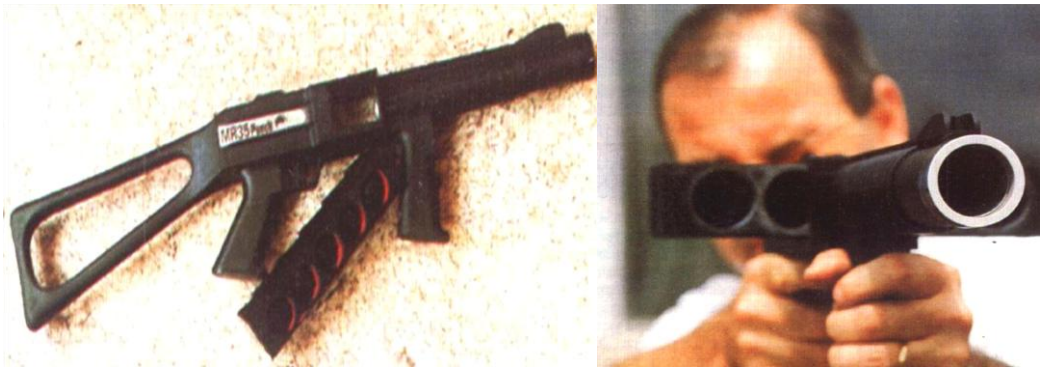
Някои автори смятат, че не е далеч времето, когато ООН ще изпраща в операции за поддържане на мира само подразделения, имащи на въоръжение несмъртоносни оръжейни системи [5].

Несмъртоносни оръжия могат да се използват за:

- разпръскване на тълпи;
- неутрализация на въоръжени лица;
- предотвратяването на бягството и укриването на заподозрени лица;
- временно изваждане от строя на техниката и личния състав на противника.

Класификацията на несмъртоносните оръжия е изградена по вид на използването им и приложената технология както следва [5]:

- оръжие с кинетично действие;
- газово кинетично оръжие;
- електрошоково оръжие;
- бариери и механични препятствия;
- електромагнитно несмъртоносно оръжие;
- акустично оръжие;
- химическо оръжие;
- лазерно оръжие;



Фиг. 1. Несмъртоносното оръжие MP-35.

Фиг. 2. Гранатохвъргачка FN303

Оръжието с кинетично действие поразява чрез силата на еластичен поразяващ елемент, изстрелян от огнестрелно оръжие или посредством силата на силно сгъстени газове. Като поразяващи елементи се използват пластмасови и гумени куршуми, куршуми съдържащи торбички с метални (оловни) сачми, или гумените сфери. Този тип оръжие е широко разпространен и се използва масово от полицията. Един от представителите на този вид оръжия са глаткоцевните многозарядни пушки тип „ПОМПА“.

Амуниците, които могат да се използват с този вид оръжие са от различен вид, като най-разпространени са полимерните куршуми, боеприпасите с маркиращ куршум, боеприпаси с немиеща се боя, боеприпасите със „СИ-ЕС“ газ, боеприпасите излъчващи лоша миризма, боеприпасите тип „Тейзър“ и др. Тези оръжия (LTLB,LTL-1,XM-25) са особено ефективни в разпръскването на тълпи с минимален риск за тяхното здраве и живот. Приети са за използване в цял свят, включително и в България в помощ на полицията за поддържането на реда и законите на страната [1].

Оръжията от този тип могат да бъдат решение за охрана и отбрана на граничните територий на страната и за справяне с нелегално преминаващи мигранти, а така също и да послужат на органите на военните формирования за охраната на обекти от критичната инфраструктура.

Газово кинетическо оръжие.

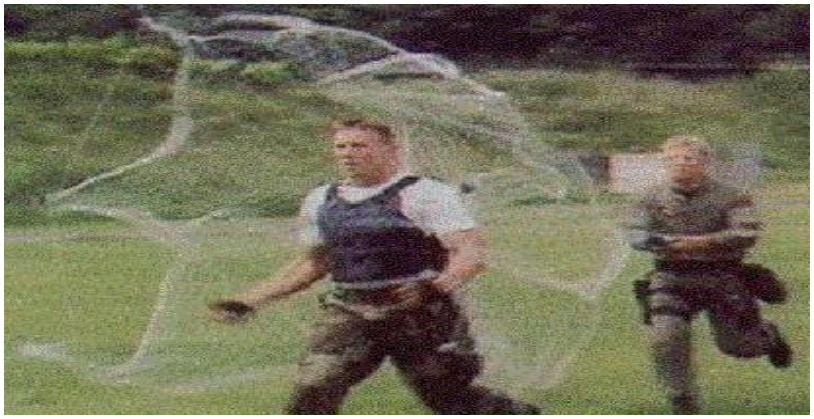
Друг представител на несмъртоностните оръжия е газово кинетичното оръжие. Едно от най-разпространените такива е гранатохвъргачката FN 303.

Това е хибриден модел между газово и травматично оръжие. Използва се за да доставяне на заряд от сълзотворен газ на голяма дистанция. При удар поразяващия елемент изстрелян от това оръжие изпускат облак от дразнещо вещество. Полицията използва това средство за справяне с безредиците. Ниската му цена и опростеният дизайн дават възможност да бъде използвано за охрана на военни обекти и залавяне на нарушители навици за използване на нелетални оръжия.

Бариери и механични препятствия.

Бариерите и механичните препятствия използват механичната здравина или специалната форма на конструкцията на бариерата, или други механични качества на препятствието и са предназначени за спиране, затрудняване или ограничаване движението на мобилна техника и хора, както и за ограничаване на достъпа до сгради и инфраструктура [1]. Това е традиционен и широко използван клас несмъртоносни оръжия, като през последните години се забелязва развиване и разширяване на номенклатурите им с нови изделия, каквито са лепкавите мрежи [1].

Удачен вариант за използване в специалните сили би било оръжието изстрелващо мрежи. Това оръжие е предназначено за блокиране на агресивно настроени граждани. Далечината на стрелба е няколко десетки метра. При изстрел под действие на насрещния въздушен поток мрежата се разтваря и се оплита около обекта. Тези устройства могат да бъдат средства за охрана на контролно пропускателните пунктове (КПП), както и за спиране на превозни средства, които превозват терористи и бежанци без да се застрашава здравето и живота на цивилните лица, които се намират наоколо, както и на пасажерите в превозното средство. Тези оръжия могат да бъдат носими и возими, като представител на носимите може да се посочат 23 mm подцевен гранатомет, изтрелващ поразяващ елемент, който отделя лепкава или електрошокова мрежа, а като представител на возимите - специализирани инсталации за спиране на леки и тежки превозни средства [12].



Фиг. 3. Електрофицирана мрежа

Електрическите несмъртоносни оръжия използват електрическа енергия за създаване на разряд на високо напрежение от порядъка на стотици хиляди волта [1].

При употребата им в живия организъм проникват микровълни на дълбочина до 0,5 mm, което предизвиква мигновено нагряване. Това въздействие води до непоносимо усещане за болка и отказ от съпротива [4, 5].

Този клас несмъртоносни оръжия също така предизвиква мигновени технически неизправности и срив в работата на съвременните електронни устройства на стотици метри разстояние. Представители на електромагнитните несмъртоносни оръжия са автомобилните планински възпиращи системи с електромагнитна енергия от типа Vehicle - Mounted Active Denial System - MADS, мобилните високоенергийни микровълнови възпиращи системи от типа SARA, така наречените „електронни бомби“ и други.

Този вид оръжейни системи могат да бъдат използвани в среди, в които се предполага, че ще бъде извършен терористичен акт, като заглушат и нарушат радиопредаването. По този начин нарушават комуникацията на врага. Също така биха могли да предотвратят отдалечената детонация на експлозиви посредством деструкция на електрониката. В случаи на гражданско неподчинение в особено големи размери тези оръжия притежават мощността да разпръснат, обезкуражат и откажат от всякъкъв вид съпротива живата сила.

Електрошоково оръжие.

Главният представител на електрошоковото оръжие е „Taser“. Това оръжие действа като изстрелва сонди, които предават вълни с висок волтаж върху мишената.

Фиг.5. Електрошоково несмъртоносно оръжие TASER.

В резултат - улученият изпада в силна мускулна контракция - изпитва силна болка, като губи контрол над тялото си. Най-често е използвано за неутрализация на престъпници, за да може полицията да ги арестува без съпротива. Производител е компанията „Taser“ в САЩ. Оръжието има няколко модела: M26C, X26C и C2.

Акустичните несмъртоносни оръжия са създадени на основата на звук с различни характеристики. Силата на този звук обикновено е над прага на човешката поносимост от 120 dB или характерът му предизвиква нетърпимост, например силният шум, предизвикван от взрива на звукова ръчна граната, или предварително записаният и излъчен характерен пронизителен рев [1].

Фиг. 6. Long Range Acoustic Device – LRAD

Към акустичните несмъртоносни оръжия се отнасят звуковият огнен шланг (Sonic Firehose), насоченият звуков излъчвател, далекобойният акустичен генератор (Long Range Acoustic Device – LRAD), вихровият генератор на акустични снаряди и др.

Основните звукови боеприпаси биват: звукови куршуми, звукови гранати, звукови мини или звукови оръдия (звуковите оръдия са най-големите по размер такива оръжия, като в началото са правени разработки на акустични автомати [7].

Някои от тях действат чрез фокусиран „сноп“ от звукови вълни, докато други използват широко звуково поле. Използването на звуково или ултразвуково оръжие върху индивидите причинява аудиторни промени, промяна във виброактивната чувствителност.

Обикновено симптомите са: силно главоболие, дезориентация, загуба на паметта. Нискочестотните звукови оръжия, макар и да не засягат слуховият апарат, въздействат чрез резонанс върху дихателния апарат и могат да предизвикат задушаване или припадък заради липса на кислород, достигащ до мозъка. Целта на този тип оръдия е да се използват предимно при масови безредици.

LRAD за първи път са използвани в САЩ от полицията в Питсбърг срещу протестиращи през септември 2009 г. [6].

Полицията в Сейнт Луис, САЩ, на 18 август 2014 г. използва LRAD срещу демонстранти. При пряко предаване от Фъргюсън на 18 август, репортерът Майк Тобин коментира, че оръжието: „няма ефекта да прави хората инвалиди”. Просто е шумно и дразнещо, и те кара да разбереш, че нещо голямо и официално идва, и че това се случва сега“ [5].

В Балтимор, САЩ, на 29 април 2015 г. са използвани модернизирани LRAD устройства [6].

Характеристиките на това оръжие го правят подходящ избор за използване за прогонване на неоторизирани лица от граници и КПП-ве, без това да провокира допълнителна агресия, както и за избягване на близък контакт с нарушителя.

Химическо оръжие.

Включените химични агенти (иританти), като CN, CS и CR газ, или „лютив спрей“ (натурално получен иритант, съставен от продукти на лютиви чушки) и други въздействат основно върху лигавиците на носа, очите и дихателните пътища. По-непознати и по-рядко използвани, но

също с голяма ефективност са зловонните, така наречени „скункс изстрели“, успокояващите агенти [8, 4].

Към химичните несмъртоносни оръжия се отнасят и „антиматериалните“ (разяждащи, корозиращи, замърсяващи) и променящите сцеплението, като хлъзгавата или залепващата пяна [12]. Химическо оръжие е най-удачно да се използва в ситуации със заложници в помещения. След пускането на химичните агенти те биха неутрализирали враждебните лица като ги правят уязвими в безсъзнание и лесни за задържане [8, 4].

Като цяло използването на газове е особено ефикасно, но изисква използването на лични предпазни средства от своите сили.

Лазерно оръжие.

Лазерното оръжие „Saber 203” временно намалява способността на противника да стреля с оръжие. Лазерът има ефективен обхват до 300 метра. [10].

Изделието има размерите на щурмова пушка. Въздействието им върху човек се характеризира с временна дезориентация и частична загуба на зрение. За поразяването на материални обекти и извеждането им от нормален режим на работа се използват преносими лазерни излъчватели с голяма мощност. Този клас несмъртоносни оръжия включва лазерни заслепители и осветяващи фенери за индивидуално оръжие, противопехотни пулсиращи лазерни пушки, возими тактически лазери за въздействие. Основно разработени за армията, такива оръжия навлизат и на въоръжение в полицията и жандармерията. Прототип на нелетален лазерен блясък, разработен от Дирекцията за насочена енергия на Научноизследователската лаборатория на ВВС, Министерството на отбраната на САЩ. Феизър „Personnel Halting and Stimulation Response Rifle (PHASR)“ [11, 4].

Въоръжените конфликти в наши дни коренно са се променили, мащабните военни операции са все по-редки и изискват повече ресурс, фронтът се размива, врагът е скрит между цивилното население в града и атакува чрез засада и терористични актове. Врагът трудно би се различил от невинните граждани и по този начин става заплаха за сигурността. В такива моменти органите на реда и мироопазващите сили трябва да действат с особена предпазливост като използването на летални оръжейни системи в такива случаи би било немислимо и допълнително би усложнило обстановката.

Характеристиките на несмъртосното оръжие го правят идеално за използване във всички видове антитерористични операции. По този начин би се избегнала смъртта на невинни жертви, а извършителите биха стигнали до съд и наказание от закона, което при използване на една летална система не винаги може да бъде постигнато. В голяма част от изследванията, посветени на тероризма, се долавя тезата, че с все по-широкото използване на несмъртоносните оръжия терористите ще губят все повече привърженици и симпатизанти, които ще бъдат постепенно обезсърчавани от агресията, благодарение на модерните средства на противостоящите сили.

Фиг. 7. Лазерен заслепител “Saber 203”.

ИЗВОДИ:

1. Несмъртоносните оръжия са удачен вариан за въоръжение на мироопазващите сили.
2. Несмъртоносните оръжеини системи биха могли да заменят напълно смъртоносните но същите навлизат все повече като оръжие, използвано от ВС.

References

1. Радев В., Несмъртоносните оръжия и съвременният тероризъм, СЕПТЕМВРИ 22, 2011.

2. Давидов К.С., Цонев Ц.Г., Оръжейна подготовка за охранителни фирми и частни детективи., ВСУ “Черноризец Храбър” Варна, 2013 ISBN 978-954-715-610-4.

3. Цонев Ц.Г., Димитрова С., Несмъртоносни оръжия ., списание „Клуб оръжие” бр. 2 и бр. 3, 2004г., ISSN 1311-4654.

4. Stamen Antonov, Ivan Hristozov, Information systems for armament and equipment exploitation control, Сборник доклади от Международна научна конференция на Военна академия „Георги Стойков Раковски” – „105 години знание в интерес на сигурността и отбраната“, София 2018, стр. 268–374, ISBN 978-619-7478-00-6

5.Golio M., Microwave and RF Product Applications. CRC Press. ISBN 9780203503744. Retrieved November 1, 2014

6. Onion A., ABC News. Technology & Science. 25 august 2004. RNC to Feature Unusual Forms of Sound: Unusual Forms of Sound to Emanate From RNC (http://abcnews.go.com/Technology/story?id=99472&page=1) 2019-05-29

7. Nutley E.L., Lieutenant Colonel, Air University Research Template: "NON-LETHAL WEAPONS: SETTING OUR PHASERS ON STUN?” Potential Strategic Blessings and Curses of Non-Lethal Weapons on the Battlefield"; USAF; August 2003; Occasional Paper No. 34; Center for Strategy and Technology; Air War College; Air University; Maxwell Air Force Base, Alabama; PG12

8. Wheelis, M., Biotechnology and Biochemical Weapons. The Nonproliferation Review. Volume 9, Number 2002. (https://www.nonproliferation.org/wp-content/uploads/npr/91whee.pdf) 2019-06-21

9. Colonel W.B. Leimbach, Jr., JNLWD Director U.S. Department of Defense. The Joint Non- Lethal Weapons (https://jnlwp.defense.gov/) 2019-06-03

10. https://defense-update.com/20050128_saber-203-laser-dazzler.html 2019-06-15

11. Mark Harris., (27 May 2009). "US cops and military to get laser guns". Retrieved 28 July 2010 (https://en.wikipedia.org/wiki/Personnel_halting_and_stimulation_response_rifle) 2019-06-01.

12. Zabalza J., historical leader from the MLN-Tupamaros urban guerrilla mentioned this use against official vehicles as a main tactic on book "0 from the left" (https://ipfs.io/ipfs/QmXoypizjW3WknFiJnKLwHCnL72vedxjQkDDP1mXWo6uco/wiki/Area_denial_weapon.html) 2019-06-16

13. Colonel Dennis B. Herbert., Nonlethal weaponry: From tactical to strategic applications at the Wayback Machine; USM(Ret .) institute for non-lethal defense technologies at Pennsylvania state University 2003-12-23.

14. John M.Mcdonald, Phd Robert J. Kaminski., phd Michael R Smith., . The effects of less lethal weapons on injuries in police use-of-force events. 2009 December; (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2775771/) 2019-05-30

Aleks R. Aleksiev,

PENETRATION OF ELECTRONICS INTO FIRE SYSTEM AND GUNS

Aleks R. Aleksiev

"Vasil Levski" National Military University,
Shumen, Bulgaria, 1"Karel Shkorpil" str.,

Abstract*: Nowadays, electronics are increasingly taking up arms. It gives some key advantages:*
- reduces the mass and gauges of the mechanisms in which it is used;
- results in lengthening the life of the mechanisms due to the lack of friction, wear and tear as well as moving metal parts.
The main mechanisms in which the current state of electronics has been applied are:

Keywords*: penetration of electronics*

НАВЛИЗАНЕ НА ЕЛЕКТРОНИКАТА В СТРЕЛКОВОТО ОРЪЖИЕ И ОРЪДЕЙНИТЕ СИСТЕМИ

Алекс Р. Алексиев

"Васил Левски" Национален военен университет,
Шумен, България, 1"Карел Шкорпил",

В днешно време електрониката започва все по-сериозно да навлиза в стрелковото оръжие. Тя дава някои основни предимства:

- намалява масата и габаритите на механизмите в които се използва;
- води до удължаване живочестта на механизмите поради липсата на триене, износване и удари, както и движещи се метални детайли.

Основни механизми, в които на сегашния исторически етап електрониката е намерила приложение, са:

- механизми за серийна стрелба;
- механизми за изменение темпа на стрелбата;
- ударни и спускателни механизми;
- оптични и оптико-електронн мерни прибори (колиматорни мерници, далекомери и прибори за нощно виждане) [4].

Основните оръжейни системи, в които широко е застъпено използването на електроника са **оръжията без система за презареждане.** Същите на този етап на развитие на стрелковото оръжие са на стадий - експериментални образци. Основната особеност при тях е липсата на традиционната подвижна система, механизми за презареждане, механизми за екстракция и места за съхраняване на боеприпасите (лентии пълнители). При изстрел няма движение на детайли за

извършване на пр оцесите по презареждането на системата. Представители на този клас системи са експериментален пистолет VLE и експерименталната гранатохвъргачка „Metal Storm” [5].

***Фиг. 1**. Австралийски експеримен-тален пистолет VLE.*

Видове системи изградени на базата на електрически механизми

Австралийската разработка на експериментален пистолет под наименованието VLE, боеприпасите, които са 7 на брой са поместени един зад друг в цевта. Същите нямат традиционните гилза и капсул - възпламенител, а са снабдени с електро-възпламенители. Традиционният механичен ударен механизъм е заменен с електрически, което осигурява изключително висок темп на стрелба. При натискане на спусъка към боеприпасите се подава електрически импулс от външен източник на захранване (батерия поместена в ръкохватката) .

***Фиг.2**. Австралийска оръжейна система AICW с експериментална гранатохвъргачка „Metal Storm”*

Спускателният механизъм на пистолета позволява воденето на единичен и автоматичен огън. Управлението на стрелбата се извършва от електронна система, която задава продължителността на откоса при автоматичен огън, след като стрелящият предварително е въвел желаният брой изстрели, посредством датчик разположен до спусъка.

Основният недостатък на оръжието се явява презареждането му. Същото се извършва чрез подмяна на цевта с друга. На сегашният етап от разработката презареждането на самата цев е възможно само в заводски условия.

По същата схема е разработена и гранатохвъргачка „Metal Storm”. Устройството й е пределно опростено, сведено до сменяема цев-пълнител и електронна схема. Изстрелите във вид на гранати от различен тип се разполагат направо в цевта. Благодарение на конструктивното обединяване на цевта и пълнителя чрез смяна на цевта е възможно да се промени типа на бойния припас и техния калибър. Разработени са цеви с 20 mm осколочно-фугасни гранати и цеви с 40 mm димни или сълзотворни гранати. При необходимост новата цев се поставя на оръжието, като при това нейната електронна схема за управление се съединява с мерниковия модул и му предава данните за типа на използваните бойни припаси, което позволява без

***Фиг.3**. Гранатохвъргачка"Metal Storm.*

участието на стрелеца мерниковата система да се адаптира за водене на точен огън. Възпламеняването на зарядите се извършва чрез електрически сигнал посредством специална електронна схема. Електро-възпламенителите на гранатите са разположени в стените на цевта. За осъществяване на стрелбата електронната схема подава напрежение на възпламенителя на най-предния барутен заряд в цевта и първата граната се изстрелва. При следващо натискане на спусъка се възпламенява вторият заряд и се изстрелва втората граната. В зависимост от калибъра и типа на гранатите в цевта на гранатохвъргачния модул могат да се поместят от 3 до 6 гранати.

Предимствата на този тип системи се заключават в липсата на движещи се части и просто механично устройство.

Основни недостатъци са невъзможността да се презарежда цевта в други освен в заводски условия, изискването за специален тип боеприпас и зависимостта от източник на захранващо напрежение.

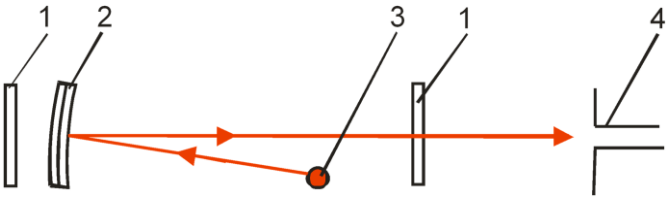
При картечен пистолет „Bushman” („Бушмен”) е внедрен **електрически механизъм** за забавяне на темпа на стрелба. Същият има в състава си електрическо реле за време, което дава възможност плавно да се изменя темпа на стрелба в широки граници. При някои конструкции темпът може да се променя и по желание на стрелящия. Основен **недостатък** на този тип механизми се явява необходимостта от източник на захранване, поради което е по-приложим за картечници монтирани на танкове и други бойни машини. Регулаторът на темпа е разположен в херметична опаковка в ръкохватката на оръжието и е разчетен за 30000 изстрела, след което се подменя. На опаковката на регулатора има монтирани светодиоди, даващи информация за състоянието на батериите. Регулаторът дава възможност за изменение на темпа на стрелба от 450 до 1400 изстр./ мин.

Фиг.4. *.Картечен пистолет „Bushman” („Бушмен”) с електрически механизъм за забавяне на темпа на стрелба.*

Оптични мерни прибори за леко стрелково оръжие.

При оптичните мерни прибори могат да се включат далекомерни скали в конструкцията на самият мерник. Тези скали дават приблизително разстоянието до целта. Основен недостатък при тях е трудното боравене с тях при движещи се цели. Но в най-новите конструкции на оптични мерни прибори за стрелково оръжие, конструктивно са заложени лазерни далекомери, употребата на които не води до нанасяне на вреда на очите. Тези конструкции позволяват да се получи голяма точност при определяне на разстоянието до целта, но имат усложнено устройство и висока себестойност, което ги прави неприложими (на съвременния етап) за масова употреба и налага използуването им само в оръжия предназначени за специалните подразделения.

Електрониката се използва и при мерници използвани за бързо премерване, при които червената точка е видима само за стрелеца, понеже тя се проектира само в прицела. Мерниците от този тип са известни като колиматорни мерници.



Фиг. 5. *Оптична схема на колиматорен мерник.*
1- защитно стъкло; 2- дублет; 3- светодиод; 4- изходен отвор.

***Фиг. 6**. Колиматорни мерници.*

Оптичната система на колиматорните мерници се състои от следните елементи: вдлъбнат сферичен огледален дублет; предно и задно защитно стъкло; блок на светодиодния излъчвател. Огледалният дублет не позволява на идващият под определен ъгъл светлинен лъч от светодиода да премине през него и го отразява назад към окото на стрелеца. Оптичната система на прицелите не съдържа елементи даващи увеличение на обекта.

Механичната част на прицела може да включва: корпус, колиматор, механизми за хоризонтална и вертикална корекция на мерната линия, управляващ ключ (галетен превключвател) за регулиране на яркостта на мерния знак (червената точка), електронен блок, приспособление (стойка) за закрепване на мерника към оръжието.

В състава на колиматора влизат наклонено под ъгъл 4,5° спрямо механичната ос сферично огледало (дублет) и точков светлинен източник (светодиод), поставен във фокусната равнина на огледалото под същия наклон. Колиматорът е захванат шарнирно в предния си край към корпуса посредством сферичен шарнир. При настройка на мерната линия, колиматорът се завърта около този шарнир посредством механизмите за корекция.

***Фиг. 7**. 5,45 мм АК-74 с нощен мерник.*

Механизмите за корекция на мерната линия се състоят от два винта, които контактуват със задния край на колиматора и са предназначени за корекции в хоризонталната и вертикалната равнина.

Управляващият ключ служи за регулиране на яркостта на мерния знак. Той има фиксирани степени, като първите няколко се използват в тъмната част на денонощието при съвместна работа с уред за нощно виждане. Следващите степени се използват при работа в светлата част на денонощието. Последната степен е режим на супер яркост.

Електронният блок е предназначен да осигури захранващо напрежение на излъчващия диод. Електронният блок съдържа DC конвертор за преобразуване на напрежението и делител на напрежението, осигуряващ необходимата работна точка на диода.

Използването на електрониката при приборите за нощно виждане е застъпена в конструкцията на ектронно-оптичният преобразовател (ЕОП – усилва яркостта на построеното от обектива изображение).

Електронно - оптичният преобразовател представлява електронно-вакуумен прибор, който преобразува невидимото инфрачервено изображение във видимо изображение с достатъчна яркост. Основни части на стандартен тип ЕОП се явяват: чувствителен към светлинни излъчвания фотокатод, електронно-оптична система за фокусиране на електроните и луминисцентен екран.

***Фиг. 8**.Оптичен мерник с поставен на него колиматорен мерник.*

Обективът проектира изображението на

наблюдавания обект върху фотокатода на ЕОП обърнато и с малка яркост. Светлинните лъчи въздействат върху фотокатода и избиват от него електрони. Количеството електрони, излитащи от фотокатода е пропорционално на количеството светлина в проектираното от обектива изображение. Под действие на високото напрежение електроните, избивани от фотокатода, придобиват висока скорост и летят към положително заредения луминисцентен екран. По пътя към екрана *(5)* електроните преминават през фокусиращо устройство *(4)* и дават на екрана изправено електронно изображение. Луминофорът на луминисцентния екран, под действието на падащите върху него електрони, свети и то толкова по-ярко, колкото по-голямо е количеството електрони и колкото по-голяма е тяхната скорост. По такъв начин на екрана се получава право и увеличено изображение на местността и целта. Това изображение, наблюдавано в мерника, има жълто-зелен цвят в следствие на цвета на светене на луминофора на екрана.

С цел получаване на по ясно изображение в приборите за нощно виждане могат да бъдат поставени няколко ЕОП, но броят им трябва да е нечетен за да се получи изправено изображение.

Класификация на ЕОП

Според характера на въздействието върху светлинния поток, който идва от обектите ЕОП се делят на:

- спектрални преобразуватели – преобразуват изображението от една област на спектъра на електромагнитните колебания в друга;
- спектрални преобразуватели с усилватели на яркостта.

Според работната област на чувствителния им слой (фотокатода) ЕОП се делят на:

- за видимата област;
- за инфрачервената област;
- за ултравиолетовата област;
- за рентгеновата област.

Според способа за фокусировка на изображението ЕОП се делят на:

- с електростатична фокусировка на изображението;
- с електромагнитна фокусировка на изображението.

Според конструктивни особености ЕОП се делят на:

- съгласно броя на камерите:
  - ✓ еднокамерни;
  - ✓ многокамерни.
- съгласно броя на стъпалата за усилване на изображението:
  - ✓ едностъпални;
  - ✓ многостъпални [2].

Една от най-авангардните разработки, в които широко е използвана електроника е израелската системата “Corner Shot”, която може да се използва от основните типове обикновени и картечни пистолети и гранатомети, намиращи се на въоръжение в израелската армия, и която позволява да се стреля под ъгъл 90^0. В състава на системата

Фиг. 9*. Система за стрелба под ъгъл “Corner Shot”.*

влизат и цветна видеокамера и монитор, като по-този начин се дава възможност на стрелящият да поразява цели като остава извън обсега на полезрението му.

В заключение трябва да се отбележи, че въпреки безспорните предимства механизмите от стрелковото оръжие, използващи електроника имат и сериозни недостатъци, които не им позволяват да заменят изцяло традиционните метални такива. По-важни от тези недостатъци са следните:

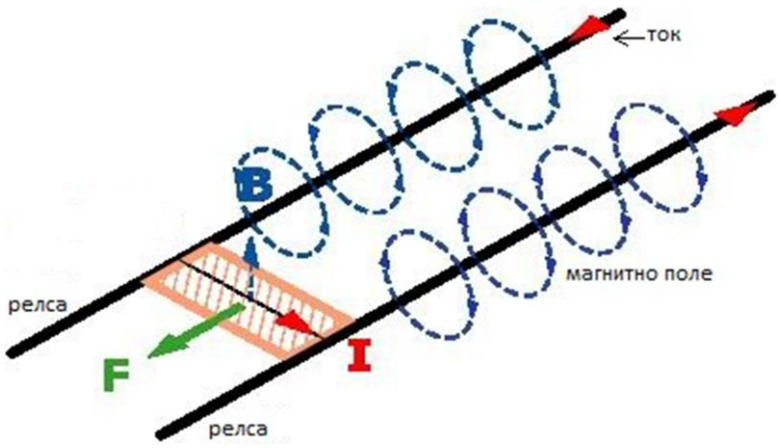
- изискват източник за захранване, който има ограничен живот и налага смяна след отработването на ресурса си;
- изискват специални мерки за херметизация;
- имат значително по-малка здравина от металните механизми;
- електронните ударни механизми изискват специални видове капсул–възпламенители за бойните припаси ,което усложнява устройството им.

Поради тези недостатъци цялостната подмяна на основните механизми на стрелковите системи с електронни такива все още се намира на експериментално ниво.

Електромагнитно РЕЛСОВО ОРЪДИЕ

***Фиг.10**. Разработка на релсово оръдие на BAE SYSTEM.*

Релсовото оръдие,или повече познато като “Railgun” е оръдейна система използвана от американската армия за борба с противник на далечни разстояния като за изстрелването на снарядите се използват електромагнитни полета създавани от електромагнити с високи мощности достигащи до 25MW с капацитет от 1 000 000 ампера.Релсите и снарядите при този тип оръдейна система трябва да са направени от силно проводящи материали,поради това че се изисква токът да създаде достатъчно силно магнитно поле експоненциално растящо за да се придава движение на снаряда напред със сила блозо 50MJ,а като пример 50MJ се равняват на движение на 5 тонен училищен автобус със скорост 509км/ч.Снарядът на релсовот оръдие не съдържа разривен заряд,а разча за поразяване на целите от високите кинетични сили които биват придавани и с високата скорост на неговот движение към целта,като сккоросттана снаряда е 2500м/сек., около Mach7. Един снаряд за електромагнитното релсово оръдие струва околко 25000 долара.



***Фиг.11** Принципна схема на работа на електромагнитното релсово оръдие.*

ЕЛЕКТРИЧЕСКО ОРЪЖИЕ "ТЕЙЗЪР"

Новите електропреносни оръжия TASER са най-ефикасното до момента изобретение за обезвреждане на противник, без да се използва смъртоносна сила.

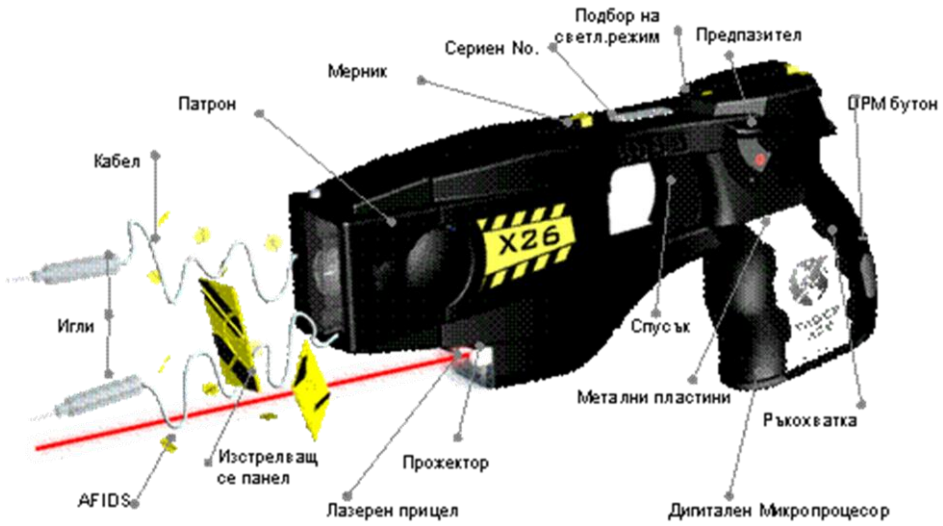
Те имат широк спектър на приложение както от граждани, така и от силите на реда.

Оръжията масово навлизат в полицейските подразделения на САЩ, Канада (най-вече патрулните отряди и пътна полиция), а вече и в Западна Европа.

TASER е идеално средство за самоотбрана, от органите на реда при арестуване на заподозрени лица, от охранителите на места за контрол (летища, гари), в самолети, кораби и др.

Начин на действие

Първото поколение TASER оръжия са от типа електрошокови оръжия и са въведени на пазара през 1974 година. Те въздействат върху субекта при допир посредством електрическа вълна, която има парализиращ ефект. Подадените електрически импулси въздействат на сетивната нервна система, като се смесват с комуникационните сигнали, които циркулират в нейните рамки. Електрическите вълни, подавани от електрошоково оръжие (първо и второ поколение TASER), достигат до сетивните нервни клетки. Те не влияят пряко върху опорно-двигателния апарат на човека.



Фиг.13 *Елементи на електрострелящо оръжие Тейзър X26.*

В случай че субектът, върху когото се използва оръжието, е под влияние на упойващи вещества - алкохол, наркотици и др., той е умствено нестабилен и съответно комуникацията в нервната му система е разстроена. Или пък ако е изключително съсредоточен, възможно е електрическите импулси да не достигнат до мозъка и последният да продължи да задава команди на опорна-двигателната система да извършва нападателни действия.

Чрез новите TASER електропреносни оръжия обаче, по-мощните електрически вълни проникват не само в горния слой под кожата, а достигат по-дълбоко до рецепторите от двигателната нервна система. По този начин новото оръжие влияе не само върху сетивната нервна система, но и ДИРЕКТНО върху поведението на мускулите на човека и задължително води до тяхната контракция, т.е. до падане на земята.

Ето защо, независимо от състоянието на самия субект,оръжията TASER действат сигурно и безотказно. Новите модели на Taser - M26, X26 и X26C (за използване от граждани) имат форма на пистолет.

При последната разработка боеприпаси параметърът на въздействие е увеличен до 11 м, като високоволтовото напрежение (50 000 V) достига нападателя чрез 2 сонди. Натискането на спусъка води до едновременното изстрелване на двете сонди и 5-секундно подаване на електричество, което стига до целевия обект по проводниците. Електрическите Т-вълни се предават в тялото през сондите.В по-достъпен вид на обяснение начина на действие на TASER е електро-физическо ,рефлексно свиване на мускулната тъкан.

References

1. Бабах Ф. К., Основы стерелкового оружия, С-П., 2003.
2. Вълков Н.В., Давидов К.С., Цонев Ц.Г.,Ганев В.Г., Основи и правила за стрелба с огнестрелни оръжия. Материална част на стрелковото оръжие., СТЕНО, 2009.
3. Матасов В. Ф. Улянцев В. П., Проектирование автоматики оружия., Т., 2001.
4. Цонев Ц.Г., Давидов К.С., Класификация на стрелковото оръжие и механизмите му, СТЕНО, 2010.
5. Цонев Ц.Г. Давидов К. С., Основи за устройството на стрелковото оръжие – част I., Ш., 2013.
6. Antonov S.I., Tsonev T.G., Possibilities for automation of designing elements of small arms using CAD/CAM/CAE systems, Collection of papers: „Defense And Security, Mechanical Engineering And Military Technology, Communication And Computing Technologies, Social Science", Shumen, Bulgaria 2016, p.p. 319-324, "Vasil Levski" National Military University - Artillery, Air Defense and CIS Faculty, Shumen, Bulgaria, ISSN 2367-7902
7. Harris W. How Rail Guns Work-11 Octomber 2005 https://science.howstuffworks.com/rail-gun1.htm-26.08.2019

[5]Common Foreign and Security Policy;