INTERNATIONAL SCIENTIFIC CONFERENCE 2018

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

SOCIAL SCIENCE

Shumen, Bulgaria
2018

TO THE READERS

This collection is divided in three parts and includes science papers presented on the International Scientific Conference "Defense Technology Forum 2018" in "Artillery, Aircraft Defense and CIS" Faculty, Shumen, Bulgaria.

Authors are responsible for the contents and the papers are not further edited after sending for publication.

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

Reviewers committee

REVIEWERS COMMITTEE

Prof. D.Sc.Tech. Hristo HRISTOV, "Prof. Tsvetan Lazarov" Defence Institute, MoD

Prof. Anatoly MASLAK, D. Sc.Tech, Kuban State University, Russia

Prof. Dr. Atanas RADENSKI, Chapman University, USA

Prof. PhD. Zhaneta TASHEVA, Artillery, Air Defense and CIS Faculty, "Vasil Levski" National Military University, Bulgaria

Prof. Eng. DSc Zbigniew LECIEJEWSKI, Military University of Technology, Poland

Prof. Eng. DSc Ryszard WOŹNIAK, Military University of Technology, Poland

Colonel Prof. Eng. Krasimir KALEV Ph.D., Artillery, Air Defense and CIS Faculty, "Vasil Levski " National Military University, Bulgaria

Colonel Eng. Prof. Traian ROTARIU Ph.D., Military Technical Academy "Ferdinand I", Bucharest, Romania

Col. Assoc.Prof. Eng. Marin LUPOAE Ph.D., Military Technical Academy "Ferdinand I", Bucharest, Romania

Colonel Assoc. Prof . Vasile SANDRU, Ph.D., "Henri Coanda" Air Force Academy, Romania

Col. Eng. Assoc. Prof. Atanas ATANASOV Ph.D., Artillery, Air Defense and CIS Faculty,"Vasil Levski " National Military University, Head of "Air Defense" Department

Colonel Eng. Assoc. Prof. Vanko GANEV Ph.D., Artillery, Air Defense and CIS Faculty, Bulgaria, Head of "Arms and Design Technologies" Department

Colonel Vasile SANDRU, Ph.D., "Henry Coanda" Air Force Academy, Romania

Col. Prof. Eng. DSc Marek ROŚKOWICZ, Military University of Technology, Poland

Col. Prof. Eng. DSc Jacek JANISZEWSKI, Military University of Technology, Poland

Col. Prof. Eng. DSc Adam KOZAKIEWICZ, Military University of Technology, Poland

LTC Assoc. Prof. Eng. Bartosz BIERNACIK, Ph.D., CIS Department, Military Studies Faculty , War Studies University, Warsaw, Poland

LTC Eng. Assoc. Prof. Stanco STANCHEV Ph.D., Artillery, Air Defense and CIS Faculty,"Vasil Levski " National Military University, Head of "Artillery" Department

LTC Prof. Adrian LESENCIUC Ph.D., "Henri Coanda" Air Force Academy, Romania

LTC Assoc. Prof. Laurian GHERMAN Ph.D., "Henri Coanda" Air Force Academy, Romania

LTCol. Krystian FRĄCIK, Adiunkt, PhD Eng., Military Faculty, Military Studies Faculty , War Studies University, Warsaw, Poland

LTC Daniel STEFANESCU, "Henri Coanda" Air Force Academy, Romania

Maj. Witold MATERAK, War Studies University, Warsaw, Poland

Dr. Samarjeet BORAH, Assoc. Prof. in Computer Science & Engineering Department, Sikkim Manipal Institute of Technology, India

Prof. PhD Lyubomir LAZOV, D.h.c, Leading researcher Lasertechnology, Rezekne Academy of Technologies, Latvia

Prof. Dr.sc.ing. Artis TEILANS, Rezekne Academy of Technologies, Latvia

Assoc. Prof., Ph.D. Margarita VASSILEVA, Artillery, Air Defense and CIS Faculty,"Vasil Levski " National Military University, Bulgaria

© "Vasil Levski" National Military University - Artillery, Air Defense and CIS Faculty, Shumen, Bulgaria, 2018.
c/o Jusautor, Shumen

ISSN 2367-7902

Table of Contents

PLENARY SESSION **5**

Şomoiag Pamfil, INFLUENCE OF BARREL EROSION ON THE BALLISTIC PARAMETERS AT ARTILLERY FIRING 6

Lyubomir Lazov, Edmunds Teirumnieks, APPLICATION OF LASER TECHNOLOGY IN THE ARMY 10

Moldoveanu Cristian-Emil, INSTABILITY MECHANISMS OF THE AIRCRAFT WAKE VORTICES 23

DEFENSE AND SECURITY **29**

V. P. Petrov, H. A. Hristov, COMBATING CORRUPTION AND ORGANIZED CRIME IN THE EUROPEAN UNION 30

V. P. Petrov, COMBATING CONTRABANDA AND THE UNLAWFUL TRADE WITH WEAPONS IN THE EUROPEAN UNION 40

Zh. St. Yordanov, INTERACTION BETWEEN THE ARMED FORCES AND THE INSTITUTIONS FOR THE PROTECTION OF SECURITY IN THE LITTORAL AREA 47

M. M. Alashki, MANAGEMENT OF NATIONAL SECURITY BASED ON CAPABILITIES 53

D. D. Farazov, THE COMPREHENSIVE APPROACH IN THE OPERATIONAL LEVEL DECISION-MAKING PROCESS 61

H. A. Desev, OBJECTIVES OF PROTECTION OF INTELLECTUAL PROPERTY IN THE CONTEXT OF INFORMATION SECURITY 67

H. A. Desev, COORDINATION DECISIONS FOR IMPLEMENTING CIVIL PROTECTION IN THE EUROPEAN UNION 71

S. N. Chanev, STATISTICAL MODEL OF SURFACE-TO-AIR MISSILE SYSTEM75

S. N. Chanev, MATRIX OF TARGETING FOR AIR DEFENCE FORCE 85

K. A. Iliev, DETERMINATION OF POTENTIAL POTENTIAL OF PERSPECTIVES OF THE MODELS INSTALLATION AND POWER TECHNIQUES 91

K. A. Iliev, METHOD FOR DETERMINING THE WATER FORMULATION POTENTIAL POTENTIAL 96

ARMS, TECHNOLOGIES, LOGISTICS **101**

Rotariu Adrian-Nicolae, Trana Eugen, ON THE DEVELOPMENT OF AN INTERIOR BALLISTIC MODEL FOR SMALL CALIBER ARMOR PIERCING AMMUNITION 102

Andrada Cirneanu, SMART VIDEO SURVEILLANCE FOR BACKGROUND ANALYSIS 108

M. N. Mutafchiev, MATHEMATICAL MODEL OF THE INTERNAL BALTIC PROCESS RUNNING IN A RELEVANT SOLID FUEL ENGINE 116

G. I. Dzhurkov, SUPPLY AS A BASIC LOGISTIC FUNCTION IN CONTEMPORARY MILITARY CONFLICTS 123

G. I. Dzhurkov, GUIDELINES FOR IMPROVING AMMUNITIONS SUPPLY IN OPERATIONS 130

R. B. Chalakov, D. K. Markov, FACTORS INFLUENCE ON FIRE SUPPORT IN OPERATIONS 137

K. S. Davidov, Ts. G. Tsonev, APPLYING OF THE SYSTEMATIC APPROACH FOR THE CANNON BARRELS DESIGN 143

R. N. Lazarov, ANALYSIS OF THE FACTORS AFFECTING THE STABILITY OF THE BULLET WHEN IT MOVES IN ENVIRONMENTS WITH DIFFERENT DENSITY 149

S. I. Antonov, TRENDS IN COMPUTER DESIGN OF REDUCTION GEAR..... 155

COMMUNICATION AND COMPUTING TECHNOLOGIES **164**

R. A. Bogdanov, Zh. N. Savova, D. K. Hubenov, A COMPARATIVE ANALYSIS OF HARDWARE PLATFORMS FOR DEVELOPMENT AND REALIZATION OF SOFTWARE DEFINED RADIO SYSTEMS 165

T. G. Peshev, RADAR WITH INVERSE SYNTHESIZED ANTENNA APERTURE – EVALUATION OF PARAMETERS OF MOVING TARGET 171

V. M. Vasilev, ANALYZE SCANNED AREA BY METRIC RADARS 176

V. T. Atanasov, SMART EDUCATIONAL CLUSTER CONCEPTIALIZATION... 181

V. T. Stoyanova, N. Kulev, ANALYSIS OF THE CAPABILITIES OF GRAPHIC TABLETS AS A MEANS OF EDUCATION IN COMPUTER GRAPHICS 191

Zh V. Zhivkov, BINARY PHAZE MANIPULATED SIGNAL 195

L. G. Nikolov, V. O. Slavyanov, NETWORK INFRASTRUCTURE FOR CYBERSECURITY ANALYSIS 200

D. I. Sumulyov, FORMING OF RADAR IMAGE OF TARGET, CONSISTING OF BRIGHT POINTS IN ULTRA WIDEBAND RADAR 206

D. K. Hubenov, R. A. Bogdanov, SOFTWARE DEFINED RADIO AS PART OF COGNITIVE RADIO 212

D. K. Hubenov, Y. V. Yosifov, N. Zh. Kulev, 5G CONCEPTS FOR WIRELESS COMUNICATIONS 219

D. K. Hubenov, STUDY OF RADIOSIGNAL RADIATION OF USB 3.0 DEVICE224

G. N. Mazadzhiev, FROM A TECHNOLOGY ASSOCIATED MAN TO POST-HUMAN 231

S. A. Aliev, P. Ribarski, THE INTERNET OF THINGS AND ITS APPLICATION IN VIRTUAL ECOSYSTEMS 242

A. A. Dimitrova, A COMPARATIVE ANALYSIS OF DIGITAL SIGNATURE CRYPTOGRAPHIC SYSTEMS 248

Sht. R. Stoyanova, BLOCKCHAINS AND SMART CONTRACTS FOR THE INTERNET OF THINGS 255

D. M. Koleva, FACTORS CONCERNING THE PRACTICE OF INFORMATION SECURITY IN TRAINERS 262

S. B. Pavlova, D. V. Velev, ONE ALGORITHM FOR SPECTANOGRAPHY BASED ON THE SPATIAL AREA 268

SOCIAL SCIENCE 274

K. M. Markov, COMMUNICATIONS, DISTRIBUTION AND MANAGEMENT.. 275

Sungjae Choo, Lukas Birsak, Tjeerd Tichelaar, Marin Marinov, THE OLD MAPS OF THE WORLD, EUROPE AND BULGARIA FROM GEOGRAPHICAL POINT OF VIEW. AND THEY REPRESENTATIVE IN THE GEOGRAPHIC MAPS AND GEOGRAPHIC ATLASES 283

A. L. Atanasov, CONTENTS AND CHARACTERISTICS OF THE INNOVATION PROCESS IN MILITARY EDUCATION IN BULGARIA 298

A. L. Atanasov, E-LEARNING - AN ALTERNATIVE TO THE TRADITIONAL.. 304

V. P. Petrov, STRATEGIC COMMUNICATIONS OF THE USA..... 310

PLENARY SESSION

ŞOMOIAG PAMFIL,

INFLUENCE OF BARREL EROSION ON THE BALLISTIC PARAMETERS AT ARTILLERY FIRING

Şomoiag Pamfil

Military Technical Academy "Ferdinand I"
39-49 Av. George Cosbuc, Bucharest, Romania
Fax: +32(0)2 7376352
E-mail: somoiag.pamfil@mta.ro

Abstract*: The erosion of barrels ends up in reduced gun performance. The damage spreads forwards toward the muzzle because the gun is unemployed ceaselessly. Worn barrels area unit objectionable because of they permit gas to flee past the shot therefore reducing speed, vary and accuracy. Because the muzzle begins to wear the shot loses directional stability. Its worth depends on the scale of the gun, the specified accuracy and the issue of safety that must be maintained against harmful fatigue failure. on the average barrels area unit condemned once the bore diameter will increase by concerning five-hitter. Wear depends not solely on the thermal load however additionally on the surface scientific discipline of the bore and the chemical interactions between the propellant gas and also the bore surface. The erosivity of {various} propellants are investigated over the years mistreatment various numerical ways and a few works have tested propellants or propellant gases in some style of simulated gun.*

1. Introduction

The capacity of the barrel walls to resist a certain pressure of the gases that form inside it is called the barrel resistance. In order not to increase the weight of the barrel, they are built to withstand a pressure 1.5 - 2 times higher than that to which they are normally subjected. Since gas pressure is not uniform over the length of the barrel channel during drawing, then the thickness of the barrel walls is not uniform but thicker at the back and thinner at the front.

If for various reasons the gas pressure inside the barrel has values much higher than those for which its resistance has been calculated, then swelling or even explosion may occur. In most cases, swelling of the tube occurs due to the presence of foreign bodies inside it. The projectile moving on the barrel channel, when meeting these foreign bodies, decreases its speed. The gas that follows the projectile, when it suddenly decreases its speed, is rejected backwards. The influx of gas flowing in the opposite direction produces an instantaneous increase in pressure, which leads to swelling or sometimes even to the explosion of the barrel.

Under the influence of all these factors, the channel of the barrel is widened and the surface of the barrel changes, which is why it increases the possibility of gas leakage through the projectile and the wall of the pipe channel, the initial projectile speed decreases and the scattering surface is increased.

Erosion of the gun barrel leads to poor performance and availability and increases the cost of barrel replacement over the life of an armament system. The wear of the gun barrels usually leads to an increase in the diameter of the pipe interior at the beginning of the riveting part. Wear progressively extends to the mouth of the barrel when firing continuously. The maximum wear point remains close to the beginning of the ribbed portion.

As the wear advances to the mouth of the barrel, the kick loses its steadiness in the direction. Total wear that can be tolerated is called usage limit. Its value depends on the size of the weapon, the precision required and the safety factor to be maintained due to the fatigue resistance of the material. On average,

the barrels are compromised when the inside diameter of the pipe increases by about 5%. Wear depends not only on the thermal variation but also on the type of material at the surface of the pipe interior and on the chemical interferences between the loading charge and the surface of the barrel interior. The barrel's internal erosion due to various drilling loads has been investigated over the years using various numerical methods, and in the course of some research, simulation load tests have been tested.

2. Theoretical and experimental study on the mechanical causes of wear

The mechanical contribution of wear comes from the action of gas jet and projectiles. Unwashed powder and small solid particles in the primary explosive and other sources are entrained in the rapid gas leakage and have an abrasive effect on the inside of the pipe. For a riveting pipe, mechanical wear occurs from the moment when the forcing grip is engaged. This process leads to considerable pressure on the pipe. The movement of rotation of the projectile as it progresses into the pipe causes additional mechanical wear. For the ribbed pressed pipes, the radial pressure between the guide rail and the interior of the pipe produces abrasive action.

The most important part of the wear occurs at the beginning of the barrel portion. However, a significant part of the wear can also occur at the mouth of the barrel due to the movement of the projectile, but also to the abrasive particles.

In order to increase the resistance of the barrel interior to wear caused by rubbing of the projectile, gas corrosion and erosion, and consequently the durability of the inner surface, it is coated electrochemically with a layer of hard chromium that adheres quite strongly to the metal.

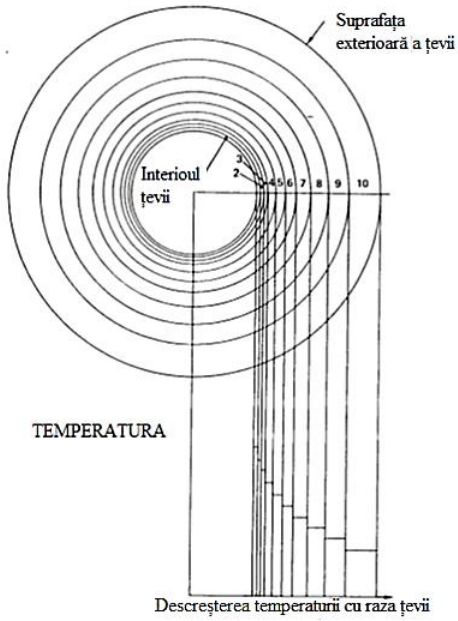


Figure 1. Decreasing temperature at the barrel level

Under ordinary atmospheric conditions, chromium theoretically does not corrode. Therefore, if the surface of the interior of the pipe could be covered with a continuous chrome layer, and if this layer would not be destroyed during drawing, the surface of the pipe interior would be perfectly protected against corrosion. However, it is not possible to deposit a hard, pore-free chrome layer on the steel. During the deposition of chrome, small cracks can occur, which in some places reach to the basic material of the pipe, through which gases and humidity can penetrate the steel, causing its corrosion.

At the time of firing, the maximum barrel temperature rises to almost 1800K at about the same time as the gas reaches the maximum pressure. The temperature rise is highest at the beginning of the ribbed part and corresponds to the maximum wear point. The increase in temperature at the surface of the barrel also produces a decrease in surface hardness. The layer of the removed material can vary between 0.1μm and 100μm per shot, depending on the kinetic energy of the gases, the thermal level and the surface

hardness. It is assumed that the erosion area extends as the projectile advances toward the mouth of the barrel.

Calculation of the layer friction from the surface of the barrel interior and the heat flow inside the barrel begins with the following slightly modified equations (the case without the material erosion of the barrel).

$$\tau_{wo} = \frac{1}{2} \cdot C_{fo} \cdot \rho_{\infty} \cdot u_{\infty} \cdot u_{\infty} \quad 1)$$

$$q_{wo} = \frac{1}{2} \cdot C_{fo} \cdot \rho_{\infty} \cdot u_{\infty} \cdot e_{\infty} + \frac{p}{\rho_{\infty}} \cdot 1 - \frac{T_w}{T_{\infty}} + \frac{u_{\infty}^2}{2} \quad (2)$$

where:

τ_{wo} - friction at the surface of the barrel interior;
C_{fo} - the coefficient of friction on the surface of the inner wall of the barrel;
ρ_{∞} - the average density of the material of the inner wall of the barrel;
u_{∞} - the average velocity inside the barrel;
q_{wo} - the heat flow inside the barrel;
e_{∞} - the average energy inside the barrel;
p - the average pressure inside the barrel;
T_w - temperature at the surface of the barrel;
T_{∞} - the temperature inside the barrel.

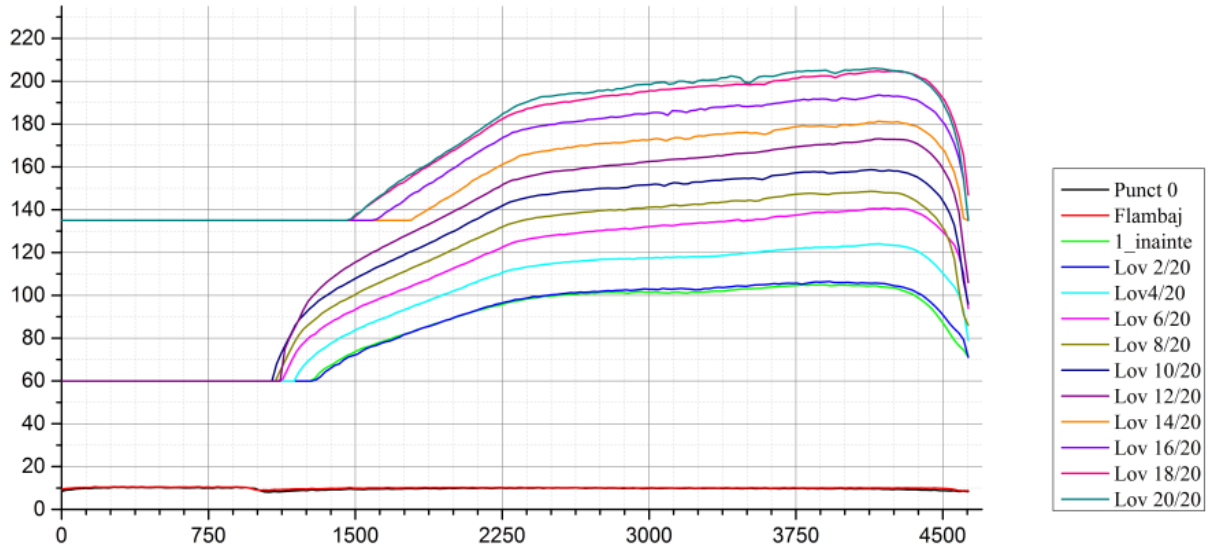


Figure 2. Temperature at the barrel level

3. Conclusions

Understanding all of the above mentioned mechanisms can lead to the development of various means of reducing the wear of the pipe. The most commonly used tools for erosion eradication are: the development of less erosive tailings, the use of protective coatings, improved pipe treatment materials, additives and lubricants to reduce erosion.

The following recommendations can be made to reduce the wear of armor systems barrel: the use of low-temperature firing loads; avoiding the use of lubricants that help reduce the amount of hydrogen; use of viable materials for the surface protective layer, such as chrome, non-metallic coatings such as foam, special powders that reduce wear; the use of nitrogen-loaded sanding loads.

References:

1. Lawton, B. (2001) Thermo-Chemical Erosion in Gun Barrels, Wear 251(10), 827-838 Lawton, B. (1984), Thermal and Chemical Effects of Gun Barrel Wear, in 8th InternationalSymposium on Ballistics, Orlando, United States.
2. Kimura, J. (1996) Hydrogen Gas Erosion of High-Energy LOVA Propellants, in 16thInternational Symposium on Ballistics, San Francisco, United States S. Sopok, C. Richard, S.

Dunn(2005), Thermal–Chemical–Mechanical Gun Bore Erosion of an Advanced Artillery System part one: Theories and Mechanisms, Wear 659–670,

3. John H. Underwood,(2005) Thermo- Mechanically Controlled Erosion in Army Cannons: A review, Gun Tubes Conference, , Keble College Oxford.

4. Lawton, B. (2003) Influence of Additives on the Temperature, Heat Transfer, Wear, Fatigue Life, and Self Ignition Characteristics of a 155 mm Gun, Journal of Pressure Vessel Technology 125(3), 315-320.

Lyubomir Lazov, Edmunds Teirumnieks,

APPLICATION OF LASER TECHNOLOGY IN THE ARMY

Lyubomir Lazov, Edmunds Teirumnieks

Rezekne Academy of Technologies, Faculty of Engineering
Address: Atbrivosanas aleja 115, Rezekne, LV-4601, Latvia

Abstract: *Every year, the use of lasers for military purposes continues to grow. Many armies from different countries use different types of laser systems for their specific combat tasks and actions. Traditional troops of land forces, artillery, air defence, and aviation forces today recognize the laser as a major operational element in increasing the accuracy and effectiveness of combat operations. Lasers are also part of various training sessions in the educational process of military servicemen in military schools and universities.*

The purpose of this document is to provide the necessary and adequate information about lasers and their application to the army. An additional purpose of this report is to minimize the dangers associated with laser radiation when using lasers in military operations.

***Резюме**: С всяка една изминала година употребата на лазери за военни цели продължава да расте. Много армии от различни страни използват различни видове от лазерни системи за свои специфични бойни задачи и действия. Традиционните военни части на сухопътните войски, артилерията, въздушната отбрана и авиационните сили днес разпознават лазера, като основен оперативен елемент за увеличаване на точността и ефективността на бойните операции. Лазерите също са част от разнообразни обучения, свързани с образователния процес на военнослужещите във военните училища и университети.*

Задачата на този документ е да предостави необходимата и адекватна информация за лазерите и тяхното приложение в армията. Допълнителна цел на този доклад е да се минимизират опасностите, свързани с лазерната радиация при използването на лазерите във военните операции.

Keywords: *laser, combat lasers, technology, beam divergence, reflectivity, interaction, continuous and pulsed lasing, laser safety*

1. Introduction

The idea of using light as a weapon can be traced back to Archimedes. In the second century AD, the author Lucian wrote that during the siege of Syracuse (214-212 BCArchimedes destroyed the enemy ships with fire. He may have used mirrors acting collectively as a parabolic reflector to burn the Roman ships attacking Syracuse.

At the dawn of laser technology, French physicist Louis des Brailles said, "The laser has a great future. It is difficult to predict where and how it will find its application, however, I think that it is a whole new age of technology."

The laser has moved in 58 years from "a solution looking for a problem" to a key technology that contributes to major sectors of the world economy. Laser devices are the core technology in instruments performing vital functions in many industries including transportation, healthcare, and telecommunications.

The first laser was developed in the 1960s and it was the beginning of a drastic change in the way the military sees war. During the Cold War, the US government relied on military strength through technological advances and, in the 1960s, multiplied its budget. In 1962, according to "Aviation Week

and Space Technology", the Department of Defence alone promoted the laser spending about 1.5 million US dollars.

The late 1970s and 1980s were difficult in terms of laser development in different types of weapon systems and their application. All branches of the military and industry have sought to master high levels of laser output power, beam management and creation of appropriate optics.

In 1999, the Department of Defence (US) officially recognized the lasers as future weapons and started research and development.

In 2000, the Joint Technology Bureau for High-Energy Lasers was created to bring all laser technologies together to develop a comprehensive laser weapon system that could be used by the Air Force. With continued advances in laser development in recent years, modern laser weapon systems have become a reality and an important part of the weaponry [1].

Types of military lasers

Today, several decades after the demonstration of the first laser in 1960 by T. Maiman, advances in a wide range of scientific disciplines have allowed laser technology to evolve and improve not only for civilian but also for military purposes. High-energy lasers cast intensively focused energy rays on the subject, typically powered by chemical fuel, electricity, or a stream of electrons. [2] Over the last 20 years, their application has accelerated rapidly in the commercial sector where they are routinely used for tasks such as cutting, welding, marking, engraving and drilling holes. Lasers are also used by military and law enforcement agencies to define targets, transfer information, maintain target, determine distances.

What types of laser sources exist in the military arsenal? The type of laser is determined by the lasing medium. The three categories in which lasers are usually classified are chemical, gas, and solid state. Laser can also be continuous wave (CW) or pulsed. Each laser type produces a specific wavelength of radiation. It is important to note that different wavelengths of radiation interact with the atmosphere differently. A laser beam is either scattered or absorbed by air molecules, water vapour, or dust.

Longer wavelengths scatter less and are absorbed more than shorter ones; the sky is blue because the shorter blue wavelengths of light are scattered more than the longer ones. Gamma rays are so highly absorbed that they cannot propagate more than a few feet in the air. Thus, some laser wavelengths are scattered or absorbed more than the others. This makes laser wavelengths with minimum absorption better for use as directed-energy weapons since they propagate through the atmosphere better. For example, the carbon-dioxide (CO_2) laser is strongly absorbed by water vapour, therefore any use of such a laser near the ocean would be negatively affected. Near-infrared and infrared lasers have shorter wavelengths with negligible absorbance. The optimal laser choice, therefore, would be a wavelength-tunable laser that could vary depending on the atmospheric conditions, such as the free-electron laser (FEL).

Chemical laser

The first chemical laser, hydrogen fluoride (HF), was built in 1965, producing an output of 1 kW. Since then, the Department of Defence (DoD) has been interested in the research and development of more powerful chemical lasers for weapon applications. Subsequently, in 1968, the base demonstration laser of the Agency for Advanced Research Projects (DARPA) produced 100 kW, and in 1975 the naval-ARPA chemical laser (NACL) produced 250 kW.

Solid state lasers

Solid state lasers (SSLs) use a solid laser medium, such as glass or crystal, or gemstone (ruby, etc.). Rare-earth impurities such as Cr (chromium), Nd (neodymium), Er (erbium), Ho (cholemium) or Ti (titanium) are placed in the crystal (active medium). Chromium is the material used in ruby crystals. Nd (neodymium) is used in the most commonly used lasers, namely the Nd: YAG lasers. For pumping the active medium (crystal), a flash lamp, an arc lamp, or another laser is used. This type of solid-state lasers operate at 1064.5 nm and can operate both in pulse mode and CW mode. A great advantage of these lasers is the wide range of wavelength and pulse duration. The power level can reach megawatt when using Q-switching to achieve short pulse lengths. Different interactions with laser and other crystalline materials can double the electromagnetic frequency, which will reduce the wavelength by half, resulting in the laser beam in the visible range of 532 nm (green). The wavelength can be further divided into

three or four, making this laser from the near infrared to ultraviolet wavelength. These lasers are usually used to indicate targets, measure distances, and so on. Other advantages of these lasers are that they can be made very small, user-friendly, cheap and battery-powered. The characteristics of SSL are shown in Table 1.

Modern **fiber laser** is a variety of solid SSL lasers. It is powered by electricity that excites diode lasers pumping the active medium (glass fibers). This makes such lasers extremely mobile and subject to support on the battlefield. In most cases, the active medium is a fiber treated with rare-earth ions such as Er^{3+}, Nd^{3+}, Ytterbium (Yb^{3+}), Tyllium (Tm^{3+}) or Praseodymium (Pr^{3+}). The principle scheme of a fiber laser is shown in Figure 1.

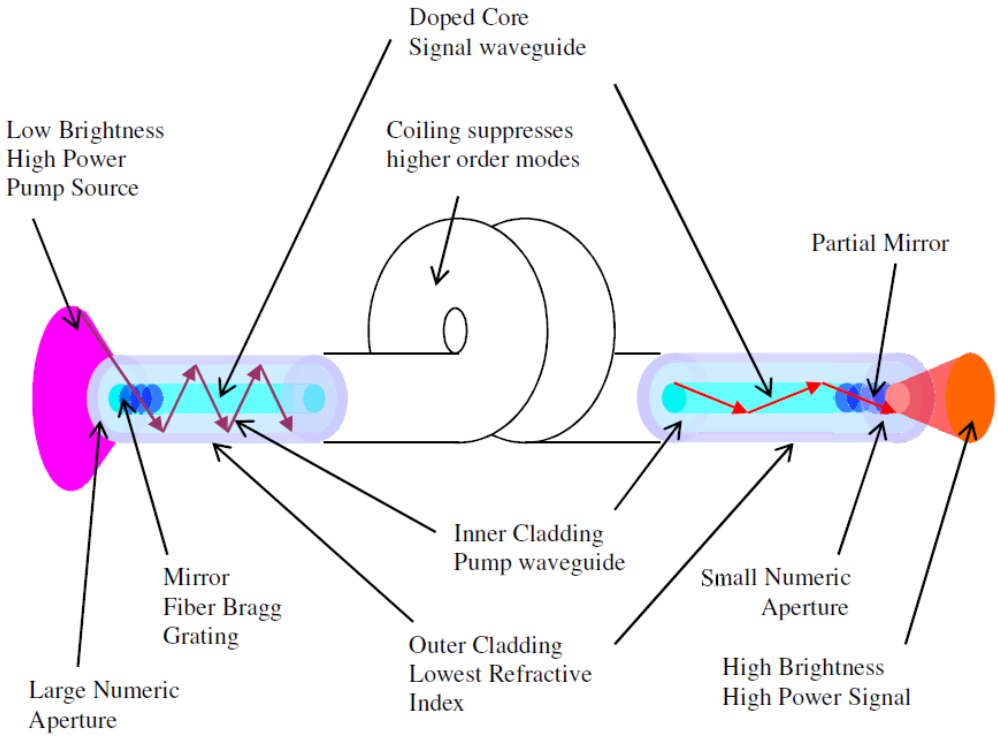


Fig. 1. Fiber laser – principle schema [3]

Fiber lasers have proven to have much benefit over traditional SSLs. They are resistant and do not require a clean room to operate or to be maintained, as most other laser systems do.

They are also extremely efficient; however, they cannot operate well in all weather conditions. One example is the IPG CW fiber laser that produces high quality laser beams causing damage to materials and components by thermal heating and burn-through. The Naval Surface Warfare Centre, Dahlgren Division (NSWCDD) purchased eight commercially available 5.5 kW IPG lasers, where two multimode (seven fibers) lasers are housed per cabinet. This type of laser is easy to mount due to the flexible fibers.

Table 1. Effects of a laser beam on the eye *(from UCELA Laser Safety Line 2009)*

Laser Type	Wavelength, µm	Power	Output	Purpose
Deuterium Fluoride (DF)	3÷4.2	0.01÷100 MW	CW and Pulsed	weapon
Hidrogen Fluoride (HF)	2.6÷3	Up to 150 MW	CW /Pulsed	weapon
Krypton Fluoride (eximer)	0.249	100 W	Pulsed	weapon
Nd:YAG	1.06/0.532	0.5÷1000 W	CW /Pulsed Q switched	Atmospheric Communication

Nd:YAG	1.06	0.5÷1000 W	Pulsed	LFT/LTD
Nd:YAG	1.06	0.5÷1000 W	Pulsed Q switched	LIDAR
Raman shifted Nd:YAG	1.54÷1.55	>10 W	Pulsed	LIDAR
Nd:YAG	1.06	1 J =10s *1W	CW/Pulsed	Sensor
Nd:YAG	1.06	1 J =10s *1W	CW/Pulsed	Illuminator
Tunable Laser (Titanium:Sapphire)	0.66÷1.18	1 J =10s *1W	CW	Atmospheric Communication
Fiber Laser	Variable	10kJ=10s*1kW	CW	weapon
GaAs (Gallium - Arsenide)	0.85	>10 W	CW/Pulsed	LIDAR
GaAs (Gallium - Arsenide)	0.83	Up to 5 W	Pulsed	Illuminator
InGaAs (Indium-Gallium-Arsenide)	1.55	Up to 5 W	Pulsed	Illuminator
Vertical-cavity surface-emitting laser	1.06	5 mW÷150 kW	CW	Illuminator
He-Cd (Helium Cadmium Laser)	0.4416	1mJ=10s*1mW	CW	Underwater Communication
Ar (Argon Laser)	0.514 green 0.488 blu	0.1÷5 W	CW	Underwater Communication
CO2	9 - 12	>100 kW	CW/Pulsed	weapon
CO2	10.59/11.17	4 kW÷5 kW peak	CW/Pulsed	Long range LIDAR

Gas lasers

Gas lasers are also widespread in the industry. They use a pure gas or gaseous mixture for an acoustic environment in the optic resonator. A typical gas laser contains a tube filled with the working gas and there is a pair of mirrors at the edges of this tube. At one end of the tube the radiation leaves the resonator. Most gas lasers use electric current to cause gas discharge in the active substance. Helium Neon (HeNe) laser is a very well-known gas laser. It produces a bright red, continuous beam of low power. It is used for many applications, such as scanning, alignment, measurement and stabilization devices. University students use them in optical training laboratories. Larger lasers contain HeNe inside the beam path, as well as checking beam alignment. HeNe lasers are relatively inexpensive and very user-friendly. They can work continuously for thousands of hours.

CO_2 lasers are also classified as gas lasers. These lasers were the earliest truly high-power lasers and have been among the most crucial lasers used in the research and development of high-energy laser (HEL) weapons. In the industry, the more powerful CO_2 lasers are used for welding, drilling, and cutting. There are many different types of CO_2 lasers that vary in pumping design.

CO_2 lasers work by burning hydrocarbon fuel (like kerosene or methane) in oxygen or nitrous oxide. The hot gas flows through a comb of nozzles, expands quickly, and achieves population inversion. The gas then flows through an optical resonator at supersonic speeds, resulting in stimulated emission and a laser beam. CO_2 lasers have been researched for use as non

-lethal weapons. The wavelength produced by a CO_2 laser is also absorbed by glass. For example, the beam does not penetrate a windshield. Thus, shooting a CO_2 laser at a vehicle's windshield could deter a threat by damaging the windshield or by causing a dazzling effect to reduce the visibility of the driver, while not reaching the driver at all.

Laser characteristics

The output power of modern lasers ranges from mW to MW (when delivering constant output power), or even patawatts (10^{15} W) for short pulsed lasers, and the wavelengths emitting from the ultraviolet waves (UVC) to the far infrared (IRC) waves of the electromagnetic spectrum (see Table 1).

In military terms, lasers with continuous output powers greater than 20 kW are classified as High Energy Lasers (HEL). Output powers in the range of kW or even MW allow the creation of laser beams with potential harmful intensity over distances of up to several hundred kilometres. These beams can be used to heat up targets, which then may lead to structural failure of the target object. Besides, falling into the eyes of the opposing army can lead to irreparable damage and blindness.

Advantages of laser weapons

Why are lasers so attractive for military purposes? The answer to this question lies in the advantages they offer to conventional weapons. The advantages of using laser weapons in military operations, depending on the tasks to be solved (the objectives set) and the tests that have been carried out, have shown the following:

- Very fast and can strike at targets with the speed of light (300,000 km/s);
- Targeting without waiting (both in height and in the side directions);
- Quick targeting opportunities, agile and in a short time span can intercept several targets or a one single target multiple times (compared, for example, with missiles or projectiles already launched to reach the goal);
- Absence of the possibility to shoot down a striking beam (as a projectile or a rocket) can not be distracted by a heat trap, is resistant to jamming systems (resistant to electromagnetic interference), etc.;
- Low price in comparison with some classical means of destruction (exceptionally cost effective when compared to conventional ammunition, with each laser shot costing as little as one US dollar);
- Ability to control the shot power that allows you to hit different targets at different distances;
- High localisation of destruction, which makes it possible to use such systems, for example, in urban conditions without incidental losses;
- Relative silence of the shot and invisibility for the eyes (for IR, UV ranges, especially pulsed lasers);
- Logistic support of the combat use of laser weapons (especially on the basis of solid-state lasers) is much simpler than for a number of classical systems of defeat.

Laser technology is introduced in military affairs according to specific guidelines that have been developed in the following areas:

Figure 1. Laser location (ground, air, underwater);
Figure 2. Laser communication (see Fig. 2);
Figure 3. Laser navigation systems;
Figure 4. Laser weapons;
Figure 5. Laser systems for missile defence and anti-satellite protection.

Due to the limitations of the volume of the report, we are discussing only a few specific laser applications for military purposes.

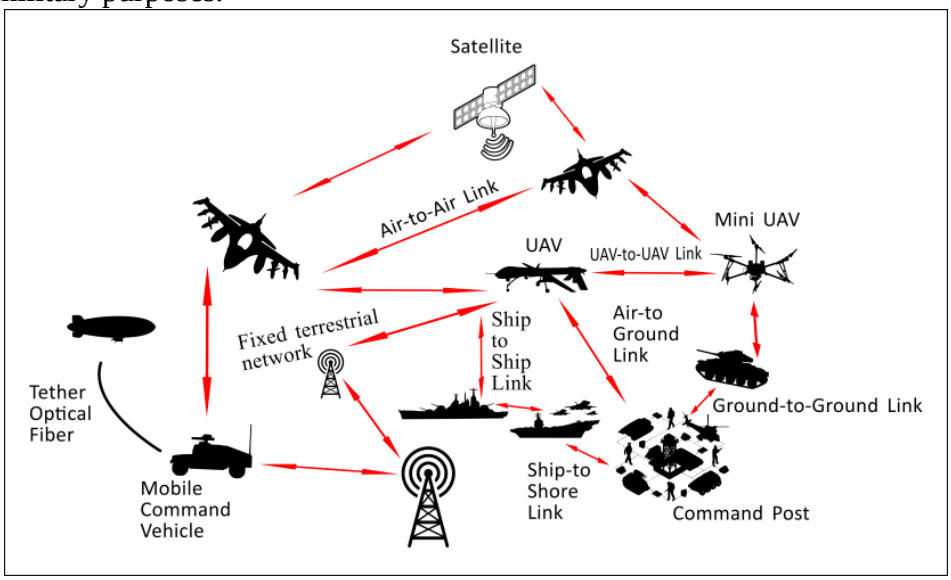


Fig. 2. Military laser communication: illustration of spatial diversity

Applications and discussions

According to their purpose, laser weapons can be classified as strategic and tactical. Strategic or high-power laser weapon systems are space or ground-based that intercept enemy intercontinental ballistic missiles and satellites. Tactical or low-power laser weapons are generally used for short-range air defence or self-defence for individual warfighter or weapon platforms.

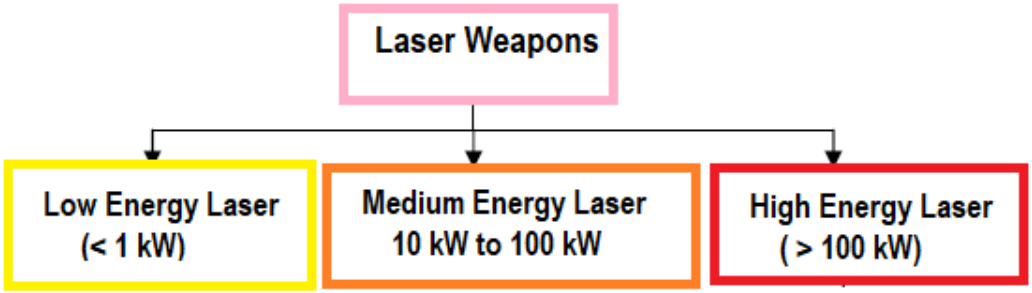


Fig. 3. Classification of laser weapons on the basis of energy/power levels

Laser weapons are classified on the basis of their energy/power levels: high, medium or low energy weapons (Fig. 3). They are distinguished into three broad areas ranging from jamming of sensors to the destruction of optoelectronic devices and ultimately destruction of the complete mechanical structure.

Low energy lasers usually give less than 1 kW of power and are used in weapon simulation systems for training or for jamming the sensors in communication systems, or can be used in anti-personal mode against the human eye. The use of these laser weapons for future military tactical operations will radically change the situation on the battlefield. These lasers are more silent and less detectable by the enemy.

Medium energy lasers produce 10 kW to 100 kW of power and are used for the destruction of optical or optoelectronic devices on ground or space-based targets.

High-energy lasers (HEL) generate more than 100 kW of power and are used for anti-aircraft or anti-missile systems. The main components and modules from which one HEL is constructed are shown in Fig.4. Having the speed of light, these lasers provide short engagement time for the target, depending on the terrain and speed of the target.

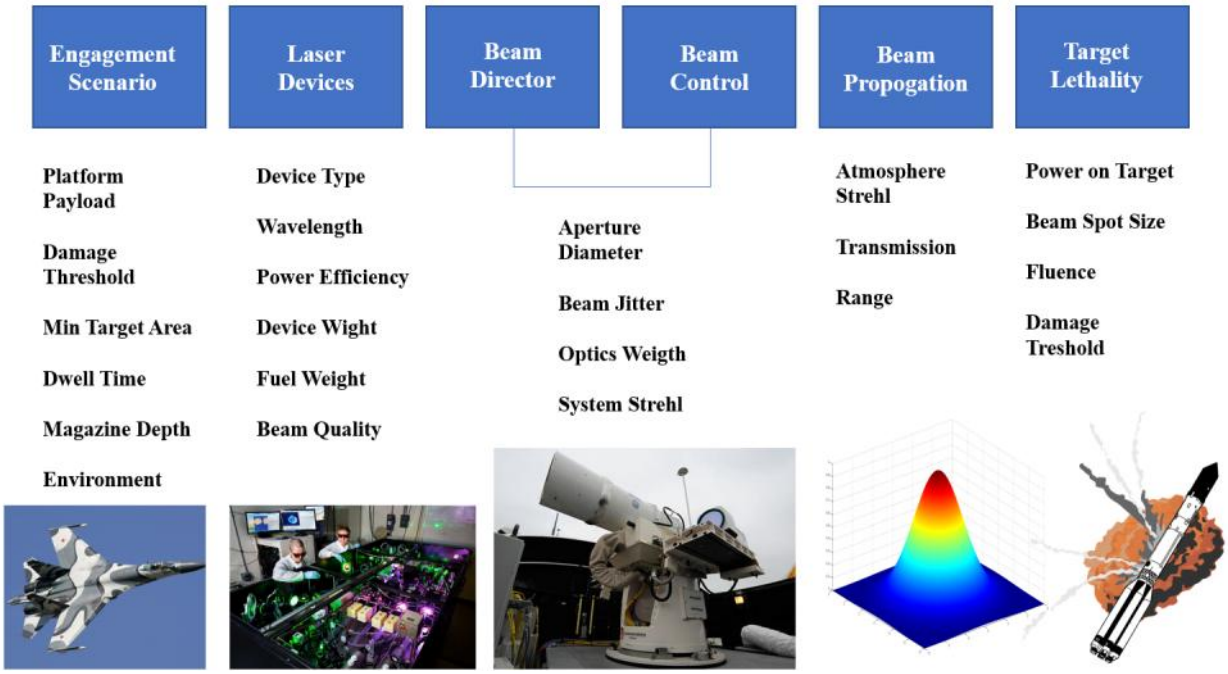


Fig. 4. Components of the HEL weapons system

Today many countries, such as USA, Russia, China, India and Germany, are carrying out extensive research on HEL for navy or air defence purposes [4, 5, 6]. High-energy lasers, due to high costs and bulkier structure, will probably be limited to the protection of costly high-technology targets such as air and navy bases, high-level command posts and aircraft carriers.

As previously discussed, when capable of generating higher power levels, ranging from kW to MW, any laser can be used as a laser weapon. However, these lasers have special needs to operate efficiently, i.e. cooling requirements, laser fuel storage requirements, environment and personal safety requirements, pointing and tracking requirements. For these lasers, the cooling requirement is essential to compensate for the enormous amount of heat generated by generating the laser beam in the resonator. If the cooling devices are not properly made, the heat will weaken the power of the laser beam, which will affect the interaction of laser radiation with the target substance. These weapons require adequate supply of fuel or electricity to allow the simultaneous impact of multiple target commitments.

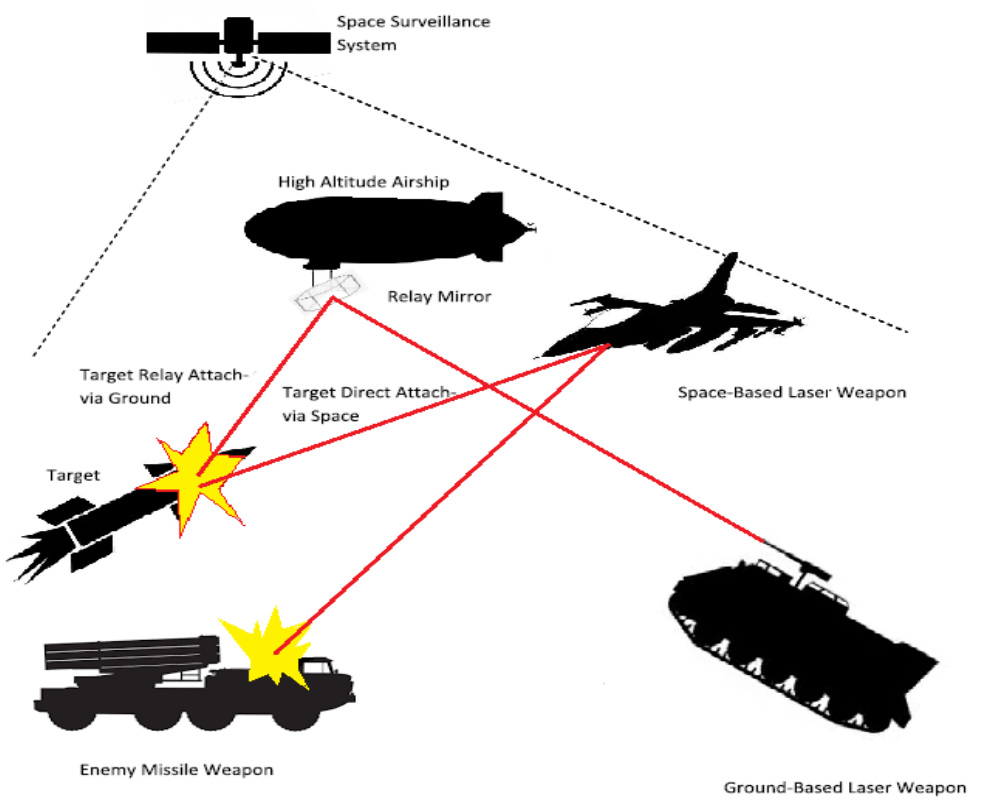


Fig. 5. Demonstration of ground–based and space–based laser weapon

Laser weapons can be either ground-based or space-based as depicted in Fig. 5. Ground-based laser weapons utilize multiple relay mirrors in space to destroy an inter-continental ballistic missile. These relay mirrors are used to extend the range of high-energy laser weapons, as it compensates for the limiting factors caused due to atmospheric absorption, turbulence and curvature of the Earth. A high-energy laser beam from a ground station is relayed to a missile with the help of these mirrors. Since the beam has to pass through the atmosphere to reach the constellation of relay mirrors in space, the energy requirement of ground-based lasers is substantially higher than space-based lasers, leading to greater losses due to atmospheric transmission, thermal blooming and larger distances. The use of bifocal relay mirrors effectively puts the laser source at the mirror. This increases the intensity on the target at a specific range or extends the range of the laser while retaining the original brightness or intensity. These lasers have evolved during the strategic defence initiative (SDI) era but have not received significant emphasis due to the variety of technical challenges involved relating to its design and development [7].

The main types of lasers that are good candidates for laser weapons include: chemical laser, solid state lasers, free electron laser (FEL), fiber laser, and liquid laser [8,9,10]. Each of these lasers has its own unique characteristics that make it suitable for certain operational applications.

Chemical lasers are the most mature laser weapon technology that generates high power from exothermic chemical reactions to strong laser IR radiation. Characteristics of some of the most popular lasers, e.g. Hydrogen Flouride (HF) laser, deuterium fluoride (DF) and chemical oxygenated iodine laser (COIL), have been described earlier in this article (see Table 1). Following the success of the first 1 kW HF laser in 1965, diverse military organisations have been interested in producing more powerful lasers (> 100 kW) for tactical missions. These lasers are somewhat bulky because they require a large amount of chemical fuel and a good cooling of the resonator for their proper functioning. Various high-energy chemical laser weapons have been demonstrated over the past 45 years including MIRACL [11], ALPHA and Navy-ARPA chemical laser (NACL). ALPHA HF laser is a small-sized MW power laser for space applications. Tactical high-energy laser (THELDF chemical laser), Mobile THEL (MTHEL-DF chemical laser) and advanced tactical laser (ALT-COIL with beam control) are compact field-ready weapons that have successfully demonstrated their capabilities of shooting down short and medium-range targets. With some modifications to THEL, a deployable ground-based directed energy weapon, known as high-energy laser for rockets, artillery and mortars (HELRAM), is used for short range military threats.

Laser equipped aircraft like airborne laser (ABL) [12] is equipped with multiple laser systems: primary laser (COIL) with MW power for target destruction, illuminating laser for ISR and high precision laser for target tracking beam control systems. ABL is capable of detecting the missiles shortly after the cloud break and provides real-time warning about its launch and location to the rest of the forces. It also provides trajectory information and impact point predictions shortly after burning out.

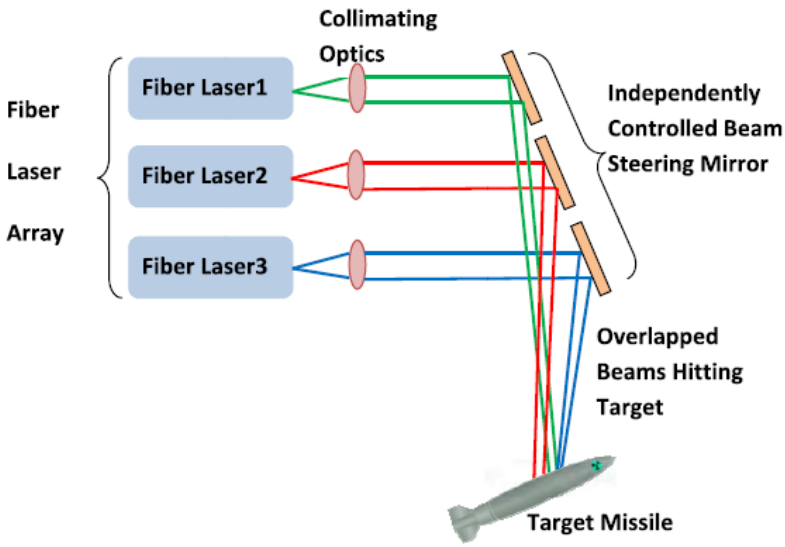


Fig. 6 Simultaneous impact of 3 Fiber lasers on the target

Solid state lasers: fiber laser architecture for high power and long range directed energy weapon. This type of laser offers a very good ratio of size, weight and power (SWaP) and is therefore considered a portable laser weapon. Boeing's HEL-MD is a 10 kW solid state fiber laser with around one micron wavelength designed to destroy rockets, artillery, mortars and drones (RAMD) from ground-based vehicles [13]. Fiber lasers are more compact and require less power to maintain the beam quality than any other HEL design. Its beam control system comprises mirrors, high-speed optical sensors, processors and adaptive optics system to precisely align the beam onto the target in real time. A single mode fiber laser is capable of producing 10 kW of power sufficient to shoot down any missile at an approximated distance of 1.5 km. In order to further achieve the required power levels, multiple fiber lasers can be combined so that a high power overlapped beam, from an individual laser, strikes the

target. The Fig. 6 shows the incoherent combining of fiber lasers, which is individually controlled by a beam steering mirror, to direct each beam onto the target. Such fiber lasers are highly efficient, robust, compact and require low maintenance, which makes them suitable for tactical energy-directed military applications.

The Laser Weapon System (LaWS) is a navy defence system that has successfully demonstrated the shootdown of an UAV from a HEL weapon deployed on a small ship. The system consists of an array of solid state lasers, generating IR beams at a varying output power, in the range from 15 to 50 kW, so as to warn or damage the designated target. The Office of Naval Research (ONR) will now extend the experimentation by performing a shipboard test with a 150 kW laser weapon system in the near future [14].

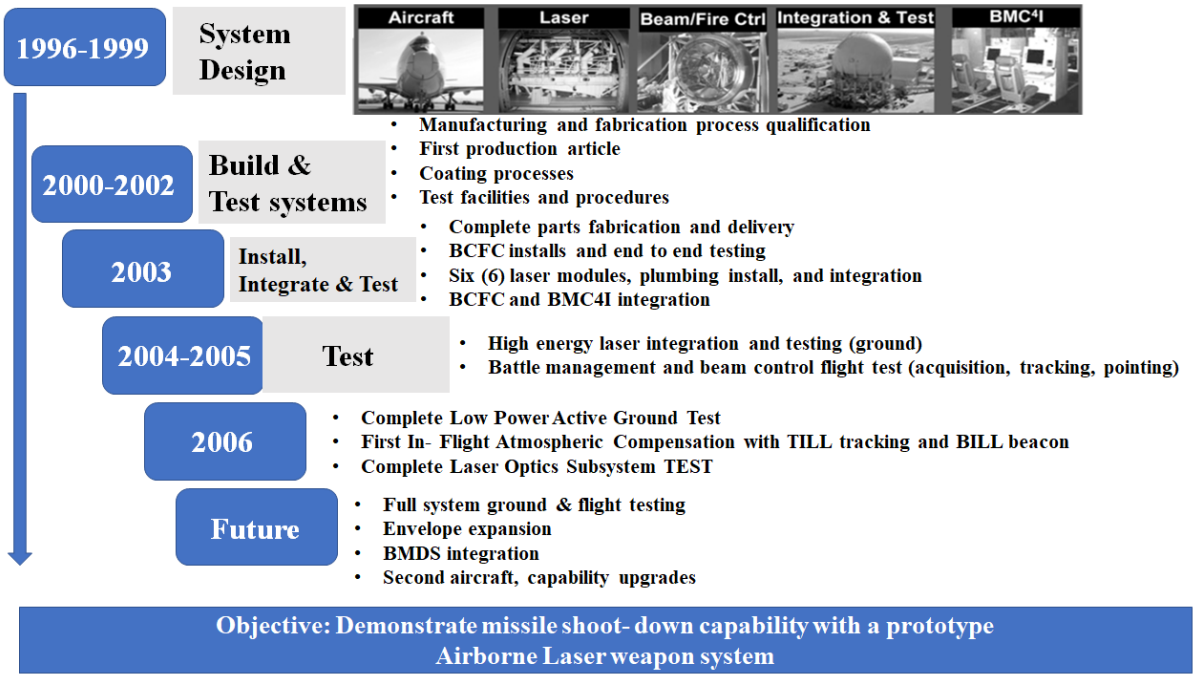


Fig. 7. The long way we have to go to create an ABL. Program Progression

Chemical oxygen-iodine lasers (COIL) used in Airborne Laser (ABL) to attack ICBM and Advanced Tactile Laser (ATL) to defeat armoured vehicles.

What is the future trend for the development of laser weapons?

Laser weapons are efficient and powerful countermeasure utilities against any form of external threat, including ground-based or space-based military menaces. They offer several advantages over conventional weapon systems. Since laser beams travel at the speed of light, they provide near-realtime transfer of information to the soldiers immediately after the target detection. The coherence of laser beams provides a highly focused energy which causes physical destruction to the structures, by converting laser energy into thermal energy.

Nowadays, chemical lasers are replaced by solid-state laser systems with semiconductor (diode) pumping. A huge advantage of chemical lasers is the fact that the laser power does not require any cumbersome and heavy power plant because the chemical reaction is the source of energy. The main disadvantage of these systems is environmental hazard and bulkiness of the structure.

Since these devices are constantly powered or reloaded by chemical/electricity energy storage, they have the capacity to engage multiple targets with fewer moving mechanical parts. Lasers weapons provide promising and cost-effective solutions for tactical missions, unlike conventional ballistic missiles. The incremental cost per shot for ballistic missiles is essentially the cost of the ammunition expended, whereas, on the other hand, laser weapons expend only energy. Hence, the cost per shot equals the cost of the chemical fuel or the fuel required to generate the electricity, which is much less as compared to conventional weapons. Besides, these directed energy weapons provide exceptional striking accuracy, which results in little collateral damage and allows the use of lasers for lethal or non-lethal

applications. The Fig. 8 demonstrates the applications of laser weapons for ground, space and maritime environments.

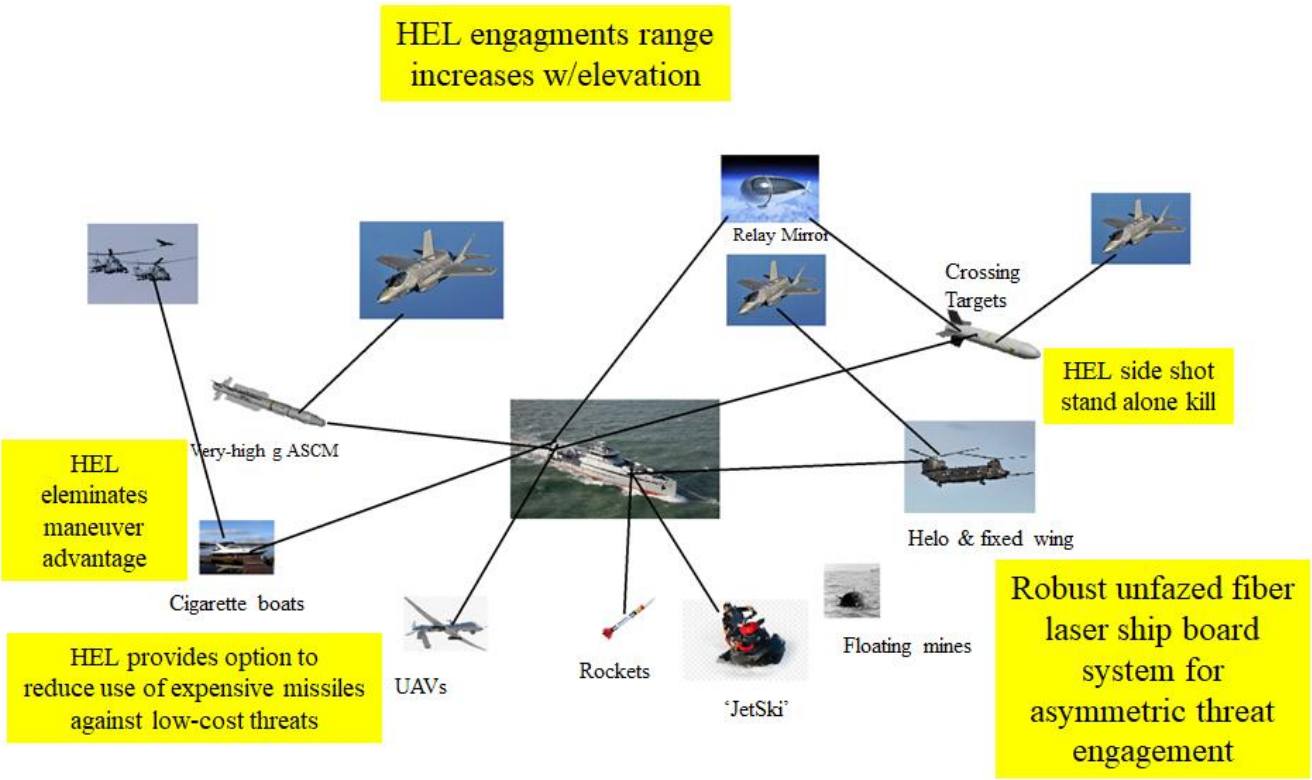


Fig. 8. Directed energy weapons for force protection and self-defence

Wavelength	Area of Damage	Pathological Effect
180 - 315 nm (Ultraviolet UV-B, UVC)	CORNEA; Deep-ultraviolet light causes accumulating damage, even at very low power	Photokeratitis; Inflammation of the cornea, similar to sunburn
315 - 400 nm (Ultraviolet UV-A)	CORNEA and LENS	Photochemical cataract; Clouding of the lens
400 - 780 nm (Visible)	RETINA; Visible light is focused on the retina	Photochemical damage; Damage to retina and retinal burns
0.78 – 1.4 µm (Near Infrared)	**RETINA; Near IR light is not absorbed by iris and is focused on the retina**	**Thermal damage to cataract and retinal burns**
1.4 – 3.0 µm (Infrared)	**CORNEA and LENS; IR light is absorbed by transparent parts of eye before reaching the retina**	**Aqueous flare; Protein in aqueous humor, cataract, corneal burn**
3000 – 10000 nm (Far Infrared)	CORNEA	Corneal burn

Table 2. Effects of a laser beam on the eye (*from UCELA Laser Safety Line 2009*)

To use laser beams as weapons, a significant amount of laser power is necessary. The required output power is determined and strongly depends on the type and distance to the target. On the other hand, researchers of the new laser weapon have to adhere to the international protocol on dazzling laser weapons that prohibits the use of dazzlers to blind the enemy. This is a great paradox because the minimum power that causes eye damage can be very low. Dazzler lasers, for example, are designed to temporarily or permanently affect the human eye [15]. Since the eye is a very sensitive human organ,

these weapons need only a small amount of output power. Within a few meters, even an output power of several miles may damage the eye because the eyes focus the beam on the retina FIG. Blinding lasers were used in the Falklands conflict and in the war between Iran and Iraq in the 1980s [16].

Blindness can also occur when working with powerful and moderately powerful lasers at occasional reflections or deviations of the laser beam. The laser effect on the eye in this case may be multifaceted: besides the burning of the retina, the laser pulse can also destroy the blood vessels in the eye or cause the process of slow retinal decay and others (see Fig. 9 and Tab. 2).

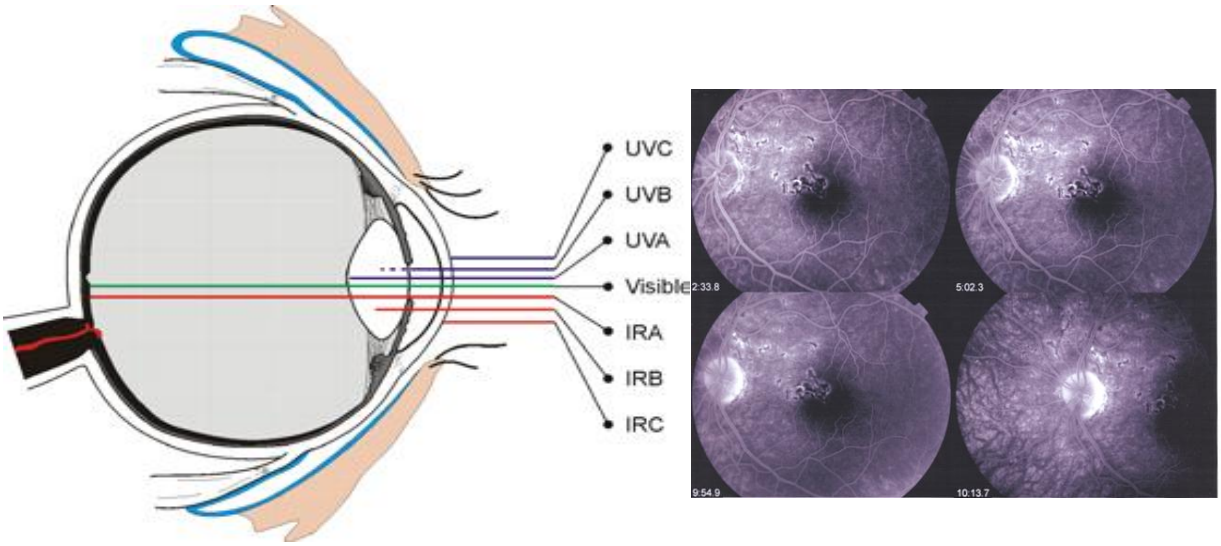


Fig. 9. Schematic diagram of the eye, penetration and possible damage to the eye from laser radiation of different wavelength [17], mesh defects due to dazzler effects [18].

In 1995, these weapons were officially banned according to the International Humanitarian Law. However, if the aim is to destroy hard targets rather than to blind the enemy, the laser requires an output power which is many orders of magnitude higher than that of blinding lasers. As mentioned above in this article, many countries and research institutes develop and test lasers with continuous output power over 20 kW or impulse energy over 1 kJ [19]. As stated above, the use of blinding laser weapons is illegal under International Humanitarian Law. In particular, these weapons violate the Fourth Protocol (1995) to the Convention on Prohibitions or Restriction on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to Have Indiscriminate Effects. This protocol outlaws the use and transfer of laser weapons which are intended to cause blindness. Additionally, the signatories are obliged to take the necessary steps to prevent blindness caused by other laser weapon engagements [20]. However, the protocol is not applicable if collateral blinding occurs as a result of military laser applications that are otherwise considered legitimate. As a consequence, the protocol might be applicable to High Energy Lasers (HEL) weapons only, if they are especially designed for blinding purposes. Nevertheless, the protocol seems to have had some positive effects so far. The protocol is the first step towards a comprehensive ban of all laser weapons. This would be the first step towards preventive arms control, a concept which was developed to ban the introduction of new destabilising weapon systems [21].

Whether and to what extent a complete ban is realistically achievable is obviously another question.

Conclusion

Laser weapon systems have seen rapid development in recent years. Dedicated R&D has advanced the state of the art considerably. What was unimaginable only a few years ago, has become a reality today. Accordingly, if appropriate research and development strategies are applied, warfighters, in the near future, will have additional weapon options to choose for dealing with a spectrum of threats and contingencies.

In this paper, we have discussed various prospects of laser technology for tactical military applications. Laser technology addresses the need of today's battlefield that requires ability to detect the target at longer distances and exchange massive amount of information in a secure and timely manner.

Lasers have revolutionized the warfare as accessories to high-energy weapons. This technology serves as a power tool of warfighters when used as battle field illumination elements, range-finders, target designators, LIDARs, communication systems, power beamers or active remote sensors. Because of the high frequency of the laser system, these devices provide broadband capacity links with SWaP benefit and have a remarkable angular resolution, which is very crucial for tactical laser device deployment. Besides higher bandwidth, laser device is used where anti-jam is required or RF spectrum is not available. The use of laser, as a directed high-energy weapon, requires sufficient amount of power in MW to cause substantial damage to a distant target. Even though laser weapons are used to destroy targets, they can also cause damage to the user if handled improperly. These weapons require sufficient cooling between firing, therefore they cause certain problems for ground vehicles, especially for hand-held laser weapons. Also, during highly turbulent weather conditions including heavy smoke, dust or humidity, these weapons may be deflected from the actual path and can miss the target.

The military is still working on many engineering problems, in order to compensate for the beam wander due to bad weather conditions, movement of the target or motion of the platform.

Further, these HEL poses a significant threat to sensors and military equipments on the battlefield. These sensors may require a protection mechanism such as laser jamming feature built into the sensor platform to ensure reliability and integrity of these devices in a hostile electromagnetic warfare environment. Also, quantum computing and cryptography are a game-changing technologies in cyber warfare, possibly safeguarding tactical communication against eavesdroppers. With all of this ongoing development and current capacities, laser technologies will dominate the battlespace in the near future.

Obviously, when working with all the new developments and applications of laser weapons, we have to stick to the global protocol on laser dazzling, which prohibits the use of lasers specially designed for dazzling personnel but also by accidental deviations of the radiation to the unintended directions, thus creating a risk of damaging health of unrelated people and other objects.

References:

[1] Albertine, John R., "History of Navy HEL Technology Development and Systems Testing," (Proceedings Paper), *Proc. SPIE*, Vol. 4632, Laser and Beam Control Technologies, Santanu Basu and James F. Riker, Eds., pp. 32–37.

[2] Dave Ahearn, ONR Laser Power Jumps 10 Fold; Further 10-Fold Leaps Seen, Defense Today, August 4, 2004, p. 4.

[3] R. A. Motes, R. W. Berdine, Introduction to high-power fiber lasers. Albuquerque: Directed Energy Professional Society, 2009.

[4] D. Litovkin Laser weapons development in full swing in U.S. and Russia, December, (2014)

[5] V.V. Apollonov. American journal of modern physics 1 (1), (2012).

[6] V.V. Apollonov. High power lasers and new applications. International journal of engineering research and development, v. 11, issue 03, March (2015).

[7] W. H. Possel, ``Laser and missile defense: New concept for spacebased and ground-based laser weapons," Maxwell Air Force Base,Montgomery, AL, USA, 1998. [Online]. Available: http://www.au.af.mil/au/awc/awcgate/cst/csat5.pdf

[8] Marc Selinger, "U.S. Army Studying Guns, Lasers, Interceptors to Destroy RAMS," Aerospace Daily & Defense Report, October 28,

2004.http://www.aviationnow.com/avnow/news/channel_aerospacedaily_story.jsp?id=news/RAM10284.xml
[9] M. Selinger, DOD Solid-state Laser Demos Delayed Three Months, Aerospace Daily & Defense Report, December 23, 2004.
[10] Hampton Stephens, Air Force, Army Effort is Advancing Tactical Laser Technology, Inside the Air Force, July 16, 2004.
[11] Pike John, Mid-Infrared Advanced Chemical Laser (MIRACL), FAS Space Policy Project, Military Space Programs, March 1998, http://www.fas.org/spp/military/program/asat/miracl.htm
[12] S. E. Lamberson, The airborne laser, Proc. SPIE, Gas Chem. Lasers, vol. 2702, pp. 2702-1_2702-6, Mar. 1996.
[13] High Energy Laser Mobile Demonstrator HELMD. (2016). [Online]. Available: http://breakingdefense.com/tag/high-energy-laser-mobiledemonstrator-hel-md/
[14] K. D. Atherton. The Navy is Going to Test a Big Laser Soon. (2016), [Online]. Available: http://www.popsci.com/navy-is-going-to-testbig-laser-soon
[15] A. Peters, Blinding Laser Weapons: The Need to Ban a Cruel and Inhumane Weapon, Human Rights Watch Arms Project, September 1995, vol. 7, no. 1, , pp. 1–49
[16] J. H. McCall, Jr, Blinded by the Light: International Law and the Legality of Anti-Optic Laser Weapons, Cornell International Law Journal, vol. 30, no. 1, 1997, pp. 1–44
[17] Princeton University: Laser Safety Training Guide http://web.princeton.edu/sites/ehs/laserguide/index.htm
[18] B. Rivers, C. Crawford, Chorioretinal Injury Caused by Presumed Laser Dazzler, Surgery: Current Research, ISSN: 2161-1076 SCR, an open access journal 2014.
[19] US Defense Threat Reduction Agency, Section 11: Lasers and Optics Technology, in US Department of Defense, Devloping Science and Technologies List, Ft. Belvoir, 2000, http://www.dtic.mil/mctl/DSTL/Sec11.pdf.
[20] ICRC, Treaty database of the International Comitee of the Red Cross, http://www.icrc.org/ihl.nsf/WebFULL?OpenView – viewed May 2005.
[21] T. Petermann, M Socher & C Wennrich, Präventive Rüstungskontrolle bei Neuen Technologien. Utopie oder Notwendigkeit?, Studien des Büros für Technikfolgen-Abschätzung beim Deutschen Bundestag 3, Edition Sigma, Berlin, 1997.
[22] Volume 4, Issue 4, pp. 1-4

Moldoveanu Cristian-Emil,

INSTABILITY MECHANISMS OF THE AIRCRAFT WAKE VORTICES

Moldoveanu Cristian-Emil

Military Technical Academy "Ferdinand I"
39-49 Av. George Cosbuc, Bucharest, Romania
Fax: +32(0)2 7376352
E-mail: moldoveanu.cristian@mta.ro

Abstract: *Developing air traffic and introducing large aircrafts in use in the group of transport aircrafts has led to the necessity to optimize separation distances between aircrafts, especially near airports. These distances are imposed by airport safety and security conditions, related to the action of the wake turbulence generated by an aircraft on another. At the edge of the aircraft wings, longitudinal vortices are created by pressure differences inside the boundary layers and rotated in opposite senses. It can constitute a danger to another aircraft that flies in this wake, especially during takeoff and landing. This study presents the modelling methods of the turbulence using Large Eddy Simulation and some applications in the case of wake vortex.*

1. Introduction

Any object moving in the air leaves behind it a more or less organized wake. In the case of an aircraft, wake turbulence is composed of persistent vortices, which constitute a danger for the following aircraft. These vortices are due to the flow of air at the end of the wing. Indeed, the difference in pressure between the bottom and the top tends to cancel at the extremity of the wings. It is this pressure difference that generates lift on each wing and the generated vortex will be even more intense if this lift will be great. As the lift is directly proportional to the weight of the aircraft, the intensity of wake vortex is bound also [3].

Typically, a pair of contrarotatifs vortices is very persistent. It descends into the atmosphere with a vertical speed of approximately 5 m/s (20 km/h). A small aircraft that is experiencing these vortices can be influenced by a violent rolling motion of the air. In the presence of the wind, the atmosphere is generally turbulent. If this turbulence is sufficiently intense, it is capable of destroying wake vortex by causing their misalignment and by promoting their interaction (if two opposed direction of rotation vortices are touching, they will decay). In most cases, the presence of atmospheric disturbances eliminates the danger: aircraft often encounter these phenomenon residues without being able to distinguish them from the ambient atmospheric turbulence. But in a calm atmosphere, wake vortices persist long time. This makes them dangerous [2].

2. Large Eddy Simulation of Turbulent Flow

There is a large number of mathematical methods for the resolution of disturbed flows equations which here are the main three:

- the statistical method, designated under symbol RANS-"Reynolds Averaged Navier-Stokes", uses Navier-Stokes equations by passing at the average, the result is therefore a loss of information;

- Large Eddy Simulation (LES) - this simulation's major idea is to calculate the contributions to the large scales of flow while modelling is reserved for structures whose size is less than a characteristic dimension calculation mesh.

- Direct Numerical Simulation (DNS) - exclude any modelling of turbulent agitation. We operate numerically at the resolution of Navier-Stokes equations. Thus, obtaining statistical data on the flow is

reported after the resolution. This method requires more memory space and calculation time than large scales simulation method and is therefore more expensive. It still belongs to the domain of research and is useful to analyze phenomena associated with small scales and in particular sub-meshes schemas. It can be said that this method allows some real "numerical experiences" whose results can both give complete knowledge drawn from traditional physical experiments or provide support for developing models for other categories.

The phenomenon of turbulence, although chaotic, does not occur outside the laws and the known equations for fluids flow. The general framework where we model fluid flow is given by a set of equations: the continuity equation, equation of quantity of movement, equation of energy and perfect gas law. The unknown of the system are: velocity, with its three components u, v and w, the pressure p, the fluid density ρ and temperature T. All these parameters are functions variable in time and space [4].

The continuity equation is expressed by the relation:

$$\frac{\partial \rho}{\partial t} + \frac{\partial\ \rho u}{\partial x} + \frac{\partial\ \rho v}{\partial y} + \frac{\partial\ \rho w}{\partial z} = 0, \tag{1}$$

where ρ is the fluid density and u, v and w are the components of the fluid velocity.

The continuity equation may be written in the vector form:

$$\frac{\partial \rho}{\partial t} + \rho \mathrm{div} V + V \mathrm{grad} \rho = 0. \tag{2}$$

In the case of a constant fluid volume, density is independent of time and space variables. Equations of quantity of movement are the equations of the balance between forces of inertia, mass forces, pressures and constraints due to friction. The vector form of the quantity of movement equation is expressed by:

$$\rho \frac{dV}{dt} = \rho f - \mathrm{grad} p + \frac{1}{3} \mu \mathrm{grad}\ \mathrm{div} V\ + \mu \Delta V, \tag{3}$$

where f is the external mass force acting on the unit of mass and μ is the dynamic viscosity.

Momentum equations can be projected in the Cartesian coordinates for an incompressible fluid neglecting the external mass forces:

$$\frac{\partial u}{\partial t} + u\frac{\partial u}{\partial x} + v\frac{\partial u}{\partial y} + w\frac{\partial u}{\partial z} = -\frac{1}{\rho}\frac{\partial p}{\partial x} + \frac{\mu}{\rho}\ \frac{\partial^2 u}{\partial x^2} + \frac{\partial^2 u}{\partial y^2} + \frac{\partial^2 u}{\partial z^2}\ , \tag{4}$$

$$\frac{\partial v}{\partial t} + u\frac{\partial v}{\partial x} + v\frac{\partial v}{\partial y} + w\frac{\partial v}{\partial z} = -\frac{1}{\rho}\frac{\partial p}{\partial y} + \frac{\mu}{\rho}\ \frac{\partial^2 v}{\partial x^2} + \frac{\partial^2 v}{\partial y^2} + \frac{\partial^2 v}{\partial z^2}\ , \tag{5}$$

$$\frac{\partial w}{\partial t} + u\frac{\partial w}{\partial x} + v\frac{\partial w}{\partial y} + w\frac{\partial w}{\partial z} = -\frac{1}{\rho}\frac{\partial p}{\partial z} + \frac{\mu}{\rho}\ \frac{\partial^2 w}{\partial x^2} + \frac{\partial^2 w}{\partial y^2} + \frac{\partial^2 w}{\partial z^2}\ , \tag{6}$$

where μ is the dynamic viscosity.

Large Eddy Simulation aim is to solve the complete Navier-Stokes equations while reducing the number of node of the mesh necessary to resolve a fully turbulent flow. Reynolds numbers encountered in natural turbulent flow prohibit current computers perform a numerical simulation of all scales involved. The idea of LES is to practice a cut to a wavelength $k = k_c$ (figure 1). We simulate directly large scales corresponding to $k < k_c$ and we model small scales corresponding to $k > k_c$ [1].

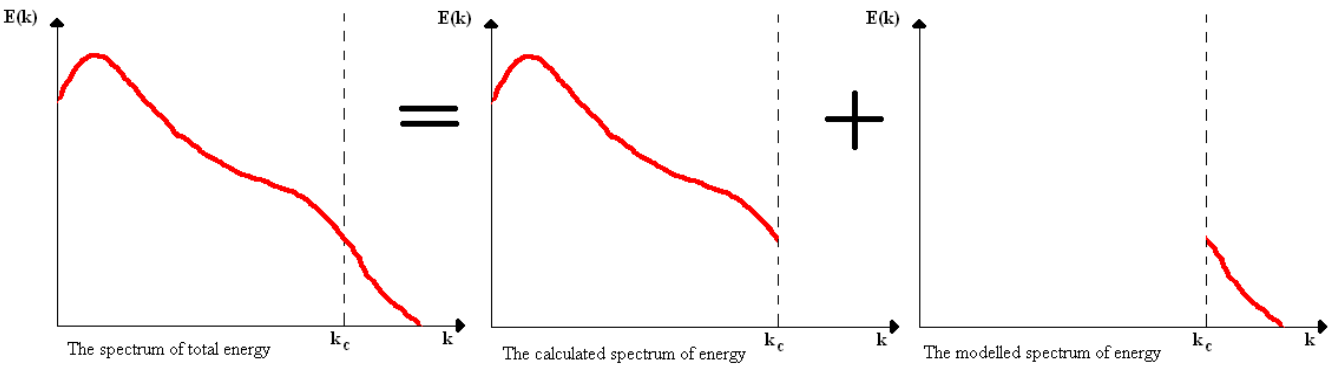


Figure 1. Decomposition of the energy spectrum of the solution associated to the LES simulation

Large scales (see figure 3) are less universal and are more dependent on the geometry of the flow. Small scales are less affected by the geometry of the flow, so it should be easier to find universal models to represent their effects. Velocity field is in this case divided into the sum of a velocity field corresponding to the large scales and a sub-mesh velocity field that represents the wavelengths not

picked up by the mesh. It should be noted that this separation between different scales is not related to an average operation statistics [7].

The formalization in mathematical terms of this separation of scales is to express the passage through a low pass filter in frequency and in number of wave. The application of this filter to the Navier-Stokes equations allows obtaining the constituent mathematical model for the simulation of the large scales. Part of the resulting terms can be calculated directly from resolved scales, the other must be modelled.

The separation of scales is performed by the application of a high pass filter in spatial scale and low pass in frequency to the exact solution. Thus, for any quantity associated $\varphi\ x,t$ with the turbulent movement it sets the quantity resolved $\varphi\ x,t$ by:

$$\varphi\ x,t\ =\ _V G_\Delta\ x-x'\ \varphi\ x',t\ dx', \tag{7}$$

where the convolution kernel $G_\Delta\ x-x'$ is characteristic to the used filter that is associated with cut-off in space scales Δ (bandwidth filter) [1].

This paragraph is realised to bypass the constituent equations of simulation techniques of the large scales, i.e. filtered Navier-Stokes equations. Navier-Stokes system variables are written as follows:

$$u_i\ x,y,z,t\ = u_i\ x,y,z,t\ + u'_i\ x,y,z,t\ , \tag{8}$$

$$p\ x,y,z,t\ = p\ x,y,z,t\ + p'\ x,y,z,t\ . \tag{9}$$

This modelling must not only have a role of dissipation of the surplus energy not absorbed by the small structures which are not resolved by the code, but also take account of the energy return - that exists in some parts of a turbulent flow of these small structures - to the resolved scales of the field.

The system of Navier Stokes equations for the non-filtered field is:

$$\frac{\partial u_j}{\partial x_j} = 0, \tag{10}$$

$$\frac{\partial u_i}{\partial t} + u_j \frac{\partial u_i}{\partial x_j} = -\frac{1}{\rho}\frac{\partial p}{\partial x_i} + 2\frac{\mu}{\rho}\frac{\partial S_{ij}}{\partial x_j}. \tag{11}$$

Assuming that the filter characteristics allow the use of commutative property between operator filtering and operator derivative, after we apply the filter to the equations of Navier – Stokes, we obtain the following equations [1]:

$$\frac{\partial u_j}{\partial x_j} = 0, \tag{10}$$

$$\frac{\partial u_i}{\partial t} + \frac{\partial u_i u_j}{\partial x_j} = -\frac{1}{\rho}\frac{\partial p}{\partial x_i} + \frac{\partial\ 2\frac{\mu}{\rho}S_{ij} - \tau_{ij}^{sm}}{\partial x_j}, \tag{11}$$

where: $\tau_{ij}^{sm} = \overline{u_i u_j} - u_i u_j$ is the constraints tensor of the sub-mesh;

$S_{ij} = \frac{1}{2}\ \frac{\partial u_i}{\partial x_j} + \frac{\partial u_j}{\partial x_i}$ is the tensor of the filtered deformations rate.

We can write the constraints tensor of sub-meshes if we introduce decomposition in the first term:

$$\tau_{ij}^{sm} = \overline{u_i u_j} - u_i u_j = L_{ij} + C_{ij} + R_{ij}, \tag{12}$$

where

$L_{ij} = \overline{u_i u_j} - u_i u_j$, the Leonard term;

$C_{ij} = \overline{u_i u'_j} - \overline{u'_i u_j}$, the term of the crossed constraints;

$R_{ij} = \overline{u'_i u'_j}$, the term of Reynolds constraints.

The non-linear term is now fully deconstructed depending on the amount $u_i$and the fluctuation u'_i.

Large scales simulation is a technique for reducing the number of degrees of freedom for the solution. This reduction operates separate scales that conduct to obtaining the exact solution into two categories: large scales and sub-meshes scales.

Decreasing of the solution complexity is obtained by retaining only the large scales for the numerical resolution. Information related to small scales is obtained after an implementation of a specific model. Subsequently, all terms that make them appear, i.e. the term in u' in physical space, may not be calculated directly. These terms are grouped together in the sub-mesh tensor. However, to ensure that the dynamics of the scales resolved remains correct, the term of sub-mesh must be taken into account.

The sub-mesh scale modelling consists in expression of this term function of the resolved scales. In this case we have to use additional hypothesis, derived from knowledge on mechanics of the fluid that permit to link the existence of sub-mesh modes to certain properties of resolved scales.

3. Simulation of aircraft wake vortex

During the evolution of a pair of contra-rotating longitudinal vortex in the presence of an external turbulence, we observe the generation of the instability at large wavelength, named Crow instability. We have to study the behaviour of a pair of vortices in the presence of such disturbance.

In the aim to achieve this disturbance, we disturb the vortices centre position. As parameters to this disturbance we use: the magnitude of the disturbance Amp, the angle of the disturbance plane θ, the phase difference ϕ and the longitudinal wave number k (figure 2). In the transverse plane, disturbed vortex centre coordinates are [7]:

$$y_{c_{\text{pert}}} = y_{c_{\text{nepert}}} + Amp \sin\ kx + \phi\ \ \cos\theta, \tag{13}$$

$$z_{c_{\text{pert}}} = z_{c_{\text{nepert}}} + Amp \cos\ kx + \phi\ . \tag{14}$$

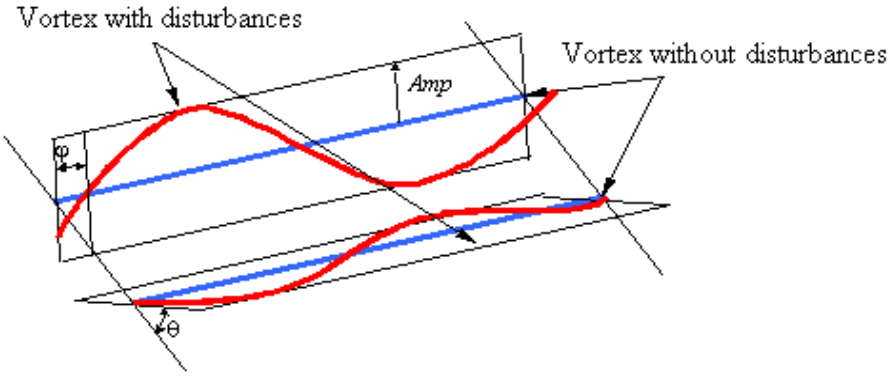


Figure 2. Crow type disturbance

To initiate the calculations, we use a vortex dipole model, whereas two longitudinal vortices with circulations $\Gamma_{01} = -\Gamma_0$, $\Gamma_{02} = \Gamma_0$, $\Gamma_0 = 1$with the same radius $r_0 = 0.2 \cdot b$, located at a distance $b = 1$ to each other, b being the distance between the edges of the wings. Basis positions for vortices cores are given by the coordinates $y_{c_1}, z_{c_1} = 2.5, 2.5\ \cdot b$ and $y_{c_2}, z_{c_2} = 3.5, 2.5\ \cdot b$, in the transversal planeOyz. This position is disturbed by the explicitly introduction of the Crow instability. The Crow disturbance parameters used are the maximum amplitude $Amp = 0.2$, the longitudinal wavelength $\lambda = 7.5$ and the phase difference $\phi = 0$. Disturbance plan is rotated as 45 degrees.

The computation field, with a regular mesh, is a rectangular box with dimensions: $L_x = 7.5 \cdot b$ with $n_x = 95$ points, $L_y = 6 \cdot b$ with $n_y = 95$ points, $L_z = 5 \cdot b$ with $n_z = 64$ points (577,600 calculation meshes). The centre of the vortex is represented by 7 points in the direction y and by 6 points in the z direction. The used boundary conditions are periodic in x (the longitudinal axis of the vortex) and z directions (the vortex pair descent direction) and symmetry in y. The characteristic time for the evolution of a pair of the vortex is based on the movement of descent of the two vortices,

$$t_0 = \frac{2\pi b_0^2}{\Gamma_0} = 6.28\ \text{s}. \tag{14}$$

The flow parameters evolution is expressed using the dimensionless time,

$$T = \frac{t}{t_0}. \tag{15}$$

Figures 3 and 4 present the iso-surfaces of vorticity function of the characteristic time. A pair of longitudinal vortex, influenced explicitly by a Crow disturbance, will generate the vortex rings. We observe that in absence of other external disturbances, vortex rings deform and after 20 seconds ($T = 3.2$), the computation field will not be large enough to process correctly the evolution of these vortex rings.

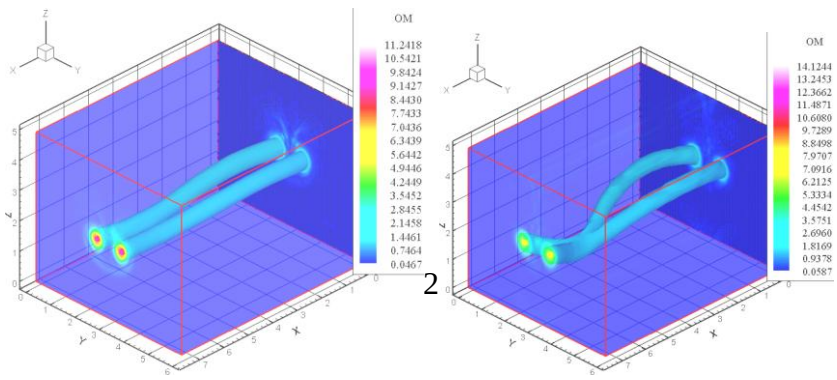


Figure 3. Iso-surface of vorticity ω after T= 0.31 and T= 1.27

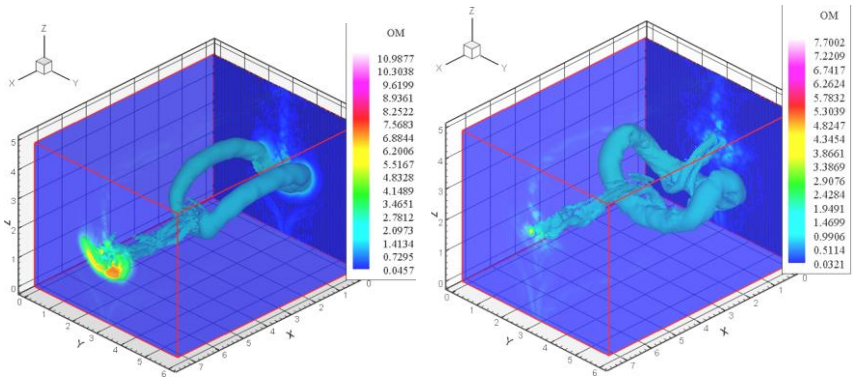


Figure 4. Iso-surface of vorticity ω after T= 1.90 and T= 2.54

4. Conclusions

This paper contains studies regarding the mathematical modelling of turbulent aerodynamic phenomena. As physical phenomena that take place in aircraft wakes can be assimilated to turbulent flows, it was necessary to realize a study of the main theoretical methods and models that can be used in numerical simulation of turbulent phenomena. The choice of the most appropriate method is based on the analysis of the turbulent energy spectre. These methods are based on finding a solution through the method of finite volume of fundamental equations of turbulent fluid flow, the Navier-Stokes equations.

The Large Eddy Simulation (LES) method of modelling turbulent flow consists of directly simulating large turbulent structures, the small ones being modelled by specific methods. The reasoning of this method is based on the fact that large turbulent structures are directly influenced by the geometrical characteristics of the studied situation, while small structures have a universal character, and the errors introduced by modelling them are insignificant. The advantage of this method is that it offers results as precise as those obtained through the direct numerical simulation method, but using a smaller amount of calculus numbers, therefore a smaller calculus power. The study shows the receptivity of a pair of longitudinal vortices contrarotatifs against the Crow disturbance. Through the perturbation of vortices filaments with a Crow disturbance, unsteadiness is inducted with big wavelength, that leads to the destruction of linear vortices and the formation of vortices rings

References:

1. Calmet I., Magnaudet J., Large eddy simulation of high-Schmidt number mass transfer in a turbulent channel flow, Physics of Fluids Review, Volume 9, Issue 2, pag. 438-455, American Institute of Physics, Maryland, USA, 1996;
2. Giovannini A., Boisson H., Moldoveanu C.E., Effect of wind conditions on the evolution of an aircraft vortex wake model near the ground, Proceedings of the 6th International Conference on Computational Fluid Dynamics, pag. 94, St. Petersburg, Rusia, 12-16 iulie 2010;
3. Moldoveanu C.E., Giovannini A., Boisson H., Turbulence receptivity of longitudinal vortex-dominated flows, Lecture Notes in Computational Science and Engineering, Vol. 69: BAIL 2008 - Boundary and Interior Layers, Proceedings of the International Conference on Boundary and Interior Layers- Computational and Asymptotic Methods, Springer Berlin Heidelberg, pag. 227 – 236, ISBN: 978-3-642-00604-3, 2009;
4. Moldoveanu C.E., Giovannini A., Boisson H., Moraru F., Large Eddy Simulation of vortex pair submitted to ground effect, New Aspects of Engineering Mechanics, Structures, Engineering Geology, Proceedings of the WSEAS International Conference on ENGINEERING MECHANICS, STRUCTURES, ENGINEERING GEOLOGY (EMESEG '08), Heraklion, Crete Island, Greece, 22-24 iulie 2008, pag. 265-270, ISSN 1790-2769, ISBN 978-960-6766-88-6;
5. Moldoveanu C.E., Safta D., Şomoiag P. – Analyze of the Counter-Rotating Vortices Pair Stability under the External Turbulence Influence, Lecture Notes in Engineering and Computer Science,

WCE2008 Proceedings of The World Congress on Engineering 2008, The 2008 International Conference of Mechanical Engineering, Londra, United Kingdom, 2-4 iulie 2008, Volume II, pag. 1463-1467, ISBN 978-988-17012-3-7;

6. Moldoveanu C., Boisson H., Giovannini A., Moraru F."Numerical simulation of longitudinal counter-rotating vortices pair in interaction with ground", Fluid Mechanics and Aerodynamics, Proceedings of the 5th IASME/WSEAS International Conference on Fluid Mechanics and Aerodynamics (FMA'07), Vouliagmeni, Grecia, 25-27 august 2007, pag. 223-228, ISSN 1109-2769, ISBN 978-960-8457-99-7 ;
7. Moldoveanu C.E., Boisson H., Giovannini A., Receptivity of a longitudinal contrarotating vortices in an external flow: a numerical experimentation, Conference on Boundary and Interior Layers, BAIL 2004, Toulouse, Franța, 5-9 iulie 2004.

DEFENSE AND SECURITY

V. P. Petrov, H. A. Hristov,

COMBATING CORRUPTION AND ORGANIZED CRIME IN THE EUROPEAN UNION

Veliko P. Petrov, Hristo A. Hristov

National Military University "Vasil Levski", Faculty of Artillery, Air Defense and Communications and Information Systems, Department of Information Security; town of Shumen.
Shumen university ,,Bishop Konstantin Preslavski'', Shumen city, Faculty of technical sciences, Department ,,Management of security systems''

Abstract**:** *This report aims to familiarize readers with two very serious problems of our time, namely organized crime and corruption, which are one of the greatest threats to the security and stable economic development of the countries of the European Union. The phenomena of organized crime and corruption usually have a cross-border dimension which requires close cooperation from national competent authorities supported by EU instruments and a European action plan to eradicate these phenomena. The fight against corruption in the EU is becoming more and more of a Community nature, largely because of the proven criminal symbiosis between it and organized crime, and its destructive impact on measures relating to the area of freedom, security and justice. Action programs and action plans adopted by the EU to combat organized crime, terrorism, fraud, money laundering and other serious crimes also include a special anti-corruption section.*

Keywords**:** *corruption, organized crime*

БОРБАТА С КОРУПЦИЯТА И ОРГАНИЗИРАНАТА ПРЕСТЪПНОСТ В ЕВРОПЕЙСКИЯ СЪЮЗ

Велико П. Петров, Христо А. Христов

Организираната престъпност, корупцията и изпирането на пари в Европейския съюз (ЕС) и в останалата част на света нарастват и оказват неблагоприятно въздействие върху сигурността на европейските граждани и интересите на европейските предприятия, което може да доведе до подкопаване на общественото доверие в демокрацията и нейните институции. Явленията, свързани с организираната престъпност, корупцията и изпирането на пари, обикновено имат трансгранично измерение, което изисква тясно сътрудничество от страна на националните компетентни органи, подпомагано от инструменти на ЕС, и европейски план за действие за изкореняване на тези явления.

Корупцията и организираната престъпност са проблеми, с които се сблъскват всички модерни общества, включително и страните-членки на Европейския съюз. Корупцията продължава да бъде предизвикателство за Европа, която засяга всички държави-членки на Европейския съюз и коства около 120 милиарда евро годишно на икономиката на ЕС. По показател на „Трансперънси интернешънъл" за усещане за корупция България се справя най-зле в сравнение с всички останали държави от ЕС.

Корупцията е явление, познато на човечеството от хилядолетия. Това явление представлява злоупотреба със служебното положение за неслужебни цели, като към корупционните действия се отнасят: *подкуп, изнудване, влияние върху незаконната търговия, измама*. Въздействието на корупцията върху обществото е толкова негативно, разрушително и мащабно, че необходимостта

от предприемането на мерки за нейното ограничаване не подлежи на съмнение. През последните години то отново е обект на засилен обществен интерес и предмет на множество социологически, политологични, икономически, правни и други изследвания.

Определението на термина „корупция" в изготвената от Съвета на Европа ***Гражданска конвенция за корупцията*** е следното: *„Искането, предлагането, даването или приемането, пряко или косвено, на подкуп или всяка друга неследваща се облага или обещаването на такава, което засяга надлежното изпълнение на някое задължение или поведението, което се изисква от приемащия подкупа, неполагащата се облага или обещаването на такава"*[1]. Същото определение се използва и в българското законодателство. Друга дефиниция за „корупция" може да бъде открита в Юридическият речник от 1994 г. В него корупцията има следното определение: „*Антиобществено явление, характеризиращо се с морална поквара на личността или социялна група и с противозаконно използване на служебно или друго положение за получаване на противозаконна облага. Най-ярката проява на корупция е подкупът*".

Корупцията е лост за създаване на благоприятни условия за проникването на организираната престъпност в законната икономика, най-вече чрез възлагането на обществени поръчки или реализирането на публично-частни партньорства. Тези отрицателни явления застрашават демокрацията, правата на човека и върховенството на правото, подкопават икономическото и социалното развитие, разклащат нравствените устои на обществото.

Организираната престъпност се появява при наличието на определени исторически условия – дезорганизирано общество, в което престъпленията са източник на доход. При тези условия обикновено се създават тайни затворени организирани общества, подчинени на закона на мълчанието. Другата линия предпоставя икономически условия, свързани с развитието на търговията, пазара и нови икономически отношения като в по-ново време тези условия създават организации, целящи големи печалби, с определена икономическа роля в обществото и стремеж към политическата и финансова власт.

Големите престъпни организации, които са с господстващо положение в съвременната престъпност са интернационални. Реформираната организирана престъпност използва нови средства, основните сред които са рекетът и корумпирането. Постепенно силовите методи биват изоставяни за сметка на използване на корупционни практики. Легитимират се престъпни структури, след като бива допусната съвместна икономическа дейност между държавни и частни групировки. Организираната престъпност придобива силно влияние в политическата власт и в органите на съдебната власт, а това води до финансово обвързване на групировките с политици, магистрати, високопоставени лица в администрацията на дадена страна.

Много от престъпленията и митническите нарушения по границите са свързани с организираната престъпност и се съпътстват от реална опасност от корумпиране на митнически служители, гранични полицаи, дознатели и магистрати. Нарастването на общественоопасните прояви в световен мащаб налагат създаването на международни инструменти за противодействието им.

Ангажираността на държавите и международните организации се проявява в приемането на актове, съдържащи мерки за борба с престъпността. Сътрудничеството между тях се осъществява чрез конвенции, резолюции и препоръки, визиращи различни прояви на общественоопасно поведение – тероризъм, трафик на наркотици, корупция, компютърни престъпления и др. Актове в тези области имат ООН, Съветът на Европа, Европейският съюз, Г-8 и други[2].

Ангажираността на държавите и международните организации се проявява в приемането на актове, съдържащи мерки за борба с трансграничната организирана престъпност. Сътрудничеството между тях се осъществява чрез конвенции, резолюции и препоръки, визиращи различни прояви на общественоопасно поведение.

Корупцията, заедно с организираната престъпност и въвеждането на повече ред и сигурност в държавата, бе един от трите съществени проблема, които бяха посочени като възможна основна пречка за присъединяването на България към Европейския съюз на 01.01.2007 г. Единадесет го-

1 Гражданска конвенция за корупцията, изготвена от Съвета на Европа, ратифицирана със закон, приет от 38-то НС на 10.05.2000 г., обн., ДВ, бр. 42 от 23.05.2000 г., издадена от Министерството на правосъдието, обн., ДВ, бр. 102 от 21.11.2003 г., в сила за Република България от 01.11.2003 г.

2 Велико П. Петров, Международно правно сътрудничество между страните от Европейския съюз за противодействие на корупционните престъпления, Научна конференция 2012 „Защитата на информацията – състояние и перспективи", Сб. научни трудове на факултет „А, ПВО и КИС" при НВУ„В. Левски", Шумен, 2012 г., ISBN 978-954-9681-49-9

дини след присъединяването на страната ни към ЕС борбата с корупцията, особено в правоохранителните и правоприлагащите институции като основен стълб на сектора за сигурност, продължава да има първостепенно значение. Високото равнище на корупция в България продължава да бъде причина част от държавите, включени в Шенгенското пространство, да се противопоставят на идеята нашата страна да бъде приета в него.

В борбата с корупцията България е най-зле представящата се държава в ЕС въпреки факта, че е поставена под специален механизъм за сътрудничество от Комисията от 2007 година насам. Механизмът за сътрудничество и проверка (МСП) беше създаден при присъединяването на България към Европейския съюз през 2007 г.[3], за да се преодолеят слабостите в съдебната реформа и борбата срещу корупцията и организираната престъпност. Оттогава досега докладите по МСП са имали за задача да способстват за насочването на усилията на българските органи чрез конкретни препоръки и са отразявали постигнатия напредък.

Основен измерител за корупционната среда е ежегодното изготвяне на индекс от асоциацията „Прозрачност без граници". Според Индекса за възприятие на корупцията през 2016 г. на „Прозрачност без граници", България за поредна година остава най-корумпираната страна в Европейския съюз, а в световната класация е на 75-то място от общо 176 страни[4] [5], а през 2017 година страната заема 71-во място в световната класация.

Световният опит показа, че дори в страните с развита административна система и контролни механизми корупцията не може да бъде овладяна без съдействието на гражданското общество и независимите средства за масово осведомяване. Практиката в развитите демокрации свидетелства за нарасналото значение на включването на професионалните организации и другите граждански структури в усилията за утвърждаване ценностите на прозрачността, публичността и демокрацията. Особено важен е потенциалът на изграждането на механизми и успешни практики на партньорство между държавните институции, неправителствените организации и частните медии в сфери като обществения контрол върху дейността на администрацията, защитата на правата на гражданите, саморегулирането чрез въвеждане в практиката на ефективни кодекси на поведение, инициирането на независим мониторинг, разгръщането на антикорупционна разяснителна и образователна дейност.

Противодействието на корупцията залегна в дневния ред на редица международни организации и финансови институции като ООН[6], Световната банка, Организацията за икономическо сътрудничество и развитие, Съвета на Европа, Европейския съюз и др. Антикорупцията се наложи като основно поле на дейност за множество национални и международни правителствени и неправителствени организации, в рамките на което гражданското общество отстоява съвременните стандарти за прозрачност и публичност на държавните институции и допринася за превенцията на корупцията във всички обществени сектори. Същевременно редица държави в света приеха комплексни програми и мерки за ограничаване на корупционните рискове в контекста на реформите в публичната сфера и утвърждаването на стандартите на почтеност в международните икономически отношения.

Корупцията и необходимостта от противодействие на нейните прояви все повече се тълкуват като ключови критерии за утвърждаването на демократичните институции и за въвеждането на съвременните стандарти на прозрачност и демократичен контрол в управлението на обществото. Понятието „антикорупция" е в много отношения по-широко и обхватно от действията на правоохранителните и правораздавателните органи за пресичане и санкциониране на корупцията. То включва противодействие както на криминализираните форми на подкупност, така и практики, които се определят като меки форми на корупция.

Усилията на всички организации, участващи в сектора за сигурност, имат особено важно място в дефинирането на приоритетите и ефективното противодействие на корупцията, включващо превенцията в най-широкия смисъл на тази дума. Превенцията и противодействието на ад-

3 Заключения на Съвета на министрите, 17 октомври 2006 г. (13339/06); Решение на Комисията от 13 декември 2006 г. за създаване на механизъм за сътрудничество и проверка на напредъка на България в постигането на специфични цели в областите на съдебната реформа и борбата срещу корупцията и организираната престъпност (нотифицирано под номер С(2006) 6570).

4 Индекс за възприятие на корупцията за 2016г., Асоциация „Прозрачност без граници"

5 Център за превенция и противодействие на корупцията и организираната престъпност, кратък доклад „Анализ на органите по превенция и противодействие на корупцията в Република България", София, април 2017 г., стр. 6.

6 Конвенция на ООН срещу корупцията, приета с резолюция 58/4 на Генералната асамбея от 31 октомври 2003 г. Ратифицирана със закон, приет от 40-то Народно събрание на 03.08.2006 г., ДВ, бр. 66 от 15.11.2006 г. Издадена от Министерството на правосъдието, обн., ДВ, бр. 89 от 3.11.2006 г., в сила за Република България от 20.10.2006 г.

министративната и на политическата корупция изискват по-тясно взаимодействие и координация между публичните институции и изграждане на ефективни антикорупционни звена.

Борбата срещу организираната престъпност заема ключово място в политиките на Европейския съюз за създаване на европейско пространство на свобода, сигурност и справедливост. Транснационалната престъпност с организиран характер се превръща в сериозна заплаха за ЕС с разгръщането на процесите на глобализацията, специфичен елемент от който е и европейската интеграция. Основните сфери на престъпна дейност с организиран характер са незаконния трафик на наркотици, оръжие и хора, международните финансови измами, рекет, корупция, проституция, хазарт, изпиране на пари и други. Придобитите по престъпен начин средства се включват чрез операции по изпиране на пари в легалната икономика, като с това се затруднява разкриването на този вид престъпност. Организираната престъпност ражда корупцията, а тя превръща държавните служители в престъпници.

Борбата срещу организираната престъпност изисква преди всичко засилено полицейско сътрудничество, ангажиращо 1,2 млн. полицейски служители в страните-членки на ЕС и е важно да не се допусне разнобой и разпиляване на този потенциал, тъй като новият характер на заплахите изисква наднационално сътрудничество. Обмяната на полицейска информация между страните-членки изисква общи стандарти и достъп до информационните масиви на полицията. В ЕС се поставя задачата за сформиране на съвместни митнически учреждения, както и по-честото и системно сътрудничество между полицейските и съдебните органи в страните-членки.

По-голяма част от проявите на организираната престъпност са предвидени като престъпления в националните законодателства на държавите. На международно равнище обаче предстои редица общественоопасни форми на организирана престъпност да бъдат определени като международни престъпления.

Организираната престъпност, корупцията и изпирането на пари обикновено имат трансгранично измерение, което изисква тясно сътрудничество между компетентните национални органи и между националните органи и съответните агенции на ЕС. Полицейското и съдебното сътрудничество чрез обмен на информация между националните органи е от съществено значение, за да се предприемат ефективни мерки за борба срещу корупцията и организираната престъпност. Трансграничното полицейско и съдебно сътрудничество се характеризира с прекомерно дълги бюрократични процедури, които възпрепятстват неговата ефективност и застрашават ефикасността на борбата с организираната престъпност, корупцията и изпирането на пари на равнището на ЕС.

Необходимо е да се подобри трансграничното полицейско и съдебно сътрудничество, чрез споделянето на информация между тях и посредством Европол и Евроюст и осигуряване на подходящо обучение и техническа подкрепа, включително чрез Европейския полицейски колеж и Европейската мрежа за съдебно обучение.

Законодателната рамка в правото на отделните държави при регулирането на противодействието и борбата с корупцията се очертават два подхода:

1) Подробна законодателна уредба в законодателството относно наказателното правораздаване – в Белгия (Централно антикорупционно бюро към федералната полиция и Централно бюро за разследване на корупция в системата на Прокуратурата); Испания (Специализираната прокуратура Антимафия), Великобритания, Германия. Този подход се отличава:

– със стремеж за относително подробно и детайлно уреждане на основните корупционни престъпления и способите за тяхното разкриване и разследване;

– изграждане на специализирани звена в рамките на съдебната система и/или полицията;

– предвиждане на допълнителни мерки в гражданското законодателство за превенция на корупционно поведение и извършване на корупционни престъпления;

– ратифициране на международноправни актове относно корупцията.

2) Самостоятелно законодателно уреждане на противодействието и борбата с корупцията – Румъния, Полша, Казахстан. Този подход се отличава:

– със самостоятелен антикорупционен закон;

– с изграждане на отделна система от специализирани органи с разследващи и превантивни функции;

– липса на „дублиращи" функции с органи от правосъдната система;

– приемане на комплекс от закони, ограничаващи корупцията;

– присъединяване към единни международни стандарти и добри практики в борбата с корупцията;

Законодателната рамка в актовете на ЕС за противодействие и борбата с корупцията се отличава със следните особености:

1) Могат да се очертаят три групи актове:

– актове, пряко регулиращи обществените отношения във връзка с борбата с корупцията;

– актове, които имат препоръчително - рамкиращ характер по отношение необходимостта от въвеждане на определени правни институти в националните законодателства;

– актове, които имат смесен характер: въвеждат някои основни понятия и/или дават легални дефиниции относно корупцията и свързаните с нея последици и дават препоръки за изграждане на националното законодателство. Много от актовете на Европейския съюз дефинират понятията активна и пасивна корупция, измама, както и лицата, които могат да бъдат субекти на корупционни правонарушения. В някои от случаите тези актове са отворени и към държави, които не са членове на ЕС.

2) Съществуват тенденции към изграждане на единни международни стандарти за разкриване, разследване и доказване на корупционни престъпления;

3) Създава се система от нормативни актове, които не регламентират пряко противодействието на корупцията, но имат пряко отношение към изграждане на правила, свързани с регулиране на последиците от корупционни действия и поведение;

4) В структурно отношение повечето международни договори се отличават с типизирана структура, която обхваща: преамбюл, общи разпоредби, в които се дават някои определения, посочват се целите на акта и неговото приложно поле, мерките, които трябва да се осигурят на национално ниво, разпоредби относно международното сътрудничество, разпоредби, уреждащи влизането в сила, изменението и денонсирането на договорите;

5) Прокарва се идеята макар и плахо за създаване на единна система на наказателно правораздаване в рамките на ЕС. Една от стъпките е създаването на CORPUS JURIS, в който се предлага кодификация на наказателното правораздаване. Предвижда се:

- система от престъпления в която са обхванати престъпленията, извършвани от длъжностни лица, като на първо място е посочено престъплението корупция (чл. 5 от CORPUS JURIS);

– създаване на институциите на европейския прокурор и съдия по свободите;

– единна процедура за разглеждане на делата за предвидените в CORPUS JURIS престъпления.

Държавите-членки предприемат действия за борба с измамите и всяка незаконна дейност, засягаща финансовите интереси на Съюза. С цел повишаване ефективността на действията за борба с измамите и други незаконни дейности в ущърб на интересите на Общността на 28 април 1999 г. с Решение на Комисията 1999/352/ЕО е създадена ***Европейската служба за борба с измамите*** (***ОЛАФ***) и е приет Регламент (ЕО) № 1073/1999 на Европейския Парламент и на Съвета от 25 май 1999 година относно разследванията, провеждани от Европейската служба за борба с измамите. Службата е натоварена с отговорност за провеждане на административни разследвания, като средство за борба с измамите, и има специален статут на независим орган за разследване в рамките на Европейската комисия. ОЛАФ упражнява правомощията за разследване на Комисията в съответствие със законодателството на ЕС и влезлите в сила споразумения с трети страни. Европейската служба за борба с измамите провежда своята дейност в тясно взаимодействие с Координационните служби за борба с измамите – АФКОС на държавите-членки (Anti-Fraud Coordination Service – AFCOS), с които осъществява ефективно сътрудничество и обмен на информация, включително информация от оперативен характер, като по този начин осигурява в рамките на Съюза единодействие и координация на борбата с измамите и нередностите. Наред с посочените задължения в чл. 325 (1) от ДФЕС, в чл. 325 (2) се предвижда, държавите-членки да предприемат същите мерки за предотвратяване на измами, засягащи финансовите интереси на Съюза,

каквито биха предприели при предотвратяване на измами, засягащи собствените им финансови интереси.

С приемането на Хагската програма за укрепване на свободата, сигурността и правосъдието в ЕС през 2004 г. Съветът на ЕС определи противодействието и превенцията на организираната престъпност като приоритет в политиката на Общността. В плана за изпълнение на програмата и в Съобщението на Комисията до Съвета и Европейския парламент от 2 юни 2005 г. се предвижда разработването на стратегическа концепция за борба с организираната престъпност, основаваща се на проактивно събиране на информация и разузнавателни данни, превенция и сътрудничество между правоприлагащите и съдебните органи, трети страни и организации. Така се поставя началото на ***европейската оценка на заплахите от организираната престъпност*** (на англ. съкратено OCTA), изготвена за първи път в края на 2005 г. от Европол[7]. OCTA е документ, насочен към бъдещето, който поставя акцент върху качествената оценка на многоаспектния феномен организирана престъпност.

На 5 октомври 2010 г. Постоянният комитет за оперативно сътрудничество в областта на вътрешната сигурност (COSI) постигна съгласие за установяването на цикъл на политиката на ЕС за борба с организираната и тежката международна престъпност и набеляза отделните стъпки, необходими за пълното му прилагане. Заключенията на Съвета относно създаването и прилагането на ***цикъл на политиката на ЕС за борба с организираната и тежката международна престъпност*** бяха приети от Съвета на 8 ноември 2010 г.

Новият цикъл на политиката започна с представянето от Европол на 9 март 2017 г. на доклада EU SOCTA за 2017 г. В доклада се разглеждат потенциалните **връзки между тежката и организираната престъпност и тероризма**[8]. В EU SOCTA за 2017 г. се препоръчва вниманието да се съсредоточи върху петте приоритетни заплахи от престъпност: 1) **киберпрестъпност**, 2) **производство, трафик и разпространение на наркотици**, 3) **контрабанда на мигранти**, (4) **организирани обири и кражби** (организирана престъпност, засягаща собствеността) и 5) **трафик на хора**. В доклада се препоръчва също така да се разрешат три взаимосвързани проблема, които способстват или насърчават всички форми на тежката и организираната престъпност: а) документните измами, б), финансирането на престъпления, включително изпирането на пари, и в) онлайн търговията с незаконни стоки и услуги.

Въз основа на EU SOCTA за 2017 г. Комисията и председателството на Съвета са в процес на изготвяне на своите предложения за приоритетите на новия цикъл в политиката на ЕС за периода 2018-2021 г. за справяне с престъпността, които се обсъжда в рамките на Постоянния комитет за оперативно сътрудничество в областта на вътрешната сигурност и се одобрява през юни 2017 г. от Съвета по правосъдие и вътрешни работи.

В EU SOCTA за 2017 г. е подчертан следния ключов проблем, а именно **използването на нови технологии от престъпниците**. За почти всички видове организирана престъпност престъпниците разширяват обхвата на технологиите и ги приспособяват все по-умело и с все по-голямо въздействие. Използването на интернет за всички видове незаконна търговия със стоки и услуги се увеличи значително. Това налага правоприлагащите органи да бъдат оборудвани с подходящи средства за борба с този вид онлайн престъпност и да се обучават и учат заедно. Агенцията на Европейския съюз за обучение в областта на правоприлагането ще изиграе ключова роля при осигуряването на подходящо обучение за правоприлагащите служители на първа линия в съответствие с приоритетите на политиката и установените заплахи.

В EU SOCTA за 2017 г. се подчертава, че съществува и важно **външно измерение на тежката и организираната престъпност**. Хора от над 180 различни националности - пребиваващи в ЕС или извън него, участват в организирана престъпна дейност в рамките на ЕС. Около 40 % от заподозрените лица не са граждани на държавите членки. Основните пътища за трафик, свързани със заплахите от организираната престъпност, тръгват от държави извън ЕС. Работи се за преодоляване на заплахите от организираната престъпност във външен план[9]. Важно е да се отговори

[7] Оценка на заплахите от тежка организирана престъпност 2010г.-2011г., Център за изследване на демокрацията, София 2012 г., стр.10

8 COM(2016) 230 final, 20.4.2016 г.

9 Това включва проекти, финансирани от ЕС (например в Западните Балкани и региона Сахел), мисии по линия на общата политика за сигурност и отбрана (като например EUNAVFOR Med операция Sophia, която изрично е разработена така, че да се разруши също бизнес моделът на контрабандистите), както и мисиите за управление на границите в трети държави.

на заплахите от тежката и организираната престъпност, като се продължи осигуряването на връзки между вътрешната сигурност на ЕС и външната му дейност, включително чрез сътрудничество на Европол с трети държави.

Приоритетите за периода 2018–2021 г. на ЕС в борбата с тежката и организираната престъпност са:

1) киберпрестъпност;
2) производство, трафик и разпространение на наркотици;
3) контрабанда на мигранти;
4) организирана престъпност, засягаща собствеността;
5) трафик на хора;
6) трафик на огнестрелни оръжия;
7) трансгранични измами с ДДС;
8) престъпления против околната среда.

SOCTA се изготвя от Отдела по операции на Европол, който се основава на широк принос от външни партньори, включително държави-членки, трети държави и организации: Eurojust (Евроюст) и Frontex (Фронтекс)

Програмата за сигурност определя три приоритета за действия на ЕС, като се насочва към областите, в които съюзът би могъл да има значителен принос:

1) Тероризмът и радикализацията са значителни заплахи за вътрешната сигурност на ЕС;

2) Организираната престъпност има огромна човешка, социална и икономическа цена – в това число незаконното превеждане на хора през граница, трафика на хора, трафика на огнестрелни оръжия, наркотици, екологичните, финансовите и икономическите престъпления;

3) Киберпрестъпността предлага огромна потенциална печалба за престъпниците, тъй като животът ни, в това число търговията и банкирането, се преместват в онлайн пространството. Подобряването на ответните действия на правоприлагащите и съдебните органи спрямо киберпрестъпността е приоритет в Европейската програма за сигурност.

Международните организации за борба с корупцията и организираната престъпност са следните:

– **Организацията на обединените нации е международна организация,** основана през 1945 г., която е отговорна за поддържането на международния мир и сигурност; развиване на близките отношения между народите; насърчаване на социалния прогрес, по-добри стандарти на живот и права на човека;

– **Световната банка** е международна финансова институция, която предоставя заеми на развиващите се страни за капиталови програми. Тя се състои от две институции: *Международната банка за възстановяване и развитие* и *Международната асоциация за развитие*. Световната банка е компонент на Групата на Световната банка и е член на Групата за развитие на ООН. Официална цел на Световната банка е намаляването на бедността. Според нейните членове на споразумение, всички свои решения трябва да се ръководят от ангажимент за насърчаване на чуждестранните инвестиции, международната търговия и за улесняване на капиталовите инвестиции;

– **Международната академия за борба с корупцията (IACA)** е млада институция със седалище в Лаксенбург (Виена), Австрия. Тя има уникален двоен характер като международна организация и академия, създадена по силата на международното право. „IACA" се стреми да преодолее пропуските в знанията и практиката в областта на борбата с корупцията. Нейният избирателен район се състои от 68 държави-членки на ООН и 3 международни организации;

– **Групата на държавите, борещи се срещу корупцията (ГРЕКО) към Съвета на Европа** е антикорупционна мониторингова организация със седалище в Страсбург, Франция. Целта на организацията е да подобри капацитета на своите членове за борба с корупцията чрез мониторинг на спазването на стандартите на Съвета на Европа за борба с корупцията посредством динамичен процес на взаимно оценяване и партньорски натиск;

– **Организацията за сигурност и сътрудничество в Европа (ОССЕ)** е най-голямата световна междуправителствена организация в областта на сигурността, която включва всички стра-

ни от Европа, САЩ и Канада и ОНД. Мандатът ѝ включва контрол над въоръжаването и утвърждаване на човешките права, свободата на пресата и честните избори. Има персонал от 550 души в седалището си във Виена, Австрия и 2 300 души на други места. Началото и е поставено на Конференцията за сигурност и сътрудничество в Европа (CSCE), състояла се през 1975 г. в Хелзинки, Финландия. В нея участват 57 държави, покриващи повечето от Северното полукълбо;

– **Европейската служба за борба с корупцията (ОЛАФ)** е генерална дирекция в структурата на Европейската комисия, задължена от Европейския съюз със защитата на финансовите му интереси. Нейната задача е да се бори по отговорен, прозрачен и ефективен начин с финансовите измами, засягащи бюджета на Съюза, с корупцията, както и с други нередни дейности, включително с лошото управление на европейските институции;

– **Евроюст е агенция на Европейския съюз (ЕС),** занимаваща се с съдебно сътрудничество по наказателноправни въпроси. Седалището на Евроюст се намира в Хага, Холандия. Основана през 2002 г., тя е била създадена, за да се подобри работата с тежката трансгранична и организирана престъпност чрез стимулиране на следствени и прокурорски координации между агенциите на държавите-членки на ЕС;

– **Европейски партньори срещу корупцията (EPAC)** е независима, неформална мрежа, обединяваща повече от 60 антикорупционни власти и полицейски надзорни органи от Съвета на страните-членки в Европа. Те имат различни видове умения, компетенции и разнообразни правни форми. Европейската служба за борба с измамите (OLAF) също е член. EPAC предлага среда за обмяна на опит измежду партньорите, за откриването на нови възможности и сътрудничество отвъд националните граници в разработването на общи стратегии и високи професионални стандарти.

– **Европол** е правоохранителна организация на Европейския съюз със седалище в Хага, Холандия. Има за цел да координира дейността на полицейските служби на европейските държави в предотвратяването и борбата им с тежката международна организирана престъпност. Акценти в работата на Европол са борбата с тероризма, превенция на нелегалната търговия с оръжие, борба с наркотрафика, детската порнография и прането на пари;

– **Международната организация на криминалната полиция, широко известна като Интерпол**, координира международното сътрудничество на полицейските органи в различните страни в борбата с криминалната престъпност. Седалището на Интерпол се намира в Лион, Франция.

Изводи:

1) Корупцията вреди сериозно на икономиката и на обществото като цяло. Много държави по света страдат от дълбоко вкоренена корупция, която спъва икономическото развитие, разклаща основите на демокрацията и вреди на социалната справедливост и върховенството на закона. Държавите-членки на ЕС, не остават незасегнати от тази реалност. Корупцията е явление, което трудно може да бъде изкоренено. Необходимо е усилията да се насочат към ограничаване на това явление, да се приложат методи и техники, а така също и модели за противодействие на корупцията с оглед нейното ограничаване в общественото развитие на дадена страна.

2) Държавите-членки на ЕС, разполагат с необходимите правни инструменти и институции за превенция и борба с корупцията. Резултатите от тях обаче не са задоволителни навсякъде в ЕС. Антикорупционните разпоредби не винаги се прилагат убедително, не се предприемат достатъчно ефективни действия за решаване на всеобхватните проблеми, а компетентните институции не винаги разполагат с достатъчен капацитет да прилагат съответните разпоредби. Заявяването на намерения е все пак твърде далеч от постигането на конкретни резултати и често изглежда, че липсва истинска политическа воля за изкореняване на корупцията.

3) Борбата с корупцията в ЕС придобива все повече общностен характер предимно поради доказаната престъпна симбиоза между нея и организираната престъпност, както и поради разрушителното ѝ въздействие върху мерките, свързани с изграждането на пространството на свобода, сигурност и правосъдие. В приетите от ЕС програми и планове за действие за борба с организи-

раната престъпност, тероризма, измамата, прането на пари и други сериозни престъпления, има включен и специален раздел за борба с корупцията.

4) Оценката на заплахата от тежката и организираната престъпност от 2017 г. е добра основа за определяне на приоритетите на ЕС в борбата с престъпността за следващите четири години. Одобрени са следните осем заплахи от престъпност като приоритети в цикъла на политиката на ЕС за борба с организираната и тежката международна престъпност за периода 2018-2021 г.: киберпрестъпността, престъпността, свързана с наркотици, организираната престъпност, засягаща собствеността, трафика на хора, трафика на огнестрелни оръжия, измамите с ДДС и престъпленията против околната среда.

5) Създаването на законодателство за противодействие на корупцията и организираната престъпност е само първата стъпка от тяхното предотвратяване. Следващата и не по-малко важна дейност е свързана с приложението на съответното законодателство, защото, както е известно, дори и най-съвършеният закон е неефективен, ако не се прилага стриктно.

References:

1. Център за превенция и противодействие на корупцията и организираната престъпност, кратък доклад „Анализ на органите по превенция и противодействие на корупцията в Република България", София, април 2017 г.
2. Доклад относно борбата срещу корупцията и действия, произтичащи от резолюцията на специалната комисия по организираната престъпност, корупцията и изпирането на пари (2015/2110(INI)) Комисия по граждански свободи, правосъдие и вътрешни работи, Докладчик: Лаура Ферара, 7.10.2016, A8-0284/2016.
3. Резолюция на Европейския парламент от 25 октомври 2016 г. относно борбата срещу корупцията и действия, произтичащи от резолюцията на специалната комисия по организираната престъпност, корупцията и изпирането на пари (2015/2110(INI)), октомври 2016 г.
4. Доклад на Комисията до Съвета и до Европейския парламент от 3 февруари 2014 г., озаглавен „Доклад на ЕС за борбата с корупцията" COM(2014)0038
5. Резолюция на Европейския парламент от 23 октомври 2013 г. относно организираната престъпност, корупцията и изпирането на пари: препоръки относно действията и инициативите, които следва да бъдат предприети (окончателен доклад) (2013/2107(INI)), октомври 2013 г.
6. Любомир Авджийски, Антикорупционната политика на България, Институт за пазарна икономика, април 2016, avdjiiski@ime.bg
7. Работен документ относно организираната престъпност, Специална комисия по организираната престъпност, корупцията и изпирането на пари, Докладчик: Salvatore Iacolino, 1.10.2012,
8. Велико П. Петров, Международно правно сътрудничество между страните от Европейския съюз за противодействие на корупционните престъпления, Научна конференция 2012 „Защитата на информацията – състояние и перспективи", Сб. научни трудове на факултет „А, ПВО и КИС" при НВУ„В. Левски", Шумен, 2012 г., ISBN 978-954-9681-49-9
9. Венета Кокалова, Европейско сътрудничество за борба срещу организираната престъпност, 2009 г.
10. Лидия Ст. Велкова, Корупцията – заплаха за икономическата сигурност, 2015 г., Издателство „Дио Мира", ISBN 978-954-2977-22-3
11. Велико П. Петров, Възникване и развитие на трансграничната организирана престъпност в света, Международна научна конференция „Отбранителни технологии" Шумен, България 2017, Издателски комплекс на НВУ „В. Левски" – факултет „А, ПВО и КИС", Шумен, България 2017, ISSN 2367-7902
12. Велико П. Петров, Цикъл на политиката на европейския съюз за борба с организираната и тежката международна престъпност, Международна научна конференция „Отбранителни технологии" Шумен, България 2017, Издателски комплекс на НВУ „В. Левски" – факултет „А, ПВО и КИС", Шумен, България 2017, ISSN 2367-7902

13. Предложение за Директива на Европейския парламент и на Съвета за обезпечаване и конфискация на облаги от престъпна дейност в Европейския съюз, Брюксел, 12.3.2012 г., COM(2012) 85 final, 2012/0036 (COD)

14. Резюме на законодателно проучване на тема: „Законодателен опит и нормативна база относно статута на институции и органи за борба с корупцията в страни от ЕС”, 2007 г.

15. Павлина Панова,. Ралица Илкова, Корупционни престъпления. София, Сиби, 2006 г.

16. Оценка на заплахите от тежка организирана престъпност 2010г.-2011г., Център за изследване на демокрацията, София 2012 г.

17. Доклад относно организираната престъпност в Европейския съюз, (2010/2309(INI)), Комисия по граждански свободи, правосъдие и вътрешни работи, (A7-0333/2011), Европейски парламент 6.10.2011 г.

18. Проучване за оценка на цикъла на политиката на ЕС за борба с организираната и тежката международна престъпност за периода 2013-2017 г., окончателен доклад, 30.1.2017 г.

19. Заключения на Съвета за определяне на приоритетите на ЕС в борбата срещу тежката и организираната престъпност за периода 2014–2017 г. (док. 12095/13)

20. Конвенция на ООН срещу корупцията, приета с резолюция 58/4 на Генералната асамбея от 31 октомври 2003 г. Ратифицирана със закон, приет от 40-то Народно събрание на 03.08.2006 г., ДВ, бр. 66 от 15.11.2006 г. Издадена от Министерството на правосъдието, обн., ДВ, бр. 89 от 3.11.2006 г., в сила за Република България от 20.10.2006 г.

COMBATING CONTRABANDA AND THE UNLAWFUL TRADE WITH WEAPONS IN THE EUROPEAN UNION

Veliko P. Petrov

National Military University "Vasil Levski", Faculty of Artillery, Air Defense and Communications and Information Systems, Department of Information Security; town of Shumen.

Abstract: *This report aims to familiarize readers with the challenge that affects not only Europe but also undoubtedly affects the whole world, namely the problem of illicit proliferation of weapons. In the age of globalization, it is irrational for EU countries to have so many different laws that allow the development of such dangerous criminal activity. The proliferation of small arms and light weapons is through a well organized network that reaches all over the world. In addressing this important issue of EU security, it is necessary to fight effectively this extremely dangerous criminal activity. These illegal activities are fueling insecurity in Europe and its neighboring regions, as well as in many other regions of the world, exacerbating conflicts and undermining the post-conflict reconstruction and thus posing a serious threat to peace and security in Europe. Increasing effectiveness in combating illicit arms trafficking requires EU Member States and supranational organizations in Europe to take effective measures in the short and longer term. It is important to improve the co-operation between states and organizations that fight organized crime and illicit arms trafficking.*

Keywords: *illicit proliferation of weapons, illicit proliferation of weapons, illicit arms trafficking.*

БОРБАТА С КОНТРАБАНДАТА И НЕЗАКОННАТА ТЪРГОВИЯ С ОРЪЖИЕ В ЕВРОПЕЙСКИЯ СЪЮЗ

Велико П. Петров

Незаконните огнестрелни оръжия, малки оръжия и леки въоръжения (МОЛВ) продължават да допринасят за нестабилността и насилието в Европейския съюз (ЕС), в непосредственото му съседство и в останалата част от света. Незаконните оръжия подхранват световния тероризъм и световните конфликти, като възпрепятстват развитието, управлението на кризи, хуманитарните усилия и усилията за стабилизация на ЕС в части от съседните на ЕС държави и в Африка. В рамките на ЕС незаконните огнестрелни оръжия оказват очевидно въздействие върху вътрешната сигурност, като подхранват организираната престъпност и осигуряват на терористите средства за извършване на нападения на европейска територия[10].

Проблемът с незаконното разпространение на оръжия засяга не само Европа, но и несъмнено засяга целия свят. В епохата на глобализацията е безрасъдно държавите от ЕС да останат с толкова различни законодателства, позволяващи развитието на такава опасна престъпна дейност. Разпространението на малките оръжия и лекото въоръжение се извършва чрез добре организирана мрежа, която достига всички краища на света. При решаването на този важен въпрос за сигурността на ЕС е необходимо да се води ефективна борба с тази изключително опасна престъпна дейност.

10 Съвместно съобщение до Европейския парламент и Съвета, Елементи за стратегия на ЕС срещу незаконните огнестрелни оръжия, малки оръжия и леки въоръжения и боеприпаси за тях, „Гарантиране на сигурността на оръжията и защитата на гражданите", Брюксел, 13.6.2018 г., JOIN(2018) 17 final, стр.3.

Незаконното производство, трансфер и движение на конвенционално оръжие, включително МОЛВ, както и прекаленото им натрупване и безконтролно разпространение, са в основата на това предизвикателство за Европа. Тези незаконни дейности подклаждат несигурност в Европа и съседните ѝ региони, както и в много други региони по света, като изострят конфликтите и подкопават възстановяването на мира след приключването на конфликта и по този начин създават сериозна заплаха за мира и сигурността в Европа. Новите предизвикателства пред сигурността в XXI-ви век включват контрабандата като част от организираната престъпност. Контрабандата е заплаха вътре в съюза, но е значителна опасността от разпространението ѝ към Европа от външни източници.

С понятието „контрабанда”[11] се обозначава всяко внасяне в страната или изнасяне на стоки в нарушение на местното законодателство. Контрабандата има международен характер, тя предполага нарушаване на митническия режим с пренасянето или превозването на стоки от една в друга страна през границите им. Контрабанда се извършва, за да се избегне заплащането на дължимите мита, данъци и такси, с цел да се постигнат финансови и търговски изгоди, като се избегне митническият, данъчният, полицейският и друг вид контрол и процедурите, свързани с регистрационни, разрешителни и лицензионни режими, заобикаляне на ограничения, свързани с вноса или износа на стоки и т.н.

„Незаконен трафик“ означава вносът, износът, продажбата, доставката, движението или преместването на огнестрелни оръжия, техни части и основни компоненти и боеприпаси от или през територията на една държава-членка към територията на трета държава, ако е изпълнено някое от следните условия:

а) заинтересованата държава-членка не е дала разрешение за това в съответствие с разпоредбите на настоящия регламент;

б) огнестрелните оръжия нямат маркировка съгласно член 4, параграфи 1 и 2 от Директива 91/477/ЕИО;

в) към момента на вноса внесените огнестрелни оръжия нямат дори просто маркиране, което позволява да се установи първата държава на внос в рамките на Европейския съюз, или ако огнестрелните оръжия нямат такова маркиране – уеднаквена маркировка, с която се идентифицират внесените огнестрелни оръжия[12].

Основна стъпка за превенция на контрабандата е изграждането на ефективно действаща система за информация и мрежи за разпространение, механизми за вътрешен контрол и достатъчна материално-техническа обезпеченост на физическите и юридическите лица.

Законодателството на Европейския съюз за износ на огнестрелни оръжия, техните части и компоненти и боеприпаси обхваща:

- Регламент (ЕС) № 258/2012 на Европейския парламент и на Съвета от 14 март 2012 година за изпълнение на член 10 от Протокола на Организацията на обединените нации срещу незаконното производство и трафика с огнестрелни оръжия, техните части и компоненти и боеприпаси, допълващ Конвенцията на Организацията на обединените нации срещу транснационалната организирана престъпност ("Протокол за огнестрелните оръжия"), и за установяване на разрешения за износа и мерки за вноса и транзита на огнестрелни оръжия, техни части и компоненти и боеприпаси;
- На национално ниво в Р. България се прилагат разпоредбите на:

– Закон за оръжията, боеприпасите, взривните вещества и пиротехническите изделия[13];

– Компетентен орган – Министерство на вътрешните работи.

Незаконните огнестрелни оръжия улесняват трафика на наркотици и на хора чрез сплашване и принуда, подклаждат конфликти за разпределяне на територии между градските банди и дават мощ на терористите. Терористичните нападения в Европа нагледно показаха връзката меж-

11 „Корупция и контрабанда: мониторинг и превенция. Методи за оценка и модели на противодействие на трансграничната престъпност в България. Второ преработено и допълнено издание”; Център за изследване на демокрацията, С., 2000 г.

12 Регламент (ЕС) № 258/2012 на Европейския парламент и на Съвета, от 14 март 2012 година, за изпълнение на член 10 от Протокола на Организацията на обединените нации срещу незаконното производство и трафика с огнестрелни оръжия, техните части и компоненти и боеприпаси, допълващ Конвенцията на Организацията на обединените нации срещу транснационалната организирана престъпност („Протокол за огнестрелните оръжия“), и за установяване на разрешения за износа и мерки за вноса и транзита на огнестрелни оръжия, техни части и компоненти и боеприпаси

13 Закон за оръжията, боеприпасите, взривните вещества и пиротехническите изделия, в сила от 17.09.2010 г., Обн. ДВ. бр.73 от 17 Септември 2010г., посл. изм. и доп. ДВ. бр.20 от 6 Март 2018 г.

ду организираната престъпност и тероризма, по-специално що се отнася до трафика на огнестрелни оръжия, и са ясен показател за една многоизмерна заплаха, обхващаща различни области на престъпността. В оценката на заплахата от тежката и организираната престъпност (SOCTA) на Европол от 2017 г. се отбелязва, че неотдавнашните терористични нападения както в ЕС, така и на други места по света, извършени от терористи джихадисти с огнестрелни оръжия, придобити в резултат на трафик, доказват смъртоносните последици от тази незаконна търговия[14].

През 2005 г. Европейският съвет прие Стратегия на ЕС за борба с незаконното натрупване и трафика на МОЛВ и боеприпаси за тях[15] в подкрепа на Програмата за действие на ООН за предотвратяване, борба и ликвидиране на незаконната търговия с малки оръжия и леки въоръжения във всичките ѝ аспекти, приета на 20 юли 2001 г. Целта на стратегията е да осигурява план за действие за борба със заплахите, свързани с незаконното натрупване и трафика на малки оръжия и леки въоръжения и боеприпаси за тях, като се използва широкият набор от механизми, налични за ЕС. Основните аспекти в стратегията са следните:

• Стратегията за МОЛВ обединява гражданските и военните възможности на държавите от ЕС, инструментите на общата външна политика и политика за сигурност (ОВППС) и на общата политика за сигурност и отбрана (ОПСО), както и на полицията, митниците и съдебните производства в рамките на ЕС за постигането на своите цели.

• Необходимо е ефективно многостранно сътрудничество за разработване на международни, регионални и национални механизми.

• На международно равнище се дава приоритет на:

– реализирането на програмата за действие на ООН относно МОЛВ;

– проследяването на МОЛВ чрез глобален механизъм за докладване (iTrace II);

– ратифицирането на Протокола срещу незаконното производство и трафика на огнестрелни оръжия.

• ЕС насърчава активно държавите извън ЕС, които са износители на МОЛВ, да спазват горепосоченото.

• На регионално равнище ЕС предоставя финансова подкрепа за конкретни програми, насочени към справяне със заплахите за сигурността, свързани с незаконните МОЛВ, в Либия, Югоизточна Европа и Организацията за сигурност и сътрудничество в Европа.

• Стратегията се допълва от Инструмента, допринасящ за стабилността и мира, който помага за предотвратяването и реагирането на кризи, и за създаване на безопасна и стабилна среда в целия свят.

• Съветът на ЕС непрекъснато наблюдава реализирането на Стратегията на ЕС за МОЛВ. На всеки 6 месеца Европейската служба за външна дейност представя доклад за напредъка на Съвета за одобрение.

В ***Европейската програма за сигурност***[16]**,** приета на 28 април 2015 г от Комисията незаконният трафик на огнестрелни оръжия се определя като един от приоритетите в рамките на всеобхватната цел за осуетяване на дейностите на терористите и организираните групи, извършващи тежки престъпления. Европейската комисия прие пакет от мерки за засилване на борбата с тероризма и незаконния трафик на огнестрелни оръжия и взривни вещества. Пакетът включва два основни елемента: *предложение за директива относно тероризма*, с която ще бъдат усъвършенствани средствата на ЕС за предотвратяване на терористични нападения, като се криминализират подготвителните действия, а именно обучаването и пътуването в чужбина за терористични цели, както и подпомагането или подбуждането и опитите за извършване на терористични актове; *план за действие за засилване на борбата срещу престъпници и терористи*, които си набавят и използват оръжия и взривни вещества, чрез повече контрол на незаконното притежаване и вноса в ЕС.

14 Съвместно съобщение до Европейския парламент и Съвета, Елементи за стратегия на ЕС срещу незаконните огнестрелни оръжия, малки оръжия и леки въоръжения и боеприпаси за тях, „Гарантиране на сигурността на оръжията и защитата на гражданите", Брюксел, 13.6.2018 г., JOIN(2018) 17 final, стр.3.

15 Съвет, 5319/06 http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%205319%202006%20INIT

16 „Европейска програма за сигурност", съобщение на Комисията до Европейския парламент и Съвета (COM(2015) 185 final, 28.4.2015 г.).

Програмата бе последвана от ***План за действие на ЕС относно незаконния трафик и използване на огнестрелни оръжия и взривни вещества***[17] и от преразгледана регулаторна рамка на Съюза относно законното придобиване и притежаване на огнестрелни оръжия[18].

Целта на *Плана за действие за борба с незаконния трафик на огнестрелно оръжие и използването на взривни вещества*[19] е да се подобри разкриването, разследването и изземването на огнестрелни оръжия, взривни вещества и прекурсори на взривни вещества, които ще се използват за престъпни и терористични цели.

Планът за действие допълва мерките, приети на 18 ноември 2015 г., чиято цел е да се затегне контролът върху законното придобиване и притежаване на огнестрелни оръжия и да се прилагат общи минимални стандарти за деактивирането на огнестрелни оръжия. Целта на плана за действие е да се подобри оперативното сътрудничество на равнище ЕС и с трети страни, за да може борбата с черния пазар на оръжия и взривни вещества да бъде по-ефективна. Неговите основни елементи са:

- ***ограничаването на достъпа до незаконни огнестрелни оръжия и взривни вещества***: планът за действие приканва всички държави-членки да създадат взаимосвързани *национални координационни центрове* за огнестрелните оръжия с цел развиване на експертни умения и подобряване на анализа и стратегическите доклади относно незаконния трафик на огнестрелни оръжия, по-конкретно чрез комбинираното използване на балистични данни и криминална разузнавателна информация. Той също така предвижда засилване на ролята на *Европол* по отношение на онлайн трафика и отклоняването от законна търговия чрез наскоро създаденото звено за сигнализиране за незаконно съдържание в интернет (*EUIRU*). С плана за действие държавите-членки се приканват да прилагат изцяло правилата на ЕС относно прекурсорите за взривни вещества;
- ***засилването на оперативното сътрудничество***: планът за действие призовава държавите-членки да създадат или да разширят съществуващите *киберпатрули*, за да обхванат също огнестрелните оръжия, взривните вещества и прекурсорите на взривни вещества; *Контролът по външните граници*, както и полицейското и митническото сътрудничество следва да бъдат засилени чрез основан на риска контрол на стоките, пристигащи в рамките на търговския трафик (напр. контейнери), пътническия транспорт (напр. автомобили) или в багажа на пътниците. Планът за действие също така предлага да се изготвят заедно с държавите членки *приоритетни действия за митнически контрол* на незаконния трафик на огнестрелни оръжия по външните граници на ЕС;
- ***подобряването на събирането и обмена на оперативна информация***: планът за действие призовава държавите членки да *използват в пълна степен съществуващите инструменти, за да се улесни обменът на информация*, както и системно да включват информация относно търсени огнестрелни оръжия в Шенгенската информационна система и в iARMS на Европол, когато е налична такава. *Обменът на балистична информация* следва да се улесни чрез специфична платформа;
- ***засиленото сътрудничество с трети страни:*** с цел да се намали незаконният внос на огнестрелни оръжия и достъпът до взривни вещества в Европейския съюз, в плана за действие се предлага да бъде засилено сътрудничеството с трети страни чрез системно включване на въпроси, свързани с трафика на огнестрелни оръжия и използването на взривни вещества, в диалозите в областта на сигурността с ключови партньорски държави и организации. В допълнение към засилването на сътрудничеството с ключови държави от Западните Балкани, Европейската комисия предлага да се подобри сътрудничеството с държави в Близкия изток и Северна Африка, както и с Турция и Украйна. По-специално внимание се отделя на установяването на диалог със страните от региона на Сахел, с Арабската лига и с международни организации. В някои случаи може да се

17 „Изпълнение на Европейската програма за сигурност: план за действие на ЕС относно незаконния трафик и използване на огнестрелни оръжия и взривни вещества", съобщение на Комисията до Европейския парламент и Съвета (COM(2015) 624 final, 2.12.2015 г.).

18 Директива 91/477/ЕИО относно контрола на придобиването и притежаването на оръжие (OB L 256, 13.9.1991 г., стр. 51) и Регламент (ЕС) № 258/2012 на Европейския парламент и на Съвета от 14 март 2012 г. за изпълнение на член 10 от Протокола на ООН срещу незаконното производство и трафика с огнестрелни оръжия, техните части и компоненти и боеприпаси, допълващ Конвенцията на Организацията на обединените нации срещу транснационалната организирана престъпност („Протокол за огнестрелните оръжия"), и за установяване на разрешения за износа и мерки за вноса и транзита на огнестрелни оръжия, техни части и компоненти и боеприпаси (OB L 94, 30.3.2012 г., стр. 1).

19 Съобщение на комисията до Европейския парламент и Съвета, Изпълнение на Европейската програма за сигурност: план за действие на ЕС относно незаконния трафик и използване на огнестрелни оръжия и взривни вещества, Брюксел, 2.12.2015 г. COM(2015) 624 final, Annex 1.

предвиди финансова помощ от ЕС по отношение на конфискацията и извеждането от употреба на огнестрелни оръжия.

На 18 ноември 2015 г., след нападенията в Париж, Комисията прие Регламент за изпълнение относно общите минимални стандарти за **дезактивиране на огнестрелни оръжия**[20]. Регламентът за изпълнение влезе в сила на 8 април 2016 г. и в него се предвижда дезактивираните огнестрелни оръжия да бъдат привеждани в състояние на необратима нефункционалност. През септември 2016 г. беше проведено заседание на комитета, отговарящ за изпълнението на мерките за дезактивиране на огнестрелни оръжия, за да се прецени дали са необходими по-нататъшни изменения на стандартите за дезактивиране. Комисията също така представи предложение за преразглеждане на **Директивата за огнестрелните оръжия** (Директива 477/91) с цел ограничаване на достъпа до най-опасните категории огнестрелни оръжия за гражданска употреба[21].

Европейският парламент гласува на пленарно заседание на 14 март 2017 г. за одобряване на преразглеждането на ***Директивата за огнестрелните оръжия***. Представеното предложение разширява значително обхвата на забранените оръжия (категория А), като най-опасните оръжия се забраняват за употреба от цивилното население. С него също така в приложното поле на директивата се включват акустичните и дезактивираните оръжия и се подобрява проследимостта на оръжията чрез усъвършенствани правила за обозначаване и обмен на информация между държавите членки. Очаква се Съветът да даде окончателното си съгласие по предложението на 25 април. Държавите членки ще разполагат с 15 месеца, за да транспонират новите правила в националното си законодателство и с 30 месеца, за да въведат системи за архивиране на данни, така че да се регистрира цялата информация, необходима за проследяването и идентифицирането на огнестрелните оръжия[22].

За да се активизират на международно равнище предотвратяването на незаконната търговия с МОЛВ, борбата с нея и нейното ликвидиране, със *съвместно съобщение на Комисията и на върховния представител на Съюза по въпросите на външните работи и политиката на сигурност*[23] от 13.6.2018 г. се представят елементи за ***преразгледана стратегия относно МОЛВ***, като се вземат под внимание променящият се контекст на сигурността, ръководните принципи от Глобалната стратегия на ЕС от 2016 г., развитията в областта на контрола на конвенционалните оръжия (например влизането в сила през декември 2014 г. на Договора за търговия с оръжие (ДТО) и действията в рамките на ЕС за изпълнение на Европейската програма за сигурност от 2015 г., с цел да се напредне към постигането на истински и ефективен Съюз на сигурност. В това съобщение терминът „*МОЛВ*" се използва конкретно за оръжия за военни цели, а използваният термин „*огнестрелни оръжия*" изрично включва оръжията за граждански цели.

С преразгледаната стратегия относно МОЛВ се цели воденето на интегрирани, колективни и координирани европейски действия за предотвратяване и ограничаване на незаконните МОЛВ и боеприпасите за тях, извършвана от терористи, престъпници и други неоправомощени лица, и за насърчаване на отчетността и отговорността, що се отнася до законната търговия с оръжия.

За намаляване на заплахата от незаконно разпространение и трафик на МОЛВ и боеприпаси за тях в Европа са набелязани следните конкретни цели:

– засилено регионално сътрудничество, обмен на знание и споделяне на информация, водещи до повишаване на капацитета за основано на факти създаване на политики;

– подобрен капацитет за физическа сигурност и управление на запасите посредством подобрения на инфраструктурата в областта на сигурността, намаляване на излишъка и обучение;

– повишен капацитет за маркиране, проследяване и поддържане на регистри;

– намаляване на незаконното притежаване на огнестрелни оръжия и злоупотребата с тях посредством подкрепа за кампаниите за повишаване на осведомеността и за събиране.

20 Регламент за изпълнение (ЕС) 2015/2403 на Комисията от 15 декември 2015 г. за определяне на общи насоки относно стандартите и методите за дезактивиране с цел осигуряване на гаранции, че дезактивираните огнестрелни оръжия са приведени в състояние на необратима нефункционалност.

21 Предложение за директива на Европейския парламент и на Съвета за изменение на Директива 91/477/ЕИО на Съвета относно контрола на придобиването и притежаването на оръжие.

22 Доклад на комисията до Европейския парламент, Европейския съвет и съвета, Шести доклад за напредъка по създаването на ефективен и истински Съюз на сигурност Брюксел, 12.4.2017 г., COM(2017) 213 final

23 Съвместно съобщение до Европейския парламент и Съвета, Елементи за стратегия на ЕС срещу незаконните огнестрелни оръжия, малки оръжия и леки въоръжения и боеприпаси за тях, „Гарантиране на сигурността на оръжията и защитата на гражданите", Брюксел, 13.6.2018 г., JOIN(2018) 17 final, стр.4.

По данни на Стокхолмския международен институт за изследване на проблемите на мира[24] през 2017 г. имаше тридесет и пет случая на действащо многостранно ембарго върху оръжията: 13 оръжейни забрани са наложени от ООН, 21 – от Европейския съюз (ЕС) и 1 – от Лигата на арабските държави. 9 от 21 оръжейни забрани на ЕС имат пряко съответствие с оръжейно ембарго на ООН, 3 са сходни със забрани, наложени от ООН, като се различават по географски обхват или по видовете обхванато оръжие, и 9 нямат съответствие с наложени от ООН забрани. Повечето от тези оръжейни забрани обхващат само конвенционални оръжия. Но забраните на ООН и ЕС върху Иран и Северна Корея, и ембаргото на ЕС върху Русия обхващат също и експорт на изделия с двойна употреба. През 2017 г. беше наложено едно ново многостранно оръжейно ембарго: ембаргото на ЕС върху Венецуела. Както и в предишни години, разследването на ООН разкри проблеми в прилагането на наложените от нея забрани, с множество докладвани случаи на нарушения. Обхватът и значимостта на тези нарушения варират значително, като някои включват големи пратки от оръжие в разрез с ембаргото, а други – неотправяне на уведомление за трансфера до комитета по санкциите от страна на държавата-доставчик или получател.

Изводи:

1. Въпреки съществуващото законодателство на равнище ЕС, огнестрелните оръжия, взривните вещества и прекурсорите на взривни вещества са все още твърде лесно достъпни. Необходим е всеобхватен подход в подкрепа на разбиването на незаконния трафик и използване на огнестрелни оръжия и взривни вещества, като същевременно се действа в защита на законната търговия с огнестрелни оръжия и законното използване на химически вещества.

2. От страна на държавните агенции и участниците на национално, регионално и световно равнище е необходимо да се определят норми и правила, изпълнение, правоприлагане и комуникация за ефективното противодействие на незаконното производство, отклоняване, търговия и трафик с *огнестрелни оръжия/МОЛВ* и боеприпаси. То налага предприемането на действия на всички етапи от жизнения цикъл на огнестрелните оръжия/МОЛВ и боеприпасите: производство, износ, складиране и обезвреждане.

3. Съществуващата нормативна уредба в ЕС изразява безспорната готовност на съюза да се справи с незаконния трафик на оръжия, но все още има разминаване между желание и възможност, т.е. целите, които си поставя общността са действително големи и оправдани, а инструментите, с които тя разполага са силно ограничени. Повишаването на ефективността при борбата с незаконния трафик на оръжия изисква държавите-членки на ЕС и наднационалните организации в Европа да вземат ефективни мерки в краткосрочен и в по-дългосрочен план. Важно е да се подобри съвместната работа между държавите и организациите, които се борят с организираната престъпност и нелегалният трафик на оръжия.

4. Със съвместното съобщение до Европейския парламент и Съвета от 13.6.2018 г. се представят елементи за общо разбиране и общи бъдещи стъпки на ЕС във връзка с начините за справяне със заплахата от незаконни огнестрелни оръжия, МОЛВ и боеприпасите за тях, набор от действия, които ЕС и неговите държави членки да предприемат на територията на Съюза, както и предложения за сътрудничество и помощ с цел контрол на МОЛВ в съседните на ЕС държави и в останалата част от света.

References:

1. Стратегия на ЕС за борба с незаконното натрупване и трафика на МОЛВ и боеприпаси за тях, Съвет на Европейския съюз, Брюксел, 13 януари 2006 година, Съвет, 5319/06 http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%205319% 202006%20INIT

2. Регламент (ЕС) № 230/2014 на Европейския парламент и на Съвета от 11 март 2014 година за създаване на Инструмент, допринасящ за стабилността и мира, ОВ L 77, 15.3.2014 г., стр. 1-10.

24 Годишникът на СИПРИ за 2018 г. (Стокхолмски международен институт за изследване на проблемите на мира), Въоръжаване, разоръжаване и международна сигурност, стр. 16, ISBN 978-0-19-186088-1, *www.sipriyearbook.org*.

3. „Корупция и контрабанда: мониторинг и превенция. Методи за оценка и модели на противодействие на трансграничната престъпност в България. Второ преработено и допълнено издание”; Център за изследване на демокрацията, С., 2000 г.

4. Съобщение на комисията до Европейския парламент и Съвета, Изпълнение на Европейската програма за сигурност: план за действие на ЕС относно незаконния трафик и използване на огнестрелни оръжия и взривни вещества, Брюксел, 2.12.2015 г. COM(2015) 624 final, Annex 1.

5. Доклад на комисията до Европейския парламент, Европейския съвет и съвета, Шести доклад за напредъка по създаването на ефективен и истински Съюз на сигурност Брюксел, 12.4.2017 г., COM(2017) 213 final

6. Решение (ОВППС) 2015/1908 на Съвета от 22 октомври 2015 година в подкрепа на глобален механизъм за докладване относно незаконни малки оръжия и леки въоръжения и други незаконни конвенционални оръжия и боеприпаси с цел намаляване на риска от незаконна търговия с тях („iTrace II“), OB L 278, 23.10.2015 г., стр. 15-25.

7. Годишникът на СИПРИ за 2018 г. (Стокхолмски международен институт за изследване на проблемите на мира), Въоръжаване, разоръжаване и международна сигурност, ISBN 978-0-19-186088-1, www.sipriyearbook.org.

8. Съвместно съобщение до Европейския парламент и Съвета, Елементи за стратегия на ЕС срещу незаконните огнестрелни оръжия, малки оръжия и леки въоръжения и боеприпаси за тях, „Гарантиране на сигурността на оръжията и защитата на гражданите“, Брюксел, 13.6.2018 г., JOIN(2018) 17 final

9. „Европейска програма за сигурност“, съобщение на Комисията до Европейския парламент и Съвета (COM(2015) 185 final, 28.4.2015 г.).

10. Велико П. Петров, „Контрабандата и незаконната търговия с оръжие”, Научна конференция 2014 „Новата парадигма за сигурност в киберпространството”, Сб. научни трудове на факултет „А, ПВО и КИС” при НВУ„В. Левски”, Шумен, 2014 г., ISBN 978-954-9681-49-9

11. „Изпълнение на Европейската програма за сигурност: план за действие на ЕС относно незаконния трафик и използване на огнестрелни оръжия и взривни вещества“, съобщение на Комисията до Европейския парламент и Съвета (COM(2015) 624 final, 2.12.2015 г.).

12. Регламент (ЕС) № 258/2012 на Европейския парламент и на Съвета, от 14 март 2012 година, за изпълнение на член 10 от Протокола на Организацията на обединените нации срещу незаконното производство и трафика с огнестрелни оръжия, техните части и компоненти и боеприпаси, допълващ Конвенцията на Организацията на обединените нации срещу транснационалната организирана престъпност („Протокол за огнестрелните оръжия“), и за установяване на разрешения за износа и мерки за вноса и транзита на огнестрелни оръжия, техни части и компоненти и боеприпаси

13. Закон за оръжията, боеприпасите, взривните вещества и пиротехническите изделия, в сила от 17.09.2010 г., Обн. ДВ. бр.73 от 17 Септември 2010 г., посл. изм. и доп. ДВ. бр.20 от 6 Март 2018 г.

Zh. St. Yordanov,

INTERACTION BETWEEN THE ARMED FORCES AND THE INSTITUTIONS FOR THE PROTECTION OF SECURITY IN THE LITTORAL AREA

Zhivko St. Yordanov

***Abstract**: Security environment analysis present the increasing number of crimes, migratory pressure to the border as well as the worldwide terrorism increased threat for internal security. That is why it requires interaction between different institutions for the protection of internal security, including the Armed Forces of the country. National Maritime Spaces and Littoral zone are border areas through which various threats can penetrate. It is therefore necessary to impose national sovereignty and protect the law order in these areas.*

***Keywords:** National security, Interior security, Defense, Interaction, Military operation, Police operation, Joint operations, Law Enforcement, Guard, Protection; Littoral, Maritime operations, Security environmen;*

ВЗАИМОДЕЙСТВИЕ МЕЖДУ ВЪОРЪЖЕНИТЕ СИЛИ И ИНСТИТУЦИИТЕ ПРИ ЗАЩИТА НА СИГУРНОСТТА В ЛИТОРАЛНАТА ЗОНА

Живко С. Йорданов

Военно формирование 32300 - Варна
Телефон: 56080, GSM: +359887881809 и +359895456954

Анализът на средата за сигурност, направен в Доклада за състоянието на националната сигурност на Република България през 2016 г., представен от Министерски съвет пред Парламента през 2017г., става ясно, че нарастващия брой престъпления, миграционния натиск на границата, световния тероризъм и нарастващата радикализация, увеличават заплахата за вътрешната сигурност на страната. Тази заплаха може да прерасне в състояние на криза, за чието овладяване е необходимо намесата на различни институции, които да действат в изключително кратки срокове при максимално напрежение на силите за нейното овладяване. С нарастването на взаимозависимостта между държавите и глобализационните процеси в съвременния свят вътрешната несигурност не остава затворена в рамките на обществото, а е възможно да прерасне в регионална несигурност и логично да достигне до глобална криза. [2] Това налага необходимостта за участие на Въоръжените сили в защитата на вътрешната сигурност на страната.

Гореизброените заплахи за вътрешната сигурност могат да възникнат както в пределите на Република България така и да проникнат от чужди страни за което спомагат различни фактори като замразените конфликти в Черноморския регион, продължаващите войни и високата нестабилност в Близкия изток и северна Африка [19]. Държавната граница, националните морски пространства и крайбрежната зона са входни точки, през които различните заплахите и влияещите върху тях фактори могат да проникнат в страната и да окажат значително влияние върху нейната вътрешна среда за сигурност. Ето защо е необходимо да бъде защитен националния суверенитет в граничните райони на страната, в това число националните морски пространства и крайбрежието на Република България, като се гарантират основните права и свободи на гражданите и законно уста-

новения в страната правов ред. Според Закона за управление на черноморското крайбрежие то обхваща територия от страната до 2 км. от плажовете или бреговата линия и акваторията на Черно море с ширина 200 м. измерена от бреговата линия, както и всички острови намиращи се във вътрешните морски води и териториалното море. Това легално определение за „крайбрежие" не може да се приложи за целите на националната сигурност, защото ако една заплаха бъде открита на 200 м. или на 2 км. от пристанищата, стратегически обект, или от друг обект от критичната инфраструктура то тази заплаха ще се реализира за изключително кратко време, поради което силите за сигурност няма да имат време за реакция, а ще могат единствено да отстранят последствията от реализираната заплаха. Ето защо за целите на защитата на националната сигурност е необходимо или понятието „крайбрежие" да бъде допълнено, или да се дефинира пространство, чиито измерения да позволяват своевременно откриване на заплахите, ранно предупреждение и осигуряване на достатъчно време за организиране и развръщане на силите за сигурност, които да противодействат на възникналата заплаха.

През 1992г. Департамента на флота на САЩ издава публикацията «From The Sea: Preparing the Naval Service for the 21st Century», в която отчитайки новите реалности и променената среда за сигурност в световен мащаб обръща особено внимание на факта, че за защита на сигурността на страната стратегията на флота ориентирана към сражения и операции в откритие океан трябва да се преориентира към провеждане на операции съвместно с Морската пехота на САЩ в литоралната зона [22]. Понятието „литорална зона" дефинирано в същата публикация означава район от откритие окена към брега, в който трябва да се осигури поддръжка на операциите на сушата или район на сушата, който може да бъде пряко поддържан и защитаван от към морето.[22] Така дефинирано понятието „литорална зона" включва в себе си националните морски пространства и частта от сушата до където могат да изпълнят задачи съвременните корабни оръжия или това е дистанция около 600 морски мили към сушата. Очевидно понятието „литорална зона" е различно от понятието „крайбрежие" и въпреки, че района дефиниран като „литорална зона" отговаря на изискванията за дефинирано пространство, което да позволи откриване, ранно предупреждение и своевременно противодействие на заплахите понятието не може да бъде директно използвано от всички крайбрежни държави поради различни особености на техните географски характеристики. Освен това крайбрежните държави не са в състояние да съперничат на по-големите ВМС в откритите морски пространства, а имат собствени интереси в крайбрежните и прилежащите към тяхната територия водни пространства, които се различават от поддържаните от външните за даденият район държави [14]. Според доктрината за морските операции НП – 3.1. на Република България, „литоралната зона" е място, в което операции на ВМС се провеждат във взаимодействие с останалите видове въоръжени сили на страната. Следователно като се вземе в предвид географските характеристики на Република България, хидрографските характеристики на нейните национални морски пространства и способностите на системите, намиращи се на въоръжение в Българската армия **литоралната зона** може да се определи като **район, който включва националните морски пространства и територията на страната на около 100 км. от бреговата линия или пристанищата, в който ВМС извършват съвместни операции с останалите видове въоръжени сили.**

За защитата на сигурността във всичките й аспекти е необходимо да бъдат защитени обектите от морската инфраструктура, обектите от критичната инфраструктура и стратегическите обекти в този район, поради което отговорност за сигурността носят много институции като Министерство на транспорта, чрез ИА „Морска администрация" и ДП „Пристанищна инфраструктура", Министерство на вътрешните работи чрез своите органи, Министерство на отбраната, чрез Въоръжените сили, Министерство на околната среда и водите, Министерство на финансите, ДАР, ДАНС и другите институции имащи отношение към защита на националната сигурност на страната. В тази връзка законите на страната предвиждат различни правомощия на отделните институции и техните органи. Така на пример чл. 39, ал. 3 от Закона за МВР оправомощава органите на Главна дирекция „Гранична полиция" да извършват оперативно–издирвателна, охранителна, информационна, контролна, превантивна и административно–наказателна дейност както и разследване на престъпления във вътрешните морски води, териториалното море, прилежащата зона, континен-

талния шелф, българската част на река Дунав и другите гранични реки и водоеми. Законът за опазване на околната среда дава правомощия на органите на Министерство на околната среда и водите да извършват превантивен, текущ и последващ контрол за замърсяване на околната среда и да съставят актове на нарушителите на закона. Закона за морските пространства, вътрешните водни пътища и пристанищата на Република България дават правомощия на изпълнителна агенция „Морска администрация" да извършва контрол на корабоплаването, да задържа кораби нарушители да им съставя актове за допуснати административни нарушения или да им разпореди да напуснат националните морски пространства.

Правомощие на държавен орган означава, че компетентният държавен орган има едновременно право и задължение да извърши определена дейност в рамките на неговата компетентност. Това ще рече, че държавният орган освен правото да извърши определено действие, пред него стои и задължението да извърши това действие при предвидени в закона определени обстоятелства. В този смисъл определени правомощия по защита на сигурността на страната в мирно време имат и органите на Министерство на отбраната в кръга на тяхната компетентност. В този смисъл чл. 56 и чл. 57 от ЗОВСРБ дават правомощия на Въоръжените сили да поддържат готовност за оказване на хуманитарна помощ и да извършват спасителни действия на територията и в морските пространства на страната и извън нея в съответствие с националното законодателство и международните договори, по които Република България е страна; да подготвят и обучават формирования за провеждане на спасителни и неотложни аварийно-възстановителни работи за овладяване и/или преодоляване на бедствия; да участват в превантивната и непосредствената защита на населението и да провеждат спасителни и неотложни аварийно-възстановителни работи по ред, определен в Закона за защита при бедствия; да извършват неутрализиране на невзривени бойни припаси на територията на Република България; да оказват съдействие на органите за сигурност в борбата им срещу разпространяване на оръжия за масово унищожение, незаконен трафик на оръжие и тероризъм; охраната на стратегически обекти, на обекти и системи от критичната инфраструктура. Освен това чл. 30 от закона за морските пространства, вътрешните водни пътища и пристанищата на Република България дава правомощия на Морска администрация и на органите на МВР, и на МО в пределите на вътрешните морски води и териториалното море по отношение на чуждестранен невоенен кораб:

- да поискат да вдигне държавното си знаме;
- да му отправят съответни запитвания при съмнение за нарушаване на правилата за мирно преминаване;
- да му предложат да измени курса си, ако той води към забранен за плаване район;
- да го спрат и да извършат проверка или да го задържат, ако не отговори на отправеното му запитване или наруши закона или когато такива мерки се предвиждат в международен договор, по който Република България е страна;
- да го спират и арестуват в предвидените от закона случаи;
- да снемат от него и да задържат лицата, извършили престъпления, и да ги предават на следствените органи, като уведомят прокурора в срок до 24 часа.

В случай, че чуждестранният невоенен кораб откаже да спре или се възпротиви на задържането му, или прибегне до насилствени действия, органите на Министерството на вътрешните работи и на Министерството на отбраната могат да вземат съответни принудителни мерки, включително и употреба на оръжие и бойна техника. Предоставените сходни правомощия на различните институции, а понякога и препокриването на правомощия дава основание тези служби да изпълняват съвместни действия и задачи за постигане на по-голямо бързодействие и икономия на ресурси. Това взаимодействие на първо място е предвидено в нормативната рамка, която създават законите. Така освен в ЗМВР, ЗОВС и ЗМПВПП, такова взаимодействие се предвижда в Закона за управление и функциониране на системата за защита на националната сигурност. Този закон дава легално определение на понятието национална сигурност, регламентира органите, участващи в системата за защитата на националната сигурност и реда за тяхното управление. Освен това чл. 3 на този закон предвижда взаимодействие между органите участващи в защитата на националната сигурност чрез писмена кореспонденция, работни срещи, създаване на съвместни работ-

ни групи и провеждане на координирани мероприятия, както и други форми съобразно тяхната компетентност както и ги задължава да се информират и съгласуват действията си при постъпване на информация от интерес за дейността на друг орган или структура. Законът предвижда създаване на консултативен орган - съвет по сигурността към Министерски съвет в който са включени министърът на вътрешните работи; министърът на отбраната; министърът на външните работи; министърът на финансите; началникът на отбраната; главният секретар на Министерството на вътрешните работи; председателят на Държавна агенция "Национална сигурност"; председателят на Държавна агенция "Разузнаване"; директорът на Служба "Военна информация"; началникът на Националната служба за охрана; секретарят на Съвета по сигурността; двама представители на президента на републиката, изрично определени от него с указ. Интересното в този състав на съвета по сигурността е, че в него не се предвижда участието на министъра на транспорта информационните технологии и съобщенията или поне на негов представител. Важно е да се отбележи, че Министерството на транспорта, информационните технологии и съобщенията отговаря за стратегическите комуникации на страната в мирно време, които включват автомобилният, въздушният морският и речен транспорт, телефонните, телеграфните, мобилните и пощенски комуникации и услуги, регулира движението на гражданското мореплаване и въздухоплаване. Друг момент в ЗУФСЗНС е факта, че т. 3 от параграф 1 от преходните и заключителни разпоредби на закона дефинира понятието „криза" като *събитие, което нарушава състоянието на национална сигурност в резултат на целенасочени действия или бездействия на лица, групи или организации.* Интересен е факта, че ЗОВС в своя параграф 1 от преходните и заключителни разпоредби, т.20 гласи *"Криза е нестабилност в политическата и обществената сфера, предизвикваща рязка промяна на установеното състояние на икономиката и обществения живот."*, т.е. съществуват две легални определения на понятието криза като в зависимост от това кое понятие ще се използва води до различни последствия. Друг закон, в който се предвижда взаимодействие между въоръжените сили и останалите институции за защита на вътрешната сигурност е Закона за противодействие на тероризма(ЗПТ). Този закон предвижда планиране и провеждане на операции по противодействие на тероризма, в които да бъдат включени сили и средства на Българската армия, за което този закон дава допълнителни правомощия на военнослужещите от Българската армия. Тези правомощия обаче могат да бъдат упражнявани само по време на участие на военнослужещите в операция по противодействие на тероризма. Освен това ЗПТ предвижда изготвянето на планове на местно ниво, които да бъдат съгласувани с МВР и ДАНС, но не се предвижда съгласуване с началника на гарнизона или друг представител на въоръжените сили като при това закона не предвижда механизъм за въвеждане на формирования от въоръжените сили, а за това препраща към Закона за защита при бедствия.

От написаното до тук може да се направи извода, че съществуващата правна рамка, която регламентира дейността на институциите гарантиращи сигурността на страната, определя правомощията на техните органи, като дори на моменти предвижда дублиране на правомощия и функции. Въпреки това съществуват противоречия и празноти, като дублиране на понятия, предвиждане на различни действия от различните органи в една и съща ситуация, което пречи на доброто взаимодействие между институциите и техните органи.

Начина на взаимодействието между институциите и конкретните съвместни действия от техните органи за защита на сигурността се регламентира чрез редица подзаконови нормативни и административни актове. Така на пример определянето на режима на корабоплаване при въвеждане на военно положение, положение на война или провеждане на дейности за осъществяване на отбраната на страната се определя от наредба № Н-8 от 9 март 2011 г. за режима на корабоплаване в териториалното море, вътрешните води, пристанищата и рейдовете при осъществяване отбраната на страната, обн. ДВ. бр. 23 от 22 март 2011г. Един от изключително важните актове за взаимодействие между институциите е 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. Тази инструкция предвижда реда за взаимодействие между органите на МВР и структурите на Въоръжените сили като определя реда за обмен на информация между ОДЦ на МВР и ВКЦ, дава ограничени правомощия на въоръже-

ните сили за участие в охраната на държавната граница. В мирно време и при обявяване на извънредно положение инструкцията предвижда Командира на ВМС и началника ГДГП да съгласуват плановете си за взаимодействие и да определят реда за обмен на информация касаеща наблюдението и контрола на корабоплаването в морските пространства на Република България. Чл.9, ал. 3 от инструкцията гласи, че по искане на оперативния дежурен на ГДГП в Бургас оперативният дежурен на Военноморските сили разрешава работата на брегови и корабни радиолокационни станции на отделни райони и участъци в интерес на охраната на морската граница на страната. Тук трябва да се отбележи, че инструкцията не предвижда обратен механизъм. По този начин до известна степен се нарушава един от основните принципи на взаимодействието, а именно принципа на равнопоставеност между институциите. Въпреки това наличието на такава инструкция е признак на сравнително добра комуникация между ведомствата. За сравнение трябва да се отбележи, че инструкции за взаимодействие между МО и други ведомства следва те първа да бъдат обсъждани, утвърдени и приети като на пример инструкция за взаимодействие между МО и НСО. Друг административен акт, който регламентира взаимодействие е Националния план за противодействие на тероризма, приет от Министерски съвет през 2017 г., който предвижда комплекс от мероприятия при различни степени на заплаха от терористичен акт, както и разпределя отговорностите между компетентните институции. Трябва да се отбележи, че този план значително разширява кръга на участващите институции при използването на мерки против тероризма и при участие в антитерористична операция като предвижда създаване на Национален оперативен щаб /НОЩ/, който да ръководи и координира действията на институциите при противодействие на тероризма. Този план също предвижда и дейности на МВР и МО по защита на стратегически обекти и обекти от критичната инфраструктура на страната. Тук е важно да се отбележи, че въпреки че ЗОВСРБ предвижда участие на Въоръжените сили в подобен вид операции то отново не съществува механизъм по който формированията от БА да бъдат привличани в подобен вид дейности в мирно време. Съществуват и редица други актове които регламентират правомощията на различните институции и взаимодействието между тях като Наредба за условията и реда за постигане сигурността на корабите, пристанищата и пристанищните райони, приета с ПМС № 374 от 25.11.2014 г., обн. ДВ. бр. 99 от 2 декември 2014г., Инструкция № 8121з-1244 от 14 октомври 2015 г. за наблюдението на държавната граница на Република България, специфичната охранителна дейност за участие в мерките за постигане на летищна сигурност в обществените зони и периметъра на летищата и прилагане на компенсиращи мерки ДВ, бр. 83 от 27 октомври 2015 г., в сила от 31.10.2015 г., Инструкция № 8121з-915 от 1 декември 2014 г. за условията и реда за осъществяване на оперативна защита при наводнения, издадена от Министерството на вътрешните работи, обн. ДВ. бр.101 от 9 декември 2014 г. и др. Следователно като извод може да се направи, че съществуващата подзаконова рамка, която регламентира конкретните съвместни действия между институциите в много случай регулира обществените отношения едностранно, само в полза на едната институция като нарушава принципа на равнопоставеност между тях. Освен това тази рамка е непълна, поради факта че съществуващите наредби и инструкции се разработват само между отделни ведомства, а не между всички институции имащи правомощия за защита на сигурността в дадения район.

В заключение може да се каже, че защитата на сигурността в литоралната зона следва да бъде наложен националният суверенитет в националните морски пространства, а пристанищата, фарватерите, стратегическите обекти и обектите от критичната инфраструктура в зоната да бъдат надеждно защитени. Видно от горенаписаното обаче за това има редица правно-нормативни и административни пречки, които могат да бъдат отстранени, чрез допълване на законодателството и промяна на подзаконовите нормативни и административни актове, което да даде основа за пълноценно взаимодействие между различни институции в тази насока. Като добър пример от миналото може да се посочи Инструкция № I – 121 от 29 юли 1992г. за реда за взаимодействие между органите на Министерство на вътрешните работи, Министерство на отбраната, Министерство на транспорта, Министерството на селскостопанското развитие, земеползването и възстановяване на поземлената собственост, министерството на околната среда с контролни правомощия по смисъла на закона за морските пространства. Тази инструкция е разработена съвместно от министерст-

вата, които са имали контролни правомощия по закона за морските пространства и установява точни и ясни правила за комуникация и взаимодействие между определените в закона институции.

References:

1. Гоцев, Г. Защита на сигурността и общественият ред, София: ВИ, 2016.
2. Георгиев, Х. Политика на сигурност на Република България в началото на 21 век: теоретични и приложни аспекти, София, 2011г., ISBN: 9789545356926
3. Доктрина на морските операции, НП – 3.1., Варна: 2013 г.
4. Доклад за състоянието на националната сигурност на Република България през 2016г, София: 2017 г.
5. Закон за Министерство на вътрешните работи, обн. ДВ. бр.53 от 27 юни 2014г., с посл. доп. ДВ. бр.10 от 30 януари 2018 г.
6. Закон за морските пространства, вътрешните водни пътища и престанищата на Република България, обн. ДВ. бр.12 от 11 Февруари 2000г., посл. изм. и доп. ДВ. бр.28 от 29 Март 2018 г.
7. Закон за отбраната и въоръжените сили на Република България, Обн. ДВ. бр.35 от 12 Май 2009г., посл. изм. ДВ. бр.7 от 19 Януари 2018 г.
8. Закон за управление и функциониране на системата за защита на националната сигурност обн. ДВ. бр.61 от 11 август 2015 г.
9. Закон за управление на черноморското крайбрежие,Обн. ДВ. бр.48 от 15 Юни 2007г., посл. доп. ДВ. бр.28 от 29 Март 2018 г.
10. Иванов, В. Охраната на държавните граници и новият световен ред: [Изследване], София: Военнно издателство, 2005г., ISBN 954-509-324-2.
11. 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.
12. Инструкция № I – 121 от 29 юли 1992г. за реда за взаимодействие между органите на Министерство на вътрешните работи, Министерство на отбраната, Министерство на транспорта, Министерството на селскостопанското развитие, земеползването и възстановяване на поземлената собственост, министерството на околната среда с контролни правомощия по смисъла на закона за морските пространства.
13. Йорданов Н. Проблеми на военноморското изкуство, София: Военно издателство 2003 г.
14. Костадинов К. Теоретични основи на оперативното използване на Военноморските сили, София: ВА „Г. С. Раковски"2018 г.
15. Методология и сценарии за отбранително планиране, София, Военно издателство.
16. Медникаров Б. Зашита на морския суверенитет, Варна: ВВМУ „Н. Й. Вапцаров", 2008г.ISBN 978–954–8991–57–5.
17. Наредба № Н-8 от 9 март 2011 г. за режима на корабоплаване в териториалното море, вътрешните води, пристанищата и рейдовете при осъществяване отбраната на страната, обн. ДВ. бр. 23 от 22 март 2011 г.
18. План за развитие на въоръжените сили до 2020 г.
19. Програма за развитие на отбранителните способности на въоръжените сили на Република България 2020.
20. Стоянов, Г. Рискове и заплахи за вътрешната сигурност на Република България, София 2000.
21. Стоянов Н. Рискове и заплахи за сигурността на водната транспортно – преносна система, Варна: 2017г. ISBN:978–61–90844–0–3.
22. Sean O'Keefe, Frank B. Kelso II, C.E. Mundy, jr. From The Sea: Preparing the Naval Service for the 21st Century" Navy and Marine Corps White Paper,Sep 1992
23. Wayne P. Hughes, Jr. Fleet Tactics and Coastal Combat (Second Edition). Annapolis, MD: Naval Institute Press, 2000.

MANAGEMENT OF NATIONAL SECURITY BASED ON CAPABILITIES

Maxim M. Alashki

Address: 3, Dyakon Ignatii Str., 1092 Sofia, Ministry of Defence, Defence Acquisition Directorate

***Abstract**: There is brief information (including definitions) on what is national security capability, the need to build a System for managing the development of national security structures in order to achieve management based on these capabilities, as well as the component parts of the system, with their definitions, characteristics and basic principles. The process of managing the development of structures is illustrated in a schematic and figurative principle.*

***Keywords**: National Security Strategy, National Security Capability, Defense Acquisition, System of Required Capabilities, Defense Acquisition System, Budgeting System, Development.*

УПРАВЛЕНИЕ НА НАЦИОНАЛНАТА СИГУРНОСТ, БАЗИРАНО НА СПОСОБНОСТИТЕ

Максим М. Алашки

Адрес за кореспонденция: 1092 гр. София, ул. Дякон Игнатии № 3, Министерство на отбраната, дирекция „Отбранителна аквизиция"

Стратегията за национална сигурност [1] изисква оптимално разпределение на ресурсите за постигане на ефективно управление на системата за сигурност (т. 4), прилагане на принципите на откритост, прозрачност и отговорност при формирането и провеждането на политиките за сигурност и ефективност и ефикасност на управленските и изпълнителските дейности (т. 18), както и повишаване на ефективността, прозрачността и отчетността при функциониране на институциите и ясно разпределяне на задълженията и правомощията на политическите и административните равнища в органите на изпълнителната власт (т. 69). Стратегията определя и мисиите и задачите, които трябва да изпълняват отговорните за нейната реализация национални структури и ведомства, както и свързаните с тях необходими за придобиване способности – отбранителни, на МВР и на другите свързани с националната сигурност структурни звена. Същите са допълнително и специално развити в отделни стратегически документи – програми, стратегии, концепции и др.

Способността [5, 6] е възможността за успешното изпълнение на мисия, стратегическа цел, оперативна цел или задача на структурата от националната сигурност. Тя е възможността за постигане на определен желан краен резултат, при определени условия и в съответствие с приети стандарти. Някъде в свързаните документи са използвани понятията *потребност* и *удовлетворяване на потребности*. Потребност е необходимост, нужда, която трябва да бъде удовлетворена за да бъдат постигнати определени заложени цели и задачи. Връзката между способност и потребност е по отношение изискването да бъде реализирана необходимост – в единия случай задоволяване на способност, а в другия удовлетворяване на потребност. В този смисъл те са сродни понятия, като удовлетворяване на потребност се явява функция (с по-ниска степен на йерархичност по отношение на обхват) на по-основното понятие задоволяване на способност.

Употребата на понятието способност (или *необходима способност*) се налага от неговото използване във връзка със съюзните ангажименти по линия на ЕС и НАТО, както и в Европа и САЩ като цяло, където то (Capability) е широко и основно третирано в свързаната литература и документи, включително и в общи такива. Съгласно тях способността е съвкупност и синергия от следните елементи: (**DOTMLPFI/P**) [5, 6]:

- доктрини (**D**octrine) – всички документи по реализиране на способността;
- организационна структура (**O**rganization) – необходими елементи и функции;
- подготовка (**T**raining);
- оборудване и материални средства (**M**aterial);
- командване и обучение (**L**eadership and Education);
- личен състав (**P**ersonnel);
- инфраструктура (**F**acilities);
- оперативна съвместимост или политика (**I**nteroperabilities or **P**olicy).

За постигането, развитието на тези необходими за структурите способности или задоволяване на техния дефицит е необходимо създаването на подходяща Система за управление развитието на тези структурите (СУРС). Идеологията на тази система предполага разделяне между три независими една от друга подсистеми, сами по себе си определени във функционално отношение като отделни системи, на функциите и отговорностите относно вземане на решения по определяне на потребностите във ведомството и тяхната приоритизация, дефиниране и разпределяне на ресурсите, и за необходимата аквизиция, която да материализира потребностите, произтичащи от способностите за изпълнение на определените мисия, цели и задачи на ведомството. Дейността на тези три отделни системи е подходящо да се управлява от съвети, като колективни консултативни органи на съответния ръководител на ведомство, с участието в тях на представители на всички заинтересовани и функционално отговорни подструктури, които ще предлагат решения за определяне на потребностите и оптималните пътища за тяхното задоволяване в рамките на разполагаемите бюджетни средства. Правилата и редът за функциониране на тази система следва да бъдат описани в регламентиращ документ (правилник, наредба, вътрешни правила, указания или др.), който след неговото утвърждаване да се има за изпълнение. Такова управление от страна на колективен консултативен/съвещателен орган не бива да се схваща буквално, а като цялостно ръководство и координация по линия на подпомагане на министъра на вътрешните работи в съответната област.

Целта на внедряването на такава система е да създаде по-добри условия за практическото реализиране както на политиките на съответното ведомство в различните направления на дейност, така и на бюджета, съгласно съответните бюджетни програми, да повиши прозрачността и ефикасността при разпределяне на финансовите средства в съответствие с мисиите, целите и задачите на структурите по отделно и на Системата за национална сигурност като цяло. Освен това ще разпредели отговорностите при вземане на решения и ще бъде основа и за по-добро интегрирано дългосрочно планиране и цялостно развитие на структурите, като не на последно по важност място и за намаляване на обективните предпоставки за корупционни практики.

В Министерството на отбраната бе създадена такава система, наречена Система за управление на развитието на Въоръжените сили (СУРВС). Тя бе регламентирана с постановление на Министерския съвет (ПМС) [2] № 301 от 10.11.2004 г., обнародвано в държавен вестник (ДВ) бр. 103 от 23.11.2004 г. С него се прие Плана за организационно изграждане и модернизация на ВС до 2015 г., както и графиците и разчетите към него.

Целта на заложената в плана СУРВС [5] е осигуряване способностите на Въоръжените сили в рамките на организационните структури от МО, БА и структурите на подчинение на министъра на отбраната, за постигане на националните цели и задачи в областта на сигурността и отбраната на Република България чрез разработване на изисквания, управление на ресурсите за отбрана и придобиване на отбранителни продукти. Съгласно този документ СУРВС се състои от четири взаимно свързани подсистеми, проектирани като:

- Подсистема за необходимите оперативни способности (НОС), предназначена за определяне на изискванията и приоритетите за постигане на необходимите оперативни способности, произтичащи от националните документи и задачи в областта на сигурността и отбраната.

- Интегрирана подсистема за управление на ресурсите за отбрана (ИСУРО), предназначена за определяне на необходимите ресурси за отбрана и кога и как те да бъдат използвани за постигане на дефинираните и подредени по приоритети (приоритизирани) НОС.

- Подсистема за отбранителна аквизиция (СОА), предназначена за определяне на възможно най-оптималния начин, по който следва да бъдат постигнати НОС.

- Подсистема за управление на човешките ресурси (УЧР).

Подсистемата за НОС инициира процесите на СУРВС. Тя осигурява строго определен и документиран процес на анализ и определяне на способностите, които са необходими на МО, БА и структурите на подчинение на министъра на отбраната. Системата изготвя серия „продукти", които документират решенията за необходимите способности и предоставя входяща информация на другите подсистеми. Разработените и заложени в плана параметри са продукт на подсистемата на НОС. Продукти на подсистемата са: дефиниране на мисиите (писмено описание), необходими оперативни способности (списък), сценарии за планиране, доклади за определяне потребностите на мисиите, структура на необходимите ВС, план за дислокация, интегриран списък с приоритетни проекти, интегриран списък на приоритетните войскови части (организационни структури), предварителен план за интегриране на способностите, план за интегриране на способностите и др.

ИСУРО определя с колко ресурси и кога приоритизираните НОС ще бъдат постигнати и изпълнени чрез процесите на планиране, програмиране, бюджетиране и изпълнение на бюджета. Продукти на ИСУРО са: указания на министъра на отбраната за програмирането, програмен меморандум, меморандум на програмните решения (МПР), предложение за бюджет, преразпределяне на бюджета и др.

Ролята на СОА е по най-ефективен начин да се придобият отбранителните продукти, необходими за изпълнение на мисиите и да се осигури дългосрочната им поддръжка при спазване на изискванията и приоритетите, посочени в Подсистемата за НОС и утвърдените ресурси в ИСУРО. Продукти на СОА са: Стратегия за отбранителна аквизиция, предложения по аквизиция, дългосрочен план за модернизация на ВС и годишни планове за снабдяване и за снемане от употреба.

Проблемен момент при разглеждането на СУРВС като водеща система за управление на дейностите и процесите в МО е обстоятелството, че ПМС, с което бе регламентирана през 2004 г., е отменено в преходните и заключителните разпоредби на ПМС[3] № 135 от 12.05.2011 г. за приемане на Устройствен правилник на МО, обнародвано в ДВ, бр. 39 от 20.05.2011 г., в сила от 01.06.2011 г. Тази отмяна на регламентирането на СУРВС може и да е търсена, целенасочена, може да е и поради невнимание, но е факт, че СУРВС понастоящем е без действащ регламент. Но тъй като и без нарочен регламент, и с наличието на такъв, тази система работи, функционира и чрез нейните продукти се управляват специфични и важни за МО дейности и процеси, приемаме, макар и условно, че СУРВС съществува, в това число и съставляващите я подсистеми, които само по себе си са големи и самостоятелни системи - СНОС, ИСУРО и СОА.

През тази, 2018 г., подобна система бе документално разработена и в МВР, приета от министъра на вътрешните работи, но все още не е внедрена за използване, защото условията и т.нар. зрялост на ведомството на сегашния етап от развитието му не позволяват това - смесват се множество чисто обективни и чисто субективни фактори и причини, както и микс от тях, които не са тема на настоящо разглеждане.

Системата, наречена Система за управление развитието на структурите на МВР (СУРСМВР) [6] е система, която се създаде с основна цел да подобри и усъвършенства връзките и процесите между ангажираните и функционално отговорни структури в МВР на основата на определяне на потребностите и начините за тяхното задоволяване в рамките на разполагаемите ресурси. По своя смисъл и идеология това е система за функционален мениджмънт с линейно-функционална структура. Целта на системата е осигуряване на способностите на министерството, в рамките на организационната му структура, за постигане на националните цели и задачи в областта на националната сигурност и опазване на обществения ред и осигуряване на пожарна бе-

зопасност и защита при пожари, бедствия и извънредни ситуации в страната, чрез разработване на изисквания, подходящо управление на ресурсите и придобиване на необходимите продукти - материални средства, строителство, услуги и др.

СУРСМВР също се състои от три основни взаимно свързани подсистеми:

- Подсистема за необходимите способности в МВР, предназначена за определяне на изискванията и приоритетите за постигане на необходимите способности, произтичащи от националните документи и задачи в областта на националната сигурност и опазване на обществения ред, в това число и от потребностите на мисиите, целите и задачите във ведомството.

- Подсистема за бюджетиране, предназначена от една страна за определяне на необходимите ресурси на ведомството и кога и как те да бъдат използвани за постигане на дефинираните и подредени по приоритети (приоритизирани) необходими способности, а от друга страна как това да става по най-оптимален начин по отношение на наличните такива.

- Подсистема за аквизиция, предназначена за материализиране (постигане/задоволяване) на необходимите способности.

Тези три основни подсистеми по своя генезис, връзки и процеси представляват по отделно и сами за себе си също отделни крупни и цялостно завършени системи: Система за необходими способности (СНС-МВР), Система за бюджетиране (СБ-МВР) и Система за аквизиция (СА-МВР). В СУРСМВР се съдържат и участват със своите обекти, субекти и връзки и други подсистеми: кадрова (или за човешките ресурси), логистична, комуникационна, информационна, правна, медицинска, образователна (вкл. научна) и др. Те, обаче се разглеждат като осигуряващи, подпомагащи и съпътстващи дейността и функционирането на основните три такива, и на тях няма да бъде обърнато специално внимание. Последното по никакъв начин не омаловажава тяхното място, роля и значение в Системата на МВР.

Принципно за СУРС, специално се обръща внимание на обстоятелството, че такава система по никакъв начин не се ангажира с броя и задълженията на структурите в отделното ведомство, а във фокуса са функционални връзки между тях, които се срещат/взаимодействат в нещатните консултативни органи – съветите. Там структурите изграждат отношения по линия на синергия и развитие.

Какво представляват бюджетирането и аквизицията?

Бюджетирането [5, 6] е комплекс (система) от дейностите по планиране, контрол и анализ на паричните потоци и свързания с тях финансов резултат. То е управление на процеса на създаване, разпределение и използване на финансовите ресурси на съответната финансово обособена структурна единица.

Терминът „аквизиция" (Acquisition) [5, 6] буквално се превежда като „придобиване, придобивка", „акт за придобиване". Той е специфичен и се използва предимно във военната тематика (ЕС, НАТО и др.), финансовата практика, застраховането, лингвистиката. В конкретния аспект той обхваща всичките дейности по придобиването, поддържането и развитието на способност, свързана с националната сигурност чрез изградена за това система, като е дадено следното определение:

Аквизиция в националната сигурност е (1) бюрократично управление, (2) процес на възлагане на обществени поръчки и доставки и (3) съвкупност от интегрирани процеси по управление на жизнения цикъл на продуктите за национална сигурност, на научно-изследователската дейност в тази област и политиката за придобиване/снабдяване, на проектите за инвестиции и модернизация и тяхното управление, на инфраструктурата и други съпътстващи дейности, които (1+2+3) са свързани с национални инвестиции в придобиване на продукти/способности, свързани с националната сигурност, технологии, програми и тяхната интегрирана логистична поддръжка (ИЛП), необходими за постигане на Стратегията за национална сигурност на Република България.

Целта на аквизицията е да се придобият продукти, които отговарят на определени специфични нужди и удовлетворяване на необходимите способности на допустима (в смисъл на оптимална, справедлива и разумна) цена.

Накратко и съвсем опростено може да се каже, че аквизицията в националната сигурност материализира необходимите способности на свързаните с нея ведомства/структури (удовлетворява потребностите от материални средства, строителство и услуги).

Както вече бе посочено, системата се управлява и в известна степен администрира от **съвети**, като нещатни съвещателни органи на съответния ръководител на бюджетна структура от състава на Системата за национална сигурност. Съвет за необходими способности (СвНС), Съвет по бюджетиране (СвБ, или Бюджетен съвет) и Съвет по аквизиция (СвА) са нещатни колективни консултативни органи на съответния ръководител, които управляват дейностите на трите основни (под)системи на СУРС, а над тях е възможно и подходящо да има „по-старши" съвет – напр. Съвет по отбрана или Висш съвет на МВР, който е нещатен колективен консултативен орган на съответния министър или друг ръководител за общо управление на дейността във ведомството, който се явява висшестоящ спрямо другите съвети. Последният, поради своя състав, място и роля, може да изпълнява и други функции по управлението на структурата.

Характеристики на СУРС [5,6]

Както всяка многообхватна и сложна система, така и тази притежава много и различни характеристики, в зависимост от широката гама от критерии, спрямо които тя може да се разгледа (анализира и оцени) и дефинира - по структура, по поведение, по свързаност, по функции, по въздействие, по капацитет и т.н. Основните характеристики на системата са следните:

- **Национална значимост.** Обхватът на системата надхвърля този на съответното ведомство - дейностите, процедурите и факторите (обективни и субективни) са свързани с материализиране на необходими на Република България способности за националната сигурност.

- **Бюрократичност.** СУРС е типична бюрократична система, част от държавната администрация. Тя е система, която трябва да осигури придобиването на необходимите продукти, свързани с националната сигурност (в т.ч. и дълготрайни материални активи) за осигуряване на функциите на съответното ведомство.

- **Специфичност.** Тя се изразява в наличие на особени и специфични решения и изисквания към продуктите за национална сигурност, които в някои случаи не са подчинени на икономическите закони и икономическата логика.

- **Публичност.** Поради високите разходи на държавни и обществени средства и важността за националната сигурност обществото има право да е информирано за това как и за какво (както и за сметка на какво) се изразходват средствата от държавния бюджет.

- **Корупционна чувствителност (опасност).** Чрез системата се усвояват значителни средства, със сравнително високи норми на печалба и по-особен начин за вземане на решения, които може не винаги да са напълно икономически обосновани.

- **Информационна балансираност.** Изисква се баланс между класифицираност по отношение на техническите и оперативни спецификации на продуктите за национална сигурност и достъпа до информация, необходим за осигуряване на прозрачност и отчетност пред държавните институции и обществото.

- **Интердисциплинарност.** При дефинирането, управлението, изпълнението и изучаването на процесите, елементите и връзките на СУРС се използва и прилага микс от области и професионални направления (дисциплини) на мениджмънта, образованието и науката, свързани с националната сигурност и опазване на обществения ред - социални, стопански/икономически, правни, технически/инженерни, хуманитарни и др.

- **Ресурсоемкост и дефицитност (недостиг).** Необходимите средства за задоволяване на необходимите способности като аксиома винаги недостигат и трябва да се работи в среда на перманентен дефицит от капиталови средства.

- **Елементи на монопсонност.** В качеството си на купувач/клиент понякога ведомството, свързано с националната сигурност/Държавата, е монопсон - тоест единственият купувач на продукти, свързани с националната сигурност и опазване на обществения ред, чийто ограничен пазар се характеризира с висока степен на регулация и характеристики, различни от пазарните.

- **Оперативна съвместимост.** Като страна със съюзни ангажименти по линия на ЕС и НАТО съвместимостта е необходима, а в определени случай и задължителна. Тя често влияе при

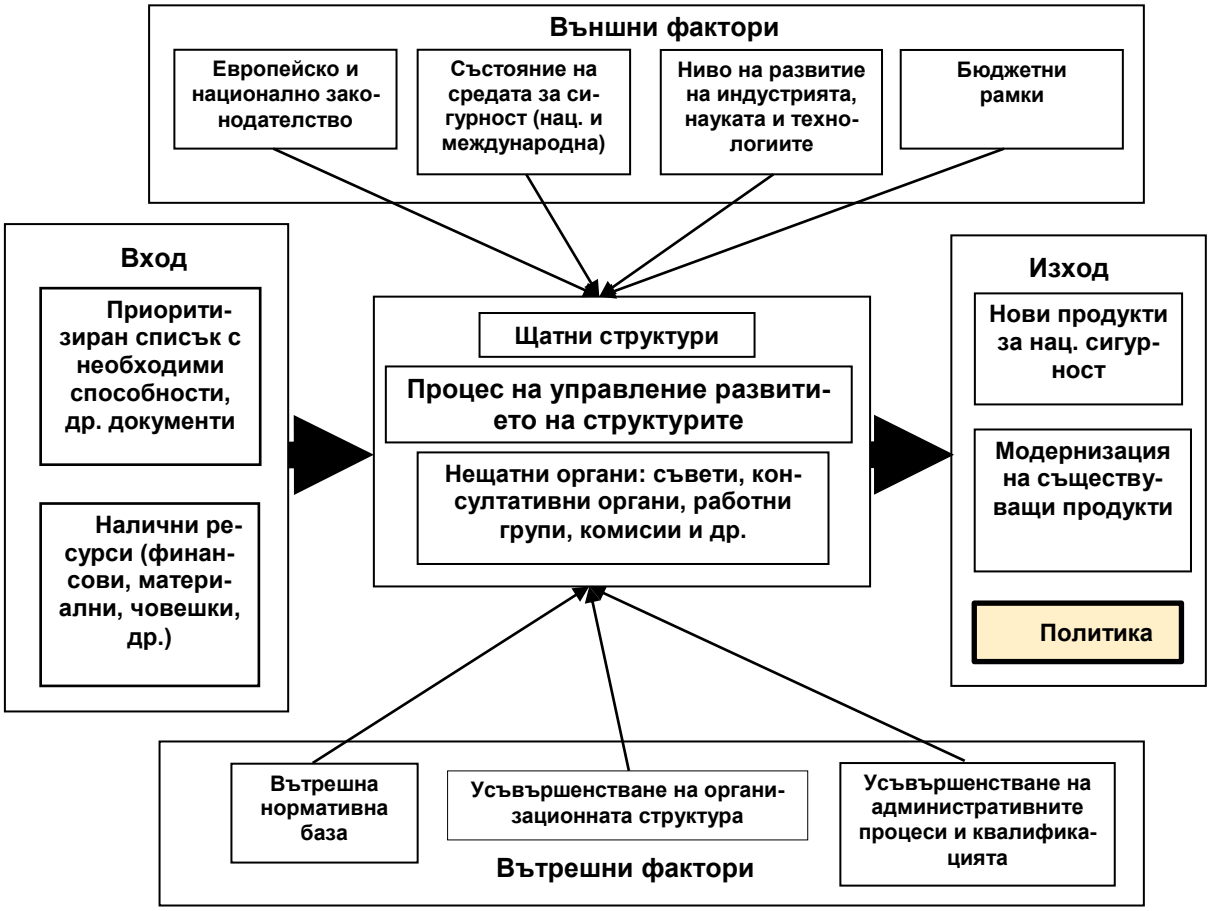
избора на доставчик, което понякога диктува избор на не най-добрата като съотношение качество/цена стока.

Основните принципи на СУРС [6] произтичат от Стратегията за национална сигурност, целите, зададени пред системата, нейните функции и задачи, както и от основните характеристики и специфични особености.

Тези принципи са следните:

- Разпределение на правомощията и компетентностите, задълженията и отговорностите.
- Постоянно функционално взаимодействие и висока степен на координация.
- Плановост и отчетност.
- Откритост и предвидимост.
- Принципност и обективност.
- Устойчивост и баланс.
- Спазване на приоритетност.
- Ефективност и ефикасност.

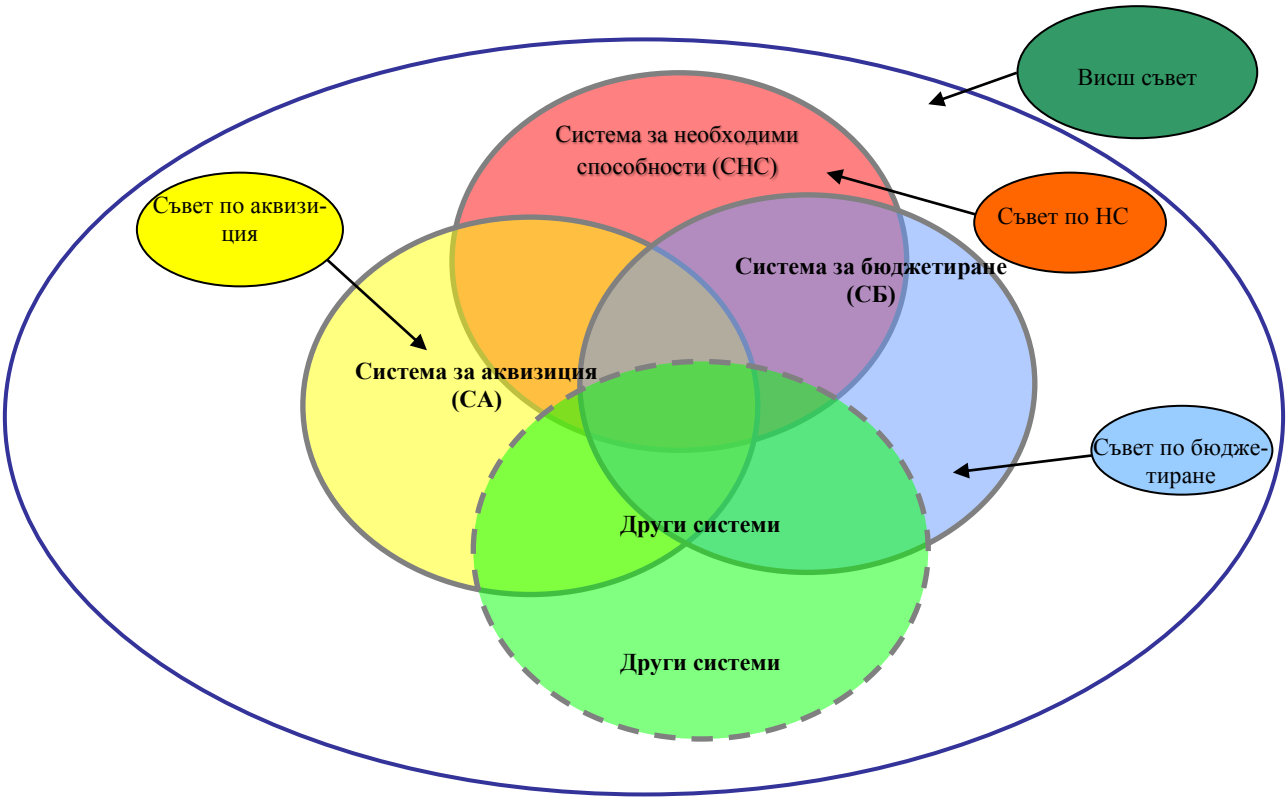
Обобщено процеса на управление развитието на структурите може да се илюстрира по следния схематичен начин (модел):



Фиг. 1

Според идеята СУРС, като система за функционален мениджмънт, трябва да съчетае в себе си, и да развие в допустимия оптимален обем, предимствата, които дава линейно-функционалната структура за управление и да ограничи нейните недостатъци. Това не е еднократен регламентиран процес и механизъм, а развитие, което би могло да се постигне чрез усъвършенстване, модернизация и надграждане в дългосрочен период, в течение на времето.

СУРС и взаимодействията в нея е представено нагледно с вариант на Диаграма на Джон Вен*[5, 6], която се състои от три равни по големина (и равнопоставени) пресичащи се кръга (фиг. 2). Всеки от кръговете има за цел да покаже еднаквото значение за правилното функциониране на съответната структура, както и областта на действие на всяка от (под)системите: Система за необходими способности, Система за бюджетиране и Система за аквизиция, и мястото на свързаните с тях съвети. Общите пресечни площи на трите кръга трябва да даде представата и разбирането, че трите системи си взаимодействат (основно чрез своите продукти) и имат една обща цел, която е ефективно управление на структурата. Показано е и взаимодействието с другите системи: логистична, правна, комуникационна, информационна, за личен състав и т.н. То също става чрез техните продукти (документи, предложения, планове и т.н.). Общата пресечна площ на трите кръга (или общият документ) би намерил своята реализация в някакъв Дългосрочен инвестиционен план или друг дългосрочен стратегически документ на структурата в областта на инвестициите, модернизацията и приоритизирането и планиране на придобиването на необходимите продукти (доставките), и като цяло на планиране базирано на способностите на ведомството.



Фиг. 2

Всяка система намира своето истинско място ако бъде приложена в практиката, където при подходящо внедряване и прилагане да докаже своята необходимост и пригодност, които да се измерват с количествени и качествени измерватели (показатели). Така верифицирана тя ще покаже дали помага и в каква степен за усъвършенстване на процесите и функционалните връзки, които следва да регулира.

Оптимизмът относно внедряването и функционирането на СУРС е свързан преди всичко с цялостното убеждение, че тя при правилно въвеждане, прилагане и управление неминуемо ще доведе до развиване в посока на усъвършенстване, модернизиране и надграждане на работата на ведомството и в резултат на това на самата структура, където ще работи. СУРС и управлението и планирането базирано на необходимите способности са по-модерен институционален функционален модел на мениджмънт и планиране, които имат за крайна цел и резултат подобряване в

*Джон Вен (John Venn)- британски логик и философ, известен с представянето на наречената на негово име диаграма, която се използва в много приложни области, включително теории на множествата, вероятностите, логиката, статистиката и компютърните науки.

количествен и качествен аспект на дейността, която осъществяват структурите във ведомствата, свързани със сигурността и отбрана и като цяло на самата Система за национална сигурност. Тяхното въвеждане и използване естествено ще развие дейността на съществуващите и работещи досега структури и функционалните връзки между тях. Целта е дефинитивно ясна и перманентна – усъвършенстване на този вид дейност за изпълнение на поставените мисии, цели и задачи пред отделните структури, съобразно нормативните и функционални изисквания и основните характеристики и принципи на системата.

References:

1. Стратегия за национална сигурност, 2018 г.
2. ПМС № 135 от 12.05.2011 г.
3. ПМС № 301 от 10.11.2004 г.
4. Програма за развитие на отбранителните способности на ВС на Р. България 2020, МО, 2015 г.
5. Система за отбранителна аквизиция на Република България - възможности за усъвършенстване, Максим Алашки, монография, МО, 2016 г.
6. Концепция за управление развитието на МВР, Максим Алашки, монография, 2018 г.

THE COMPREHENSIVE APPROACH IN THE OPERATIONAL LEVEL DECISION-MAKING PROCESS

Danko D. Farazov

PhD student in the Joint Operations and Planning Department,
National Security and Defense Faculty
1504 Sofia, Bulgaria 82 Evlogi i Hristo Georgievi Blvd.
e-mail: d.farazov@armf.bg

***Abstract**: The collapse of the bipolar model in the World has led to new forms of use of military force. Efforts to resolve conflicts using military means have resulted in changes in the way and methodology of using military force. That is why in NATO, the models of Comprehensive approach in the planning and conducting of military operations are established and approved. A keystone for efficiency and quality in the conduct of a military operation is the decision-making process by the Combined Joint Task Force.*

***Keywords:** comprehensive approach, decision-making process, joint planning, mission command, commander, guidance.*

Changes in the security environment call for new guidelines in the Alliance's policy and the implementation of new methods to prevent and resolve conflicts. This inevitably leads to change, reconfiguration and overall transformation of the organization of forces, the organization of the system of management and interaction and the planning of the methodology in the Alliance. This process leads to a change in procedures and mechanisms for information exchange in intelligence and decision-making procedures. It is clear that the rapidity of the response in the early stages of tackling the crisis situation and in the context of the rapidly changing environment, with much more flexible and adapted procedures, is of great importance. This necessitates a rapid and close interaction between the hierarchical levels of the command structure and the constant interaction with external organizations and structures in the governmental and non-governmental sector. As a result of these reasons, NATO has adopted and enforced the comprehensive approach to joint planning of operations, demonstrating the necessity, importance, and commitment of the largest military organization to change the mechanisms and structures for the adequate use of military force in the modern security environment.

COMPREHENSIVE APPROACH

According to COPD[25] NATO currently recognizes six (6) domains within engagement space. They are:

Political. Any grouping of primarily civil actors, organisations and institutions, both formal and informal, that exercises authority or rule within a specific geographic boundary or organisation through the application of various forms of political power and influence. It includes the political system, parties and main actors. It must be representative of the cultural, historical, demographic and sometimes religious factors that form the identity of a society.

Military. The armed forces, and supporting infrastructure, acquired, trained, developed and sustained to accomplish and protect national or organisational security objectives. This also covers the internal security aspects of a country.

[25] Comprehensive Operations Planning Directive 04 October 2013

Economic. Composed of the sum total of production, distribution and consumption of all goods and services for a country or organisation. It includes not only economic development of a country, but also the distribution of wealth.

Social. The interdependent network of social institutions that support, enable and acculturate individuals and provide participatory opportunities to achieve personal expectations and life-goals within hereditary and nonhereditary groups, in either stable or unstable environments. It covers the social aspects such as religion, a society's structure, the legal and judicial system, policing and supporting infrastructure, humanitarian, etc.

Infrastructure. The basic facilities, services, and installations needed for the functioning of a community, organisation, or society. Includes logistics, communications and transport infrastructures, schools, hospitals, water and power distribution, sewage, irrigation, geography, etc.

Information. The entire infrastructure, organisation, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information. Encompasses the information and communication media.

Through an analysis of the goals, strength, weaknesses and interdependencies of the main actors within these six domains, knowledge is developed about the behaviour of the main actors within the engagement space. That knowledge is then used by decision makers at all levels to determine how these actors might be influenced in ways that achieve the Alliance's strategic objectives and end state, thereby contributing to the international community aims.

Conditions in each of the six system domains of the engagement space can be influenced by the application of one, or a combination of, the four instruments of power:

Military. The military instrument refers to the application of military power, including the threat or use of lethal and non-lethal force, to coerce, deter, contain or defeat an adversary, including the disruption and destruction of its critical military and non-military capabilities. It can also refer to the constructive use of military forces to secure and/or support stabilization and reconstruction or as a tool in helping solve complex humanitarian disasters and emergencies. The military is NATO's main instrument.

Political. The political instrument refers to the use of political power, in particular in the diplomatic arena cooperating with various actors, to influence an adversary or to establish advantageous conditions[26]. NATO member nations employ NATO and other IO's to combine their political power and influence on the international scene, speaking and acting with the same purpose, to create greater effect.

Economic. The economic instrument generally refers to initiatives, incentives and sanctions designed to affect the flow of goods and services, as well as financial support to state and non-state actors involved in a crisis. The aggregation of the economic instruments of NATO nations could act as a significant lever, provided that nations would use their economic instruments in a way that supports the achievement of the NATO end state and also other stated international community goals.

Civil. The civil instrument refers to the use of powers contained within areas such as the judiciary, constabulary, education, public information and civilian administration and support infrastructure, which can lead to access to medical care, food, power and water. It also includes the administrative capacities of international, governmental and non-governmental organizations. The civil instrument is controlled and exercised by sovereign nations, IOs and NGOs. Nonetheless, through interaction and enhanced mutual understanding, NATO can work with those that have access to the civil instrument of power in order to coordinate with them, and possibly adjust our own activities to create synergies with theirs.

[26]The NCRSM (2011) refers to "diplomatic" options for dealing with a crisis.

DECISION-MAKING PROCESS

According to ADRP 5-0[27] the military decisionmaking process is an iterative planning methodology to understand the situation and mission, develop a course of action, and produce an operation plan or order (ADP 5-0). The military decisionmaking process (MDMP) integrates the activities of the commander, staff, subordinate headquarters, and unified action partners to understand the situation and mission; develop and compare courses of action; decide on a course of action that best accomplishes the mission; and produce an operation plan or order for execution. The MDMP helps leaders apply thoroughness, clarity, sound judgment, logic, and professional knowledge to understand situations, develop options to solve problems, and reach decisions. This process helps commanders, staffs, and others think critically and creatively while planning. The MDMP results in an improved understanding of the situation and a plan or order that guides the force through preparation and execution.

The MDMP consists of seven steps (figure 1). Each step of the MDMP has various inputs, a method (step) to conduct, and outputs. The outputs lead to an increased understanding of the situation and to facilitating the next step of the MDMP. Commanders and staffs generally perform these steps sequentially; however, they may revisit several steps in an iterative fashion, as they learn more about the situation before producing the plan or order.

Commanders initiate the MDMP upon receipt of or in anticipation of a mission. Commanders and staffs often begin planning in the absence of a complete and approved higher headquarters' operation plan (OPLAN) or operation order (OPORD). In these instances, the headquarters begins a new planning effort based on a warning order (WARNO) and other directives, such as a planning order or an alert order from their higher headquarters. This requires active collaboration with the higher headquarters and parallel planning among echelons as the plan or order is developed.

The MDMP facilitates collaboration and parallel planning. The higher headquarters solicits input and continuously shares information concerning future operations through planning meetings, warning orders, and other means. It shares information with subordinate and adjacent units, supporting and supported units, and other military and civilian partners. Commanders encourage active collaboration among all organizations affected by the pending operations to build a shared understanding of the situation, participate in course of action development and decisionmaking, and resolve conflicts before publishing the plan or order.

The MDMP also drives preparation. Since time is a factor in all operations, commanders and staffs conduct a time analysis early in the planning process. This analysis helps them determine what actions they need and when to begin those actions to ensure forces are ready and in position before execution. This may require the commander to direct subordinates to start necessary movements, conduct task organization changes, begin surveillance and reconnaissance operations, and execute other preparation activities before completing the plan. As the commander and staff conduct the MDMP, they direct the tasks in a series of WARNOs.

The commander is the most important participant in the MDMP. More than simply decisionmakers in this process, commanders use their experience, knowledge, and judgment to guide staff planning efforts. While unable to devote all their time to the MDMP, commanders follow the status of the planning effort, participate during critical periods of the process, and make decisions based on the detailed work of the staff. During the MDMP, commanders focus their activities on understanding, visualizing, and describing.

The MDMP stipulates several formal meetings and briefings between the commander and staff to discuss, assess, and approve or disapprove planning efforts as they progress. However, experience has shown that optimal planning results when the commander meets informally at frequent intervals with the staff throughout the MDMP. Such informal interaction between the commander and staff can improve

[27] „Army Doctrine Reference Publication" No. 5-0

the staff's understanding of the situation and ensure the staff's planning effort adequately reflects the commander's visualization of the operation.

The chief of staff (COS) is a key participant in the MDMP. The COS manages and coordinates the staff's work and provides quality control during the MDMP. To effectively supervise the entire process, this officer clearly understands the commander's intent and guidance. The COS provides timelines to the staff, establishes briefing times and locations, and provides any instructions necessary to complete the plan.

The staff's effort during the MDMP focuses on helping the commander understand the situation, make decisions, and synchronize those decisions into a fully developed plan or order. Staff activities during planning initially focus on mission analysis. The products that the staff develops during mission analysis help commanders understand the situation and develop the commander's visualization. During course of action (COA) development and COA comparison, the staff provides recommendations to support the commander in selecting a COA. After the commander makes a decision, the staff prepares the plan or order that reflects the commander's intent, coordinating all necessary details.

Step 1 - Receipt of Mission → WARNORD 1

Step 2 - Mission Analysis → WARNORD 2

Step 3 - Course of Action Development

Step 4 - Course of Action Analysis and War-Gaming

Step 5 - Course of Action Comparison

Step 6 - Course of Action Approval

Step 7 - Orders Production, Dissemination, and Transition → WARNORD 3

Figure 1. Steps in the MDMP

STEPS IN THE DECISION-MAKING PROCESS

The main activities in the decision-making process are as follows:

STEP 1–RECEIPT OF MISSION

- Alert the Staff and Other Key Participants
- Gather the Tools
- Update Running Estimates
- Conduct Initial Assessment
- Issue the Commander's Initial Guidance
- Issue the Initial Warning Order

STEP 2–MISSION ANALYSIS

- Analyze the Higher Headquarters' Plan or Order
- Perform Initial Intelligence Preparation of the Battlefield
- Determine Specified, Implied, and Essential Tasks
- Review Available Assets and Identify Resource Shortfalls
- Determine Constraints
- Identify Critical Facts and Develop Assumptions
- Begin Risk Management

- Develop Initial Commander's Critical Information Requirements and Essential Elements of Friendly Information
- Develop the Initial Information Collection Plan
- Update Plan for the Use of Available Time
- Develop Initial Themes and Messages
- Develop a Proposed Problem Statement
- Develop a Proposed Mission Statement
- Present the Mission Analysis Briefing
- Develop and Issue Initial Commander's Intent
- Develop and Issue Initial Planning Guidance
- Develop Course of Action Evaluation Criteria
- Issue a Warning Order

STEP 3–COURSE OF ACTION DEVELOPMEN

- Assess Relative Combat Power
- Generate Options
- Array Forces
- Develop a Broad Concept
- Assign Headquarters
- Develop Course of Action Statements and Sketches
- Conduct a Course of Action Briefing
- Select or Modify Courses of Action for Continued Analysis

STEP 4–COURSE OF ACTION ANALYSIS AND WAR-GAMING

- Gather the Tools
- List All Friendly Forces
- List Assumptions
- List Known Critical Events and Decision Points
- Select the War-Gaming Method
- Select a Technique to Record and Display Results
- War-Game the Operation and Assess the Results
- Conduct a War-Game Briefing (Optional)

STEP 5–COURSE OF ACTION COMPARISON

- Conduct Advantages and Disadvantages Analysis
- Compare Courses of Action
- Conduct a Course of Action Decision Briefing

STEP 6–COURSE OF ACTION APPROVAL

After approving a COA, the commander issues the final planning guidance. The final planning guidance includes a refined commander's intent (if necessary) and new CCIRs to support execution. It also includes any additional guidance on priorities for the warfighting functions, orders preparation, rehearsal, and preparation. This guidance includes priorities for resources needed to preserve freedom of action and ensure continuous sustainment.

Based on the commander's decision and final planning guidance, the staff issues a WARNORD to subordinate headquarters. This WARNORD contains the information subordinate units need to refine their plans. It confirms guidance issued in person or by video teleconference and expands on details not covered by the commander personally. The WARNORD issued after COA approval normally contains:

- The area of operations.
- Mission.
- Commander’s intent
- Updated CCIRs and EEFIs.
- Concept of operations.
- Principal tasks assigned to subordinate units.
- Preparation and rehearsal instructions not included in the SOPs.
- A final timeline for the operations.

STEP 7–ORDERS PRODUCTION, DISSEMINATION, AND TRANSITION

- Plans and Orders Reconciliation
- Plans and Orders Crosswalk
- Approving the Plan or Order

Step 7 bridges the transition between planning and preparations. The plans-to-operations transition is a preparation activity that occurs within the headquarters. It ensures members of the current operations cell fully understand the plan before execution. During preparation, the responsibility for developing and maintaining the plan shifts from the plans (or future operations) cell to the current operations cell. This transition is the point at which the current operations cell becomes responsible for controlling execution of the operation order. This responsibility includes answering requests for information concerning the order and maintaining the order through fragmentary orders. This transition enables the plans cell to focus its planning efforts on sequels, branches, and other planning requirements directed by the commander.

In conclusion, this decision-making process is sufficiently flexible, detailed and gives the commander the freedom to choose the best way to accomplish the mission. This is extremely important in mission command and join planning when we have decentralized exertion. The main figure in this process is the figure of the commander, assisted by his headquarter. Professionalization and training of staff from the headquarters are of great importance because it greatly facilitates the commander's work and improves the efficiency of the whole process.

Abbreviations:

NATO - North Atlantic Treaty Organization

CCIR - Commander’s Critical Information Requirement

EEFI - Essential Elements of Friendly Information

COA - Course Of Action

SOP - Standing Operating Procedure

WARNORD - Warning Order

MDMP - Military Decisionmaking Process

COS - Chief of Staff

OPORD - Operation Order

OPLAN - Operation Plan

IO - International Organisation

NGO - Non-Governmental Organisation

Literary sources:

1. Comprehensive Operations Planning Directive, 2013
2. Army Doctrine Reference Publication No. 5-0, 2012
3. Army Techniques Publication No. 5-19, 2014
4. Army Tactics, Techniques, and Procedures No. 5-0.1, 2011
5. Field Manual No. 6-0, 2014

OBJECTIVES OF PROTECTION OF INTELLECTUAL PROPERTY IN THE CONTEXT OF INFORMATION SECURITY

Hristo A. Desev

***Abstract**: Encouraging of innovation activity and the rightholders protection against cyber threats are the forefront of state (national) strategies for intellectual property. Intellectual property as particularly valuable intangible assets (databases, trade secrets and know-how, computer programs, etc.) are the subject of new threats in cyberspace. Intellectual property protection in cyberspace (including modern technical means) creates the required level of competitiveness for the rightholders.*

***Keywords**: intellectual property, intellectual property protection against cyberthreats, rights to the results of intellectual activity*

ОСОБЕНОСТИ НА ЗАЩИТАТА НА ИНТЕЛЕКТУАЛНАТА СОБСТВЕНОСТ В КОНТЕКСТА НА ИНФОРМАЦИОННАТА СИГУРНОСТ

Христо А. Десев

Национален военен университет " В. Левски" гр. Велико Търново
Факултет "Артилерия ПВО и КИС" гр. Шумен

Съвременните цифрови технологии и използването на глобалните информационни мрежи промениха кардинално схващанията и разбиранията за натрупване и обмен на информация. Тази информационна революция предизвиква изменения в принципите на защита на интелектуалната собственост. Глобалната интернет среда и развитието на информационно-комуникационните технологии изискват адекватно регулиране на отношенията при използване на интелектуалната собственост. Засилването на комерсиализацията на интелектуалната собственост и повишаването на инвестиционната привлекателност доведоха до изключително широко използване на правата върху нея, като средство на междуфирменната борба.

В докладите на Европейското патентно ведомство и Комисията за хармонизиране на вътрешния пазар се подчертава, че отраслите работещи с интелектуална собственост са 39%от общата промишлена дейност, като в тези отрасли средната работна заплата е с 40% по-висока от останалите. Подобни са и анализите на патентното ведомство на САЩ.

Съвременната епоха на „интелектуален капитализъм" и свободно предприемачество търговските сделки са тясно обвързани с пазарен обмен на нематериални (интелектуални продукти). Правата на интелектуална собственост осигуряват на инвеститорите своеобразни гаранции в инвестиционния риск и дори имат стойност на своеобразна обменна валута. Паралелно с това изградената система за ускоряване на инвестиционното развитие, чрез системата за защита на интелектуалната собственост се съпровожда с ефекта на понижаване на конкуренцията и по-високи разходи за достъп до продуктите и технологиите.

По експертни оценки транснационалните корпорации отделят съществено място на интелектуалната собственост в стратегиите за разширяване на позициите си на световните пазари. Основната цел е получаване на преимущество в отделни отрасли и услуги. Воденето на патентни войни чрез блокиране на научно-техническите разработки на конкурентите са свързани с активни форми на защита на перспективни сектори на пазара от всички държави. Показателен в това от-

ношение е ЕС, който инициира преразглеждането на договора Safe Harbor с търговското министерства на САЩ за трансфер на персонални данни за американски компании в ЕС. Конкретния повод е програма за обобщаване на данни PRISM на САЩ която нарушава основна директива на ЕС за защита на данните (EU Data Protection Directive).

Р. България не е изключение от тези тенденции – използване на емейли и мобилни съобщения с подвеждаща информация, подмяна или фалшифициране на официални уебсайтове и домейни, злоупотреби със социални мрежи и профили с цел манипулация, създаване на паника, бизнес измами и обществени въздействия в значителни размери.

Отворен стои въпросът за надеждността на информационни източници в интернет, за достоверност на новините, съобщенията и авторите.

Последствията от кибер заплахи и нерегламентирани действия в информационно-комуникационната среда имат икономическо измерение и морално отражение върху репутацията на фирмите които съхраняват и управляват базите от данни. По оценки на Великобритания ежегодно фирмите търпят загуби от пробив в интелектуална собственост между 18-20 млрд. лири. Показателен за степента и стойността на заплахата е случаят с „Vodafone" ФРГ. В 2014г. фирмата „изпусна" в мрежата данни за два милиона души от 36 млн. свои клиенти (имена, банкови кодове, адреси, сметки), само с бързата намеса рискът от пряка заплаха за клиентите беше минимизиран. Тези случаи и създадените около тях ситуации принуждават правителствата да предприемат активни контрамерки.

Проблемите на информационната сигурност са обект на основни законодателни инициативи от ЕС. Утвърдената Стратегия за кибер сигурност (EU Cyber Security Strategy) фиксира и задължава страните членки да спазват минимални изисквания в сферата на кибер сигурността:

- ✓ направления за профилактиране на кибер мрежи и системи;
- ✓ разкриване на механизми за намаляване на последствията;
- ✓ повишаване на нивото на готовност от бизнес организациите.

Стратегията е насочена към стимулиране създаването на високо-защитени продукти на информационната индустрия и тяхното сертифициране чрез стандарти за киберзащита обхващаща дори облачните технологии. Този документ е съобразен с останалите документи в съюза: Директива за защита на частния животв цифровото пространство (E-Privacy Directive 2002/58/EC), Директива за защита на критичната инфраструктура (European Critical Infrastructures Directive 2008/114/EC), Директива за защита на данните (Data Protection Directive 95/46/EC). Защитата на данните в информационните технологии и личните данни е разгледана в специални директиви на Евро парламента и Евро комисията (Directive 2013/40/EU on attacks against information systems) и (General Data Protection Reglament EC 2016/679 (GDPR). Редица държави са разработили собствени документи – ФРГ е утвърдила Стратегия за безопасност и мерки за взаимодействие между обществени и държавни органи и търговските дружества за взаимопомощ в сферата на кибер сигурността.

Великобритания тества иновационни форми на взаимодействие между бизнеса и държавата (CISP), които задължават операторите на данни да предприемат технически и организационни мерки за защита , а за финансовите институции да проследяват финансови операции.

Важно значение отделят и САЩ със специален указ на президента за формиране на държавна политика за подобряване на условията за кибер сигурност.

Всички разработени стратегически и доктринални документи за информационна сигурност са тясно обвързани със стратегията за интелектуална собственост.

Предприетите мерки срещу лъжливи сведения, интелектуално пиратство, нарушаване на правата в Интернет обхващат:

✓подобряване на откритостта и законосъобразността на политиките и международните преговори;

✓работа с данни за добросъвестно използване;

✓повишаване на ефективността на взаимодействията;

✓засилване на защитата на ITот нарушения в на чужди сайтове домейни от първо ниво за поддръжка на националните фирми и международния пазар.

Прилагането на разработените стратегии предполагат развитие на иновационен процес за генериране и внедряване на новите идеи на пазара за повишаване на икономическия растеж и конкурентно способността на фирмите. Патентните процедури, търговските марки и защитата на авторските права са основно средство за определяне на правата на собственост върху изобретенията и творческите идеи. Тези основни параметри на правната рамка гарантират защитата на интелектуалната собственост и икономическата изгода на инвестициите. Нещо по-вече без IT защита изобретателите, които влагат време и средства за разработване на нови продукти ще са в неизгодно положение спрямо компания, която копира продукта от Интернет без да заплаща труд, талант и т.н.т. При прилагането на тези стратегии ЕС и САЩ визират основно Китай.

Основните изводи от реализацията на подобни стратегии позволяват да се постигнат следните резултати:

- ✓ активизиране на процеса за създаване на интелектуална собственост;
- ✓ повишаване на качествата на интелектуалната собственост и инвестиционния ефект;
- ✓ подобряване защитата на авторските права;
- ✓ засилване влиянието на IP в ключови отрасли на икономиката с преференциално патентоване;
- ✓ производство на висококачествени материали и технологии за екологично развитие и нисковъглеродни емисии;
- ✓ подобряване на трансферите на важната гражданска продукция;
- ✓ права върху лицензии, уставни капитали и активи;
- ✓ подобряване на ефективността на управление на интелектуалната собственост, чрез правилно управление на информационните потоци;
- ✓ поддържащи юридически и патентни услуги при защита на търговските марки, авторските права и др.

Резултатите от интелектуалната дейност и средствата за индивидуализация на стоките, дейностите и услугите са нематериални активи, които имат материално и стойностно измерение. Патентите, промишлените образци, софтуера, ноу хау в производствата и др. съдържащи новаторски технологии и хуманитарни знания в световния пазар имат ценност за своите създатели.

Информацията за характера и съдържанието на новаторските разработки имат огромно значение за днешната конкурентна среда. Тяхното използване и разпространение се допуска при спазване на изключителните права на собственика във всичките форми на прилагане.

В този контекст следва Национална стратегията за кибер сигурност „Кибер устойчива България 2020“ да включи и насоки за по-ефективна защита на високите научно-технически разработки и авторски права. Усъвършенстването на такъв механизъм трябва максимално да защити интересите на собствениците и баланса между частното и общественото. В този аспект под кибер безопасност може да се разбира и защитата на интересите на интелектуална собственост. Кибер заплахите по отношение на интелектуалната собственост са обвързани с нарушаване на правата на собственост на самия обект.

Нарушенията на правата на интелектуална собственост включват неправомерно използване на резултатите от интелектуална дейност или средствата за индивидуализация, които причиняват вреда на притежателя във формата на неполучени приходи или загуби на имидж. Такъв тип заплаха е непосредственото използване на продукта или способа, а негова косвена проява е износа на такъв продукт или въвеждане на контрафактна функция. Заплаха за интелектуалната собственост са кибер атаките срещу възможността за използване на даден продукт, промяна в базата от данни с определена търговска информация, разгласяването на търговски тайни като заплаха за конфиденциалността. Полето на тези заплахи е Интернет от което произтичат някои систематични особености:

- ✓ лесен незаконен достъп до служебни и държавни тайни;
- ✓ хакерски атаки;
- ✓ несанкционирани намеси до програмни средства, вмешателство или промяна в бази от данни;
- ✓ разпространение на невярна информация за лица и фирми;

- ✓ нарушаване на авторските права;
- ✓ незаконно използване на търговски марки, наименования, WEB сайтове и документи;
- ✓ преднамерено използване на географски обекти, търговски обозначения за предизвикване на щети на техния истински притежател.

Трябва да отчетем, че правата върху патенти, търговски марки, микросхеми, софтуер, авторски произведения могат да са държавни, на частни лица и организации, на международни фирми и обединения. Тази особеност предизвиква допълнителна ориентация на мерките за защита към приоретизация на различни нива.

Анализът на концептуалните подходи и националните стратегии за развитие на интелектуалната собственост и насочеността на стратегиите за кибер защита позволява да се направят някои изводи:

Задачата по повишаване на ефективността на защитата на интелектуалната собственост е свързана с развитието разширяването на предмета на дейност на самите обекти към които са насочени заплахите. Проблемите свързани със защитата на документи от различно ниво, глобализацията на интернет търговията и електронните услуги, използването на виртуални валути, възможностите за 3D принтиране значително повишава изискванията към кибер безопасността. Възниква необходимост за правно регулиране на отговорностите за Интернет доставчиците и информационните посредници, които са отговорни за съхранението и разпространението на материалите в мрежата. Правила за отговорност следва да се прилагат и към лицата получаващи достъп до масивите от данни, чрез рестрикции за забрана на достъпа, ограничения в ползване на книги филми без съгласието на собственика.

Значението на защитата на ценни технологии, информация в мрежите нараства с развитие на техногенната глобализация, аутсорсинга и удължаването на веригите от потребители. Увеличава се риска от разпространение на крадена информация в трети страни за търговски цели. Повишена задълбоченост следва да се отдели на промишления шпионаж в полза на конкурентите прилаган от ползвателите на определени масиви от данни в процеса на своята работа.

References:

1. EU Directive on the protection of undisclosed know-how and business information (trade secrets)against their unlawful acquisition, use and disclosure http://ec.europa.eu/
2. Национална стратегията за кибер сигурност „Кибер устойчива България 2020"
3. Stoyanova V, Possibilities for the application of social networks in transmission of secret information, International Scientific Conference CONFSEC ISSN print 2603-2945, ISSN online 2603-2953, year 1, ISSUE 2(2), 2017, Avaible from http://confsec.eu/sbornik/1-2017.pdf
4. Friedrich Geiger and Archibald Preuschat. Hacker Hits Vodafone in Germany. Wall Street Journal (Sept. 12, 2013).
5. Подробнее см.: Карцхия А.А. Права промышленной собственности в российском праве: навстречу вызовам современности. Lambert Academic Publishing. Germany,2013.

COORDINATION DECISIONS FOR IMPLEMENTING CIVIL PROTECTION IN THE EUROPEAN UNION

Hristo A. Desev

***Abstract**: The significant increase in the number, nature and severity of natural disasters occurring in recent years, as well as the ever-increasing costs of coping with them, have led to the need to analyze a Civil Protection Disaster Response System. EU solutions facilitate the exchange of good practices and identify recommendations for improving the policy and practice of disaster management operations. Programs encourage the mutual learning and understanding process and facilitate the internal policy dialogue between states and experts.*

***Keywords**: disaster, management operations, good practices.*

КООРДИНАЦИОННИ РЕШЕНИЯ ЗА ОСЪЩЕСТВЯВАНЕ НА ГРАЖДАНСКАТА ЗАЩИТА В ЕВРОПЕЙСКИЯ СЪЮЗ

Христо А. Десев

Национален военен университет " В. Левски" гр. Велико Търново
Факултет "Артилерия ПВО и КИС" гр. Шумен

Количеството и сериозността на природните и причинените от човека бедствия през последните години показва значително нарастване. Това предполага, че бъдещите бедствия ще бъдат по-драстични и комплексни, с по-значителни и дългосрочни последици. Тези явления вследствие на промените на климата и на потенциалните взаимодействия между няколко природни и техногенни опасности, изискват един интегриран подход към управлението на защитата при бедствия.

Защитата следва да се насочи приоритетно и да обхваща преди всичко населението, но и околната среда и имуществото, включително културното наследство, при всички видове природни и причинени от човека бедствия, които възникват на територията на всяка една държава.

При всички тези заплахи се налага изграждане на работещ механизъм за съдействие, гражданска защита и друга спешна помощ в допълнение към способностите за реагиране на засегнатата държава. По отношение на бедствията, причинени от терористични актове, ядрени или радиационни аварии, мероприятията следва да обхващат само действията за готовност и реагиране в областта на гражданската защита.

Европейският съюз (ЕС) със своите директиви и решения (Директива 1313/2013/ЕС) насърчава солидарността и подпомага, допълва и улеснява координацията на действията на държавите членки в областта на гражданската защита. Основната цел е подобряване ефективността на системите за превенция, готовност и реагиране при природни и причинени от човека бедствия. Съюза предоставя възможни решения за осигуряване на еднакви условия за изпълнение на дейностите по защитата, като:

- ✓ съгласува оперативните процедури за реакция при бедствия в рамките на Съюза и извън него;
- ✓ подобрява процеса на организацията на обмена на информация;
- ✓ други способности за реагиране и експерти;
- ✓ целите по отношение на капацитет, изискванията за качеството и оперативната съвместимост, както и процедурата за сертифициране и регистриране на екипите;
- ✓ установяването на модули и изпращане на експертните екипи;

- ✓ оперативните изисквания за функционирането и оперативната съвместимост на модулите;
- ✓ организирането на програми за обучение, рамката за ученията и програмата за отчитане на извлечените поуки;

ЕС следва създава обща политическа рамка, насочена към непрекъснато подобряване на степента на готовност на системите и службите за гражданска защита, на техния персонал и на населението в рамките на Съюза. Това включва програма за учения, програма за извлечени поуки, както и програми за обучение и мрежа за обучение на равнището на Съюза и държавите членки в областта на превенцията, готовността и реагирането при бедствия.

Държавите от съюза набелязват предварително модули за реагиране и експертни способности в рамките на службите за гражданска защита Те отчитат факта, че съставът на модулите или на другите способности за реагиране зависи от вида на бедствието и конкретното бедствие.

Изграждането на модули за операции за оказване на помощ в областта на гражданската защита, състоящи се от ресурсите на една или повече държави членки, се задълбочава за да се засили и постигне пълна оперативна съвместимост и сътрудничеството. Модулите следва да се организират на равнището на държавите членки и да бъдат подчинени на тяхното командване и контрол.

Модулите обединяват ресурсите на една или повече държави и могат да изпълняват предварително определени задачи в областта на реагирането в съответствие с установените международни насоки и са в състояние:

- ✓ да бъдат изпращани в много кратък срок след искане за помощ, подадено чрез ERCC;
- ✓ да работят самостоятелно и независимо през определен период от време;
- ✓ да са оперативно съвместими с други модули;
- ✓ провеждат обучение и учения, за да изпълнят изискването за оперативна съвместимост;
- ✓ да си сътрудничат по целесъобразност с други органи на Съюза и/или международни институции, по-специално ООН.

Експертите които биха могли да изпратят като членове на екипите се определят предварително доброволен принцип, определят се и възможността да осигурят при необходимост други способности за реагиране.

Чрез своите решения ЕС подпомага, допълва и улеснява координирането на действията на държавите членки при изпълнението на следните общи специфични цели:

- ✓ повишаване на степента на готовност за реагиране при бедствия на равнище на държавите членки и на Съюза;
- ✓ улесняване на бързо и ефикасно реагиране при бедствия или непосредствена заплаха от такива; както и увеличаване на обществената осведоменост и готовност за бедствия.
- ✓ постигане на високо ниво на защита срещу бедствия чрез предотвратяване или ограничаване на потенциалните въздействия, чрез насърчаване на култура на превенция и чрез подобряване на сътрудничеството между службите за гражданска защита и съответни други служби;

Използването на военни средства под гражданско ръководство като крайно средство може да представлява важен принос към реакцията при бедствия. Когато се приеме за уместно да се използват военен капацитет при операции за гражданска защита, сътрудничеството с военните органи следва да се подчинява на реда и условията, установените процедури и критерии.

Механизмите на ЕС отделят специално отношение към превенцията и подготовката на държавите за осъществяването на гражданската защита. За да изпълни целите и да осъществи задачите в областта превенцията са набелязани отделни групи от мероприятия:

- ✓ предприемат се действия за подобряване на базата от знания за рисковете от бедствия и улеснява обмена на знания, най-добри практики и информация, включително сред държавите членки с общи рискове;
- ✓ подкрепя се и насърчава дейностите на държавите членки по оценка и картографиране на рисковете чрез обмен на добри практики, както и улесняване на достъпа до специфични знания и експертен опит по въпроси от общ интерес;
- ✓ осъществява и редовно актуализира междусекторен преглед на рисковете от природни и предизвикани от човека бедствия, като се възприема съгласуван подход на политиките, които имат отражение върху превенцията на бедствията;

✓ насърчава обмен на добри практики за подготовка на националните системи за гражданска защита с цел справяне с последствията от изменението на климата;

Процесът на повишаване на ефективността от мероприятията по защитата от бедствия в голяма степен зависи от състоянието на системата за управление.

В своето решение ЕС определя създаването на координационен център за реагиране при извънредни ситуации (ERCC), който да гарантира денонощен (24/7) оперативен капацитет. Той съгласува и съдейства за разработването и по-доброто интегриране на транснационални системи от общоевропейски интерес за откриване, ранно предупреждение и оповестяване, за да се осигури възможност за бързо реагиране между националните системи за ранно предупреждение и оповестяване и връзките им с ERCC и CECIS.

Тези системи трябва да отчитат и доразвиват съществуващите и бъдещите източници и системи за информация, мониторинг и откриване, да създават и управляват способността за мобилизиране и изпращане на експертни екипи. Системите следва да са отговорни за:

✓ улесняване на координацията на помощта на място в рамките на реагирането при бедствия и осъществяване на връзка с компетентните органи на държавата, поискала помощ;

✓ подпомагане на държавата, поискала помощ, с експертен опит относно действията за превенция, готовност или реагиране;

✓ да създават и поддържат способност за предоставяне на логистична подкрепа за експертните екипи;

✓ разработване и поддръжка на мрежа от обучени експерти от държавите членки, които могат да бъдат мобилизирани в кратък срок, за да подпомагат ERCC при извършване на мониторинг на информацията и улесняване на координацията;

✓ улесняване координацията при предварителното разполагане на способности на държавите членки за реагиране при бедствия в рамките на Съюза;

✓ подпомагане усилията за подобряване на оперативната съвместимост на модулите и други способности за реагиране, като взема под внимание най-добрите практики на равнище на държавите членки и на международно равнище;

✓ предприемане на необходимите действия в рамките на компетентността си за разработване и актуализиране на насоки относно подкрепата от приемащата държава въз основа на оперативния опит;

В процеса на прилагане на решенията на ЕС, системата за защита при бедствия в нашата държава показва недостатъци и проблеми в аспекти, които са съществени за нейното правилно функциониране.

При осъществяването на дейности в различните сектори се оказва, че крайните резултати от същите в повечето случаи не кореспондират помежду си, т.е. липсва единна политика при реализиране на мерките за защита при бедствия.

За правилното функциониране на системата за защита при бедствия е необходима по-добра координация и разпределение на отговорностите по изпълнението на дейностите свързани с превенцията, готовността, реагирането и възстановяването при бедствия, с по-активно участие на всички заинтересовани страни на национално, регионално и местно ниво.

Изградените в тази връзка правни механизми не са достатъчно ясни и прецизни, което води до значителни затруднения при осъществяване на защитата при бедствия. Липсата на яснота, относно функциите на отделните звена в системата за защита при бедствия, води до това, че като цяло институциите в Република България не припознават своите задължения и отговорности, произтичащи от Закона за защита при бедствия, с изключение на регулаторните им такива, възложени със специални закони.

Съществен проблем в процеса на управление на риска от бедствия на областно и общинско ниво са недостатъчния експертен капацитет, слабата координация и обмен на информация между отделните ведомства. Това води до неосигуряването на междусекторен подход по отношение на намаляване на риска от бедствия.

Практиката показва, че предвидени механизми за справяне с бедствията, като „въвеждане на план за защита при бедствия" и „обявяване на бедствено положение", се използват хаотично,

без да се разбира същността им. Следователно е необходимо прецизиране на реда за обявяване и прекратяване на режим „бедствено положение", с цел ограничаване на субективното му използване от страна на компетентните органи.

В отговор на тези различия и в стремежа за унифициране на подходите към защитата на населението са коригирани отделни страни от координационния процес. Тези промени са с цел осигуряване на силно институционално начало на управлението на риска от бедствия, като приоритет на национално, регионално и местно ниво.

Създаденият Съвет за намаляване на риска от бедствия за подпомагане изпълнението на дейностите на Министерския съвет по формирането и осъществяването на държавната политика в областта на защитата при бедствия. Той, разработва и предлага на Министерския съвет Националната стратегия за намаляване на риска от бедствия с перспектива за изпълнение не по-малка от 10 години. Предвижда се създаването на съвети за намаляване на риска от бедствия и към областните управители и кметовете на общини, които ще изпълняват ролята на платформи за намаляване на риска от бедствия на съответните нива. Това ще позволи ангажиране на по-широк кръг от субекти, имащи ангажименти към защитата при бедствия, като изрично са посочени членовете на тези съвети на областно и общинско ниво.

Разширяват се възможностите за ранно предупреждение, като комплекс от дейности за разпространяване на информация към обществеността за предстоящо бедствие в определена територия, чрез използване на съвременните постижения на технологиите. Създават се предпоставки за подобряване на информираността на обществото.

Ранното предупреждение изисква:

1. осъществяване на наблюдение за наличието на признаци за предстоящо бедствие;
2. анализ на данните от наблюдението по т. 1;
3. вземане на решение от страна на компетентните органи;
4. разпространение на предупредителна информация за предстоящо бедствие;
5. предприемане на подходящи действия.

Множеството бедствия и инциденти показаха, че провежданото обучение и практическа подготовка, комуникацията и координацията между органите на изпълнителната власт, силите за реагиране, доброволните формирования и населението, все още не е на нужното ниво. За осигуряването на по-голяма степен на защита и устойчивост срещу бедствия е необходимо провеждането на тренировки и учения по единен подход, с цел оценка и подобряване на способностите за реагиране. Обучението за защита при бедствия е предпоставка за правилно поведение, с оглед защитата на живота и здравето на населението. С измененията се цели в обучението за защита при бедствия да попаднат, освен органите на изпълнителната власт, както е в момента, и другите държавни органи. Обучението за защита при бедствия на държавните органи е предпоставка за осигуряване на ефективни и координирани действия.

Предвидените промени в правните норми и изпълнението на препоръките от решенията на Комисията на ЕС, се очаква да допринесат за цялостното подобряване на системата за защита при бедствия на национално, регионално и местно ниво, като се премине от система за управление, която се фокусира основно върху реакцията, към цялостна такава, която обхваща еднакво приоритетно и останалите фази на цикъла за управление (превенция, готовност, реагиране и възстановяване) при бедствия.

References:

1. Закон за защита при бедствия, изм. ДВ. бр.51 от 05.07.2016
2. Национален план за защита при бедствия.
3. Директива 1313/2013/ЕС.
4. Стратегия за защита на обектите от критичната инфраструктура в Р България - 2014-2020.
5. Гавраилов Е. Безопасност и защита на населението. Теория, традиции, практика. Варна : Варненски свободен университет „Черноризец Храбър" 2016.

S. N. Chanev,

STATISTICAL MODEL OF SURFACE-TO-AIR MISSILE SYSTEM

Stoyan N. Chanev

"Vasil Levski" National Military University, "Artillery, Air-defence and Communication and Information Systems" Faculty, "Air Defence" Department; town of Shumen

Abstract: *Presenting of surface-to-air missile system like statistical model of mass service system by simulation modeling by MS Excel allows determining mean of the number of destroying enemy aircrafts and estimating its combat effectiveness.*

Keywords: *statistical model, simulation modeling, surface-to-air missile system, mass service system.*

СТАТИСТИЧЕСКИ МОДЕЛ НА ЗЕНИТНОРАКЕТЕН КОМПЛЕКС

Стоян Н. Чанев

При оценяване на бойната ефективност на създадена групировка за противовъздушна отбрана (ПВО) е необходимо да се знае дали всички цели ще бъдат обстреляни или част от тях ще преминат през системата на зенитния огън (СЗО) необстреляни.

Използването на системи за масово обслужване (СМО) при оценката на бойната ефективност позволява изграждането на модели и последващото им изследване. При аналитично моделиране на процесите [2], като недостатък следва да се отбележат трудностите възникващи при едновременно действие на разнотипни зенитно-ракетни комплекси (зрк), поради различния им цикъл на стрелба ($t_{ц.с}$), както и разликата в $t_{ц.с}$ за еднотипни зрк, но действащи в различни условия на обстановката (смущения, наличие на ракети на пусковите установки).

Поради горепосоченото е удачно да се използва симулационно моделиране.

Всеки симулационен модел се състои от следните блокове [1]:

- дефиниране на възможните състояния на системата;
- идентифициране на възможни състояния на системата, които биха могли да се появят;
- идентифициране на възможни събития, които биха могли да променят състоянието на системата;
- часовник, който да отчита времето на симулацията;
- инструменти за генериране на случайни числа.

След формулирането на симулационния модел е необходимо да се проведат числени експерименти и получените резултати от симулациите да се обработят и анализират. В [4] е предложен друг поглед при анализа на статистически модели.

Основните данни, които са необходими за построяване на статистически модел на зрк, представен като СМО (симулационно моделиране) са плътността на налета от въздушни цели (λ) и плътността на потока от обслужени заявки (μ), както и интервала между отделните заявки (Δt).

Плътността на потока от заявки λ към определен тип зрк е възможно да се определи чрез матрица на целеразпределението (МЦР), моделираща дейността на старшия команден пункт (КП) на групировката за ПВО.

Плътността на потока от обслужени заявки или интензивността на обслужването μ се определя от израза:

(1) $\mu = \frac{1}{\bar{t}_{ц.с}}$,

където $\bar{t}_{ц.с}$ е математическото очакване на средния цикъл на стрелбата на зрк.

При еднотипни комплекси:

(2) $\mu = m\mu_i$,

тогава:

(3) $t_{ц.с} = \frac{t_{цi}}{m}$,

където m е броя на еднотипните зрк.

Веднага след започване на работа процесът в СМО няма да бъде стационарен, а ще възникне преходен процес и едва след неговото затихване вероятностните характеристики на системата практически няма да зависят от времето. Доказано е [2], че при процеси с продължителност по-голяма от (2÷3) $t_{ц.с}$ може да се използват зависимостите, получени за стационарен процес, т.е. при

(4) $T_н = (2 \div 3)t_{ц.с}$

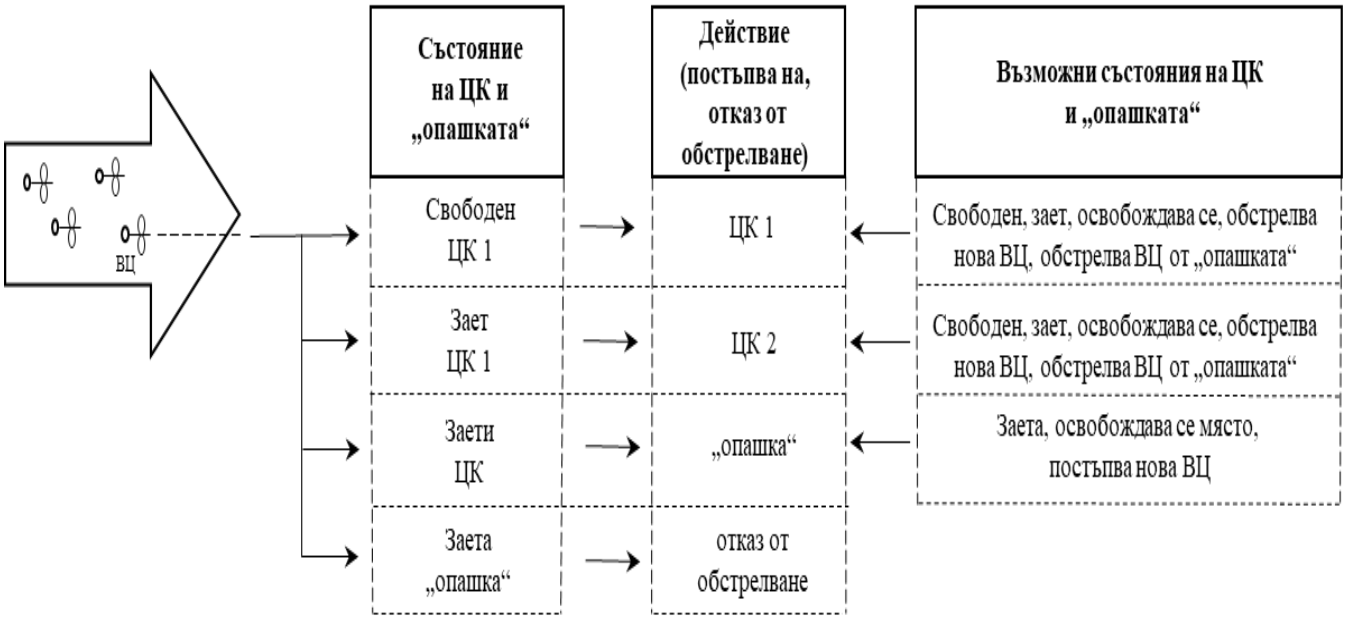
За да получим реалистични стойности за интересуващите ни величини са необходими голям брой симулирани времеви интервали [1], което ще осигури и по-голяма точност на опитните данни при анализа и статистическата обработка на резултатите от симулацията. В случая броя на симулираните интервали ще е максимално възможния за MS Excel.

Интервала между заявките/ВЦ следва да се определи така, че да не е възможно едновременното им постъпване в СМО. Отчитайки най-тежкия вариант – сгъстен боен ред на ВП и минималните взаимни отстояния на летателните апарати (ЛА), Δt = 0,005 [min] осигурява изпълнението на това условие.

Нека разгледаме зрк, представен като СМО с ограничено време за чакане в опашката (ОВЧ) с два канала на обслужване (целеви канала).

Цикъла на стрелбата, а оттам и интензивностите на обслужване μ_1 и μ_2 на двата целеви канала (ЦК) се различават поради факта, че към началото на налета броят на боеготовите ракети във всеки канал е различен и е отчетено времето за презареждане. ЦК 1 се явява старши и при равни други условия ВЦ се разпределя на него.

Съгласно [1] на фиг.1 е показан алгоритъм на модел на зрк (СМО) и възможните състояния на ЦК и „опашката“, в таблица 1 – модел на двуканална СМО с ОВЧ описващ дейността на зрк за малки разстояния - Тип II (далечна граница на ЗП – 25 km),



Фиг. 1. Алгоритъм на модел на зрк (СМО) и възможните състояния на ЦК и „опашката“

Таблица 1

	A	B	C	D	E	F	G	H	I	J	K
1											
2		Вероятност за отказ от обстрелване на ВЦ (Ротк):	0,07692308		зрк - тип II (параметри)						
3		Заети ЦК (средно):	1,2477109								
4		Брой ВЦ в "опашката" (средно):	0,27273837		Δt =	0,005					
5					λ =	1,1					
6					μ1 =	1,2					
7					μ2 =	0,3					
8					L оп. =	2					
9											
10	Начало (t = 0)	Генериране на въздушна цел (ВЦ)	0,69044842	0,998646	…	0,93312	0,87255	…	0,78736	0,19427	…
11		Генериране на обстрелване на ВЦ от целеви канал (ЦК) 1	0,04192553	0,817536	…	0,31701	0,71229	…	0,12697	0,55928	…
12		Генериране на обстрелване на ВЦ от ЦК 2	0,54266237	0,637689	…	0,84888	0,54565	…	0,34781	0,36325	…
13		№ на стъпката	1	2	…	312	313	…	16381	16382	…
14	0	Време (t), m	0,005	0,01	…	1,56	1,565	…	81,905	81,91	…
15		Постъпване на цел	0	0	…	0	0	…	0	0	…
16		Обстрелване на ВЦ от ЦК 1	0	0	…	0	0	…	0	0	…
17		Обстрелване на ВЦ от ЦК 2	0	0	…	0	0	…	0	0	…
18		ЦК 1 се освобождава	0	0	…	0	0	…	0	0	…
19		ЦК 2 се освобождава	0	0	…	0	0	…	0	0	…
20		ЦК 1 обстрелва нова ВЦ	0	0	…	0	0	…	0	0	…
21		ЦК 2 обстрелва нова ВЦ	0	0	…	0	0	…	0	0	…
22		ЦК 1 обстрелва ВЦ от "опашката"	0	0	…	0	0	…	0	0	…
23		ЦК 2 обстрелва ВЦ от "опашката"	0	0	…	0	0	…	0	0	…
24		В "опашката" се освобождава място	0	0	…	0	0	…	0	0	…
25		В "опашката" постъпва нова ВЦ	0	0	…	0	0	…	0	0	…
26	0	ЦК 1 е зает с обстрелване на ВЦ	0	0	…	1	1	…	1	1	…
27	0	ЦК 2 е зает с обстрелване на ВЦ	0	0	…	1	1	…	1	1	…
28	0	Заети места от ВЦ в "опашката"	0	0	…	0	0	…	2	2	…
29	0	Отказ от обстрелване на ВЦ	0	0	…	0	0	…	0	0	…
30	0	Всичко ВЦ	0	0	…	3	3	…	91	91	…
31	0	Всичко откази	0	0	…	0	0	…	7	7	…
32	0	Заети ЦК	0	0	…	2	2	…	2	2	…
33		Средна дължина на "опашката"	0	0	…	0	0	…	0,01	0,01	…
34		Заетост на ЦК	0	0	…	0,01	0,01	…	0,01	0,01	…

Колона А – начално състояние на системата ($t = 0$).
E2:F8 – входни данни за модела.
B2:C4 – изходни данни за модела при една реализация.

По-долу са описани елементите на модела, логическите връзки между тях и реализацията им в MS Excel в следния ред:

№ на реда (клетка) / елемент / логически връзки / реализация в MS Excel:

10, 11, 12 / Генериране на постъпването на ВЦ в системата, както и обстрелването на ВЦ от целевите канали ЦК 1 и ЦК 2 / извършва се с помощта на генератор на случайни числа в интервала (0,1) / C10, 11, 12=RAND( ).

13 / Номер на стъпката / от 1 до n (последователно нарастващи числа) в хода на симулацията / C13=1, D13=C13+1, …

14 / Време (t), [min] / 0 за началото на симулацията и нарастващо с Δt за всяка следваща стъпка / C14=$F$4, D14=$F$4+C14, …

15 / Постъпване на цел / ако случайното число (0,1) при генерирането на ВЦ е по-малко от $\lambda\Delta t$ в системата постъпва цел / C15=IF(C10<$F5*$F$4;1;0), …

16 / Обстрелване на ВЦ от ЦК 1 / ако $\Delta t\mu_1$ > от случайното число (0,1) при генериране на обстрелване на ВЦ от ЦК 1 то ВЦ се обстрелва от ЦК 1 / C16=IF($F$4*$F$6>C11;1;0), …

17 / Обстрелване на ВЦ от ЦК 2 / ако $\Delta t\mu_2$ > от случайното число (0,1) при генериране на обстрелване на ВЦ от ЦК 2 то ВЦ се обстрелва от ЦК 2 / C16=IF($F$4*$F$7>C12;1;0), …

18 / ЦК 1 се освобождава / ако канала не е бил зает или канала е бил зает и е обстрелял целта, то ЦК 1 се освобождава / C18=IF(AND(A26=1;C16=1);1;0), D18=IF(AND(C26=1;D16=1);1;0), …

19 / ЦК 2 се освобождава / ако канала не е бил зает или канала е бил зает и е обстрелял целта, то ЦК 2 се освобождава / C19=IF(AND(A21=1;C17=1);1;0), D19=IF(AND(C27=1;D17=1);1;0), …

20 / ЦК 1 обстрелва нова ВЦ / ако ЦК 1 е бил зает с обстрелване на ВЦ и се е освободил, и в системата постъпи нова ВЦ, то ЦК 1 обстрелва нова ВЦ / C20=IF(AND(A26-C18=0;C15);1;0), D20=IF(AND(C26-D18=0;D15);1;0), …

21 / ЦК 2 обстрелва нова ВЦ / ако ЦК 2 е бил зает с обстрелване на ВЦ и се е освободил, и ЦК 1 (старши канал) не обстрелва нова цел, и в системата постъпи нова ВЦ, то ЦК 2 обстрелва нова ВЦ / C21=IF(AND(A27-C19=0;C20=0;C15);1;0), D21=IF(AND(C27-D19=0;D20=0;D15);1;0), …

22 / ЦК 1 обстрелва ВЦ от „опашката“ / ако ЦК 1 е бил зает с обстрелване на ВЦ и се е освободил, и ЦК 1 не обслужва нова ВЦ (в системата не е постъпила нова ВЦ), и има ВЦ заела място в „опашката“, то ЦК 1 обстрелва ВЦ от „опашката“ / C22=IF(AND(A26-C18=0;C20=0;A28>0);1;0), D22=IF(AND(C26-D18=0;D20=0;C28>0);1;0), …

23 / ЦК 2 обстрелва ВЦ от „опашката“ / ако ЦК 2 е бил зает с обстрелване на ВЦ и се е освободил, и ЦК 2 не обслужва нова ВЦ (в системата не е постъпила нова ВЦ), и има ВЦ заела място в „опашката“ след евентуално обслужване на ЦК 1 на ВЦ от „опашката“, то ЦК 2 обстрелва ВЦ от „опашката“ / C23=IF(AND(A27-C19=0;C21=0;A28-C22>0)1;0), D23=IF(AND(C27-D19=0;D21=0;C28-D22>0)1;0), …

24 / В „опашката“ се освобождава място / ако ЦК 1 или ЦК 2 обстрелва ВЦ от „опашката“, то в „опашката“ се освобождава място / C24=C22+C23, …

25 / В „опашката“ постъпва нова ВЦ / ако в системата постъпи нова ВЦ и двата ЦК не обслужват нова ВЦ, и разликата между броя на ВЦ в „опашката“ и обслужваните от двата ЦК ВЦ от опашката е по-малка от максимално допустимата дължина на „опашката“ (L_{on}), то в „опашката“ постъпва нова ВЦ / C25=IF(AND(C15=1;C20=0;C21=0;A28-C22-C23<$F$8)1;0), D25=IF(AND(D15=1;D20=0;D21=0;C28-D22-D23<$F$8)1;0), …

26 / ЦК 1 е зает с обстрелване на ВЦ / ако ЦК 1 не се е освободил или обстрелва нова ВЦ, или обстрелва ВЦ от „опашката“ / C26=A26-C18+C20+C22, D26=C26-D18+D20+D22, …

27 / ЦК 2 е зает с обстрелване на ВЦ / ако ЦК 2 не се е освободил или обстрелва нова ВЦ, или обстрелва ВЦ от „опашката“ / C27=A27-C19+C21+C23, D27=C27-D19+D21+D23, …

28 / Заети места от ВЦ в „опашката“ / броя на местата в „опашката“, намалени с броя ВЦ от „опашката“ обстрелвани от двата ЦК плюс постъпилите нови ВЦ в „опашката“ / C28=A28-C22-C23+C25, D28=C28-D22-D23+D25, …

29 / Отказ от обстрелване на целта / ако в системата постъпи нова ВЦ и двата ЦК не обстрелват нова ВЦ, и в „опашката“ не постъпи нова ВЦ, то имаме отказ от обстрелване на ВЦ / C29=IF(AND(C15=1;C20=0;C21=0,C25=0);1;0), …

30 / Всичко ВЦ / броя на ВЦ постъпили в системата (сумирани нови ВЦ) по време на симулацията / C30=A30+C15, D30=C30+D15, …

31 / Всичко откази / броя на ВЦ постъпили в системата и получили отказ от обстрелване по време на симулацията / C31=C29, D31=C31+D29, …

32 / Заети ЦК / броя на едновременно заетите с обстрелване на ВЦ ЦК в системата / C32=C26+C27, …

33 / Средна дължина на „опашката“ / заетите места от ВЦ в „опашката“ умножени по стойността на Δt / C33=C28*$F$4, …

34 / Заетост на ЦК / заетите ЦК умножени по стойността на Δt / C34=C32*$F$4, …

C2 / Вероятност за отказ от обстрелване на ВЦ ($P_{отк}$) / C2=XFD31/XFD30.

C3 / Заети ЦК (средно) / C3=SUM(C34:XFD34)/XFD14.

C4 / Брой ВЦ в „опашката“ (средно) / C4=SUM(C33:XFD33)/XFD14.

Всяка реализация на модела се води за един опит (експеримент). За статистическа обработка на получените резултати е необходимо провеждането на множество опити.

MS Excel е в състояние да изпълни автоматично желания брой симулации.

За целта е необходимо да се създаде таблица в която освен резултатите от симулацията в първия ред се добавя и колона с нужния брой симулации (1000).

Чрез използване на вградени менюта/подменюта - Data/What-If-Analysis/Data table в таблицата с резултатите се генерират необходимия брой опити - таблица 2.

Таблица 2

Брой симулации:	Вероятност за отказ от обстрелване на ВЦ (Ротк):	Заети ЦК (средно):	Брой ВЦ в "опашката" (средно):
1	0,101851852	1,532352582	0,492186546
2	0,178217822	1,506714687	0,497802466
…	…	…	…
583	0,10989011	1,414418264	0,394213161
…	…	…	…
1000	0,091954023	1,237577829	0,300451715

За определяне на вероятността за отказ от обстрелване на ВЦ - $P_{отк}$, а оттам и на вероятността за обстрелване на ВЦ:

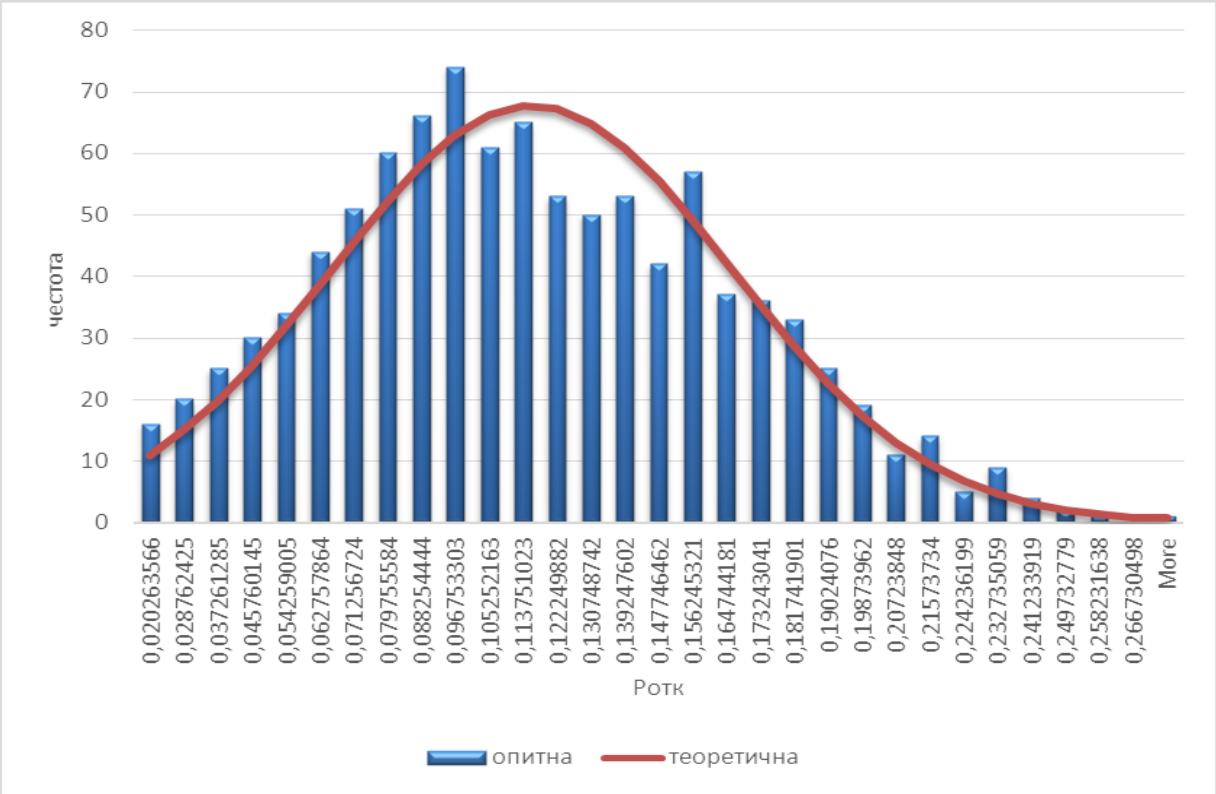
(5) $$P_{обс} = 1 - P_{отк},$$

следва да се извърши статистически анализ на получените резултати.

Чрез използване на вградени менюта/подменюта - Data/Data Analysis/Descriptive Statistics и Data/Data Analysis/Histogram са получени: статистически анализ на опитните данни (таблица 3) и хистограма на опитните данни (фигура 2).

Таблица 3

Column 1	
Mean	0,111753146
Standard Error	0,00157961
Median	0,106382979
Mode	0,166666667
Standard Deviation	0,049951641
Sample Variance	0,002495166
Kurtosis	-0,427420683
Skewness	0,270502466
Range	0,263464652
Minimum	0,011764706
Maximum	0,275229358
Sum	111,7531457
Count	1000



Фиг. 2. Хистограма на опитните данни

Проверка на хипотеза на закона за разпределение

Критериите за проверка на такива статистически хипотези са известни като критерии на съгласие. Те са основни за различието между теоретичния закон $F_t(x)$ и емпиричния закон на разпределение $F(x)$, построен чрез опитните данни. Ако означим с $F_t(x)$ функцията на разпределение на предполагаемия закон, то хипотезата, която искаме да проверим може да се формулира така:

(6) $H_0: F(x) = F_t(x)$

От всички критерии на съгласие най-голямо приложение е намерил критерият на Пирсън (χ^2 – критерий) [3]:

(7) $\chi^2 = \sum_{j=1}^{m'} \frac{(v_j - v_{tj})^2}{v_{tj}}$,

където: m' - броя на класовете (интервалите) след евентуално обединяване;

v_j – опитна честота;

v_{jt} – теоретична честота (на фиг. 2 – в червен цвят).

Критерият на съгласие χ^2 изисква всички теоретични честоти да бъдат по-големи от 5. Ако в някои класове това условие е нарушено, те се присъединяват към съседните класове (по-близо разположени до модата на емпиричното разпределение), като броят на класовете става $m' = m - \Delta$, където Δ е броят на присъединените класове.

Броя на класовете и границите им се определя чрез менюта/подменюта - Data/Data Analysis/Histogram.

Теоретичната честота във всеки клас се определя чрез използване на стати-стическата функция в MS Excel „= NORM.DIST (x;mean;standart_dev;cumulative)" (колона 5 в таблица 4), където x е дясната граница на класа, а останалите стойности се вземат от таблица 3. Теоретичната честота се получава (колона 6 в таблица 4):

(8) $v_{jt} = p_j n$,

където: p_j – вероятността за попадане на случайната величина в $j^{-тия}$ клас;

n – броя на опитите.

Опитната честота (v_j) е дадена в колона 7 на таблица 4.

χ^2 (колона 8) се определя в съответствие с формула (7).

Поради факта, че не всички v_{jt} са по-големи от 5 е извършено присъединяване в съседни класове, а броят на класовете е редуциран до m'.

За приемане/отхвърляне на H_0 се използва статистическата функция „=CHISQ.DIST(x;deg_freedom;cumulative)" (последен ред в таблица 4), където x е сумата от колона 8, deg_freedom – степени на свобода - 24, определят се като разлика между броя на класовете (m') и броя на случайните величини (3 – mean, Standard Deviation, χ^2). Задава се критичен праг (обикновено 0,95). Ако стойността на статистическата функция е по-голяма, опитните данни не противоречат на нулевата хипотеза H_0 – както е в случая.

Таблица 4

№ m	№ m'	Граници на класа		Ft(x)	ν_{tj}	ν_j	χ^2
1	1		0,0117647	0,0226582	22,658245	2	18,834781
2	2	0,0117647	0,0202636	0,0335083	10,850028	16	2,4444367
3	3	0,0202636	0,0287624	0,0483144	14,806159	20	1,8219436
4	4	0,0287624	0,0372613	0,0679441	19,629627	25	1,4692539
5	5	0,0372613	0,0457601	0,0932277	25,283653	30	0,8797749
6	6	0,0457601	0,054259	0,1248669	31,63922	34	0,176151
7	7	0,054259	0,0627579	0,1633323	38,465369	44	0,7963564
8	8	0,0627579	0,0712567	0,2087654	45,433085	51	0,682114
9	9	0,0712567	0,0797556	0,2609008	52,135407	60	1,1863689
10	10	0,0797556	0,0882544	0,3190243	58,12347	66	1,0673783
11	11	0,0882544	0,0967533	0,381979	62,954754	74	1,9378593
12	12	0,0967533	0,1052522	0,4482256	66,246627	61	0,4155245
13	13	0,1052522	0,113751	0,5159519	67,726286	65	0,1097452
14	14	0,113751	0,1222499	0,58322	67,268075	53	3,0263681
15	15	0,1222499	0,1307487	0,6481311	64,911102	50	3,4253149
16	16	0,1307487	0,1392476	0,7089848	60,853731	53	1,0135959
17	17	0,1392476	0,1477465	0,7644109	55,426018	42	3,2522265
18	18	0,1477465	0,1562453	0,8134563	49,045411	57	1,2901408
19	19	0,1562453	0,1647442	0,8556202	42,163951	37	0,6324452
20	20	0,1647442	0,173243	0,8908364	35,216194	36	0,0174451
21	21	0,173243	0,1817419	0,9194124	28,57602	33	0,6848959
22	22	0,1817419	0,1902408	0,9419403	22,527823	25	0,2712938
23	23	0,1902408	0,1987396	0,9591945	17,254202	19	0,1766417
24	24	0,1987396	0,2072385	0,9720334	12,838924	11	0,2633899
25	25	0,2072385	0,2157373	0,9813149	9,2815501	14	2,3987124
26	26	0,2157373	0,2242362	0,9878338	6,5188421	5	0,353879
27	27	0,2242362	0,2327351	0,9922819	12,166224	17	1,9205126
28		0,2327351	0,2412339	0,9952307			
29		0,2412339	0,2497328	0,9971299			
30		0,2497328	0,2582316	0,9983183			
31		0,2582316	0,2667305	0,9990407			
32		0,2667305					
						SUM	50,54855
							0,998795

Имайки предвид статистическия анализ на получените резултати за $P_{отн}$ може да получим математическото очакване на броя на поразените цели от ЗРК тип II:

(9) $M[x] = N_{обс}P_n$,

където $N_{обс}$ – броя на обстреляните цели:

(10) $N_{обс} = \lambda t_н P_{обс}$,

където: λ – плътността на налета;
$t_н$ – продължителността на налета;
$P_{обс}$ – вероятността за обстрелване на целта – определя се съгласно формула (5).
P_n – вероятност за унищожаване на целта с n ракети, броя на ракетите се назначава в зависимост от условията на стрелбата, вида на целта и разполагаемия брой ракети и обикновено е 2.

(11) $P_n = 1 - (1 - P_1)^n$,

където P_1 – вероятност за унищожаване на целта с 1 ракета. Дава се в документацията на зрк и приема различни стойности в зависимост от условията на стрелбата, разстоянието до целта и противодействието.

Пълния израз за *M[x]* ще приеме вида:

(12) $M[x] = \lambda t_н(1 - P_{отк})[1 - (1 - P_1)^n]$.

Нека $\lambda = 1{,}1$; $t_н = 11\ min$; $P_{отк} = 0{,}11$ (съгласно модела), $P_1 = 0{,}6$ (за маневрираща, групова цел, оказваща активно противодействие и летяща под прикритие на активни и пасивни смущения); $n = 2$. Съгласно формула (12) $M[x] = 9{,}04 \approx 9$ ВЦ.

В качество на критерий за бойната ефективност на зрк може да се използва коефициента на надеждност на ПВО ($K_{нпво}$):

(13) $K_{нпво} = \frac{N_у}{N_ц}$,

където: $N_у$ – броят унищожени цели от всички цели в налета, т.е. $M[x]$;
$N_ц$ – броя на целите в налета ($\lambda t_н$)

Съгласно получените резултати $K_{нпво} = \frac{9}{12{,}1} \approx 0{,}74$ за зрк тип II, при отразяване на налет с посочените параметри.

Изводи:

1. Изготвения статистически модел на зрк чрез симулационно моделиране с помощта на MS Excel позволява на база проведените експерименти да се определи по опитен път вероятността за отказ от обстрелване на ВЦ за зрк от тип II (зрк за малки разстояния) при различна интензивност на обслужването за всеки от целевите канали.
2. Изготвения модел е приложим и при зрк за близко действие (СМО с отказ), като в този случай броят на ВЦ в „опашката“ е равен на нула.
3. С този модел може да се представи и дейността на КП, като едноканална СМО с ОВЧ. За целта е необходимо да се определи максималния брой ВЦ в „опашката“ в зависимост от рубежите за поставяне на задачи към целевите канали.

References:

1. Миневски И., Стефанов С., Симулационно моделиране, учебник, ИК НВУ „В. Левски“, В. Търново, 2014.

2. Митрев Д, Оценка на огневите възможности на зрп „Куб“ по методите на теорията за масовото обслужване, учебно пособие, ВИ, София, 1987.

3. Стефанов С., Георгиев И., Анализ на експериментални данни, учебник, ИК НВУ „В. Левски“, В. Търново, 2013.

4. Stoyanova V, Possibilities for the application of social networks in transmission of secret information, International Scientific Conference CONFSEC ISSN print 2603-2945, ISSN online 2603-2953, year 1, ISSUE 2(2), 2017, Avaible from http://confsec.eu/sbornik/1-2017.pdf

S. N. Chanev,

MATRIX OF TARGETING FOR AIR DEFENCE FORCE

Stoyan N. Chanev

"Vasil Levski" National Military University, "Artillery, Air-defence and Communication and Information Systems" Faculty, "Air Defence" Department; town of Shumen

Abstract: *Formation of matrix of targeting for air defence force allows distribution of incoming target stream with certain density toward different surface-to-air missile systems presented as mass service systems. This distribution is able to estimate the effectiveness of particular parts of the whole system.*

Keywords: *matrix of targeting, surface-to-air missile system, mass service system, effectiveness*

МАТРИЦА НА ЦЕЛЕРАЗПРЕДЕЛЕНИЕ НА ГРУПИРОВКА ЗА ПВО

Стоян Н. Чанев

При представяне на групировка за противовъздушна отбрана (ПВО) като съвкупност от последователно или паралелно действащи системи за масово обслужване (СМО) /зрк за близко действие с далечна граница на зоната за поражение до 10 км. се разглеждат като СМО с откази, а тези с по-големи възможности по разстояние – като СМО с ограничено време за чакане/ е необходимо да се определят входните данни за всяка една СМО, т.е. плътността на входящия поток от заявки/въздушни цели да се раздели на плътност на потоци към всеки зрк , средна скорост и височина на полета на целта в съответния поток. За тази цел следва да се извърши целеразпределение (ЦР) към зрк.

За избиране на най-добрия вид ЦР и постигане на най-висока ефективност, се отчитат:

– пропускателната способност на командните пунктове (КП), броят на боеготовите зрк и техните възможности за унищожаване на цели;

– характерът, построението и продължителността на налета;

– относителната важност на целите;

– екстраполираните курсове на целите и курсовите параметри относно стартовите позиции на зрк;

– правилата за назначаване на зрк и броят на ракетите за поразяване на целта в зависимост от нейния параметър, условията на стрелбата и запаса от ракети.

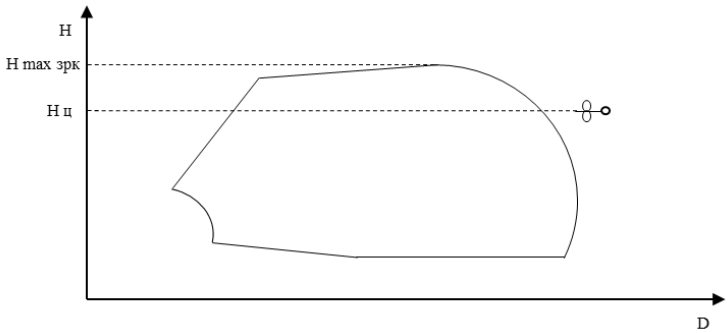
Когато зрк е представен като СМО с отчитането на пълнодостъпността на системата по курсов параметър и респективно редуциране на целевите канали вземащи участие в отразяването на въздушния удар на противника параметъра на ВЦ може да не се отчита.

Основен вид целеразпределение в групировката за ПВО се явява централизираното целеразпределение (ЦЦР). ЦЦР се използва при достоверно откриване на целите на необходимото разстояние и при неголяма плътност на налета, когато командирът може своевременно да поставя огневи задачи. При ЦЦР силите и средствата за ПВО обстрелват по-голям брой цели, което води до повишаване на броя на унищожените цели и намаляване средния разход на ракети.

Основните стратегии при целеразпределение с автоматизирани системи за бойно управление се определят от възможностите за математическо моделиране по различни показатели на ефек-

тивност на стрелбата при решаване на конкретна задача на целеразпределение и от целите, които са поставени пред групировката.

ЦЦР по математическото очакване на броя поразени цели е целесъобразно да се използва в случаите, когато вероятните загуби нанесени на прикривания обект се приемат за пропорционални на проникналите до него въздушни цели, като се отчита тяхната важност. На създадената групировка е поставена задача да унищожи максимален брой цели, т.е. командирът се стреми да обстреля колкото е възможно по-голям брой цели. За целта е необходимо да се извърши ЦР осигуряващо максимално пребиваване на ВЦ в зоните за поражение на зрк и пълно използване на бойните им възможности (в случая – пространствени). В [4] са представени възможностите, които предлага Матлаб и е удачно да се използват при симулации.



Фиг. 1. Вертикално сечение на ЗП на зрк

На фиг.1 е показано вертикално сечение на зоната за поразяване (ЗП) на зрк. Вижда се, че времепребиваването на ВЦ в ЗП на зрк е функция от височината на полета на целта, а в по-голяма степен и от скоростта ѝ.

Нека въведем понятията:

g_{ij}^{h} – показател на височината на $i^{\text{-тата}}$ цел относно $j^{\text{-тата}}$ СМО (зрк);

g_{ij}^{v} – показател на скоростта на $i^{\text{-тата}}$ цел относно $j^{\text{-тата}}$ СМО (зрк).

Определянето на g_{ij}^{h}, характеризиращ досегаемостта на СМО (зрк) по височина се извършва по формулата:

(1) $$g_{ij}^{h} = 4\frac{H_{гpi}}{H_{maxj}}\left(1 - \frac{H_{гpi}}{H_{maxj}}\right),$$

където $H_{гpi}$ – височина на полета на $i^{\text{-тата}}$ цел (групова);

H_{maxj} – максимална височина на досегаемост на $j^{\text{-тата}}$ СМО (зрк).

Определянето на g_{ij}^{v}, характеризиращ досегаемостта на СМО (зрк) по скорост се извършва по аналогичен начин:

(2) $$g_{ij}^{v} = 4\frac{V_{гpi}}{V_{maxj}}\left(1 - \frac{V_{гpi}}{V_{maxj}}\right),$$

където $V_{гpi}$ – скорост на полета на $i^{\text{-тата}}$ цел (групова);

V_{maxj} – максимална скорост на досегаемост на $j^{\text{-тата}}$ СМО (зрк).

Необходимо е да се изведе обобщен показател, който ще отчита едновременно скоростта и височината на полета на $i^{\text{-тата}}$ цел относно $j^{\text{-тата}}$ СМО (зрк).

(3) $$G_{ij} = k_1 g_{ij}^{v} + k_2 g_{ij}^{h},$$

където: k_1 и k_2 - теглови коефициенти на скоростта и височината на полета на целта, като $k_1 + k_2 = 1$ и се избират така, че да се приоритизират факторите оказващи влияние върху ефективността на стрелбата. Тъй като част от ЗП е нееднородна по височина, а скоростта на целта

оказва по-осезаемо влияние на времепребиваването на ВЦ в цялата ЗП определяме $k_1 = 0{,}6$ и $k_2 = 0{,}4$.

Матрицата за ЦР е от вида:

$$G_{nm} = \begin{Vmatrix} G_{11} \cdots & G_{1j} \cdots & G_{1n} \\ \cdots & \cdots & \cdots \\ G_{i1} \cdots & G_{ij} \cdots & G_{in} \\ \cdots & \cdots & \cdots \\ G_{m1} \cdots & G_{ij} \cdots & G_{mn} \end{Vmatrix} \quad (4)$$

Стойността на елементите ѝ е правопропорционална на ефективността на стрелбата по цел с даден номер от точно определен зрк.

Пример:

В таблица 1 е показан модел на удар на ВП, изграден на база на моделиране действията на групите с различно предназначение и състав в различни диапазони от височини и скорости

Таблица 1

Налет на ВП - вид, цел/предн., състав, последов.на д-ие, височина и скорост на групите							
№	Вид	Цел/Предназначение	Ед.	Дв.	Четв.	H_i [km]	V_i [km/min]
1	ударна	с-ма ПВО			1	0,35	12,38
2	ударна	с-ма ПВО			1	0,71	16,33
3	ударна	с-ма ПВО			1	0,42	12,29
4	демонстр. д-ия	с-ма ПВО			1	1,65	16,89
5	демонстр. д-ия	с-ма ПВО			1	1,59	19,84
6	разузн. и РЕВ	с-ма ПВО			1	5,53	36,00
7	ударна	б-ни от 1-ва поз.			1	0,46	13,79
8	ударна	на уч. за пробив			1	0,31	12,72
9	ударна	адн на с-то в напр. на гл. удар			1	0,98	13,95
10	ударна	радн на групировката на СВ			1	0,57	15,79
11	РЕВ (EW)	с-ма ПВО		1		3,04	23,15
12	патрулно съпр.	изтр. прикритие		1		2,52	28,68
13	патрулно съпр.	изтр. прикритие		1		9,88	36,00
14	доразузнаване	р-не в р-на ударите		1		7,25	36,00
		Усреднени показатели	0	4	10	2,52	20,99

В таблица 2 са изведени количествените показатели на удара.

Таблица 2

Ешелон за пробив на ПВО		Фронт на удара на ВП			
Групи	$t_{инт.пво}$ = 0,5	Групи	Δl_j	$L_ф$	
6	$t_{нпво}$ = 3	3	2	5	
$t_{инт.еш}$ = 3					
Ударен ешелон		Оперативно построение на налета на ВП			
Групи	$t_{инт.уд}$ = 1	$N_{сам}$	Групи	$t_н = t_{нпво} + t_{инт.еш} + t_{ну}$	$\lambda_н$
6	$t_{н.уд}$ = 5	48	14	11	4,28

$t_{инт.пво}$ – интервал [min] между групите в ешелона за пробив на ПВО;
$t_{н.пво}$ – продължителност на удара [min] на ешелона за пробив на ПВО;
$t_{инт.еш}$ – интервал [min] между ешелона за пробив на ПВО и ударния ешелон;

$t_{инт.уд}$ – интервал [min] между групите в ударния ешелон;
$t_{н.уд}$ – продължителност на удара [min] на ударния ешелон;
$t_н$ – продължителност на удара [min] на ВП;
$\lambda_н$ – плътност на входящия поток от заявки (ВЦ) към групировката за ПВО.

Групировката за ПВО е построена на база на три разнородни зрк с отчитане на принципите и изискванията към системата за ПВО, а така също и със задачите за изпълнение и бойните възможности на отделните компоненти (таблица 3).

Таблица 3

Тип зрк \ п-л	*Hmax* [km]	*Vmax* [km/m]
I тип	5	21
II тип	14	42
III тип	18	48

В таблици 4, 5 и 6 са изчислени показателите по височина и скорост, а така също и елементите на матрицата на ЦР (обобщен показател) съгласно формули (1÷3). Когато дадена ВЦ е извън досегаемостта на зрк се получават отрицателни стойности.

Таблица 4

Изчисляване на - g_{ij}^h $g_{ij}^h = 4 * (H_{грi} / H_{maxj}) * [1 - (H_{грi} / H_{maxj})]$			
№ на гр. \ зрк	**I тип**	**II тип**	**III тип**
1	0,2598	0,0973	0,0761
2	0,4849	0,1915	0,1507
3	0,3101	0,1173	0,0919
4	0,8842	0,4157	0,3329
5	0,8689	0,4037	0,3230
6	-0,4678	0,9558	0,8512
7	0,3310	0,1258	0,0986
8	0,2322	0,0864	0,0676
9	0,6298	0,2602	0,2057
10	0,4049	0,1566	0,1230
11	0,9526	0,6806	0,5621
12	1,0000	0,5899	0,4811
13	-7,7169	0,8306	0,9904
14	-2,6040	0,9988	0,9620

Изчисляване на - g_{ij}^v $g_{ij}^v = 4 * (V_{грi} / V_{maxj}) * [1 - (V_{грi} / V_{maxj})]$			
№ на гр. \ зрк	**I тип**	**II тип**	**III тип**
1	0,9680	0,8315	0,7656
2	0,6913	0,9506	0,8980
3	0,9708	0,8281	0,7621
4	0,6291	0,9618	0,9123
5	0,2095	0,9969	0,9699
6	-4,8980	0,4898	0,7500
7	0,9019	0,8821	0,8190
8	0,9552	0,8446	0,7792
9	0,8921	0,8873	0,8246
10	0,7462	0,9384	0,8830
11	-0,4520	0,9895	0,9988
12	-1,9987	0,8662	0,9619
13	-4,8980	0,4898	0,7500
14	-4,8980	0,4898	0,7500

Таблица 5

Таблица 6

Изчисляване на елементите на матрицата по обобщен показател - G_{ij} $G_{ij} = (k_1 * g_{ij}^{v}) + (k_2 * g_{ij}^{h})$			
зрк / № на гр.	I тип	II тип	III тип
1	0,6847	0,5378	0,4898
2	0,6087	0,6470	0,5991
3	0,7065	0,5438	0,4940
4	0,7312	0,7434	0,6806
5	0,4733	0,7596	0,7111
6	-3,1259	0,6762	0,7905
7	0,6736	0,5796	0,5308
8	0,6660	0,5413	0,4945
9	0,7872	0,6364	0,5771
10	0,6097	0,6257	0,5790
11	0,1099	0,8659	0,8241
12	-0,7992	0,7556	0,7696
13	-6,0255	0,6261	0,8462
14	-3,9804	0,6934	0,8348

Обобщеният показател с максимална стойност за всеки ред приема стойност единица (дадената ВЦ се разпределя за съответния ЗРК), а останалите – стойност нула (таблица7).

Чрез матрицата на ЦР входящият поток от ВЦ към групировката за ПВО се разделя на три потока към трите типа зрк, осигурявайки максимално използване на бойните им възможности и времепребиваване на ВЦ в зоните им за поразяване. Тези потоци имат усреднени показатели, които се различават от посочените в таблица 1 и се явяват входни за различните СМО (ЗРК), което позволява да се оцени бойната им ефективност (таблица 8). В противен случай следва да се преизчислят бойните им възможности спрямо еталонни такива, което неминуемо ще доведе до обобщени оценки на оперативните способности на групировката за ПВО, които в определени ситуации могат да се отличават значително от реалните.

Таблица 7

Матрица на целеразпределението			
зрк / № на гр.	I тип	II тип	III тип
1	1	0	0
2	0	1	0
3	1	0	0
4	0	1	0
5	0	1	0
6	0	0	1
7	1	0	0
8	1	0	0
9	1	0	0
10	0	1	0
11	0	1	0
12	0	0	1
13	0	0	1
14	0	0	1
$\Sigma N_{сам}$	20	18	10
$\lambda_{нj}$	1,78	1,60	0,89

Таблица 8

Средни показатели на налета (по зрк)			
п-ли / зрк	$\lambda_{нj}$	$H_{ср}$ [km]	$V_{ср}$ [km/min]
I тип	1,78	0,50	13,03
II тип	1,60	1,51	18,40
III тип	0,89	6,29	34,17

$\lambda_{нj}$ – плътност на потока от заявки (ВЦ) към $j^{\text{-тия}}$ тип зрк.

Изводи:

1. Матрицата на ЦР позволява разделянето на входящия поток от заявки (ВЦ) към изграждащите групировката за ПВО разнородни зрк, което позволява представянето й като последователни или паралелно действащи СМО с цел оценка на бойната й ефективност, която се явява първостепенна от оперативните способности на групировката.

2. Разделянето на потока от заявки на отделни потоци с определени плътности и средни стойности на височините и скоростите на целите позволява да се оцени приноса на всеки компонент от групировката към бойната й ефективност и да се вземат обосновани решения относно състава и бойния ред.

References:

1. Атанасов А., Необходими оперативни способности на групировка за ПВО при прикритие на обекти от критичната инфраструктура, В. Търново, 2012.

2. Митрев Д, Димитров Д., Основи на управлението на огъня на зенитните подразделения, ВА, Шумен, 2003.

3. Кругликов С., Методика решения задачи многофакторного целеразпределения в автоматизированной системе управления, Журнал „Доклады БГУИР“, бр. 5, 2013.

4. Стоянова В., Възможности на Матлаб за работа с изображения, Сборник от научни трудове, фак. „А, ПВО и КИС“, Шумен, 2014 , ISSN 1314-1953, стр.250-256.

K. A. Iliev,

DETERMINATION OF POTENTIAL POTENTIAL OF PERSPECTIVES OF THE MODELS INSTALLATION AND POWER TECHNIQUES

Kaloyan A. Iliev

"Vasil Levski" National Military University, "Artillery, Air-defence and Communication and Information Systems" Faculty, "Organization and management of the Field Artillery tactical formations" Department; town of Shumen.

Abstract**:** *When conducting military engineering to determine combat potentials, and to assess the degree of adaptation of a given model of weaponry or combat equipment to accomplish the assigned tasks and achieve the desired end result, mathematical models of military action of varying sizes are widely used. The proposed model for calculating the combat potentials of the armaments and armament models is a hierarchical set of specific analytical methods and formulas, consistent with the intended use of indicators and criteria, input and output parameters and a system of limitations and assumptions.*

Keywords**:** *combat potentials, model of weaponry, combat equipment, analytical methods.*

ОПРЕДЕЛЯНЕ БОЙНИЯ ПОТЕНЦИАЛ НА ОБРАЗЦИТЕ ВЪОРЪЖЕНИЕ И БОЙНА ТЕХНИКА

Калоян А. Илиев

Като всяка наука, така и теорията на бойните потенциали използва понятия, които разкриват нейната същност и съдържание. Но към момента разработките свързани с тази тематика показват, че въпреки важността за военната наука, към настоящия момент у военните специалисти все още не съществува единно разбиране и методология за определяне на бойния потенциал на различните образци въоръжение (В), бойна техника (БТ) и войсковите формирования (ВФ) както и единна мерна единица за него.

Според едни военни специалисти ***бойният потенциал*** представлява ***военната мощ*** на дадена държава, според други това е съвкупността от материални и духовни фактори, определящи състоянието на армията и флота и способността да изпълнят поставените им задачи, а според трети това е критерий за бойните възможности на бойните системи, с помощта, на който е възможно да се определи съотношението между противостоящите групировки [15].

В доктриналните документи и публикации на НАТО ***бойната мощ*** се разглежда като съвкупност от взаимосвързани, зависими и непрекъснато взаимодействащи си три компонента: концептуален (доктрини, концепции, съвместимост), физически (комплектоването с личен състав, въоръжение, бойна техника и материални средства) и морален (мотивация, лидерство, командване и управление)[20].

Важен принцип при формулирането на определението за боен потенциал следва да се явява възможността за неговото интерпретиране в рамките на теорията за бойна ефективност на образците въоръжение и бойна техника. От казаното по-горе можем да дадем определения за **боен потенциал, а именно**:

Боен потенциал на образец въоръжение и техника – интегрален показател, характеризиращ обема от задачи, които може да изпълни даден образец В и БТ в зависимост от своето целево предназначение при разчетни условия на бойните действия при определено ниво на възможности на системата за управление, осигуряване и подготовка на личния състав [14].

Боен потенциал на образец въоръжение и техника **-** интегрален показател, характеризиращ максималния обем изпълнявани от дадения образец задачи, по целево предназначение, при реализиране на пределните тактико-технически характеристики за определено време на функциониране в осреднени разчетни условия [16].

Боен потенциал на образец въоръжение и техника **–** интегрална характеристика на неговите пределни бойни възможности, изразена посредством основните функционални свойства и тактико-техническите данни на дадения образец В или БТ [18].

Формулирани по този начин определения за боен потенциал отразяват преди всичко абсолютните балистични, конструктивни, експлоатационни и относителни характеристики на въоръжението и бойната техниката, с които са комплектовани войсковите формирования.

Бойният потенциал се интерпретира и като сравнителен, качествено обобщен показател за влиянието на различните типове образци въоръжение и бойна техника върху хода и изхода на операцията – "Определя се делът на различните типове въоръжения в крайния резултат на бойните действия и след това се присвоява тежестен коефициент на всеки тип, който коефициент се нарича боен потенциал" [1].

В основата на методиката разработена в Центъра за военно-стратегически изследвания (ЦВСИ) на Генералния щаб на Руската федерация се използват експертни процедури за определяне и еквивалентиране на бойния потенциал на образците въоръжение, бойна техника и войскови формирования на базата на първичните ТТХ [18]. Величината на бойния потенциал се определя като средно квадратна величина от потенциалите на отделните функционални свойства P_i (огнева мощ, подвижност, управление, живучест.)

$$\mathbf{P}_{\mathrm{BT}} = \sqrt{\sum_{i=1}^{4} \alpha_i \mathbf{P}_i^2} \qquad (1.1)$$

<u>където:</u>

- P_i - Обобщен функционален показател за качество, представляващ количествена мярка на дадено функционално свойство на образеца въоръжение или бойна техника;

- α Са теглови коефициенти, определение основно по експертен път, отразяващи значимостта на отделното функционално свойство и са дефинирани в област $\mathbf{O} < \alpha_i < \mathbf{1}$; $\sum_{i=1}^{4} \alpha_i = 1$,

Определянето на бойния потенциал на войсковите формирования се извършва чрез използване на средните значения на потенциали на подсистемите на въоръжението Π_{B} , управлението Π_{Y} и осигуряването Π_{O} по следната формула:

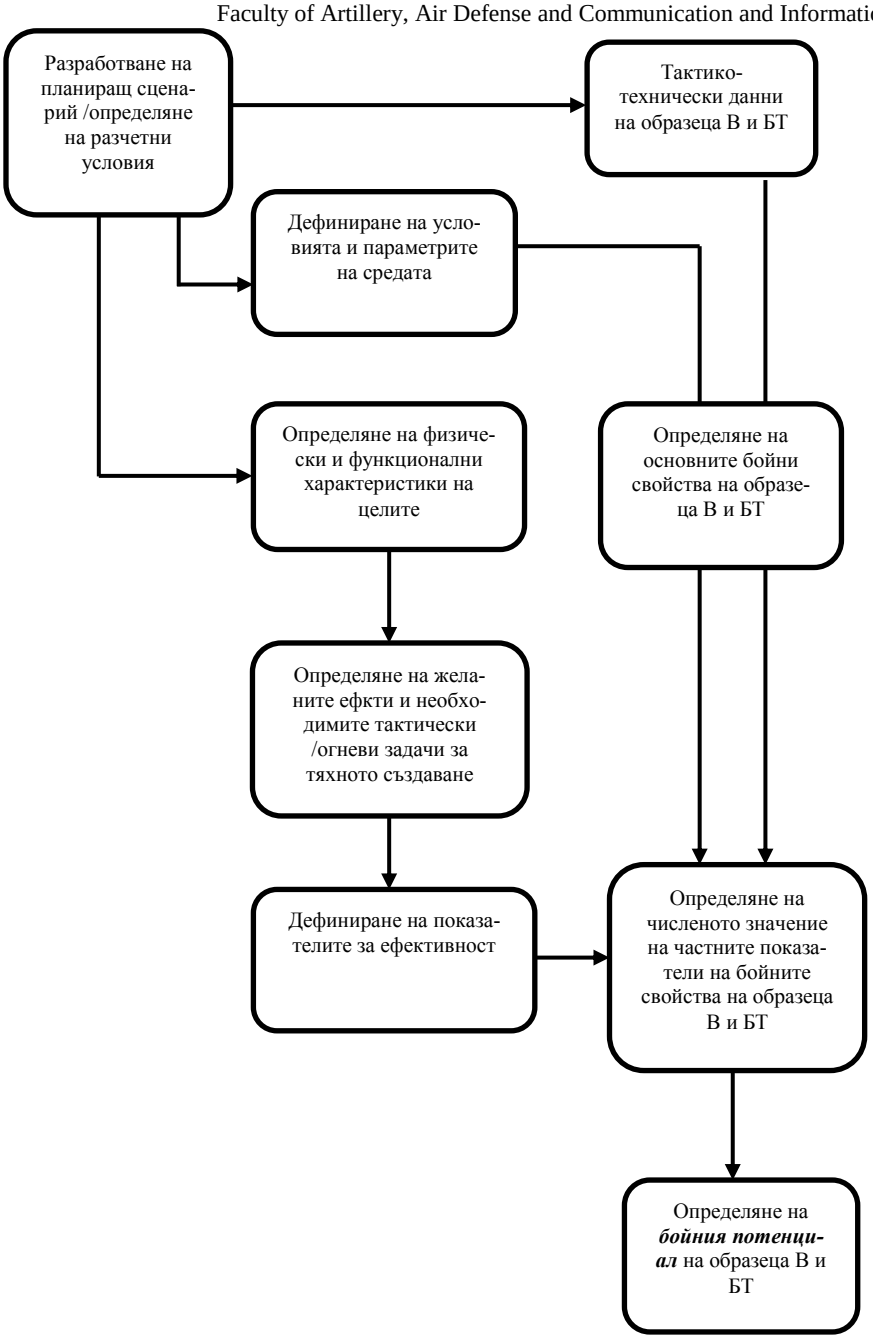
$$\Pi_{B\Phi} = \mathrm{K}_B \Pi_B + \mathrm{K}_Y \Pi_Y + \mathrm{K}_O \Pi_O \qquad (1.2.)$$

където:

- $\mathrm{K}_{\mathrm{B}}, \mathrm{K}_{\mathrm{Y}}, \mathrm{K}_{\mathrm{O}}$ са коефициенти за значимост на подсистемите за въоръжението, управлението и осигуряването, определени на базата на експертните оценки.

Разработване на методиката на базата на множество допускания без нужната обосновка, както и елемента на субективизъм при определяне на значението на тегловите коефициенти на отделните функционални свойства, поставя под съмнение възможността за реална оценка на бойните потенциали на образците въоръжение, бойна техника и войсковите формирования.

Графичното изображение на структурата на метода за определяне на бойните потенциали е представен на фиг. 1.



Фиг. 1. Метод за определяне на бойните потенциали на образците въоръжение и бойна техника.

Методът за определяне на бойните потенциали се състои от следните основни стъпки:

1. Разработване на планиращ сценарий;
2. Определяне на основните тактико-технически характеристики на оценяваният образец въоръжение и бойна техника;
3. Определянето на целите за въздействие;
4. Определяне на характера и съдържанието на решаваните тактическите /огневи задачи;
5. Формулиране на показателите (измерителите) за ефективност;
6. Определяне численото значението на частните показатели на бойните свойства на изследвания образец въоръжение или бойна техника;
7. Определяне на бойният потенциал на изследвания образец въоръжение или бойна техника

Всяка една от изложените стъпки включва следното съдържание:

1. Разработване на планиращ сценарий (определяне на разчетни условия) от гледна точка на оперативната обстановка или характера на решаваните военни задачи.

За да се извърши оценка на бойният потенциал на всеки един образец въоръжение или бойна техника е необходимо да се разработи (зададе) сценарий, отразяващ най-характерните форми и способи за бойно използване на дадена бойна система, да се определят количествените характеристики на решаваните бойни задачи и максималното време за неговото функциониране. Това означава да се зададе модел на функциониране на дадения образец въоръжение или бойна техника в зададени разчетни условия за неговото бойно използване. По този начин моделирането на процеса на бойно използване се явява водещ методологически принцип при определяне на бойните потенциали на даден образец въоръжение или бойна техника както и за оценка на степента на приспособеност на даденият образец за изпълнение на поставените задачи и постигане на желания краен резултат.

2. Определяне на основните тактико-технически характеристики на оценяваният образец въоръжение и бойна техника, които ще се отчитат при определяне на значението на бойния потенциал. Под тактико-технически характеристики следва да се разбира, съвкупността от показатели (характеристики), количествените значения, на които определят техническия облик на дадено изделие, отразяват неговите бойни свойства и характеризират способността му да изпълняват определени функции. Същите се детерминират при определяне на назначението на системата, нейните функции и задачи, технически замисъл за разработване, определяне на направленията на конструиране на системата.

3. Определянето на целите за въздействие - може да бъде дефинирано като процес на избиране на целите, подбирайки подходящо въздействие върху тях, вземайки предвид дефинираните разчетни условия. Определянето на бойния потенциал на еднотипни образци въоръжение и бойна техника трябва да се извършва на базата на поразяване на еднотипни цели и обекти притежаващи еднаква степен на защитеност, подвижност, пространственост и досегаемост.

4. Определяне на характера и съдържанието на решаваните тактическите /огневи задачи, свързани с прилагане на непосредствено въздействие, за създаване на ефекти свързани с промяна на физически и експлоатационни характеристики (получаване на определени загуби), прекратяване на функционирането за определен период от време (време за небоеспособност, време за възстановяване на загубите), способност за командване и управление, мотивация и воля за водене на бойни действия и постигане на победа.

5. Формулиране на показателите (измерителите) за ефективност – този показател е основа на измервателната скала, използвана за оценка на ефективността от дадено въздействие за постигане на един или друг желан ефект. Изборът на показател за ефективност на всяко въздействие се извършва за да се определи дали конкретното въздействие води до създаване на желан ефект върху целта.

Конкретния избор на критерии и методи и модели за тяхното изчисляване зависи от целта на провежданите изследвания, използваните образци въоръжение и бойна техника за изпълнение на задачата по поразяване, вида, размера и живучестта на целите (обектите) за поразяване както и от ред други фактори.

6. Определяне численото значението на частните показатели на бойните свойства на изследвания образец въоръжение или бойна техника.

Под понятието „бойни свойства на образец въоръжение (бойна техника)" следва да се разбира "обобщен устойчив признак, характеризиращ способността на образеца за ефективно изпълнение на определени бойни функции в съответствие със своето предназначение" [17].

Предложеният модел за изчисляване на бойните потенциали на образците въоръжение и бойна техника на практика представлява съвкупност от аналитични методи и формули за определяне на численото значение на случайни величини, свързани непосредствено с проявлението на едно или друго бойно свойство.

На базата на направения анализ на използваните методи за определяне на бойните потенциали могат да се направят следните **изводи:**

1. Въпреки важността, значимостта и актуалността на теорията за „бойните потенциали” за военната наука и практика, към момента военните специалисти не са достигнали до единно становище и тълкование на същността, съдържанието и методите за определяне на значението на „бойния потенциал” на образците въоръжение, бойна техника и войскови формирования.

2. Получените резултати при повечето от методи са базирани на обективни балистични, конструктивни и експлоатационни характеристики на въоръжението и бойната техниката, но при част от тях съществува известен субективизъм при определяне на стойностите на тежестните коефициенти, както и при избора на оценяваните показатели (качества).

3. Въпреки че разработените методи отчитат както количествените така и качествените характеристики на образците въоръжение и бойна техника - технологично усъвършенстване, маневреност, бойна устойчивост получените крайни резултати са статични. Те не могат да се използват за прогнозиране на крайните резултати от противоборството, тъй като не отразяват динамиката на събитията и промяна в условията на обстановката по време на конфликта.

References:

1. Гюргаков И. Съвместна огнева поддръжка. Учебник. ВА “Г.С.Раковски” 2010 г.
2. Гюргаков И. Планиране на огневата поддръжка от артилерията. Учебник. ВА “Г.С.Раковски” 2009 г.
3. Гюргаков И. Нов поглед към системата за поразяване на противника в операциите на Съвместните оперативни сили, Военен журнал,бр.5. С.2009
4. Гюргаков И. Оценка на бойните загуби в оперциите на Съвместните оперативни сили, Военен журнал,бр.1-2. С.2011
5. Гочев К.,Трънски Ж.,Николински В. Справочник на автобронетанковата техника в БА. С,ВИ,2006
6. Договор за обикновените Въоръжени сили в Европа.
7. Доктрина на Въоръжените сили на Република България, С.2011
8. Курс за стрелба и управление на огъня на артилерията (КСУОА - 98), С,1998
9. Методика за извършване на оперативно – тактически разчети при планиране на огневата поддръжка. С, ВИ, 2006 г.;
10. Митрев Д.,Салтиров Д., Узунов Р.Учебник за дистанционно обучение „Управление на сложни системи “.
11. Правила за стрелба и управление на огъня на земната артилерия (ПС и УО-98).С, ВИ, 1998.
12. Теория на стрелбата в земната артилерия,Държавно военно издателство,С.1968.
13. Философски речник. С.1985
14. Брезгин В.С., Буравлев А.И. О методологии оценки боевых потенциалов вооружения и военной техники и воинских формирований// Военная мысль. 08/2010.
15. Брезгин В., Буравлиев А.О методологии оценки боевых потенциалов вооружения и военной техники и воинских формирований / Военная мысль.02/2010.
16. Бонин А.С. Оценка вклада средств боевого управление и обеспечения в соотношение сил авиационньих группировок сторон// Военная мысль. 02/2004.
17. Бонин А.С. О боевих потенциалах образцов ВВТ, формирований и соотношениях сил групировок сторон.// Военная мысль.04/2010.
18. Бонин А.С.Боевые свойства и эффективность вооружения и военной техники // "Военная мысль" 01/2005
19. Буравлиев А.И., Брезгин В.С. – Основый методологического подхода к оценке боевых потенциалов вооружения и военной техники и воинских формирований//Вооружение и економика 03/2009.
20. AJP-01(d) Allied Joint Doctrine December 2010
21. Allied Land Tactics ATP-3.2.1
22. http://militaryrussia.ru/

K. A. Iliev,

METHOD FOR DETERMINING THE WATER FORMULATION POTENTIAL POTENTIAL

Kaloyan A. Iliev

"Vasil Levski" National Military University, "Artillery, Air-defence and Communication and Information Systems" Faculty, "Organization and management of the Field Artillery tactical formations" Department; town of Shumen.

Abstract**:** *The concept of integrated combat system in the theory of combat effectiveness means a set of interconnected and interacting component components that function over time to achieve unified goals and uniform tasks. At the present moment, the additive factor model is used to determine the military potentials of the military formations. The integrated combat potential determined on the basis of this model is a sum of the factorial (private) combat potentials of the individual armament and combat equipment (tanks, artillery systems, airplanes) with which the individual army formations are completed and serves to form prognostic assessments of the opportunities of formations.*

Keywords**:** *integrated combat system, combat effectiveness, military potentials, combat potentials.*

МЕТОД ЗА ОПРЕДЕЛЯНЕ НА БОЙНИЯ ПОТЕНЦИАЛ НА ВОЙСКОВИ ФОРМИРОВАНИЯ

Калоян А. Илиев

В Доктрината на Въоръжените сили на Република България термина ***"потенциал"*** е дефиниран като максималният ефект, който определен субект може да постигне за даден период от време в определена среда [7]. При това под ***"ефект"*** се разбира промяна в поведението или физическото състояние на система или елемент от системата в резултат на едно или повече действия. Ефектът позволява да се интегрира резултатът от различни действия (способности) провеждани от различни субекти.

При оценка ефективността на използването на маневрените формирования, най-често, в качеството на интегрални показатели се използват понятията "боен потенциал" (БП) и "бойни възможности" (БВ).

Бойния потенциал представлява интегрален показател, характеризиращ обема от задачи, които може да изпълнява дадено маневрено формирование съобразно получената бойна задача в средни условия на бойните действия при определени нива и с отчитане на възможностите на системите за командване и управление, логистично и бойно осигуряване, както и степента на подготовка на командирите, щабовете и подразделенията.

Бойните възможности представляват количествени и качествени показатели, характеризиращи способността на маневрените формирования за изпълнение на определени бойни задачи, за определено време при определени условия на обстановката. Те зависят от бойния състав и окомплектоваността на маневрените формирования с личен състав, бойна техника, въоръжение, запаси и имущества, от качеството на въоръжението и бойната техника, от бойната подготовка, сглобеността и опита на командирите и подразделенията.

Сравнявайки представените определенията за боен потенциал и бойни възможности, може да се каже, че те са близки по своята същност и съдържание, но различията се заключават в изходните данни и отчитането на външните фактори при определяне на числовото им значение.

При определяне на величината на бойния потенциал при разчетите, в качеството на изходни данни се вземат пределните (максималните) тактико-технически характеристики на техниката и въоръжението и се определят на единен разчетен оперативен или тактически фон. Оценката на бойните потенциали и бойните възможности на маневрените формирования се извършва при определяне на съотношението между собствени и противникови сили и средства.

Определянето величината на бойните възможности на маневрените формирования се определя за цялата операция и изпълнение на конкретна задача, при точно определени оперативни или тактически условия при отчитане моментното ниво и възможностите на системите за командване и управление, логистично и бойно осигуряване, както и степента на подготовка на командирите, щабовете и подразделенията.

Маневрените формирования могат да водят успешни бойни действия само при ефективно функциониране на всичките им подсистеми (бойни формирования, средствата за командване и управление и средствата за бойно и логистично осигуряване). Недостатъчното успешно функциониране на една от подсистемите или функционирането и на ниво по-ниско от необходимото, може да доведе до неизпълнение на мисията или до изпълнението и с недопустимо ниска ефективност.

Определянето на бойните възможности на маневрените формирования следва да се извършва и за конкретните условия на оперативната или тактическата обстановка, за конкретните условия за водене на бойните действия (денем, нощем, условия на намалена видимост), за определено оперативно или тактическо направление, всяко от които има свои специфични физико - географски условия (релеф, климат, почви, хидрография и т.н.), степен на инженерно оборудване и др. Това е така, защото, реализирането на пълния боен потенциал на маневрените формирования се извършва с отчитане и на тези фактори. А те най-често имат отрицателно въздействие върху реализирането или не на съществуващия боен потенциал. До каква степен командирите и щабовете ще отчетат намаляването на бойните възможности и нереализирането на бойния потенциал на маневрените формирования ще зависи от познаването на обстановката и подготовката на въоръжението, техниката и подразделенията да водят бойни действия в такива условия.

Като база за извършване на изчисленията се използват получените резултати за стойността на тежестните коефициенти за ефективност (WEI) за всеки един образец въоръжение и бойна техника, количеството въоръжение от всеки тип (образец) влизащи в състава на войсковото формирование (войскова единица) и теглови коефициент характеризиращ степента на важност на всеки един образец (тип) въоръжение [27].

$$\mathrm{W}UV = \sum_{i=1}^{10} (\mathrm{CW})_a \times \left(\sum_{n=1}^{m} C_n \times (WEI)_a \right) \qquad (1.1.)$$

където:

WUV – боен потенциал на войсковото формирование;

C_n – количество въоръжение от всеки един (тип) образец във войсковото формирование;

WEI_a – тежестен коефициент за ефективност за съответния тип въоръжение и бойна техника;

CW_a – тежестен коефициент, отчитащ степента на важност на съответния тип (образец) въоръжение.

Използваната методология осигурява получаването на обобщен резултат за бойния потенциал на войсковите формирования, като обединява различни видове средства за огнево поразяване и генерира единна измервателна единица за определяне на ефективността на формированието като цяло. Освен това тази методология осигурява база за извършване на сравнение между различни типове формирования. Получените числени резултати при оценка на различни критерии на оръжейните системи като огнева мощ например дават възможност сравнително лесно да бъде извършено сравнение на потенциалите на различни по големина и тип формирования в състава, на които влизат различни типове въоръжение.

Към настоящият момент за определяне на бойните потенциали на войсковите формирования се използва основно ***адитивния факторен модел***.

Определеният на базата на този модел интегрален боен потенциал, представлява сума от факторните (частните) бойни потенциали на отделните образци въоръжение и бойна техника (танкове, артилерийски системи, самолети) с които са комплектовани отделните войскови формирования и служи за формиране на прогностични оценки за възможностите на формированията.

$$БП_{вф} = \sum_{i=1}^{I_i} N_i \times БП_i \qquad (1.2.)$$

$\mathbf{N}_i$ – количество бойни средства от i тип;

$БП_i$ - боен потенциал на бойно средство от i тип;

I_i – брой на различните видове бойни средства, влизащи в състава на дадено войсково формирование (бойна система);

Основният недостатък на използваният модел е игнорирането именно на синергичния ефект.

Определянето на сумарният боен потенциал на войсково формирование в състава на което влизат както различни видове ударни средства, така и средства от комуникационно информационната система, пунктовете и органите за управление, елементи на подсистемата за логистично осигуряване е съпроводено с определени трудности. Основният проблем възниква от стремежа за изчисляване на потенциала на разнородни средства – средства за поразяване, средствата за бойно управление и осигуряване, решаващи разнотипни задачи в единна величина или с казано по друг начин проблеми свързани основно с процеса на ***еквивалентиране***.

Процесът на еквивалентиране налага необходимостта от въвеждане и използване на понятието ***„приведен боен потенциал"***- потенциалите на ударните средства и средствата за огнево поразяване на противника, средствата за бойно осигуряване и бойно управление изразени в единна измервателна величина.

Решението на задачата по еквивалентиране с цел представяне на значението на бойните потенциали на разнородните средства влизащи в състава на дадено войсково формирование в единна измервателна единица може да бъде намерено с помощта на един от следните способи:

- чрез използване на преходни коефициенти за привеждане на бойният потенциал на разнородни сили и средства към бойният потенциал на прието за ***еталонно (разчетно) средство;***
- на основата на методика за непосредствено определяне на бойният потенциал на различните образци въоръжение и бойна техника чрез използване на единни критерии (в единни показатели);
- на основата на математическо моделиране на бойните действия на разнородните сили и средства;

При определяне на бойните потенциали на войсковите формирования ***средствата за управление и бойно и логистично осигуряване*** могат да не бъдат разглеждани като самостоятелни, притежаващи свой собствен ***целеви потенциал*** (възможност на системата за изпълнение на комплекс от задачи, необходим за постигане на целта) средства.

Основната идея, на която се базира метода е, че ***средствата за бойно управление и бойно осигуряване*** оказват непосредствено влияние бойните свойства на средствата за поразяване посредством изменение на техните частни показатели и генерират мощност (целевото функциониране на системата за единица време).

По този начин основен показател за бойния потенциал на ***системите за управление*** и ***бойно и логистично осигуряване*** се явява ***изменението на величината на бойният потенциал*** на ударните и огневи средства.

Получаване на обективни резултати поражда необходимостта от изграждане на логически и коректен модел на функциониране на системата за управление, отразяващ сложните и разнообразни управленски зависимости между компонентите на системата, които в повечето случаи носят случаен характер.

За определяне на бойни потенциали на всяко ***m (n)*** – средство за бойно управление (средство за бойно осигуряване) влизащо в състава на системите за командване и управление и бойно

осигуряване се определя дела и приноса на тези средства за изменението на величината на численото значение на частните показатели на бойните свойства на поразяващата система чрез величината $\Delta E_{m,n}$ и посредством коефициент за важност (φ_{λ}) [15]. При това към частните показатели за оценка на бойните свойства на поразяващата система следва да се отнасят – вероятност за разкриване на целта (обекта), вероятност за попадение в целта, време за изпълнение на бойната задача, вероятност за бойна устойчивост.

Решаването на задачата за определяне на бойният потенциал на войсковите формирования е свързана и с определяне на оптималния качествен състав на различните типове образци въоръжение и бойна техника, обосноваване на най-рационалната организационна структура на войсковите формирования, ефективни форми и способи за тяхното използване осигуряващо успешно изпълнение на поставените им задачи при минимален разход на ресурси.

Задачата за определяне на оптималния вариант на качествено-количественото съотношение между различните типове образци въоръжение и бойна техника позволяващ достигане на максималният боен потенциал от войсковите формирования и неговото реализиране при решаване на основните бойни задачи в съответствие с тяхното предназначение може да бъде решена в следната последователност:

1. Определя се предназначението на подсистемите влизащи в състава и функциониращи в цялостната разузнавателно-информационната поразяваща система, характера на основните решавани от тях задачи и условията за тяхното изпълнение.
2. Определят се типове въоръжение и бойна техника в състава на - подсистема за поразяване, информационно управляваща подсистема и подсистема за бойно осигуряване необходими за успешно изпълнение на поставените задачи.
3. Определят се възможните структурни варианти (конфигурации) за дяловото разпределение на различните средствата (въоръжение и бойна техника) в системите за бойно управление и бойно осигуряване.
4. Определя се изменението на частните показатели на бойният потенциал на средствата от поразяваща подсистема при различните конфигурации на системите за бойно управление и бойно осигуряване.
5. Извършва се военно-икономическа оценка на алтернативните варианти и се определя най-оптималния по критерия "ефективност-икономически разходи".

Изводи:

1. Въпреки важността, значимостта и актуалността на теорията за „бойните потенциали" за военната наука и практика, към момента военните специалисти не са достигнали до единно становище и тълкование на същността, съдържанието и методите за определяне на значението на „бойния потенциал" на образците въоръжение, бойна техника и войскови формирования.
2. Разгледаните методи не отчитат влиянието на фактори, които не притежават количествено измерение, а именно - използвани тактики (прийоми за водене на бойни действия), система за командване, управление и разузнаване, логистика.
3. Синергичният ефект е игнориран. При определяне на бойните потенциали на войсковите формирования вместо „мултипликативния" се прилага „адитивния" факторен модел, при който резултативния краен показател (боен потенциал), представлява алгебрична сума от бойни потенциали на отделните образци въоръжение и бойна техника, с които са окомплектовани войсковите формирования.

References:

1. Гюргаков И. Съвместна огнева поддръжка. Учебник. ВА "Г.С.Раковски" 2010.
2. Гюргаков И. Планиране на огневата поддръжка от артилерията. Учебник. ВА "Г. С. Раковски" 2009.

3. Гюргаков И. Нов поглед към системата за поразяване на противника в операциите на Съвместните оперативни сили, Военен журнал,бр.5. С.2009
4. Гюргаков И. Оценка на бойните загуби в оперциите на Съвместните оперативни сили, Военен журнал,бр.1-2. С.2011
5. Гочев К., Трънски Ж., Николински В. Справочник на автобронетанковата техника в БА. С,ВИ,2006
6. Договор за обикновените Въоръжени сили в Европа.
7. Доктрина на Въоръжените сили на Република България, С.2011
8. Курс за стрелба и управление на огъня на артилерията (КСУОА - 98), С,1998
9. Методика за извършване на оперативно – тактически разчети при планиране на огневата поддръжка. С, ВИ, 2006 г.;
10. Митрев Д.,Салтиров Д., Узунов Р.Учебник за дистанционно обучение „Управление на сложни системи “.
11. Правила за стрелба и управление на огъня на земната артилерия (ПС и УО-98).С,ВИ,1998.
12. Теория на стрелбата в земната артилерия,Държавно военно издателство,С.1968.
13. Философски речник. С.1985
14. Брезгин В.С., Буравлев А.И. О методологии оценки боевых потенциалов вооружения и военной техники и воинских формирований// Военная мысль. 08/2010.
15. Брезгин В., Буравлиев А.О методологии оценки боевых потенциалов вооружения и военной техники и воинских формирований / Военная мысль.02/2010.
16. Бонин А.С. Оценка вклада средств боевого управление и обеспечения в соотношение сил авиационньих группировок сторон// Военная мысль. 02/2004.
17. Бонин А.С. О боевих потенциалах образцов ВВТ, формирований и соотношениях сил групировок сторон.// Военная мысль.04/2010.
18. Бонин А.С.Боевые свойства и эффективность вооружения и военной техники // "Военная мысль" 01/2005
19. Буравлиев А.И., Брезгин В.С. – Основый методологического подхода к оценке боевых потенциалов вооружения и военной техники и воинских формирований//Вооружение и економика 03/2009.
20. Фендриков Н.М.,Яковлев В.И., Метод расчетов боевой еффективности вооружения
21. AJP-01(d) Allied Joint Doctrine December 2010
22. Allied Land Tactics ATP-3.2.1
23. http://militaryrussia.ru/
24. http://www.npostrela.com
25. http://www.voina-i-mir.ru/Военный энциклопедический словарь. М.Воениздат, 2007.

Rotariu Adrian-Nicolae, Trana Eugen,

ON THE DEVELOPMENT OF AN INTERIOR BALLISTIC MODEL FOR SMALL CALIBER ARMOR PIERCING AMMUNITION

Rotariu Adrian-Nicolae, Trana Eugen

Military Technical Academy Av. George Cosbuc 39-49, Bucharest, Romania
Fax: +32(0)2 7376352
E-mail: adrian.rotariu@mta.ro

Abstract: *A new analytic continuous function for nonlinear deterred/undeterred propellant transition is proposed. Using CEA software, variable ballistic characteristics are determined for a given propellant composition. Several modifications of the interior ballistic specific equations should be operated in order to deal with variability of mean values of burned propellant characteristics: impetus, specific heat at constant pressure, adiabatic coefficient, gas constant, covolume.*

Keywords*: interior ballistics; 0D model; deterred/undeterred transition;*

1. Introduction

A permanent goal of ballistics community is to develop mathematical models able to represent accurately the interior ballistic phenomena. Currently, there are used several types of such models. Most intensively used and also the first developed models are 0-dimensional (lumped) models, like those attributed to Corner [1] or Drozdov [2] or other more recently developed like STANAG 4367 model [3] or IHGBV2 code [4]. For a more detailed analysis of the interior ballistic phenomena, multidimensional models can be used [5].

The using of grains of variable composition like deterred grains imposes supplementary hypothesis on 0D models. Usually approach is to admit a very sharp transition of the propellant properties which allows treating the propellant charge as being made of two distinct compositions, each one with its own set of characteristics, that burn in a successive way. As long as the sharp transition is in fact only an hypothesis, the alternative approaches of gradual transition, as linear or multi-step transitions, were proposed for deterred grains [4, 6].

The present work deals with the necessary adjustments of a lumped model for small caliber grooved barrel to implement the true deterred/undeterred profile transition of grains.

2. Deterrent concentration profile function

Deterring along the complex geometry represent the most used ways to assure a progressive burning of propellant grains. The impregnation of grains exterior surface with substances like DNT or DBP will reduce the characteristic burning rate of propellant on the affected volume with significant consequence on the pressure time gradient recorded during ballistic cycle. As both deterrent concentration and impregnation depth are of importance for ballistic calculations, as work of Mann has already shows [7], the interest of researches on determination of such deterring characteristics is understandable. Along time several techniques, alone or in conjunction, like Fourier transform infrared (FTIR) microspectroscopy and laser Raman microspectroscopy [8] were used to measure the above mentioned characteristics. Depending on the type of deterrent diffusion mechanism, Fickcian or non-Fickcian and the composition and manufacturing process of grains, several types of deterred/undeterred profile were calculated or identified:

- a thick layer of constant or nearly constant deterrent concentration followed by a relatively thin region were the concentration fall to zero value (case I) [7,9]

- a thin layer of constant or nearly constant deterrent concentration followed by a thick region were the concentration fall to zero value (case II) [10]
- a continuous variation of deterrent concentration from the highest value at the exterior surface till the zero somewhere inside of the grain (case III - Fickian diffusion) [8]

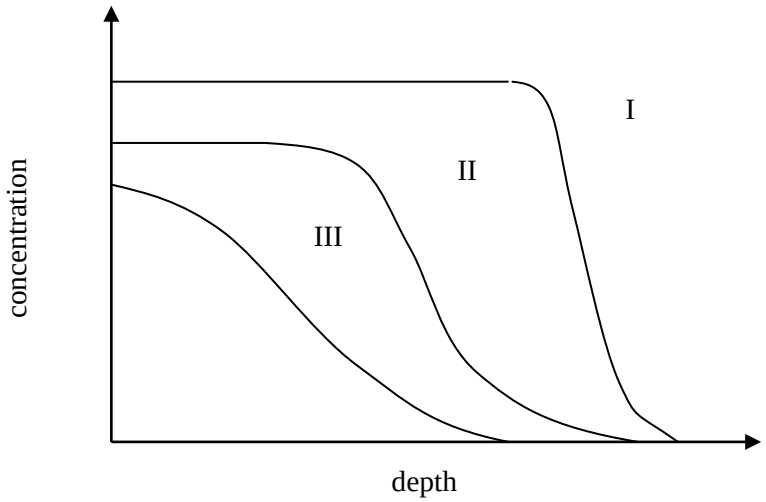


Fig. 1 The observed categories of deterrent concentration profiles

As can be seen in fig. 1, except the case I, none of the deterring profiles may be approximated in a satisfactory way with a sharp transition. As regarding the continuous functions able to describe such transitions, the following exponential analytical expression representing the solution of one-dimensional diffusion in anisotropic media when the diffusion is initiated by an instantaneous plane source was found to be well suited to several deterrent concentration profiles of case III [8].

$$c\ r,t\ = \frac{s}{\sqrt{\pi D t}} e^{-\frac{r^2}{4Dt}} \qquad (1)$$

where c is the deterrent concentration, t the diffusion time, D the constant diffusion coefficient, s is the surface concentration of deterrent and r the space coordinate.

As long as the function (1) is not able to model cases I and II, we identified another analytical function derived from the cumulative distribution function of Gumbel distribution, that admit an constant plateau followed by a decrease of similar shape to function (1):

$$c\ r\ = c_0\ \ 1 - e^{-e^{\frac{1}{\beta} r - \mu}} \qquad (2)$$

where c_0 is the concentration of deterrent in the layer of constant concentration plateau , μ is the coefficient that controls the thickness of above mentioned layer and β is the coefficient that controls the thickness of layer of variable concentration. It is obvious that this formulation allow us to model all three identified cases from Fig.1 by variation of the μ and β values. In Fig. 2 we exemplify the ability of such function to approximate the concentration profile of a spherical single base deterred propellant measured by infrared (IR) microscopy which shows a thin layer of constant deterrent concentration followed by a thick region with variable concentration [10]. For extreme high values of β the proposed function became a step function of very sharp transition.

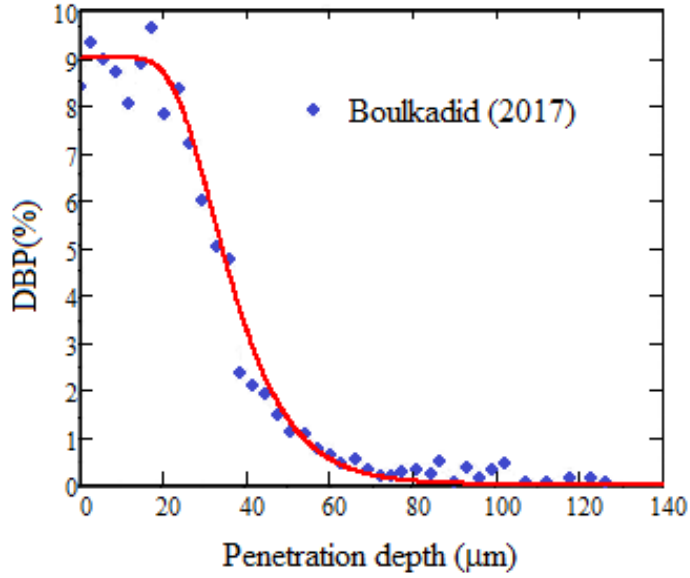


Fig. 2 The profile of function (2) for $c_0 = 9; \beta = 10; \mu = 32$ against the experimental data provided by Boulkadid [10] for DBP concentration in a spherical single base propellant

3. Influence of deterrent concentration on the propellant properties

As is wide know, the deterrent presence has an influence on all relevant propellant ballistic characteristics, each characteristic varying from y_d, the value specific to maximum concentration of deterrent to y_u, the value specific to undeterred propellant. Establishing the deterrent concentration profile law,$c\ r$, and assuming an known variation of the characteristic, $y(c)$, allow us to find the $y(r)$ relationship between an characteristic and the burning surface position r. If it assumes that the $y(c)$ relationship is monotonic one, e. g the impetus decreases as the concentration of deterrent increases, we may use the polynomial function

$$y\ r\ = y_u - \ y_u - y_d \ \ \frac{c(r)}{c_0}^{\ n} = y_u - \ y_u - y_d \ \ \ 1 - e^{-e^{\frac{1}{\beta}r-\mu}}{}^{\ n} \qquad (3)$$

where the index n allows the description on nonlinear relationship.

In the development of our ballistic model we have considered the relation (3) in order to describe the variation of flame temperature T_1, impetus f, covolume α, adiabatic coefficient γ and propellant density ρ . Beside those above mentioned characteristics the modification of the burning rate coefficients a and ν from the Saint Robert's relationship $\frac{dr}{dt} = ap^{\nu}$ is expected too. The Saint Robert's expression became

$$\frac{dr}{dt} = a\ r\ p^{\nu(r)} \qquad (4)$$

where $a\ r$ and $\nu\ r$ functions can expressed by (3) or another relationship type.

For the present case study we considered the spherical propellant analyzed by Boulkadid [10], with the deterred/undeterred transition profile given in Fig.1, used in experimental shooting tests with 5.56 mm EPVAT barrel. In order to establish the propellant characteristics variation, namely isochoric flame temperature T_1, impetus f, covolume α and adiabatic coefficient γ we have utilized NASA CEA thermochemical equilibrium [12].

In the absence of any other relevant information about the distribution of all others propellant ingredients along the radius of the propellant grain in question we consider that relative ratio of such ingredients remain unchanged. By doing so, having the propellant ingredients global concentrations given by Boulkadid [10], we were able to calculate the propellant ingredients local concentrations for different DPB concentrations. The results for six different DBP concentrations are listed in Tabel 1.

Tabel 1. Concentrations values of ingredients as function of DBP concentration

	Concentrations (%)						
Substance	Global value	for 9% DBP	for 7% DBP	for 5% DBP	for 3% DBP	for 1% DBP	for 0% DBP
NC	81.52	77.92	79.64	81.35	83.06	84.77	85.63
H2O	0.66	0.63	0.64	0.66	0.67	0.69	0.69
KNO3	1.2	1.15	1.17	1.20	1.22	1.25	1.26
NGL	10.7	10.23	10.45	10.68	10.90	11.13	11.24
DBP	4.8	9.00	7.00	5.00	3.00	1.00	0.00
DPA	0.59	0.56	0.58	0.59	0.60	0.61	0.62
NDPA	0.53	0.51	0.52	0.53	0.54	0.55	0.56
Total	100	100.00	100.00	100.00	100.00	100.00	100.00

For each such compositions the isochoric flame temperature T_1, impetus f, and adiabatic coefficient γ were directly calculated with CEA software for an initial temperature of 21°C, a load density of 0.2 g/cc and a NC nitration of 13.16%. The covolume α was determined with the approximation formula

$$\alpha \cong 0.001 w_1 \quad (5)$$

where specific volume w_1 was determined with CEA software in the same conditions. The calculated values for each compositions of Tabel 1 are listed in Tabel 2. The influence of deterrent concentration on characteristics values are shown in a normalized way in Fig 3. The index power n of (3) formula for each characteristic is given in the last line of Table 2.

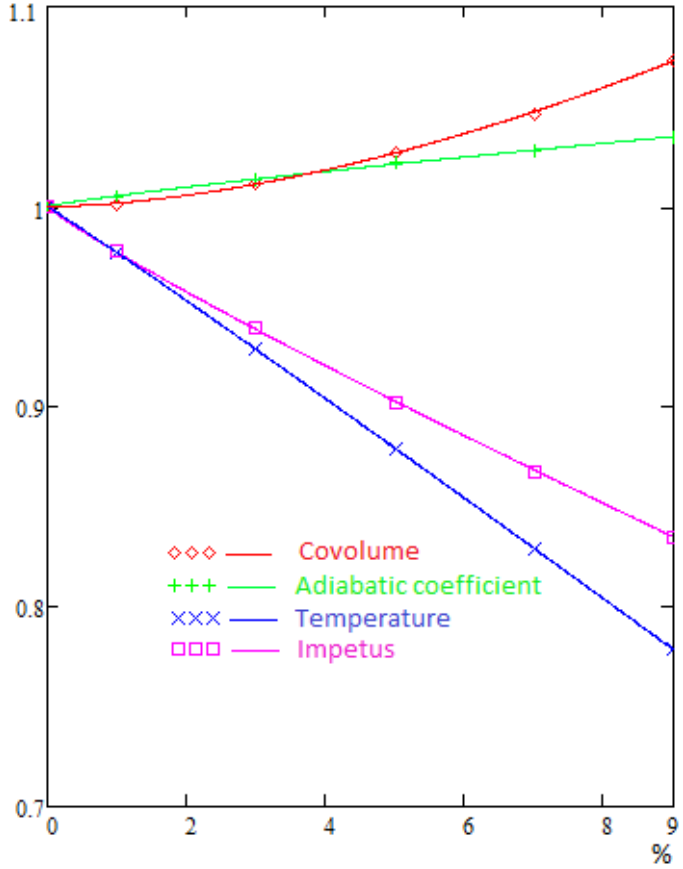


Fig. 3. Relative variations of propellant characteristics as functions of DBP concentration

Tabel 2. Characteristics values for different DBP concentrations

	Impetus [MJ/kg]	Isochoric flame temperature [°K]	Adiabatic coefficient	Covolume [m^3/kg]
0%DBP	1.151	3368	1.200	0.000931
1%DBP	1.126	3290	1.206	0.000932
3%DBP	1.081	3127	1.216	0.000942
5%DBP	1.038	2960	1.226	0.000956
7%DBP	0.998	2791	1.234	0.000974
9%DBP	0.961	2622	1.242	0.000999
Index coeff.	0.9	1.03	0.85	1.7

4. Development of 0D model for small caliber grooved barrel with continuous nonlinear deterrent/undeterred transition

Other several modifications are necessary in the equations where the variable propellant characteristics are present. Firstly, the expression of mean pressure p, derived from energy conservation principle, used to calculate the burning rate will be

$$p = \frac{{}_0^r f(r)\frac{d\omega_b}{dr}dr - \frac{{}_0^r \gamma(r)\frac{d\omega_b}{dr}dr}{\omega_b} - 1 \quad \frac{\varphi q v^2}{2} + \quad E}{W_0 + sx - \frac{\omega}{\delta_m} \; 1 - \psi \; - \; {}_0^r \alpha(r)\frac{d\omega_b}{dr}dr}, \qquad (6)$$

where ω is total mass of propellant, ω_b burned mass of propellant, ψvolume fraction of burned propellant, q projectile mass, v projectile velocity, φ supra-unitary coefficient used to taking account the secondary losses proportional to projectile kinetic energy $\frac{qv^2}{2}$, E secondary losses not proportional to projectile kinetic energy, W_0 initial volume of cartridge, s barrel cross section area, x space traveled by projectile inside of barrel and δ_m mean solid propellant density. Denominator expression $W_0 + sx - \frac{\omega}{\delta_m} \; 1 - \psi \; - \; {}_0^r \alpha(r)\frac{\omega_b}{dr}dr$ represent the volume behind projectile available for propellant gasses W.

Secondly, using propellant variable ballistic characteristics imposes an amendment of mean temperature equation, which became in the absence of terms related to igniter contribution

$$T_g = \frac{pW}{{}_0^r \frac{f(r)\,\omega_b}{T_1(r)\,dr}dr}, \qquad (7)$$

where $\frac{1}{\omega_b} \; {}_0^r \frac{f(r)}{T_1(r)}\frac{\omega_b}{dr}dr$ is the gas constant for the ω_b burned propellant.

Also, the variable propellant characteristics affect the heat transferred to the barrel from the hot gasses. This secondary loss is calculated based on the heat transfer rate equation used in STANAG 4367, which became

$$\frac{dQ}{dt} = \lambda \; {}_0^r \frac{f(r)\gamma(r)}{T_1(r)\;\gamma\;r\;-1}\frac{d\omega_b}{dr}dr \frac{1}{W + {}_0^r \alpha(r)\frac{d\omega_b}{dr}dr}\frac{v}{2} + \alpha_0' \;\cdot S(x)\;\; T_g - T_p \qquad (8)$$

where $\frac{1}{\omega_b} \; {}_0^r \frac{f(r)\gamma(r)}{T_1(r)\;\gamma\;r\;-1}\frac{\omega_b}{dr}dr$ is specific heat at constant pressure of the ω_b burned propellant.

The heat loss rate depends on the difference between gas temperature T_g and wall temperature T_p, the dimension of exposed surface $S(x)$ and the thermal transfer coefficient, last term being the first parenthesis of the (7) equation right member. The Nordheim friction factor λ of thermal transfer coefficient depends on the barrel caliber D_t and α_0' is the natural convection coefficient.

Finally, the link between ω_b burned mass of propellant and the ψvolume fraction of burned propellant is given by

$$\omega_b = \frac{\omega}{\rho_m} \int_0^r \rho(r) \frac{d\psi}{dr} dr = \frac{\omega}{\rho_m} \int_0^r \rho(r) \frac{\chi}{r_1} \left(1 + 2\lambda \frac{r}{r_1} + 3\mu \left(\frac{r}{r_1}\right)^2\right) dr \quad (9)$$

where r_1 correspond to a complete burning of propellant charge and χ, λ and μ. are shape coefficients used by Serebriakov [11].

5. Conclusions

Based on previous considerations, the following conclusions can be drawn:

- analytical function derived from the cumulative distribution function of Gumbel distribution can model successfully all identified types of deterred/undeterred profiles trough variation of the specific μ and β parameters
- except the burning rate coefficients a and ν from the Saint Robert's relationship and local density the others specific propellant characteristics can be calculated based on thermochemical equilibrium algorithms like those used in NASA CEA software
- the adaptation of an lumped interior ballistic model to an continuous nonlinear deterred/undeterred profile consists in modifying several equations to account variability of mean values of burned propellant impetus, specific heat at constant pressure, adiabatic coefficient, gas constant, covolume, density and Saint Robert's law parameters.

Acknowledgment

This work was carried out through the PN III Program 1 Development of national research system - carried out with the support of MEN, UEFISCDI project no. 20PCCDI/2018.

References:

1. Corner J., Theory of Interior Ballistics of Guns. New York, 1950, John Wiley & Sons.
2. Serebryakov M., Internal Ballistics (in Russian), 1949, Moscow: Oborongiz.
3. STANAG 4367 Land (Edition 3). 2012. THERMODYNAMIC INTERIOR BALLISTIC MODEL WITH GLOBAL PARAMETERS, Military Agency for Standardization, Brussels.
4. Anderson R.D., Fickie D.K., IBHVG2 – A User Guide, BRL-TR-2829, Ballistic Research Laboratory, 1987
5. Carlucci E. D., Sidney S. J., Ballistics. Theory and Design of Guns and Ammunition (second edition), 2014, Boca Raton, FL: CRC Press Taylor & Francis Group.
6. Albert W. H. and Michael J. N., The Influence of Propellant Deterrent Concentration Profile on Interior Ballistics Predictions Using Lumped-Parameter and Multiphase Flow Codes, ARL-TR-4713, 2009
7. D. C. Mann, DEVELOPMENT OF A DETERRED PROPELLANT FOR A LARGE CALIBER WEAPON SYSTEM, Journal of Hazardous Materials, vol. 7, 1988, pp.259-280
8. Vogelsanger B., Ossola B., Bronnimann E., The Diffusion of Deterrents into Propellants Observed by FTIR Microspectroscopy - Quantification of the Diffusion Process, Propellants Explos. Pyrotech, vol. 21, 1996, pp. 330-336
9. Trewartha S., Shapter J., Gibson C. T., Mikajlo E., Jones A., Determination of Deterrent Profiles in Nitrocellulose Propellant Grains Using Confocal Raman Microscopy, Propellants Explos. Pyrotech., vol. 36, 2011, pp. 451 – 458
10. Boulkadid K. M., Lefebvre M. H., Jeunieau L., Dejeaifve A., Local Temperature Sensitivity Coefficients of a Deterred Spherical Single Base Gun Propellant, Cent. Eur. J. Energ. Mater. vol. 14, 2017, pp. 952-965
11. Serebriakov, M. E., Interior Ballistics of Tube Weapons and Solid Propellant Rocket, Moskva, 1962
12. www.grc.nasa.gov/WWW/CEAWeb/ceaguiDownload-win.htm

Andrada Cirneanu,

SMART VIDEO SURVEILLANCE FOR BACKGROUND ANALYSIS

Andrada Cirneanu

Phd, Military Technical Academy "FERDINAND I", andrada.cirneanu@mta.ro

Abstract: *This paper presents a method for motion detection and form recognition from a video stream generated by a video surveillance system. The purpose of this paper is to propose an algorithm that differentiate a person form from other types of forms. Motion detection is realized based on the comparison of 2 consecutive frames extracted at a specific time interval from the real-time video stream and based on the resulted comparison, a binarization algorithm and a region growing algorithm are used to extract all independent regions in case of*

Keywords*: person detection, motion detection, surveillance.*

1. Introduction

Nowadays computer vision is an ultramodern field that has been fully developed in recent years. Applications developed in this domain are based on a real-time analysis of images provided by one or more video camera. The possibilities of this technology are almost unlimited and reach different areas of the industry. The variety of applications in which images are used on the computer is expanding gradually as users discover unquestionable advantages of this technology. The main areas where computerized imaging can be used are control application, automation, recognition or accurate measurement.

Before analyzing the images, the most important thing is to capture the image. This process is called the acquisition of the image..

The image acquisition process is carried out in several stages. Initially, the subject of interest reflects an energy. Then an optical system concentrates that reflected energy and finally a sensor measures that amount of energy (Fig.1).

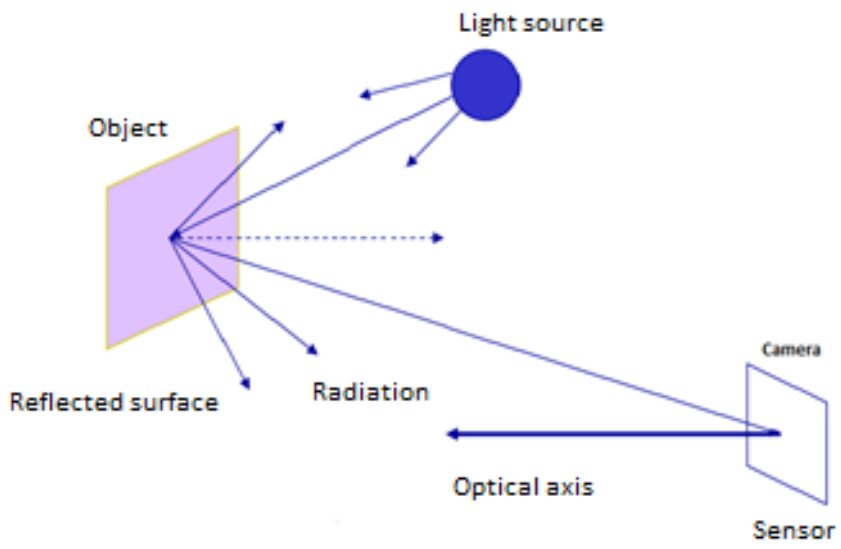


Fig. Image acquisition

The field of motion detection cameras is monopolized by two different types of technologies depending on the type of image sensor used. These two types are CCD (charge-coupled device) and CMOS (complementary metal-oxide semiconductor). Inside both types of cameras, motion detection is realized by comparing each captured image with the previous one and the cameras will interpret any noticeable changes between consecutive images as motion. Two important settings characterize almost all surveillance cameras: sensitivity and percentage. Sensitivity represents a contrast setting that determines when a change between consecutive images represents motion in the monitored area. On the other hand, percentage is set in the case of detecting motion in a sub-area of the monitored area.

Even though these motion detection cameras are an affordable option for a regular security system, there is a potential need for security systems that are also based on surveillance cameras, but the motion detection is based on an auxiliary image processing system that can also accomplish other processing stages if required. The reason for implementing such systems is represented by the scope of this paper which is motion detection in a monitored area and forms differentiation like humans from animals.

Despite the fact that great progress has been made in recent years, people detection continues to be a challenging task in the field of computer vision.

To this purpose, the authors from [1] propose a methodology which is focused on people detection and recognition. The study consists in an efficient image descriptor that is inspired from the mathematical statistics of the Brownian motion. The obtained results proved to be promising for pedestrian classification and person identification tasks. In [2], the authors present an approach for pedestrian detection based on a combination of Haar and LBP features in conjunction with AdaBoost machine learning algorithm for the learning process and Meanshift algorithm for performance improvement.

Authors in [3] present a method for human detection using a cascade-of-rejectors approach integrated with Histogram of Oriented Gradients (HoG) features. First, the detection system identifies the most appropriate set of blocks and then uses a rejection cascade to speed up the computation. The algorithm proves to have a high accuracy level. In [4], the authors came up with a solution of people detection based on RGB-D sensor. The algorithm browses through two steps: at the beginning twoRGB and depth feature fusing strategies are proposed and compared and then an improved non-maximum suppression algorithm is proposed to further boost the performance of detection without increasing the time consumption.

Paper [5] comes with an approach of people detection from depth maps produced by sensors mounted in a zenithal position. The algorithm finds the object of interest in the scene by adopting a dynamic background modelling strategy after which the noise from the foreground image is filtered out in order to determine the position of persons. The experimental results proved the efficiency of the algorithm.

The authors in [6] follow an approach based on machine learning features. This video person tracking algorithm computes a simple motion detection framework through motion blobs and has an advantage of detecting people who are stationary for a period of time.

Our methodology for people detection and differentiation from other types of forms from a video stream generated by a video surveillance system considers the development of an algorithm that detects motion by comparing two consecutive frames extracted at a specific time intervalfrom a real-time video stream. Further, on the resulted comparison,a binarization is applied and a region growing algorithm is used to extract all independent regions from the resulted comparison. Over the extracted regions, a series of features like area of the detected region, dimensions of a box that would include the detected region or the Euler number of the detected region are computed to differentiate people form from other detected forms.

2. Methodology

The video surveillance system performs real-time monitoring of a perimeter and generates an alarm only when persons are detected in the supervised area.The system must trigger the alarm to notify the supervisors of the monitored area. Thus, when the alarm is triggered, the proposed algorithm must present in a clearly way the scene in which a person was detected.

The proposed methodology for motion detection and people recognition in a specific area supervised by a surveillance camera is based on frames extraction at specific time interval from the real-time video stream and a series of processing steps that are applied over the extracted frames.

The proposed system goes through two stages.In the first stage, the system detects motion in a certain scene and identifies the form of that object (whether person or something else).In the second stage, the system triggers an alarm if the identified form is a person form based on proposed characteristics.

Motion detection from the video stream is realized by making a subtraction on grayscale level between two consecutive frames extracted at a specific time interval (one second interval was used in the current algorithm). Assuming frame F_1 is extracted at t_1 timestamp and frame F_2 is extracted at $t_2=t_1+1$timestamp, a difference frame is obtained, like in (1):

$$F_D = F_1 - F_2 \tag{1}$$

in which the absolute value of each pixel subtraction is memorized.

Even though this subtraction of consecutive frames will expose all pixels for which there is a difference in value from one frame to the other and thus, a potential motion in these pixels, a series of processing tasks for the difference frame F_D are required to eliminate the pixels that do not belong to a significant region from the supervised area.

First processing task is represented by the global binarization of the difference frame F_D. To compensate the illumination variations caused by weather conditions that can change instantaneous and a possible inadequate contrast between background and the detected moving regions and due to the fact that a fast binarization algorithm is required, the Otsu binarization method [8] is used in the proposed algorithm.

Otsu binarization method performs histogram form-based image thresholding to reduce a gray-level image to a binary image. This method takes into consideration two classes of pixels (e.g., foreground and background) and it calculates an optimum threshold *t* value that would separate those 2 classes in order to obtain a minimal combined spread (intra-class variance). Thus, the required threshold *t* is the one that minimizes the intra-class variance defined in (2) as the weighted sum of variances of the two classes [7].

$$\sigma_w^2\ t\ = q_1\ t\ \sigma_1^2\ t\ + q_2\ t\ \sigma_2^2\ t \tag{2}$$

In (2), q_1 and $q_2$represent the class probabilities of different gray-level pixels and they are computed based on image histogram *P* as it follows:

$$q_1\ t\ = \sum_{i=0}^{t} P(i) \qquad q_2\ t\ = \sum_{i=t+1}^{255} P(i) \tag{3}$$

Further, σ_1 and σ_2 represent the individual class variances for the 2 defined classes (e.g., foreground and background) [9] and they are computed as in (4).

$$\sigma_1\ t\ = \sum_{i=0}^{t} i - \mu_1\ t\ ^2 \frac{P(i)}{q_1\ t} \qquad \sigma_2\ t\ = \sum_{i=t+1}^{255} i - \mu_2\ t\ ^2 \frac{P(i)}{q_2\ t} \tag{4}$$

where μ_1 and μ_2 represent the class means for each class (5).

$$\mu_1\ t\ = \sum_{i=0}^{t} \frac{i \cdot P(i)}{q_1\ t} \qquad \mu_2\ t\ = \sum_{i=t+1}^{255} \frac{i \cdot P(i)}{q_2\ t} \tag{5}$$

After computing the optimum threshold *t* based on Otsu technique, the difference frame F_D is binarized at pixel level based on the threshold *t* and the binary difference frame F_{Dbin} is obtained, as in (6) where each pixel of F_D is compared with the Otsu threshold.

$$F_{Dbin}\ i,j\ = \begin{matrix} 0, F_D\ i,j\ < t \\ 1, F_D\ i,j\ \geq t \end{matrix} \quad (6)$$

The second processing task is the labelling of all independent regions from F_{Dbin} with the aid of a region growing algorithm[9] [10]. The input parameter of the region growing algorithm is represented by F_{Dbin}image and the output is a similar image $R_{Dbin}$with the same dimension in which each white pixel from F_{Dbin} has a value corresponding to the number of the independent region to which it belongs.

In order to compute R_{Dbin} image, the region growing algorithm starts from the top left corner pixel of F_{Dbin} and it iterates on line and column each pixel of F_{Dbin}until it finds the first white pixel $P_{i,j}$positioned at row i and column j. This means that the first element of the first independent region was found and the value of this element is set to 1 in R_{Dbin}image.

After setting the first pixel $P_{i,j}$ of the first independent region, the algorithm must check for other pixels that might belong to this region. Thus, it checks each white neighbour of $P_{i,j}$ if it is set in R_{Dbin}image and if not, the algorithm sets that the value of those specific neighbours to 1 in R_{Dbin}image. This process of neighbours check is done repeatedly until there are no white neighbours available.

Further, after labelling the elements of the first regionR_1, the region growing algorithm will iterate all the other pixels of $F_{Dbin}$and it applies the same steps as for region R_1.

Finally, a set of independent regions R is obtained as in (7).

$$R = R_1, R_2, \dots, R_n \quad (7)$$

where R_k,k=1,...,nrepresents a collection of white pixels from F_{Dbin}image that are labelled with k value in R_{Dbin} image and n represents the number of independent regions labelled in R_{Dbin} image. Consequently, all R_k,k=1,...,n regions are disjoint as in (8) meaning that any pixel from F_{Dbin}image is found in only regionR_k ,$k=1,\dots,n$ extracted by the region growing algorithm.

$$R_{k_1} \quad R_{k_2} = \emptyset with k_1 \neq k_2;\ k_1 = 1, \dots, n; k_2 = 1, \dots, n; \quad (8)$$

After identifying all independent regions from F_{Dbin}, the proposed algorithm calculates the following characteristics for each region:

- the dimensions of the smallest rectangle that contains the region
- area of the region
- the Euler number of the region.

These geometric features create an identity card of each region in order to uniquely differentiate the regions.

The smallest rectangle that contains region $R_k$is defined as a rectangle type sub-image of F_{Dbin} image that includes all pixels of region R_k. For this characteristic, 2 properties are of interest: the width W_{rec} and the height H_{rec} of the rectangle.

The area of a region R_k is computed as in (10) where p represents the number of pixels that belong to R_k region.

$$A_{R_k} = \sum_{l=1}^{p} l \quad (9)$$

On the other hand, the Euler number [11] which establishes the homogeneity of the image is computed as below since there is one compact object present in R_k region.

$$E_{R_k} = 1 - H_{R_k} \quad (10)$$

where H_{R_k} represents the number of holes from the R_k region.

The decision part of the proposed algorithm is based on the 3geometric characteristics and it establishes that a region R_k is a person if:

- ✓ $H_{rec} > W_{rec}$
- ✓ $A_{R_k} > 4000$
- ✓ $E_{R_k} > -40$

The alert module is the process of alerting the operator that the system detects a person who enters the perimeter which is surveillance with the camera. Practically, the alarm should be triggered if the form that was detected by the proposed algorithm is classified as being a person. The alert process can be replayed as a warning message or by marking the region of the detected form.

3. Experimental results

The proposed paper for the person detection that enter in a specific perimeter is based on a TCP/IP type network with specific features for acquiring, viewing and storing images obtained with a surveillance camera.

The equipment includes as it is shown in Figure 2:

- 1 IP camera
- SwitchPoE
- PC
- Power source 24 V
- Ethernetcable

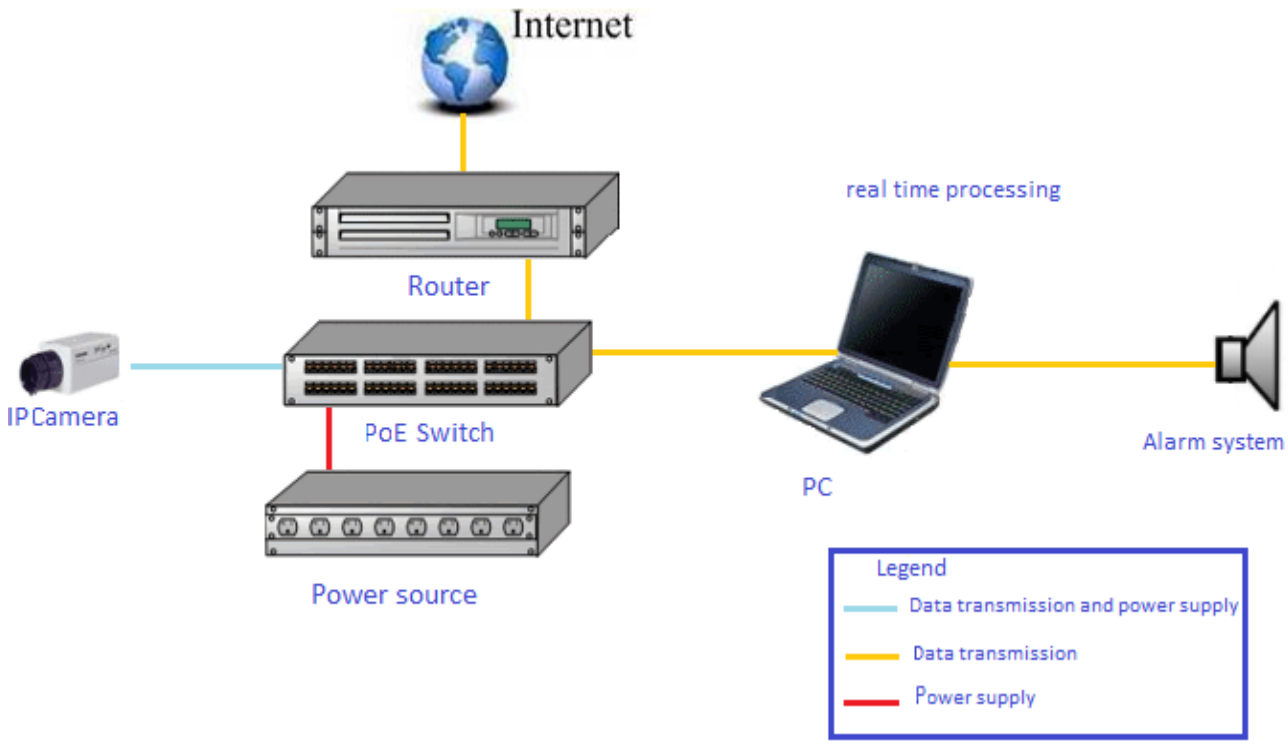


Fig. 2. Proposed System Architecture

The proposed algorithm was tested on a series of monitored areas.

In Figure 3, there are 2 frames extracted from an area where no person is present, but motion is still detected because of the weather conditions. However, after achieving the difference between the two frames extracted at some random timestamps from the video stream, motion was detected, andthe proposed algorithm computed 14 regions suitable for analysis. By computing and applying the 3 proposed characteristics for each region, all the regions are eliminated, meaning that none of regions contains a person form and in this case, the alarm is not triggered.

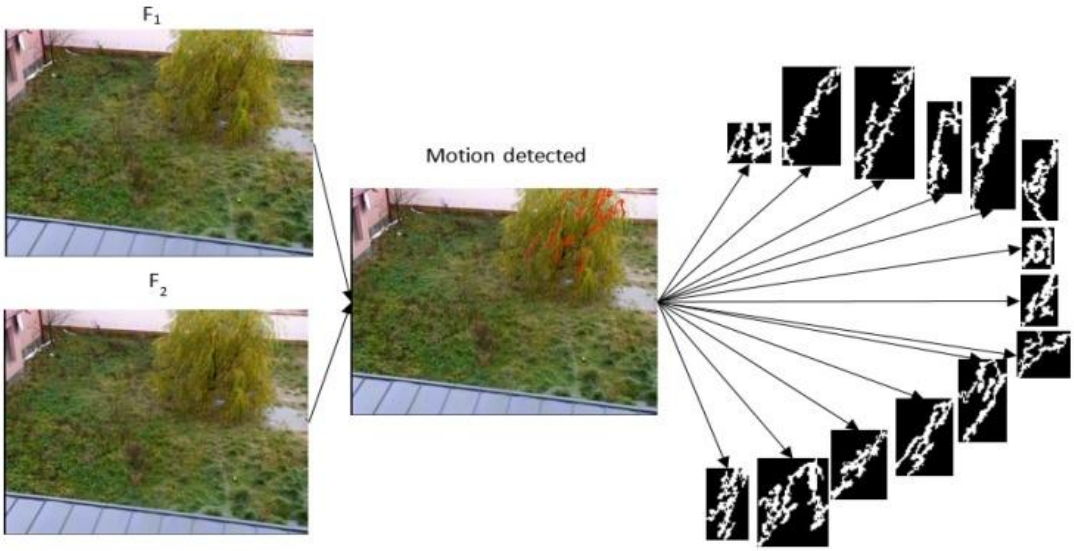


Fig. 3. Motion detection in a non-person area

Several results of the proposed methodology for the people detection in 2 different areas are presented in figures 4 and 5. In both cases, 2 frames were extracted at consecutive timestamps from the video stream of the 2 areas in which a person generates the detection of motion.

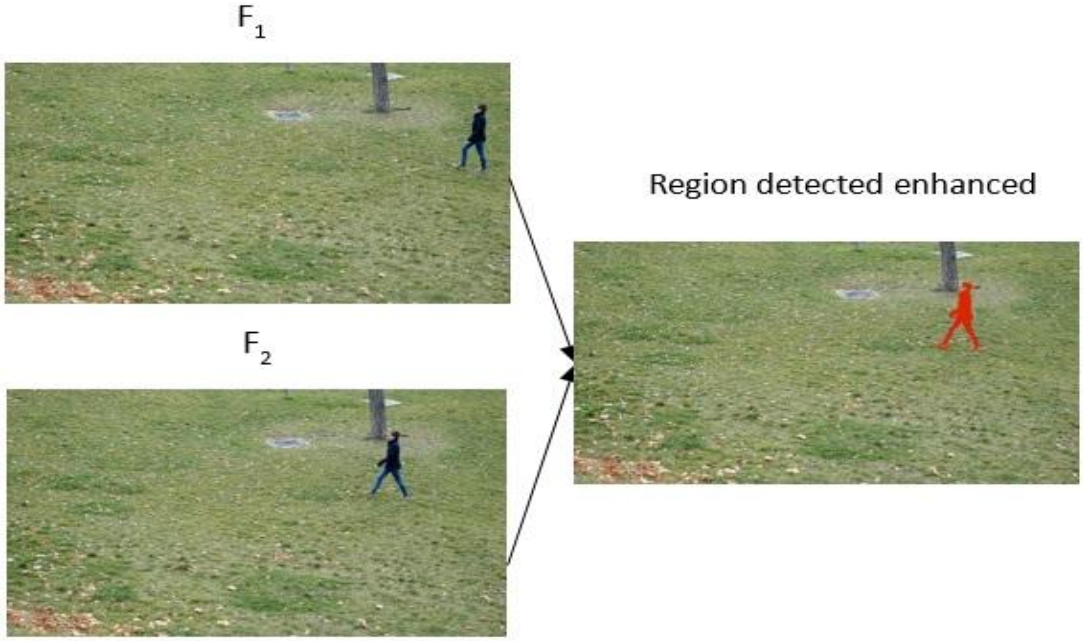


Fig. 4. Motion Detection in a person area(1)

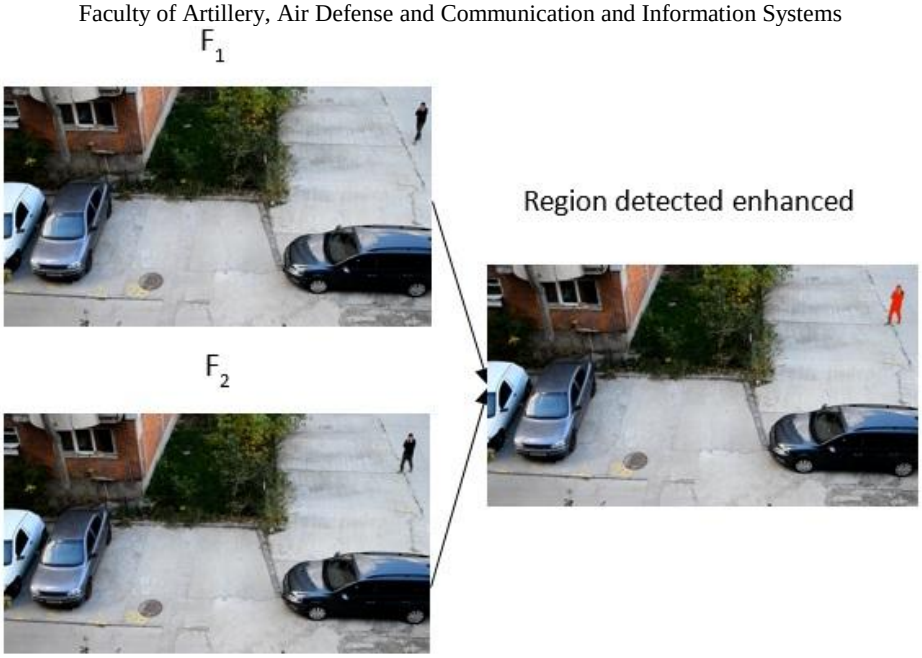


Fig. 5. Motion Detection in a person area(2)

6. Conclusions

The algorithm developed in this paper demonstrated reliable results in people detection using a video surveillance system and it also provided a satisfactory delimitation in form recognition (if is a person who entered in that perimeter or not). The algorithm was used on different environments (areas with a lot of vegetation or parking zones) and every time the results were correctly classified.

References:

[1] Zhengyan Zhang, Jingjie Yan, Guanming Lu, Haibo Li, Ning Sun, Qi Ge, "Multiscale Adaptive Local Directional Texture Pattern for Facial Expression Recognition", KSII Transactions on Internet & Information Systems, Vol. 11, Issue 9, pp. 4549-4566, 2017.

[2] Wilbert G. Aguilar, Marco A. Luna, Julio F. Moya, Vanessa Abad, Humberto Parra, Hugo Ruiz, "Pedestrian Detection for UAVs Using Cascade Classifiers with Meanshift", Semantic Computing (ICSC), pp. 509 – 514, 2017.

[3] Qiang Zhu, Mei-Chen Yeh, Kwang-Ting Cheng, S. Avidan, "Fast Human Detection Using a Cascade of Histograms of Oriented Gradients", Computer Vision and Pattern Recognition, pp. 1491 – 1498, 2006.

[4] Qi He, Kuixiang Liu, Lei Qu, "Efficient and robust indoor people detection based on RGB-D camera", Chinese Automation Congress (CAC), pp. 1063-1068, 2017.

[5] Vincenzo Carletti, Luca Del Pizzo, Gennaro Percannella, Mario Vento, "An efficient and effective method for people detection from top-view depth cameras", Advanced Video and Signal Based Surveillance (AVSS), pp. 1-6, 2017.

[6] Imran Ahmed, Awais Ahmad, Francesco Piccialli, Arun Kumar Sangaiah, Gwanggil Jeon, "A robust features based person tracker for overhead views in industrial environment", IEEE Internet of Things Journal, Vol. PP, Issue: 99, 2017.

[7] Nobuyuki Otsu, "A Threshold Selection Method from Gray-Level Histograms", IEEE Transactions on Systems, Man, and Cybernetics, Vol. 9, Issue 1,pp. 62 – 66, 1979.

[8] Ningbo Zhu, Gang Wang, Gaobo Yang, Weiming Dai , "A fast 2d Otsu thresholding algorithm based on improved histogram", CCPR, pp. 1-5,2009.

[9] N. Ikonomatakis, K.N. Plataniotis, M. Zervakis, A.N. Venetsanopoulos, "Region growing and region merging image segmentation", Digital Signal Processing Proceedings, Vol. 1, pp. 299 – 302, 1997.

[10] Weihong Cui, Zequn Guan, Zhiyi Zhang, "An Improved Region Growing Algorithm for Image Segmentation", Computer Science and Software Engineering, Vol. 6, pp. 93 – 96, 2008.

[11] William K. Pratt, "Digital Image Processing", Second Edition, John Wiley & Sons, New York, 1991.

M. N. Mutafchiev,

MATHEMATICAL MODEL OF THE INTERNAL BALTIC PROCESS RUNNING IN A RELEVANT SOLID FUEL ENGINE

Marian N. Mutafchiev

marian_mutafchiev@abv.bg
Todor Kableshkov University of transport, Transport Equipment Department
158 Geo Milev Str , 1574 Sofia, BULGARIA

***Abstract**: Presentation of a detailed quasi stationary thermodynamic model of the internal ballistics process running in a relevant solid fuel engine. A new equation and methodology for its solution is presented as well as a comparison with experimental data proving the authenticity of the learned results.*

***Keywords**: internal ballistics, rocket engine with solid fuel.*

МАТЕМАТИЧЕН МОДЕЛ НА ВЪТРЕШНОБАЛИСТИЧНИЯ ПРОЦЕС, ПРОТИЧАЩ В РАКЕТЕН ДВИГАТЕЛ С ТВЪРДО ГОРИВО

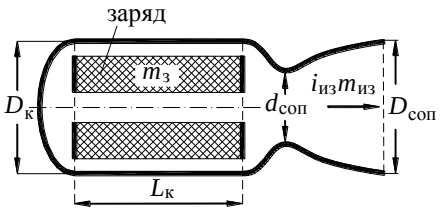
Мариан Н. Мутафчиев

marian_mutafchiev@abv.bg
Висше транспортно училище ”Тодор Каблешков”
Катедра “Транспортна техника”
ул. “Гео Милев” 158 София 1574, БЪЛГАРИЯ

Вътрешнобалистичният процес, протичащ в камерата на ракетните двигатели с твърдо гориво, може да се опише както количествено, така и качествено, като се апроксимира с отворена термодинамична система с подвижни и неподвижни граници, за която е в сила уравнението

$$dQ_з + idm_{из} = d(Mu) + pdV + dQ_w ,$$

където $dQ_з$ е елементарно количество топлина, отделено при изгарянето на заряда; $idm_{из}$ - енталпията на изтичащите газове; Mu - вътрешната енергия на газовете в камерата; pdV - работата (в случая е нула); dQ_w - топлинните загуби.



Фиг. 1. Схема на ракетен двигател с твърдо гориво

Подвижна граница на системата в случая е горящата повърхност на заряда, при което се увеличава обемът, но не се извършва работа. Примерна апроксимационна схема на ракетен двигател с твърдо гориво, по която е създаден представеният математичен модел, с основните означения е показана на фиг. 1.

След преработване се получава следното основно уравнение за определяне диференциала на температурата:

(1) $$dT=(k-1)T\left(\frac{\bar{Q}_з dm_з}{MRT}-\frac{dm_{из}}{M}-\frac{dV}{V}-\frac{dQ_w}{MRT}\right)-T\frac{dm_з}{M},$$

където k е показателят на адиабатата; $\bar{Q}_з$ - специфичната топлина на изгаряне на горивото; $m_з$ - масата на заряда; M - масата на газовете; R - газовата константа; V - обема на камерата; Q_w - топлинните загуби.

Текущата стойност на температурата се определя с израза:

(2) $$T_i=T_{i-1}+(dT)_{i-1}.$$

Налягането се определя с уравнението за състоянието:

(3) $$p=\frac{RMT}{V}.$$

Текущата стойност на обема се определя от израза:

(4) $$V_i=V_к-\frac{m_з-m_{зi}}{\rho_з},$$

където $V_к$ е обемът на камерата; $\rho_з$ - плътността на заряда; $m_з$ -масата на заряда; $m_{зi}$ - текущата стойност на масата на заряда.

Топлинните загуби се определят с израза:

(5) $$dQ_w=\lambda\pi D_к L_к(T-T_w)\Delta t,$$

където: λ е коефициент на топлопредаване; $D_к$ - вътрешния диаметър на камерата; $L_к$ - дължината на камерата; T - текущата температура на газовете; T_w - температурата на околните стени; Δt - интервала от време.

В критичното сечение на соплото се установява местната звукова скорост, която от своя страна е функция на температурата и се определя с израза;

(6) $$a=\sqrt{kRT_к}.$$

С тази скорост се определя дебитът през соплото

(7) $$\dot{m}_{изi}=a_i f \rho_{гi\text{-}1},$$

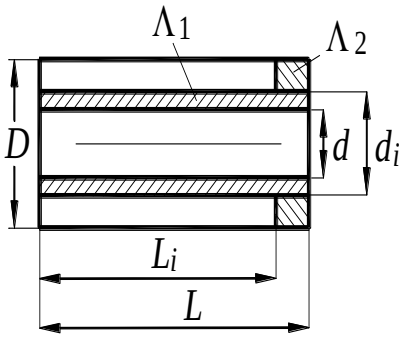
където: $\rho_{гi}=\frac{M_i}{V_{кi}}$ е плътността на газовете в камерата.

Елементарната маса на изтичащите газове се определя с израза:

(8) $$dm_{изi}=\dot{m}_{изi}\Delta t.$$

Масата на газовете в камерата се определя с израза:

(9) $$M_i=M_{i-1}+dm_{зi}-dm_{изi}$$



Фиг. 2. Схема на горенето на заряда

където: $dm_{зi}$ е елементарната маса газове, която се образува в камерата при горенето на заряда.

За определяне на елементарната маса газове, която се образува при горенето на заряда, се приема геометричен закон на горене. По-долу ще бъде доказано, че това предположение за условията на камерата на ракетен двигател с твърдо гориво е напълно оправдано. Приема се, че зарядът има цилиндрична тръбна форма и гори по вътрешната цилиндрична повърхнина и едната странична повърхнина, както е показано на фиг. 2. Останалите повърхнини се приемат за бронирани, при което се очаква прогресивен характер на горенето. Като пример за приетата апроксимация е използвана реактивната противотанкова граната ПГ9, предназначена за противотанковото оръдие СПГ9М.

Определянето на изгарящия обем от заряда за единица време се извършва съгласно фиг. 2. Горящият обем по вътрешната цилиндрична повърхнина се определя с израза:

$$\Lambda_1=\frac{\pi}{4}\left(d_i^2-d_{i-1}^2\right)L_{i-1};$$

Горящият обем по страничната цилиндрична повърхнина се определя съответно с израза:

$$\Lambda_2=\frac{\pi}{4}\left(D^2-d_{i-1}^2\right)\left(L_{i-1}-L_i\right);$$

За текущата стойност на сумарния горящ обем се получава:

(10) $$\Lambda_i = \Lambda_{i-1} - \frac{\pi}{4}\left[\left(d_i^2 - d_{i-1}^2\right)L_{i-1} + \left(D^2 - d_i^2\right)\left(L_{i-1} - L_i\right)\right],$$

където: d_i е текущата стойност на вътрешния диаметър; L_i - текущата стойност на дължината на заряда.

Текущата стойност на вътрешния диаметър се определя с израза:

(11) $$d_i = d_{i-1} + 2u\Delta t\ ,$$

където: u е скоростта на горене на твърдото гориво.

Текущата стойност на дължината на заряда се определя съответно с израза:

(12) $$L_i = L_{i-1} - u\Delta t\ .$$

Скоростта на горене на твърдото гориво се определя с израза:

(13) $$u = BT_{\text{к}}\ .$$

където: B е коефициент зависещ от естеството на горивото.

Тук трябва да се отбележи, че скоростта на горене на барута (горивото) се определя като функция на температурата в камерата, а не на налягането както се утвърждава в класическата теория на вътрешната балистика.

След като е определен обемът на изгорялата до даден момент част от заряда, става възможно определянето на масата на барутните газове, които са се образували, с израза:

(14) $$m_{\text{з}i} = m_{\text{з}} - \Lambda_i \rho_{\text{з}}\ .$$

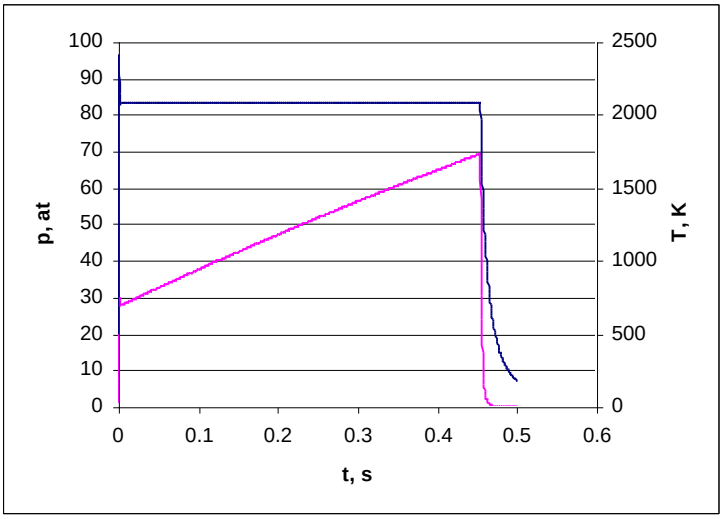
Елементарната маса газове, която се образува в камерата при горенето на заряда, се определя с израза:

(15) $$dm_{\text{з}i} = \Delta m_{\text{з}i} = m_{\text{з}i} - m_{\text{з}i-1}\ .$$

С това се затваря цикълът по определянето на параметрите в камерата на ракетния двигател с твърдо гориво.

Индикаторната диаграма на реактивна противотанкова граната ПГ-9, изчислена с гореописаната методика, е показана на фиг. 3. От фигурата се вижда, че температурата остава постоянна по време на горене на заряда, докато налягането расте прогресивно, следвайки закона за горене на заряда.

След като са определени температурата и налягането в камерата, става възможно да се определи температурата в края на соплото при презумпцията за фиг. 3.



Фиг. 3. Изменение на температурата и налягането в камерата на ПГ-9

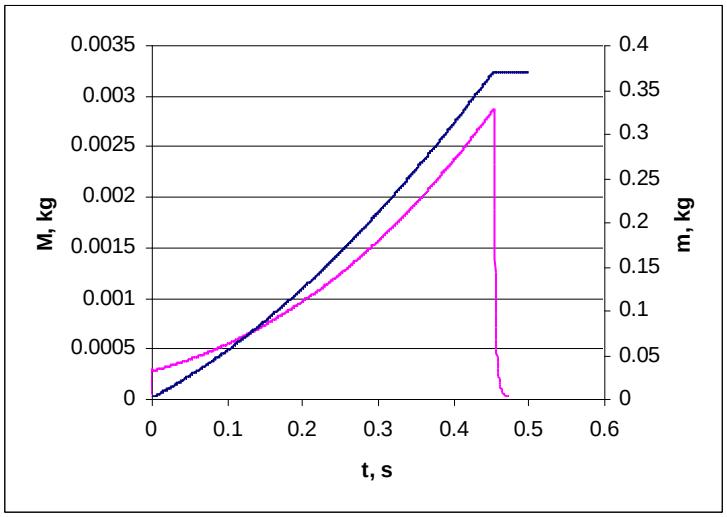
адиабатно разширение с израза:

(16) $$T_{\text{соп}} = T_{\text{кам}}\left(\frac{p_{\text{о}}}{p_{\text{кам}}}\right)^{\frac{k-1}{k}}\ .$$

Следва да се определи плътността на газовете с уравнението на състоянието:

(17) $$\rho_{соп} = \frac{p_o}{RT_{кам}}.$$

След като се определи масовият дебит на газовете през соплото със (7), при тази особеност, че изтичането през най-тясното сечение на соплото става с местната звукова скорост, се определя скоростта на газовете на сопловия срез чрез закона за непрекъснатостта с израза:



Фиг. 4. Изменение на масата на газовете в камерата и масата
на продуктите на горенето на заряда на реактивната граната ПГ-9

(18) $$w_{соп} = \frac{\dot{m}}{f_{соп}\rho_{соп}}.$$

Показателно за адекватността на методиката е изменението на масата на газовете в камерата на двигателя, което е показано на фиг. 4. От фигурата става ясно,че притокът на газове от горенето на заряда е по-голям от разхода през соплото, поради което масата на газове в камерата расте по време на горене на заряда.

След като са определени скоростта и дебитът на газовете на сопловия срез, се определя теглителната сила с израза [1, 4]:

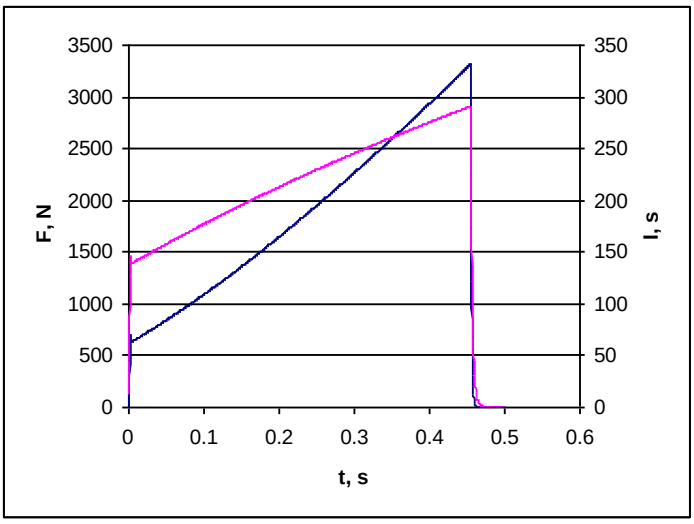
(19) $$F_т = w_{соп}\dot{m}.$$

Горният израз е пряко следствие от постановките на Мещерски и Циолковски за движение на тяло с променлива маса.

Специфичният импулс като контролен параметър се определя с израза:

(20) $$I_y = \frac{F_т}{\dot{m}.10}.$$

На фиг. 5. е показано изменението на теглителната сила (долната крива) и специфичният импулс на реактивната граната ПГ-9.



Фиг. 5. Изменение на теглителната сила и специфичния импулс
на реактивната граната ПГ-9

За проверка на достоверността на математичния модел са използвани данни за външната балистика на гранатата ПГ-9. Единствената известна информация, която може да бъде използвана за проверка, е максималната скорост на гранатата, която се получава след ускоряването `и от реактивния двигател. За целта е достатъчно да се разгледа хоризонталното движение на гранатата, като се отчете въздушното съпротивление и се пренебрегне гравитацията. В такъв случай за определяне пътя на гранатата от закона за движение се получава изразът:

$$x_i = \frac{F_{\text{т}} - R_x}{m_{\text{гр}i}} \Delta t^2 + \text{v}_{i-1} \Delta t + x_i \,,$$

където: $F_{\text{т}}$ е теглителната сила на реактивния двигател, определена с (19); R_x - силата на въздушното съпротивление; $m_{\text{гр}i}$ - текущата стойност на масата на гранатата.

Скоростта на гранатата се определя съответно с израза:

$$\text{v}_i = \frac{F_{\text{т}} - R_x}{m_{\text{гр}i}} \Delta t + \text{v}_{i-1} \,.$$

Ключов момент от това изчисление е определянето на въздушното съпротивление. Началната скорост на гранатата е 430 m/s, а максималната 700 m/s, което означава, че по време на работа на реактивния двигател тя се движи с надзвукова скорост в скоростен диапазон, в който коефициентът на челно съпротивление се променя в тесен диапазон. При това положение можем да се възползваме от теорията на Сиачи [2] и да се работи със среден коефициент на челно съпротивление за посочения скоростен диапазон. Силата от въздушно съпротивление се определя с израза:

$$R_{xi} = f_{\text{гр}} \rho_{\text{въз}} \frac{\text{v}_{i-1}^2}{2} c_x \,,$$

където: $f_{\text{гр}}$ е челната площ на гранатата; $\rho_{\text{въз}}$ - плътността на въздуха; c_x - коефициент на челно съпротивление (0,645) [2].

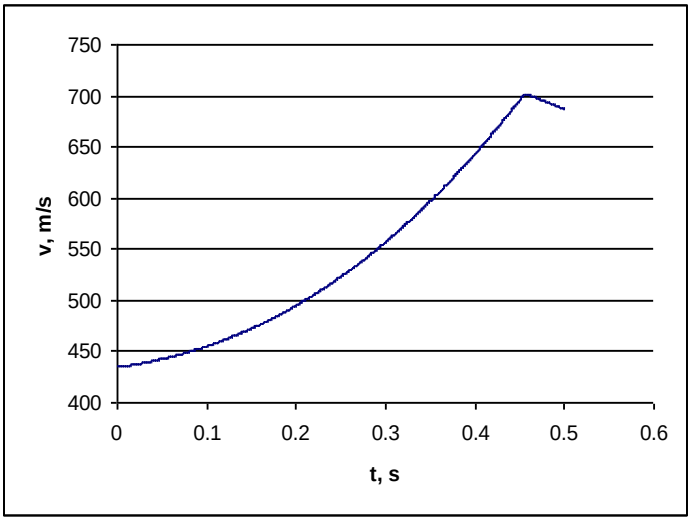
От особена важност е да се отчете изменението на масата на гранатата вследствие на горенето на заряда, тъй като масата на последния е съизмерима с масата на гранатата.

Текущата стойност на масата на гранатата се определя с израза:

$$m_{\text{гр}i} = m_{\text{гр}} - \sum dm_{\text{соп}} \,,$$

където: $\sum dm_{\text{соп}}$ е сумата от елементарните маси на газовете, изтичащи през соплото от началото на горене на заряда до текущия момент.

На фиг. 6. е показано изменението на скоростта на гранатата ПГ-9 по време на ускоряването й от реактивния двигател.

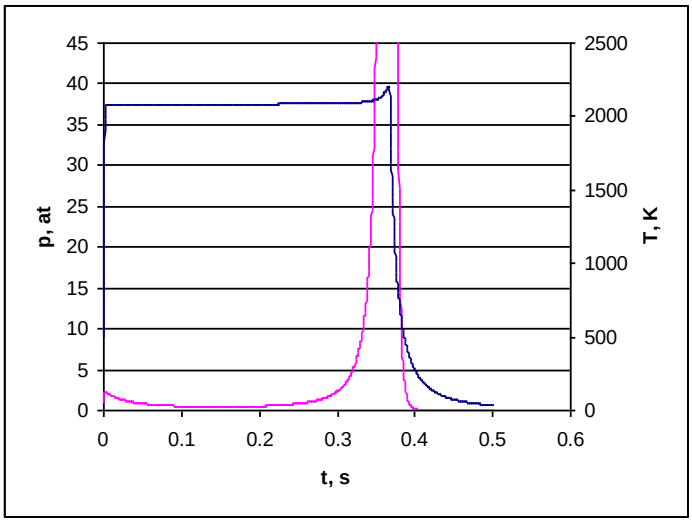


Фиг. 6. Изменение на скоростта на гранатата ПГ-9
по време на ускоряването `и от реактивния двигател

От фиг. 6 се вижда, че максимумът на кривата е точно 700 m/s. Точната изчислена стойност на скоростта е 701,95 m/s, което ще рече, че разликата със заводската стойност е 0,27%. Подозрителна точност, но това се получава при описаните по-горе условия.

Показаните сравнителни резултати би трябвало да дават достатъчно основание да се признае за висока достоверността на представената методика за определяне на вътрешнобалистичните параметри на ракетните двигатели с твърдо гориво.

На фиг. 7 е показан резултатът от изчисленията за температурата и налягането в камерата при условие, че за определяне на линейната скорост на горене на горивото е използвана зависимостта й от налягането ($u = Ap_к$).



Фиг. 7. Изменение на температурата и налягането в камерата на ПГ-9

От фигурата се вижда ясно, че резултатът за налягането е катастрофален, няма нищо общо с действителността. Това дава основание да се допусне хипотезата, че скоростта на горене на горивото при малки налягания до 200-300 at. се намира в много по-проста зависимост от температурата (13), отколкото от налягането. При това възниква въпросът: необходимо ли е да се търси сложната зависимост от налягането, при положение че простата зависимост от температурата дава достатъчно точен резултат.

Научни новости:

1. Представено е ново уравнение за количествено и качествено описание на вътрешнобалистичния процес (1).

2. Представена е методика за количествено и качествено описание на вътрешнобалистичния процес, протичащ в камерите на реактивните балистични двигатели (ракетни двигатели с твърдо гориво), без да се употребяват никакви относителни величини, като: относително количество на изгорялото гориво ψ, относителна дебелина на горящия свод z [3, 4]. и др.

3. Представени са факти, даващи основание да се издигне хипотезата, че скоростта на горене на горивото при малки налягания се намира в много по-проста и пряка зависимост от температурата (13), отколкото от налягането.

Последното твърдение се представя от автора като хипотеза, тъй като все още не са проверени всички възможности и подробности, свързани със скоростта на горене, и представената методика от него лично.

References:

1. Кувеко А. Е., Мирополски Ф. П. Внутренняя баллистика стволных систем и ракетные двигатели твердого топлива. издание ВВИА Н. Е. Жукоского, 1987. 310 с.

2. Коновалов А. А., Николаев Ю. В. Внешная баллистика. 1979. 231 с.

3. Мутафчиев М. Н. Математично моделиране на процесите, протичащи в цевните оръжия и топлинните двигатели, дисертация за получаване на научна степен „Доктор на техническите науки”. София, 2016.

4. Никитин В. А., Швыкин Ю. С., Юрманова Н. П. Термодинамические основы внутренней баллистики, ТулГУ, Тула, 2004.

SUPPLY AS A BASIC LOGISTIC FUNCTION IN CONTEMPORARY MILITARY CONFLICTS

Georgi I. Dzhurkov

National Defense College „G.S.Rakovski", Bulgaria, 1124 Sofia, Oborishte,
"Evlogi i Hristo Georgievi" Blvd 82
georgidzhurkov@abv.bg

Abstract: *The paper reveals contemporary challenges in front of supply systemss. Supply is considered as a function of solving certain tasks. The article discusses the essence, parameters and characteristics of providers. An exemplary algorithm for deciding on the type and number of providers is published. A structural diagram of the logistic support through outsourcing is presented. The advantages of using contractors are analyzed.*

Keywords*: Logistics, supply system, supply chain, type and number of providers, outsourcing, contractors.*

1. Introduction

The constant evolution of the challenges facing the security system, both national and international, is unconditionally a major driving force for the development of military capabilities. Modern security threats are a complex tangle of variable dangers. Increasingly important in our times, we find unfavorable phenomena and processes such as: international terrorism, local and regional conflicts, fragile or disintegrating states, cyber-threats, illicit trafficking in human beings and weapons, threats to energy supplies and their asymmetrical relations, forming an unfavorable environment for development. Additional factors with negative impacts are: continuous climate change, environmental degradation and consequent hazards, natural disasters and man-made accidents, pandemics, etc. While conventional military conflicts are more of a history, the flexible sharing of "hard" and "soft" tools (diplomacy, socio-economic and cultural attractiveness) is becoming an important factor in achieving strategic goals in modern reality.

2. The supply system in contemporary military conflicts

2.1. Strategy and logistics

Undoubtedly, there is a close link between the strategy of conducting the military operation ("hard" force) and its logistics, which determines the development of the logistic system as a process based on military strategic and logistic solutions. In it the logistic system depends mainly on two strategic decisions:

- Military formations readiness.
- Supposed requirements for the implementation of comprehensive logistics.

The first strategic decision determines the logistical challenges in function of the available of formations' reaction time. It is fundamental in terms of the level of material stockpile, its scheduling, its retention in readiness for military use, the deadlines for triggering pre-concluded contracts, etc. The second solution is fundamental to the requirements of the logistic system during the operation (Figure 1).

The built logistic system must ensure certain levels of autonomy, stability and mobility of the battle formations. [4].

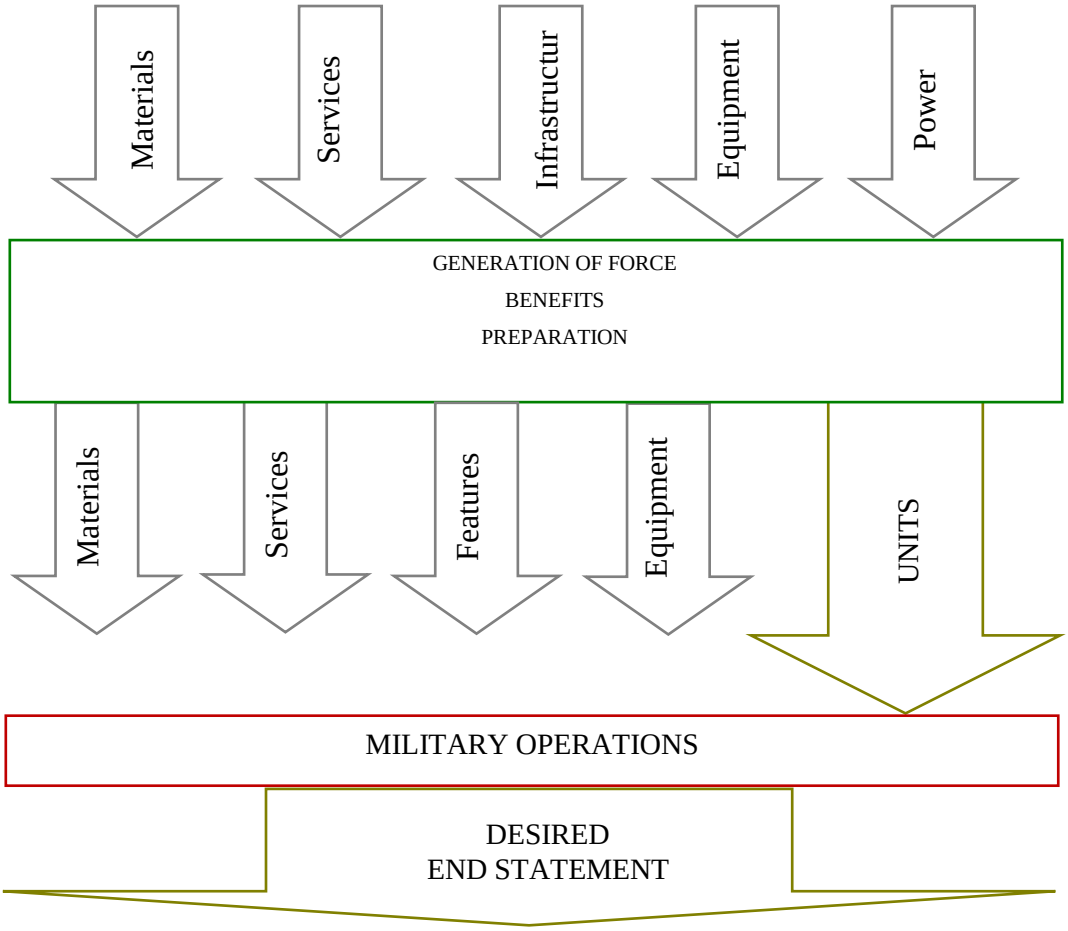


Figure № 1. Influence of logistic system on the desired end statement

A major challenge in front of logistic systems in modern military operations are supply and services. It is a basic functional logistical area which covers: organizing, conducting, coordinating and implementation of events in order to meet the needs of military materials and resources.

The procurement system is built to timely and fully meet the material needs of the formations. Its optimal construction ensures reliable information on the available resources, their qualitative and quantitative status, the available stocks and the needs for the operation.

Established supply chains are a collection of at least three elements: source of resources, supplier and user. Their continuous interaction securing the continuous movement of products, services, financial resources and information flows from and to consumers. They are considered to be internal (exist only for the needs of the military component of the operation), external (based on a comprehensive interaction between the military and civilian components) and mixed. In practice, it is virtually impossible to use any of the listed forms in pure form. The continuous interaction between them leads to the construction of a network of supply chains, which is characterized by numerous working links between physical and information flows, competences and abilities of the staff, as well as personal relationships. Their operation is based on common principles, taking into account the specific requirements of distributed material. The purely military supply chains aim to minimize distance between resources and their customers. This undoubtedly defines the requirements for reliability, flexibility and security. [6]

Supplying as a functional area of logistics in military operations is the solution of the four main tasks, which have been presented in Figure 2.

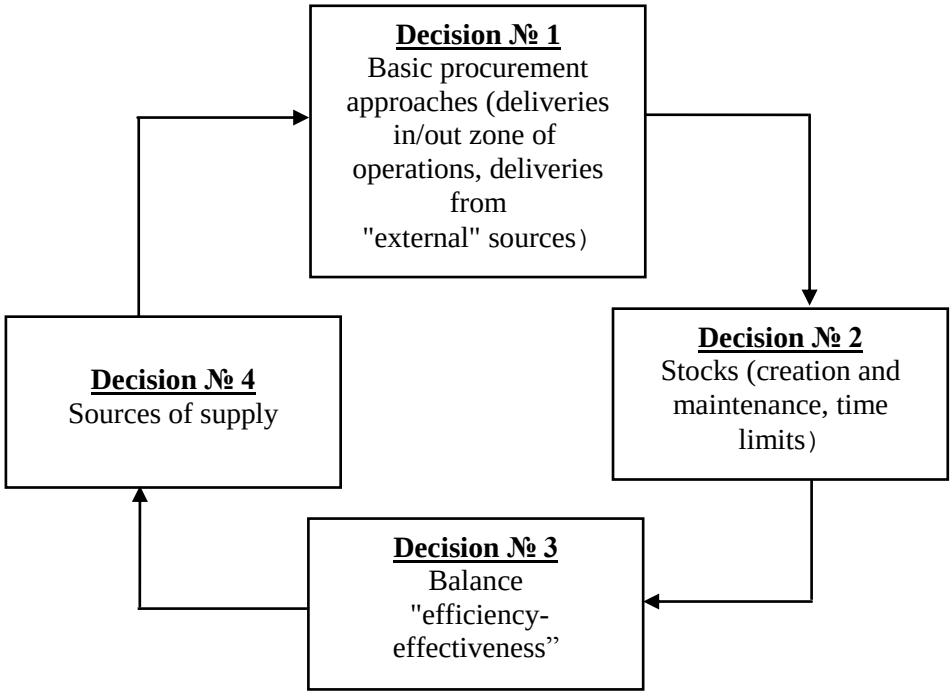


Figure № 2. Key solutions for supply

Making a decision on the deliveries, their receipt in the operation area and the use of "external" sources is justified by the likely duration of the operation and the transport capabilities of the logistic formations. Part of the total amount of materials are in the formations (battles and logistics) during their deployment. Another part is obtained in the mission area, through local suppliers or through the mechanisms of multinational logistics. The third method is delivery with a source outside the operation area. In modern military conflicts the processes of supply are mix of alternatives. The likelihood that the ratio of preferences is reciprocal is minimal. Always one of the approaches will have a leading role. Applying variance in the choice of alternatives as well as their skillful combination contributes to the high sustainability, reliability and flexibility of the supply system and increases the logistic autonomy of the formations.

The decision on stockpiling and echeloning of material means is directly related to the time of preparation of the formation and its upcoming tasks. Those with a high degree of readiness are pre-stocked with the necessary material resources. For the rest, certain postponements are acceptable. However, there is a full synchronization in the provision of material and services within the time-honored framework. There are two stock planning methodologies in NATO. The Level of Efforts methodology, based on the expected daily norms and the Target Oriented Methodology, which requires a minimum of 95% targeting and is independent of time. Applying the second method makes it possible to calculate stocks of material means decisive for the outcome of combat operations. The Sustaining Planning Module (SPM) module from the Logistics Functional Services (LOGFAS) software module is used to identify the minimal initial inventory of material resources. The same module is used to calculate the inventory needed for a long-term logistical supply of material resources.

These two solutions correlate with the operational requirements. The "efficiency-effectiveness" balance solution is actually a way of balancing the needs and budgetary frameworks that are set in the planning of the operation.

2.2. Types of suppliers and their role

The decision for supply sources is hampered by the large number of suppliers in the field, quality and quantity requirements, deadlines and financial parameters. It is possible to use different types (national, local and multinational) and number (one, only two, many) suppliers. Their characteristics are presented

in Table 1 and the main parameters influencing their choice are presented in Table 2. Combinations of suppliers are available for use (complete or partial) of the supply chains. The choice of suppliers is a function of a high degree of uncertainty and unpredictability in the military operations and possible negative consequences in case of breach of commitments.

Table № 1

Main features of type of suppliers

National supplier	***Local supplier***	***Multinational supplier***
Conduct national requirements for the goods and services provided	They support peace building on their own territory	Existence of cultural and linguistic differences
Competitiveness and competition	Provide shortened delivery time intervals, but lower quality may occur	Need for interdependence, compatibility and coordination in the operation area
High degree of influence of national resources	They fulfill specific requirements	Strong dependence on information exchange technologies
Existence of compatibility, flexibility and coordination requirements with other providers in the operation area	They work in hostile environments	Lifecycle maintenance of specific national defense products

Table № 2

Basic parameters of suppliers according to their number

One supplier	**The only one supplier**	**Two supplier**	**Multiple supplier**
The need for high reliability and quality of supply	The only possible supplier (monopolist)	Ability to use local suppliers	Supply of tangible assets and services under established standards
Low supply chain flexibility	Implementation of high specificity deliveries	Capacity to create inventory	Performance requirements
Vulnerability of supply in the operation area	Deliver high-performance deliveries	Opportunity to choose a vendor	Alternate choice of supplier

An exemplary decision-making algorithm for planning and building the logistic system, type and number of suppliers is presented in Figure 3.

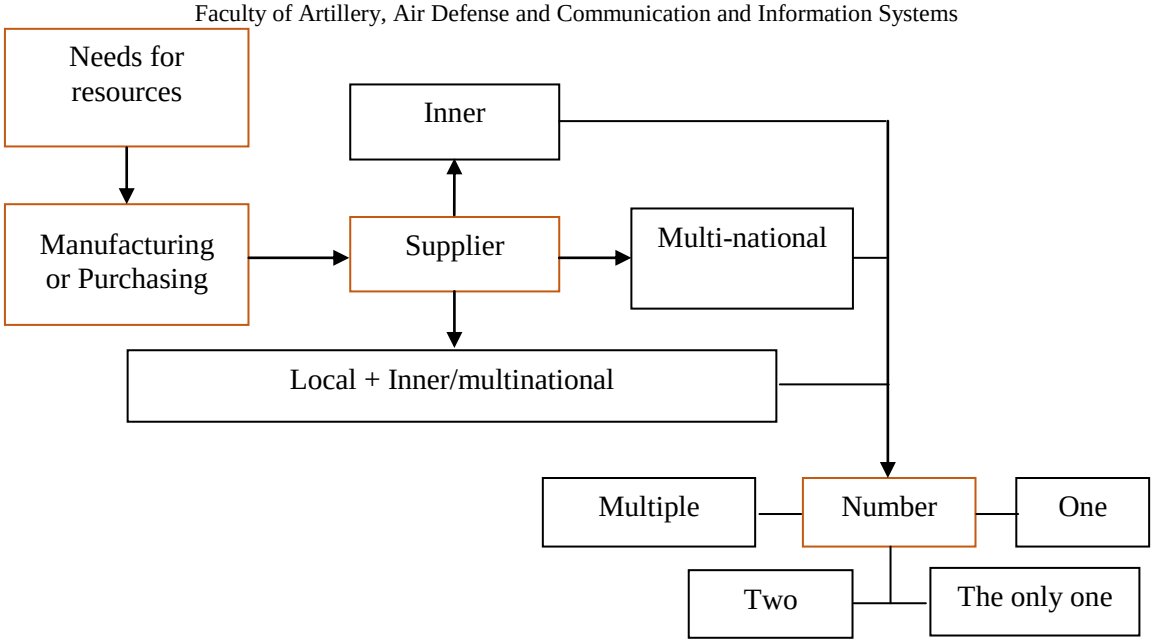


Figure № 3 Example algorithm for decision making on type and number of suppliers

In modern military operations and the constant expansion of the need for a variety of material assets, the role of outsourcing on the planning and implementation of the "supply" functional area is inevitably increasing. Its indisputable advantages can be grouped into several areas: providing specialized services in the operation area, providing high-quality delivery and service delivery over a long period of time, low cost and opportunity to realize a wide range of services. [5]

2.3. Contractors - an important element of supply chains

Contractors are part of the complete logistic system for implementing outsourcing solutions. They minimize risks to the recovery of certain deficits but can not fully realize them. The ability to use them quickly requires resources to be stored and maintained in the required characteristics (qualitative and quantitative). This inevitably impedes their operations, being one of the prerequisites for building larger and cumbersome supply chains, creating and storing buffer stocks. The clear long-term vision of their use provides an appropriate timeframe and opportunities for smooth provision of resources and services that would facilitate and optimize the operational planning process. Their use leads to a reduction of "military" logistic personnel in the mission area, but on the other hand creates prerequisites to reduce the flexibility and sustainability of supply chains in unforeseen situations. An exemplary structural diagram of the logistic outsourcing process is presented in Figure 4.

Despite the benefits this form of logistic provides, it hides its risks. Lessons learned from the EUFOR RD Congo operation show that, due to inefficient logistic intelligence, gaps in planning and practically missing controls, it has made it impossible to meet agreed deadlines and quality standards.

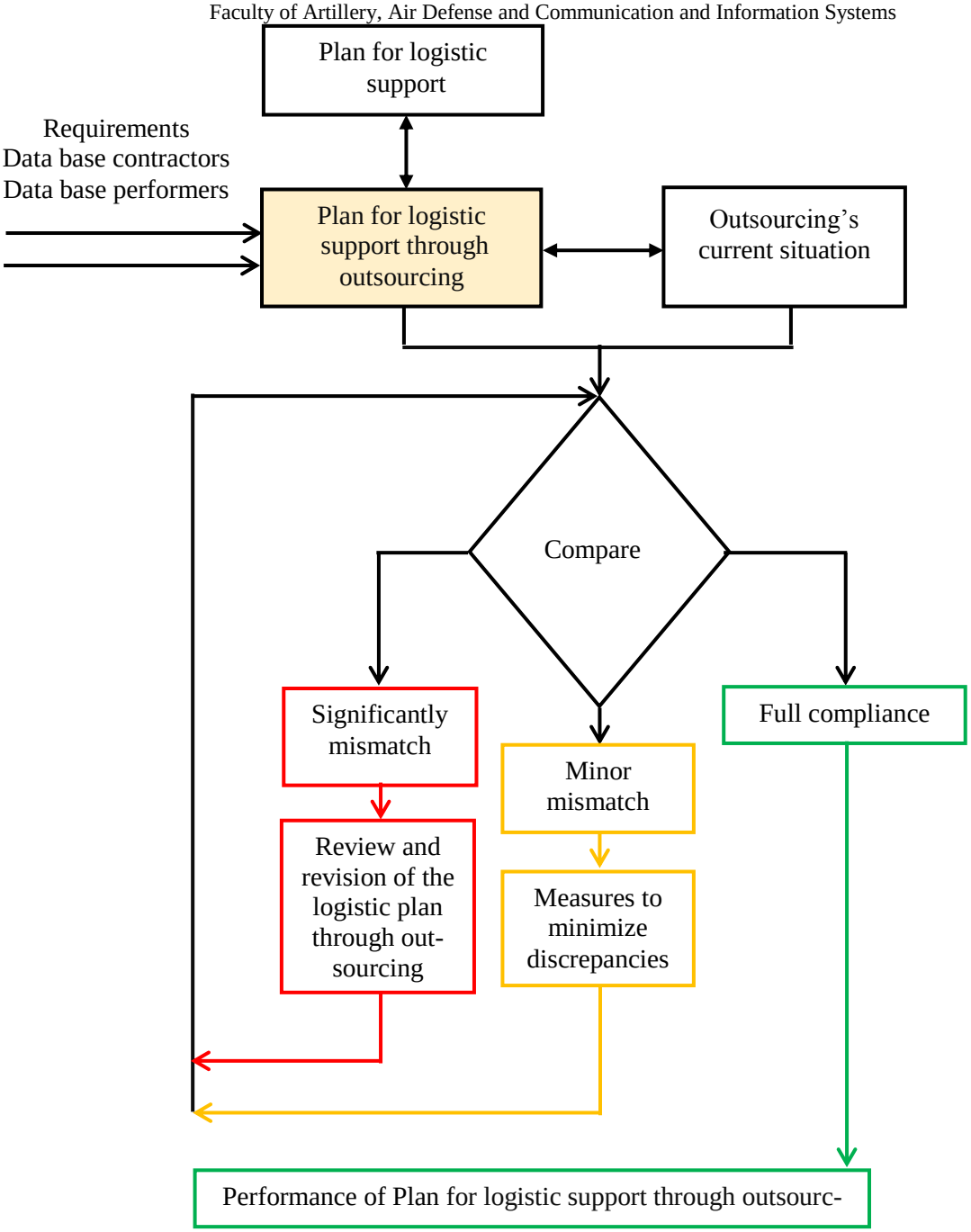


Figure № 4. Structural scheme for logistic support through outsourcing.

Possible early and accurate planning of contractors' activities as part of the overall logistic procurement system ensures a low logistical footprint on the overall planning and conduct of the operation. It takes into account all factors of strategic and operational planning and includes the following minimum requirements:

- Existence of difficulties in securing combat and/or logistic support in short or medium term;
- Opportunities for material shortages in the area of operation when increasing the duration of the operation;
- Opportunities to ensure the shortcomings in the short, medium and long term by using contractors;
- Ability to activate contractors and financial security of the process;
- Creating a reliable mechanism and procedures for controlling the activity of contractors;
- Plan for the withdrawal of contractors from the operational area and an alternative option for supplying resources and providing services to change the security environment.

Proper pre-planning of contractors' operations by phases of the operation would have the following advantages:

- Consistency and economy in the planning and financing of contractors' activities;
- Early identification of the financial parameters associated with the contractor's activity as a function of the duration of the operation;
- Define appropriate requirements for contractors' activity and financial parameters for this;
- Strict differentiation of the responsibilities of contractors and those of "military logistics", rights to use common techniques, procedures and mechanisms, order of interaction and mutual assistance;
- Defining a long-term vision for using contractors, defining requirements for them and ways to implement them.

3. Conclusion

The specificity of modern military operations places high requirements on the effective operation of the logistic system in all phases of the operation. The close interaction between the civilian and military logistic structures, as well as the use of contractors contributes to the realization of logistic support. Building sustainable supply chains would reduce the logistic footprint on operations.

References:

1. Авторски колектив, „Военна логистика”, ВА, София, 2013 г.
2. Доктрина за логистиката, Национална публикация на въоръжените сили на Република България, НП - 4, София, 2012 г.
3. EU Concept for Contractor Support to EU-led military operations, Council of the European Union, 2014
4. EU Military Rapid Response Concept, Council of the European Union, 2014
5. Outsourcing post - conflict operations: designing a system for contract management and oversight. Посетен на 27.06.2017 г. на уеб адрес: http://jpia.prАспектиinceton.edu/sites/jpia/files/2004-2.pdf
6. Skoglund, Per, Sourcing decisions for military logistics in Peace Support Operations, Jonkoping International Business School, 2012.

GUIDELINES FOR IMPROVING AMMUNITIONS SUPPLY IN OPERATIONS

Georgi I. Dzhurkov

National Defense College „G.S.Rakovski", Bulgaria, 1124 Sofia, Oborishte,
"Evlogi i Hristo Georgievi" Blvd 82
georgidzhurkov@abv.bg

Abstract: *The paper reveals proposals to optimize ammunitions supply in the operations. Suggested are the following options: use of pallets and containers, harmonization and modern systems for tracking deliveries. Types of containers are presented. The harmonization program of European Defense Agency is being considered. Projects for tracking cargo have been examined.*

Keywords*: Ammunitions supply, pallets and containers, harmonization program of European Defense Agency, projects for tracking cargo.*

НАСОКИ ЗА УСЪВЪРШЕНСТВАНЕ НА СНАБДЯВАНЕТО С БОЙНИ ПРИПАСИ В ОПЕРАЦИИТЕ

Георги И. Джурков

Военна Академия „Г.С.Раковски",
София, бул. „Евлоги и Христо Георгиев" 82

1. Увод

Въпреки сравнително ниския интензитет на бойни действия в съвременните конфликти, осигуряването на логистична автономност на формированията остава главна задача пред органите за логистично осигуряване. Обезпечаването на потребностите от бойни припаси и взривни вещества (БП и ВВ), както и запазването на качественото им състояние е основна логистична дейност. Въпреки предполагаемата им ниска потребност, те са материални средства решителни за изхода на военните операции.

2. Снабдяване с материални средства в операциите

Постигането на съвместимост на националната логистична система с аналогични системи на коалиционните партньори и с общата такава, изградена в зоната на операцията е безспорно средство за минимизиране на логистичния фактор върху провеждането на операцията. Подсистемата за снабдяване е основна съставна част на цялостната логистична система. За гарантиране на нейното устойчиво и непрекъснато функциониране тя трябва да притежава възможности за планиране, координиране, управление и реализиране снабдяването на формированията, прилагайки дефинираните последователност, форми и принципи на взаимодействие на елементите си чрез използване на изградената комуникационно-информационна система. Също така е необходимо да притежава способности относно получаване на материални средства, създаване на определени запаси, тяхното съхраняване, опресняване и раздаване на потребители. За гарантиране на логистичната автономност на формированията в зоната на операцията е удачно количествата материални средства да се завишават. Това не трябва да е самоцел, а да се основава на предполагаеми очаквани потребности.

Снабдяването с БП и ВВ се извършва чрез използване на общата логистична система. Този процес е съпроводен с извършването на голям обем от товаро-разтоварни работи, като се съчетават механизираното (предимно в стационарните складове и снабдителните формирования на оперативно ниво) и ръчното манипулиране. Допълнителни затруднения възникват от изискванията за тяхното съвместно транспортиране и съхранение, приемане и изпращане, необходимостта за извършване на регламентни работи, организиране на митнически процедури и др.

3. Усъвършенстване снабдяването с бойни припаси в операциите

Високите изисквания за мобилност на логистичните формирования, икономично използване на човешките ресурси при стриктно спазване на мерките за безопасност и все по-голямо разнообразие БП и ВВ използвани в операциите, обуславя необходимостта от усъвършенстване на снабдителния процес и повишаване на възможностите на снабдителните звена.

Един от подходите за усъвършенстване на процесите по снабдяване с бойни припаси е дефинирането и използването на Комплекти от бойни припаси (КБП). Под КБП се разбира съвкупност от бойни припаси с различно функционално предназначение за цялото или само за основното въоръжение на формированията, равна на средноденонощната им потребност и обединена в една или няколко товарни единици. При използването на КБП трябва да се спазват някои основни оперативно-тактически, технически и икономически изисквания към тях като: съответствие между наличните в КБП бойни припаси и средноденонощната потребност от тях; наличие в състава на КБП само на тези бойни припаси, които са необходими за изпълнение на задачите за огнево поразяване на противника, а другите видове бойни припаси от боекомплекта на стрелковите системи да се доставят по отделни заявки; КБП на съхранявани в Национален поддържащ елемент (НПЕ) трябва да се състои от КБП на националните формирования, консуматори на бойни припаси; транспортиране на бойните припаси до потребителите без преобразуване; използване на широко разпространени и универсални средства за уедряване на товарните единици; възможност за използване на съвременни средства за механизация на товаро-разтоварните работи с максимално натоварване; приемлива стойност. Предвид изложеното за същността и изискванията на способа за снабдяване чрез използване на КБП и изхождайки от характера на функционирането на изпълнителната подсистема за снабдяване с материални ресурси в частта й за снабдяване с бойни припаси и от масата на средноденонощната потребност от бойни припаси за ББГ е целесъобразно бойните припаси да се товарят и съхраняват в контейнерите в снабдителните подразделения на формированията. В таблица 1 са предоставени логистичните характеристиките на различните видове контейнери.

Таблица 1

Видове контейнери

Вътрешна дължина	Вътрешна ширина	Вътрешна височина	Ширина на вратата	Височина на вратата	Обем Капацитет	Тегло тара	Тегло на товара (максимално)
20 ft. стандартен контейнер							
5,900 м 19'4"	2,350 м 7'8"	2,393 м 7'10"	2,342 м 7'8"	2,280 м 7'6"	32,2 куб.м. 1,172 Cft	2 230 кг 4,916 Lbs	21 770 кг 47,900 Lbs
40 ft. стандартен контейнер							
12,036 м 39'5"	2,350 м 7'8"	2,393 м 7'10"	2,342 м 7'8"	2,280 м 7'6"	67,7 куб.м. 2,390 Cft	3 700 кг 8,160 Lbs	26 780 кг 59,040 Lbs
20 ft. (Open top) отворен контейнер							
5,894 м 19'4"	2,311 м 7'7"	2,354 м 7'8"	2,286 м 7'6"	2,184 м 7'2"	32,23куб.м. 1,136 Cft	2 400 кг 5,280 Lbs	21 600 кг 47,620 Lbs
40 ft. (Open top) отворен контейнер							
12,028 м 39'5"	2,350 м 7'8"	2,345 м 7'8"	2,341 м 7'8"	2,274 м 7'5"	65,5 куб.м. 2,350 Cft	3 850 кг 8,490 Lbs	26 630 кг 58,710 Lbs
40 ft. (High Cube) отворен контейнер							
12,036 м 39'5"	2,350 м 7'8"	2,697 м 8'10"	2,338 м 7'8"	2,585 м 8'5"	76,3 куб.м. 2,694 Cft	3 970 кг 8,750 Lbs	26 510 кг 58,450 Lbs
20 ft. (Flat Rack) контейнер							
5,620 м 18'5"	2,200 м 7'3"	2,233 м 7'4"				2 530 кг 5,578 Lbs	21 470 кг 47,333 Lbs
40 ft. (Flat Rack) контейнер							

12,080 м 39'7"	2,438 м 6'10"	2,103 м 6'5"				5 480 кг 12,081 Lbs	39 000 кг 85,800 Lbs

Източник: http://www.morfey-logistics.com/bg/menyu-spetsifikatsiya-na-morski-konteyneri.html?start=1

Стандартните контейнери са известни и като многофункционални контейнери. Те са затворени контейнери и се делят на:

- Стандартни контейнери с врата в единия или и в двата края.
- Стандартни контейнери с врата в единия или и в двата края и странични врати по цялата дължина на контейнера от едната или и от двете му страни.
- Стандартни контейнери с врата в единия или и в двата края и врата от едната или и от двете му страни.

Освен това, различните видове стандартни контейнери се отличават по размери и тегло, в зависимост от широкия си диапазон. Обикновено те са 20-футови или 40-футови.

Стените на "Open top" контейнерите в повечето случай са изработени от гофрирана ламарина. Подът е дървен. Покривът е направен от разглобяеми греди, покрити с брезент, конзолата на вратата може да се завърта. Тези две структурни особености значително опростяват процеса на товарене и разтоварване на контейнера. Много по-лесно е контейнерът да се товари и разтоварва отгоре или през вратите с помощта на кран или друг подемен механизъм, когато покривът е свален и конзолата на вратата е завъртяна. Може да се отбележи, че целта на разглобяемите греди на покрива не е само да поддържат брезента, но допринасят и за стабилността на контейнера. Халките за осигурителните въжета, с които товарът се обезопасява, са разположени върху носещите горни и долни странични греди, както и в ъгловите опори на контейнера. Чрез тях се обезопасяват товари до 1000 кг.

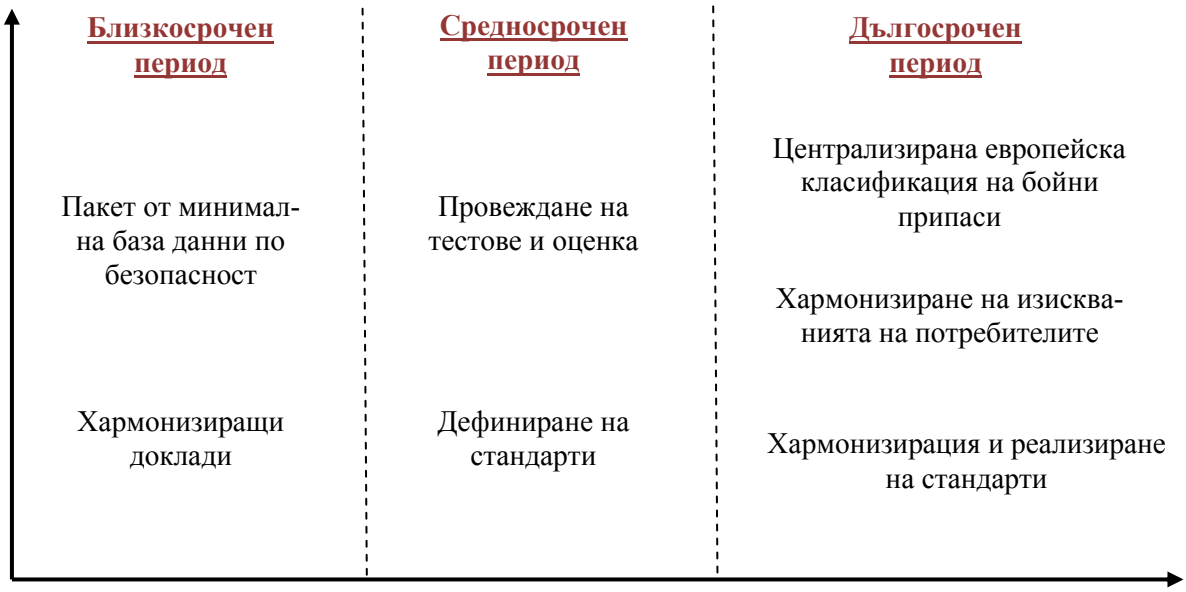
"High Cube" контейнерите са подобни на стандартните, но са по-високи. За разлика от стандартните контейнери, чиято максимална височина е 2591 мм (8'6"), "High Cube" контейнерите са високи 2896 мм (9'6"). "High Cube" контейнерите нормално са с дължина 40 фута, но понякога се използват и 45-футови контейнери.

"Flat rack" контейнерите са изработени като дървена подова платформа, около която има носеща метална рамка, и две вертикални стени в двата края, които са неподвижно закрепени. Тези стени са достатъчно стабилни, за да осигурят при необходимост подреждането на няколко контейнера от този тип, заедно с товара, един върху друг. Обикновено "flat rack" контейнерите са 20-футови или 40-футови. Халките за осигурителните въжета, с които товарът се обезопасява, са разположени върху носещите странични греди, в ъгловите опори и на пода на контейнера. Чрез тях се обезопасяват товари до 2000 кг за 20-футовите и до 4000 кг за 40-футовите контейнери. [3]

Ефективността и качеството на обработка на материалните ресурси, натоварени в контейнерите, зависи от структурата на формированията, натоварени с тези дейности, от наличните средства за товаро-разтоварните работи и от подготовката на личния състав. Тези дейности е целесъобразно да се извършват от формирование с възможности за приемане, съхранение, подвоз и предаване на количество бойни припаси, съгласно потребността за 1-2 дни. За целта то трябва да разполага със съответното количество транспортни и средства за товаро-разтоварни работи на контейнери, като най-добрата опция е използването на контейнеровози. Стратегическото транспортиране на контейнерите се реализира с морски и/или въздушен транспорт.

Друг подход за усъвършенстване на снабдяването с бойните припаси е постигане на максимално ефективна хармонизация. Европейската агенция по отбрана през 2010 г. стартира програма за хармонизация на боеприпаси, като осигурява форум и тематични симпозиуми на национални специалисти по БП и ВВ на страните членки. Тя обхваща цялата гама БП и разглежда всички дейности с тях (транспортиране, съхранение, обслужване и др.) при стриктно спазване на условията за здравословни и безопасни условия на труд. За постигане на оптимални резултати, Агенцията разчита на коректно предоставената информация за спецификата на боеприпасите и взривните вещества от страна на страните членки. Безопасността на боеприпасите и взривните вещества в проекта се разглежда в 3 аспекта: оперативен, финансов и индустриален. Постигането на хармонизация във всеки един от тези аспекти, както и цялостна такава, би довело до максимална опера-

тивна съвместимост между страните членки във всички аспекти, касаещи осигуряването с БП и ВВ, дори до създаването на общи пазари. Практическият резултат от първоначалните конференции е създаването на Европейска мрежа на националните органи по безопасността на боеприпасите-ЕМНОББП (European Network of National Safety Authorities on Ammunition-ENNSA), която работи в тясно взаимодействие с Групата за сигурност на боеприпасите на НАТО-ГСБП (CNAD Ammunition Safety Group-ASG) и експертите на страните-участнички. За дефиниране на амбициите си ЕМНОББП разработва пътна карта, представена на фигура 1.



Фигура 1. Пътна карта за реализиране на процесите по хармонизация на бойни припаси и взривни вещества.

Главните цели пред хармонизацията на бойните припаси и взривни вещества са: Постигането на максимално ефективна хармонизация, като част от стандартизацията с дълговременно влияние дейностите с бойни припаси и взривните вещества; Повишаване на сигурността, както на национално ниво, така и в международна среда и Оптимизиране на финансовите параметри на дейностите с бойни припаси и взривните вещества.

Успешната дейност по проекта е функция от решаването на следните задачи:

- Осъществяване на ефективна комуникация между експерти на всички нива и обмяна на опит;
- Идентифициране и анализиране на национални процедури за класификация на боеприпасите;
- Анализ на прилагането на национални стандарти и процедури, както и възможността за прилагането им в многонационална среда;
- Приложимост на международните стандарти на национално ниво;
- Анализиране на поуки от практиката;
- Анализиране на най-добрите национални практики, надграждането им до международни такива и внедряването им за изпълнение.

Националните изисквания се базират на предполагаемите бъдещи заплахи за националната сигурност, вероятността за участие на Въоръжените сили в бъдещи конфликти и националните военни бюджети. За постигане на пълна хармонизация по програмата на ЕАО е необходим задълбочен анализ на споменатите национални фактори и дефиниране на общи такива за ЕС.

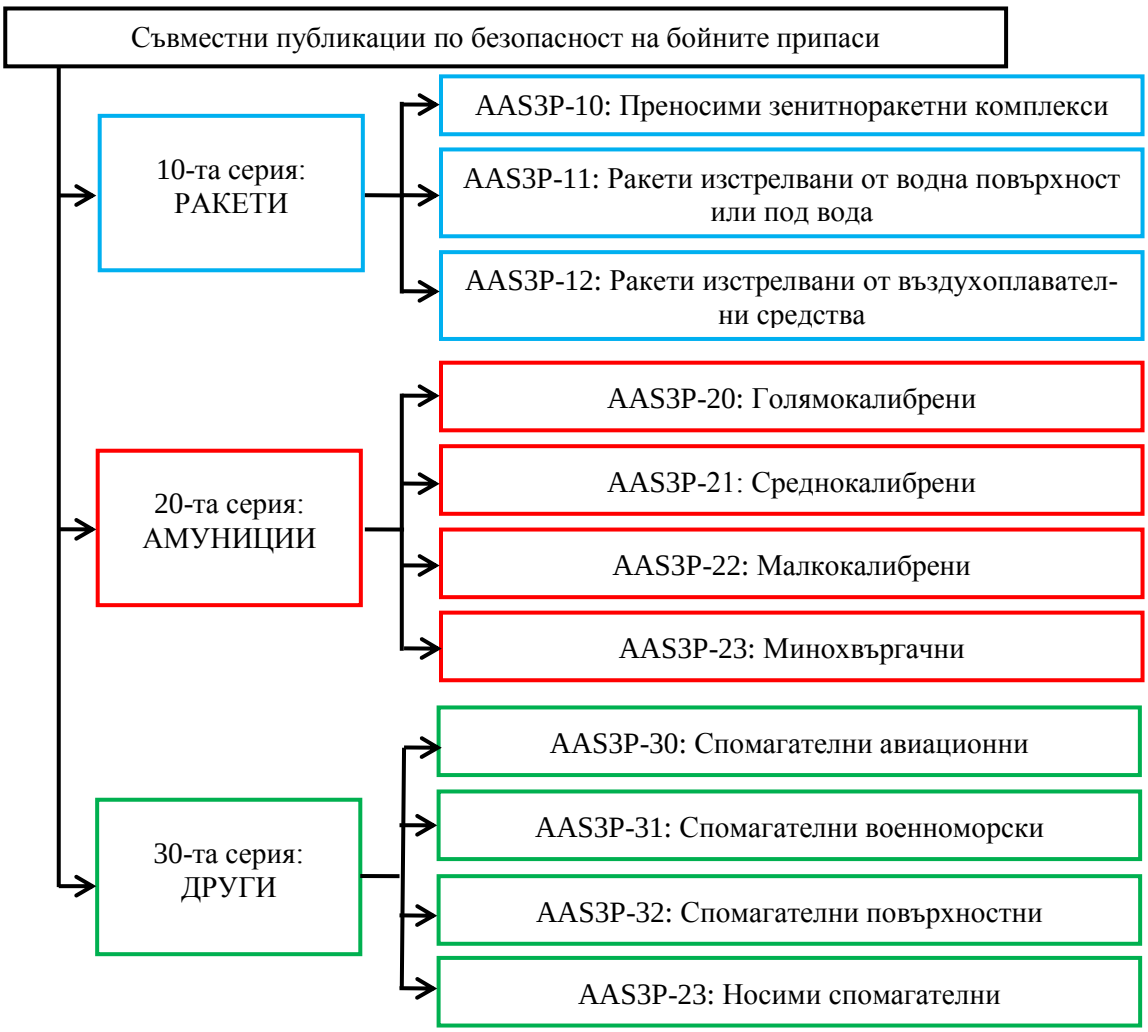
Класификацията за безопасността се обосновава на два аспекта, като това е необходимата минималната информация, представяна от страната участник в многонационална среда:

- Вид на боеприпаса и съставящите го елементи, съгласно международни стандарти;

- Оценка на безопасността, обхващаща всички фази от жизнения цикъл на определения вид боеприпас.

Първоначалната класификация цели осигуряването на приемлив риск от самовзривяване и самозадействане на стартови двигатели. За реализирането и е необходима коректна информация за всички комплектоващи елементи, вид на взривното вещество и резултати от полигонни изпитвания. Всички боеприпаси задължително трябва да съответстват на националните и международни изисквания. При наличие на по-стари образци, несъвместими със съвременните, възниква необходимост от предоставяне на допълнителна информация. Отчитането на спецификата на околната среда цели осигуряване на подходящи условия за съхранение и транспортиране. Тя обхваща следните параметри: температура, влажност, удар, вибрации, електромагнитни въздействия и др.

Постигането на пълна хармонизация се постига чрез стриктното спазване на документите, съгласно фигура 2.



Фигура 2. Съвместни публикации по безопасност на бойните припаси.

В качеството на насока за повишаване ефективността на функциониране на системата за снабдяване с бойни припаси може да се разглежда придобиването от логистичните органи на способности за получаване на информация за месторазположението и състоянието на транспортните средства в реално време чрез внедряването на система за проследяване, която да функционира във всеки един възможен район за провеждане на операция.

Съвременните системи за проследяване и новите концепции за доставки позволяват значително съкращение на доставките, които трябва да са в наличност във войските за операцията до необходимото ниво, като интегрират усилията и увеличават дела на многонационалната логистика на театъра на действие. Те допринасят за чувствително намаляване на “логистичния отпечатък”

в театъра на действие и осигуряват необходимата логистична автономност. Системите за проследяване на запасите реализират изискванията на принципа за прозрачност при движението им по цялата снабдителна верига.

Предимствата от внедряването и използването на подобна система могат да се изразят в следното:

- Ориентация на местността и точно определяне на местоположението на отделните транспортни средства, като и тези за товаро-разтоварни дейности (при наличие на такива);
- Своевременно предаване на данни за състоянието на транспортните средства;
- Оперативно и ефективно управление на снабдителния поток.

Системата трябва да притежава възможности за:

- Изпращане и получаване на съобщения към отделна транспортна единица или транспортна група и създаване на база данни с необходимата информация;
- За включване на базата данни към общата база данни на автоматизираните системи за управление на логистичното осигуряване;
- За настройване на времеви интервал за автоматично връщане на месторазположението на транспортните средства;
- Показване на изминатия маршрут, характерни географски точки и позиции на снабдителните модули върху карта подложка чрез съответната координатна система;
- Създаване и съхраняване на доклади, справки и други справочни документи относно снабдяването на формированията с бойни припаси и взривни вещества.

От съществено значение е системата за проследяване на транспортните средства да е приложима както в стационарни условия, така и от подвижен команден пункт при провеждане на различни операции.

Технологията за радиочестотна идентификация (Radio Frequency Identification-RFID) е най-широкоразпространена за подобряване на ефективността на веригата за доставки. Разработен е проект за автоматичното идентифициране на превозните средства (Automatic vehicle Identification-AVI), който е приложим във всички фази на операцията с изключение на стратегическото придвижване. Съществуват и проекти за проследяване на карго товари. За реализиране на проследяването на товари са необходими следните минимални реквизити: честотномоделирани излъчвател и приемник, декодираща система, електронен продуктов код, име на обекта и физически език за маркиране.

Внедряването на система за проследяване е целесъобразно да се съчетае с използване и на система за маркировка и контрол на материалните средства. Последната е предназначена за осигуряване на транспортната система с пълна и своевременна информация за операции по придвижване, развръщане и поддръжка, като използва един и същи военни процедури и правила в мирно и военно време. Системата трябва да е интегрирана със системите за превозване на товари, за да може да предоставя информация и документация, както за входящите, така и за изходящите транспорти. Освен това, тя трябва да включва широк спектър от възможности за автоматизиране процесите по транспортиране/получаване, развръщане, поддръжка и оттегляне, данни за движението на обектите, издаването на транспортна документация, както и навременна информация до съответното командване.

4. Заключение

Снабдяването в БП и ВВ се извършва в общата снабдителна верига изградена в зоната на операцията, като съставна част на цялостната система за логистично осигуряване на формированията. Голямото разнообразие по вид, калибър и начин на действие на БП, както и изискванията им за съвместимост при транспортиране и съхранение са утежняващи фактори при планиране и реализиране на снабдяването. Постигането на съвместимост несъмнено би повишило ефективността и ефикасността на логистичните органи.

References:

1. Авторски колектив, „Военна логистика”, ВА, София, 2013 г.
2. Доктрина за логистиката, Национална публикация на въоръжените сили на Република България, НП – 4, София, 2012 г.
3. Спецификация на контейнери. Посетен на 28.03.2017 г. на уеб адрес: http://www.morfey-logistics.com/bg/menyu-spetsifikatsiya-na-morski-konteyneri.html?start=1
4. Програма за развитие на отбранителните способности на въоръжените сили на Република България 2020, Министерски съвет на Република България, София, 2015 г.,
5. Outsourcing post-conflict operations: designing a system for contract management and oversight. Посетен на 27.06.2017 Г. на уеб адрес: http://jpia.prАспектиinceton.edu/sites/jpia/files/2004-2.pdf
6. Skoglund, Per, Sourcing decisions for military logistics in Peace Support Operations, Jonkoping International Business School, 2012.

R. B. Chalakov, D. K. Markov,

FACTORS INFLUENCE ON FIRE SUPPORT IN OPERATIONS

Radoslav B. Chalakov, Dilyan K. Markov

Annotation: *The planning and conduct of operations required a "new reading" of the problem of increasing the firepower and the processes of improving the means and forms for the management of the forces and means of fire maintenance. This in turn has led to the need for a timely process of identifying factors that will affect fire maintenance.*

Keywords: *artillery, factors, fire support.*

ФАКТОРИ, ВЛИЯЕЩИ НА ОГНЕВАТА ПОДДРЪЖКА В ОПЕРАЦИИТЕ

Радослав Б. Чалъков, Дилян К. Марков

Анализът на сегашната военна и политическа ситуация в света показва, че в основата на тенденциите в развитието на геополитическите процеси през следващите 10-20 години е възможна борба между държавите по света, чийто основни причини са: политически, икономически, енергийни, териториални, етнически, религиозни, като желанието им да разрешат противоречията помежду им ще бъде с помощта на различни средства, включително използването на *военна сила*[28].

Това води след себе си факта, че *войната на бъдещето става война на интелекта, технологиите, конфронтация, основана на информация и технологично превъзходство!*

Тези параметри, налагат не само внимателното им проследяване, но и своевременно намиране на адекватни решения за усъвършенстване на съществуващи или създаване на нови отбранителни способности.

Огневата поддръжка, като част от отбранителни способности, цели най-вече снижаване на боеспособността на противостоящите сили. Това се постига чрез съвместна огнева поддръжка на сухопътните войски, военновъздушните, военноморските и специалните сили, по военните формирования, обектите и други цели на противостоящите сили, за постигане на тактически или оперативни цели.

Особеността на огневата поддръжка в операциите може да се определи като двупосочен процес, нейната динамика и маневреност зависи от огромен брой **фактори**, чието влияние върху хода и резултата от военните действия често става нееднозначно и повишава степента на несигурност на същата. Положението, развиващо се в хода на операциите се характеризира с голямо разнообразие от връзки и отношения, а неговият специфичен анализ е най-трудният и отговорен момент при вземане на решение за дадена операция.

Както е показано на фигура 1, факторите, влияещи върху ефективността на огнева поддръжка в бойни операции, са разнообразни, но най-значими са тези, които са свързани с начините, по които ще се извършва тя.

[28] *Военна сила е професионална организация, официално упълномощена от суверенна държава да използва смъртоносна или несмъртоносна сила и оръжия, за защити интересите на държавата.*

Фиг. 1. Фактори, влияещи на огневата поддръжка в операции

Всяка една страна може да използва различни методи на водене на операция, но степента на влияние на огневата поддръжка върху посоката на развитието й ще бъде различна, тъй като ще зависи от искания резултат, който трябва да се постигне, обвързвайки се със специфичните условия на ситуацията обуславящи се от различни фактори.

Провеждането на военни операции се извършва с активно и съзнателно противопоставяне/противодействие от ПС, преследващ оперативните си цели. При тези условия ключът към успеха е използването на **изненадващия фактор**. Смачкващата сила на първия огневи налет може да изненада ПС, да ги дезорганизира, да ги доведе до пълна объркаост, така, че да не може да се осигури адекватна съпротива, което без съмнение ще повлияе на ефективността на действията на формированията и на мащабите на техните загуби. Това значително ще отслаби групирането на ПС и значително ще намали способността им за въздействие при последващи действия от страна на маневрените формирования на собствените сили.

Друг фактор от първостепенно значение е **времето,** като продължителност на събитията.

Военната история изобилства от много примери, когато за осъществяване проектирането на операции е било необходимо да се задържат основните групировки на ПС по всяко време, за да се спечели време с цел прегрупиране и концентриране на войски за последващи и евентуални действия. Същевременно увеличаване на продължителността на активните бойни операции може да се окаже неблагоприятно за тяхната ефективност, тъй като това води след себе си до увеличаване на материалните, техническите, енергийните и финансовите разходи и най-вече човешки загуби.

Важно влияние върху ефективността на огневата поддръжка в бойни операции оказва **характерът на взаимодействията**. Координираното прилагане на групи от различни типове и видове сили е възможно само в случай на единство при разбиране на целите, задачите и реда на тяхното изпълнение в пространството и времето. Това единство се постига чрез умело организиране на командването, управлението, комуникацията и взаимодействието на силите.

Опитът от минали години и особено от скорошни военни конфликти дава много примери, когато страната, която има превъзходство в средствата за въоръжена борба, бъде победена в следствие на слабата организация на командването и управлението. В съвременните конфликти изискванията за управление стават още по-строги. Това се превърна в един и същ решаващ фактор както за количеството и качеството на силите и средствата, така и за състоянието на нивата на взаимодействие. Нивото на организация на взаимодействието между силите и средствата за огнева поддръжка също оказва голямо влияние върху резултата на бойните операции, поради факта, че

зависи от използването на възможностите на различните въоръжения, както и интегриране на бойните им потенциали.

Най-важният фактор, който упражнява доминиращо влияние върху курса и резултата на огневата поддръжка в бойните операции **са силите и средствата**, с които разполагат. Средствата увеличават възможността за противопоставяне на огневата мощ на силите на всяка една страна. Възможностите за маньовъра, осигуряват хармонично съчетаване на основните елементи на бойните операции, а огневата мощ, защитата и маневреността, дават възможност за постигане на целта на военните операции за кратко време.

В съвременната военна история такива примери са военните конфликти в Грузия, Сирия и Украйна. Каквито и да са възгледите и симпатиите на експертите, анализиращи силните и слабите страни на действията на страните в конфликта в източната част на Украйна, те се съгласяват, че подобно на събитията на източния фронт по време на Втората световна война, особеността на територията и релефа оказват силно влияние върху бойните действия, а силите и средствата за огнева поддръжка стават основен фактор влияещ върху операцията.

Като основни подфактори, които са определящи за **огневите възможности** на силите и средствата за огнева поддръжка се открояват:

– характера на целта и степента на защитеност от огнево въздействие;
– степента на поразяване (унищожаване, неутрализиране и др.);
– вид на огъня, необходим за изпълнението й;
– калибъра и количеството на привличаните за стрелба средства за огнева поддръжка (минохвъргачки, артилерийски системи, РСЗО, ракетни комплекси);
– количеството и вида на бойните припаси, назначени за изпълнение на задачата;
– условията, при които се изпълнява тя (време, разстояние на стрелбата, способ за определяне на изходните данни за стрелба за поразяване, условия за наблюдение на резултатите от стрелбата и т.н.).

Сред факторите, които трябва да бъдат взети по внимание при планиране на огневата поддръжка в бойни операции е **инфраструктурата,** която обхваща:

– брой на засегнатите обекти,
– тяхното географско разположение (от гледна точка на техния обхват),
– наличието на уязвими точки, тяхната опасност за околната среда,
– нивото на оборудване на съоръженията с активни и пасивни средства за защита и др.

Характеристиките на целите имат значителен ефект върху такъв индикатор за ефективност на бойни операции, тъй като нанесените щети ще възпрепятстват действията на ПС.

Ниво на сигурност и стабилност на военните операции е фактор, влияещ цялостно върху тях, тъй като оказва значително влияние върху организираното и навременно влизане във военните операции на войските (силите) и по-нататъшното изпълнение на възложените задачи.

Степента на влияние на всеки вид сигурност върху резултата от бойни операции е различна и зависи от променящата се ситуация. Ако условията на ситуацията дават възможност за стабилно и непрекъснато снабдяване на войските (силите) с материални и технически средства, тогава влиянието на този фактор ще бъде стабилно.

От друга страна, усложняването на ситуацията може да доведе до трудности при снабдяване и вследствие на това да доведе до намаляване на ефективността на бойните операции. Реализирането на пълните възможности на средствата за огнева поддръжка до голяма степен зависи от ефективността на системите за логистично осигуряване, т.е своевременното и гарантирано снабдяване.

При оценката на нивото на материалната и техническата поддръжка на войските (силите) е необходимо да се вземе предвид икономическото състояние на зоната на операцията по отношение на възможностите за използване на местни ресурси за осигуряване на войските (транспорт, ремонт, медицинско осигуряване и др.).

Сред всички видове сигурност, оперативните видове сигурност, включително разузнаване, електронна война, оперативни прикривания, психологическа борба, ще окажат най-силно влияние върху хода и резултата от военните операции.

Околната среда е един от значимите фактори, влияещи върху планирането на огневата поддръжка. Оборудването на районите в инженерно отношение, използването на методите за повишаване жизнеспособността на войските, възможностите за свобода на действията, влияние на времето върху ефективността на огневата поддръжка в бойните операции са сред факторите на околната среда. Съвременното военно оборудване направи войските по-независими по отношение на климатичните условия, което оказа положително влияние върху живучеста.

Важен фактор за постигането на успех в огневата поддръжка в операцията и за значително минимизиране на собствените загуби е бойната оценка**. Текущият модел на бойна оценка следва да има три основни компонента:**

– оценка на бойните загуби;
– оценка на ефективността на боеприпасите;
– препоръки за повторно нанасяне на удари и водене на огън.

Тя пряко влияе върху решенията за провеждане на огневата поддръжка, както и върху решенията на командирите за поразяване на целите.

Възможности на групировката на ПС са фактор не на последно като значимост и важност влияещ на огневата поддръжка. Характерът и продължителността им зависят от трудни за прогнозиране подфактори, по-важни, от които са:

– решение за възстановяване на боеспособността на целите и на групировките на ПС като цяло;
– мероприятията по реорганизацията и бързото комплектуване на загубилите боеспособност формирования;
– обемът и характерът на ремонтно-възстановителните работи;
– възможностите за попълване на загубите в хода на операцията;
– възможността за бързо прегрупиране, извеждане от боя и въвеждане на свежи формирования и други мероприятия.

Анализът показва, че факторите, влияещи върху ефективността на огневата поддръжка в бойните операции могат да бъдат класифицирани, **чрез тяхната промяна** и **степен на сигурност** както е показано на фигура 2.

Фиг. 2. Класификация на факторите, влияещи на огневата поддръжка в операции

В зависимост от възможността им за промяна, те се разделят на променливи и непроменливи. В областта, свързана с огневата поддръжка, повечето фактори са свързани с променливи такива. Това се дължи на факта, че военните действия са труднопрогнозируеми. В съвременните конфликти отпадна понятието „непрекъснат фронт".

Необходимо е да се отбележи, че последните конфликти в Грузия, Сирия и Украйна се водят на ограничен театър на военните действия с предварително ограничени цели.

Изборът на методи за провеждане на бойни операции, организацията на контрола и взаимодействието, бойният състав и други фактори зависят от правилното планиране. Като основната цел е не унищожаването на ПС, а да бъде убеден, че продължението на конфликта е безсмислен. В този случай говорим за „Войната на изтощение на ПС". Като център на тежестта вече ще бъдат изтощените ПС, защото операциите се водят срещу неголеми професионални и непрофесионални армии.

Като пример е необходимо да се посочи, че при използване на силите и средствата за огнева поддръжка в бойни операции, се променят пространствените и времеви граници на военните действия. Промяната в стойностите на тези параметри може да позволи да се определи разумен метод за провеждане на военни операции, необходимата ефективност на използването на възможностите на огневата поддръжка в бойните операции с минимално възможно ниво на собствените загуби.

На свой ред непроменливите фактори включват тактическите и техническите характеристики на системите, географските координати на стационарните военни обекти, индустриални съоръжения и други.

По степен на несигурност факторите, влияещи върху ефективността на огневата поддръжка в бойните операции, са разделени на **предвидими и случайни**. Броят на предвидимите фактори ще е изключително ограничен. Това се дължи на факта, че ПС се опитват да скрият истинските си намерения и планове. В същото време са известни някои фактори по обективни причини: минималното време за преместване (пренасочване) на сили и средства, минималното необходимо количество на запаса от материални и технически средства, гориво за запазване на бойните способности на единици, обхват на видовете огневи средства и др.

Сред всички видове **случайности,** най-мощното влияние върху ефективността на огневата поддръжка в бойните операции се дължи на случайността, причинена от лошо прогнозираните действия на ПС. Това се обяснява с факта, че силите целенасочено се опитват да разрушат плановете на отсрещната страна и да наложат волята си върху нея в интерес на постигането на поставената цел.

В един недобре функциониращ механизъм при планиране на огневата поддръжка в бойни операции, това може да доведе до отслабване или загуба на контрол върху протичането на военните действия, водещи до загуба на инициативност и други негативни последици.

Едно от най-важните изисквания при планирането на огневата поддръжка е идентифицирането на основните фактори, които имат решаващо значение за посоката и резултата на операцията. Не е необходимо да се анализират само основните фактори. Изисква се да се изследват вторични фактори, тъй като на определен етап от бойните операции тяхното значение може да се промени в зависимост от преобладаващите условия. Такива фактори са:

– способи за преминаване на войските в настъпление (с изнасяне от дълбочина или от непосредствено съприкосновение);

– отдалечението на изходния район за настъпление от предния край на отбраната на ПС;

– организация на отбраната;

– наличните сили и средства за провеждане на огневата подготовка на атаката в настъпателни операции;

– ролята и мястото на сухопътния компонент в настъпателната операция на съвместните оперативни сили;

– ролята на близкия бой при решаването на задачата за нанасяне на главния удар в отбраната на ПС;

– началното съотношение на силите и средствата към началото на близкия бой и исканото съотношение на завършващия етап от операцията;

– наличното време за организиране и провеждане на огневата подготовка на атаката и други.

В заключение, следва да се подчертае, че при вземането на решение за операциите е изключително важно не само да се обмисли възможността тези фактори да повлияят на курса и резултата от военните действия, а да се проучат и обмислят фактори в тяхната цялост и взаимна зависимост.

Факторите, оказващи влияние върху ефективността на огневата поддръжка в бойните операции, са разделени на **предвидими и случайни.** Но и в двата случая няма разделяне по важност, защото изискванията при планирането на огневата поддръжка, е да се идентифицират основните фактори, които ще имат решаващо значение за посоката и резултата на операцията. Важно е да се изследват и вторичните фактори, тъй като на определен етап от бойните операции тяхното значение може да се промени в зависимост от преобладаващите условия.

Като най-важен фактор за постигане целите на операциите, водени с обикновени средства, може да се открои надеждната огнева поддръжка, завоюване и непрекъснато удържане на огнево превъзходство над ПС при всякакви условия на обстановката.

References:

1. Доктрина за сухопътни операции.
2. Доктрина за съвместно определяне и поразяване на целите.
3. http://dokwar.ru/publ/vooruzhenie/artillerija_i_rszo/perspektivy_razvitija_artillerii/14-1-0-942;
4. http://www.mediapool.bg/files/224/Ukraine_%20Russia%E2%80%99s%20new%20art%20of%20war%20-%20FT.pdf.

K. S. Davidov, Ts. G. Tsonev,

APPLYING OF THE SYSTEMATIC APPROACH FOR THE CANNON BARRELS DESIGN

Krasimir S. Davidov*, Tsonio G. Tsonev**

** University of Shumen "Bishop Konstantin Preslavski" Technical Sciences Faculty; Department Logistics; krasi_dav@abv.bg*
*** National Military University "Vasil Levski", Artillery, AAD and CIS Faculty, coni19@abv.bg*

Abstract: *The report scrutinizes the possibility of applying the systematic approach for designing the barrel of an artillery system.*

Key words: *logistics; modernization; combat vehicle.*

The changing of the character of combat action necessitates a constant searching for new qualitative opportunities for the creation of complexes of weapons having higher performance indicators. To achieve this, a detailed analysis of the conditions of their operation, optimization of the composition and characteristics of all subsystems is required based on an objectively chosen, physically measurable criterion. Performing a detailed analysis of the weapons complex of a self-propelled artillery or towed artillery system is inconceivable without a systemic approach. [2]

In the designing of artillery systems, it is particularly important to be justified the structure of the armament complex on the basis of new technical solutions for its elements and the system as a whole. Of particular importance is the determination of a rational combination of the complex parameters, which ensures the joint fulfillment of three requirements: sufficiency of the striking action of the ammunitions, easy exploitation and high efficiency of the armament.

When it is applied the system approach to solving the problem, the properties of the combat machine can be represented as a structural scheme. At the top level of the structure, there are four basic properties: firepower, security, mobility and the totality of operational and technical capabilities. In each of the abovementioned properties there are internal properties that can also have their own structure. Depending on the goals pursued, the division of the structure of properties can be at several levels (usually a maximum of 6 ÷ 7) [8].

The barrel is part of the artillery system designed to guide the projectile's motion when shot and to deliver his necessary speed. The construction of the barrel largely determines the combat qualities of the weapon complex as a whole. The barrel is designed based on a chosen ballistic solution and of its construction in a large extent depends the structures of the other elements of the weapon system.

The design of the cannon barrel is a logically connected set of constructive methods, ensuring the obtaining of a working structure that satisfies the specific requirements imposed on the barrels. It is necessary that the design to be preceded by an analysis of the requirements imposed on its construction, the study of existing structures of artillery barrels and their peculiarities.

The general requirements that must be met by the construction of the cannon barrel derive from the analysis of several subsystems of a different type in which the barrel is an element. The type of these subsystems depends on the type of the designed artillery complex. Performing a system analysis provides the opportunity to formulate a private technical assignment (PTA) required for the design of a weapon barrel. The same should contain all the necessary requirements and output data for the cannon barrel structure.

It is advisable to perform the system analysis in the following order:

1. The barrel is considered as an element of the ballistic system "barrel-charge-projectile" which provides the required initial velocity of a projectile with a given caliber and mass. Completing the

ballistic design of the cannon barrel gives clarity for the barrel channel construction data, charging conditions, and ballistic characteristics of the shot.

Because the internal ballistic process is characterized by particularly high power and thermal stresses of the barrel and with high dynamics and cyclic repeatability, the first requirement in the design of cannon barrel is to provide the necessary strength. This can be done using design techniques that take into account the actual barrel functioning conditions in the “barrel-charge-projectile” system. The requirements for strength of the cannon barrel can largely be satisfied by using of special steel. They provide barrel resistance against the effects of chemical products from the incineration of the charge and combine both hardness and elasticity.

2. The rear barrel portion is viewed as a part of the channel closure node, whereby requirements related to the reliability of the closure node may be set. The rear part of the barrel must have increased strength, especially at the spot where is connected with channel closure node, in order to be ensured reliable obturation of the gunpowder gasses and undertaking the strength effort of the shot.

3. The barrel is presented as the primary element of the cannon. In this case, the barrel must have a mass that provides acceptable dynamic characteristics. In the early stages of design, this can be determined by the speed of free recoil of the prototype guns. Additionally, the barrel must have a certain length according with the accepted length of the recoil. Additionally, barrel expansion caused by pressure and temperature should not result in its wedging in the cradle.

4. Consider the barrel as an element of the rising and rotating parts of the artillery system. In this case, the barrel must have an acceptable mass and rational positioning of the center of the mass relative to the axes. This will provide acceptable inertial characteristics of the movable parts and optimal characteristics of the directing mechanisms and the balancing and stabilizing mechanisms.

5. The barrel is regarded as the primary functional element of the artillery system, which it is the element of the weaponry system, which includes the artillery system, the ammunition, the vehicle, the fire control devices, etc. The barrel as part of the complex is assigned a great deal of tasks related to the accuracy of the shooting. Keeping the accuracy of the shooting when it is given a specified number of shots set in the Technical Specification depends largely on the barrel design and its resistance to wear. Taking account of these considerations, the construction of the barrel's leading barrel part must meet the requirements for reliable stabilization of the projectile and good resistance to wear.

6. The barrel is considered considering its affiliation to a specific production system. Because the cannon barrel is a very complex detail, the early stages of the design must take into account the possibilities for its manufacturing. The manufacturing system should incorporate the most economical technological means for the production, taking into account the existing equipment, technologies and production prospects.

After performing the system analysis of the subsystems to which the barrel belongs, the technical specification can be formulated. In this specification, besides the mandatory internal ballistic characteristics are included also requirements for the strength, dimensions, center of the masses and inertial characteristics, requirements for the materials used, wear and performance characteristics and other input information are included.

The general concepts of the design of cannon barrels refer not only to a barrel-monoblock but also to barrels of other types.

The construction of the barrel must be made on the basis of the private technical assignment and the requirements for modern guns. The solving of the task for designing of a cannon barrel begins with the design of the simplest barrel construction, namely: barrel-monoblock.

In the early stages of the design (conceptual design) of the barrel-monoblock the following main activities must be carried out:

1. Justification of choosing the charging method, constructing its corresponding charging chamber and carrying out the design calculations.

2. Designing the leading portion of the barrel channel including: selecting the method for guidance of the projectile in the channel; choosing the shape of the cuts and calculating the number and size of the cuts, etc.

3. Pre-selection of the external shape of the barrel and selection of material for its manufacture. Here must be noted the joining of the barrel with the closure node, the presence of additional devices, the way of guiding the barrel in the cradle when recoiling, etc.

4. Calculations of the transverse strength of the barrel and specification of its structural dimensions. Calculating the actual mass of the barrel and the position of its center of the mass. Correcting the outer contour of the barrel to obtain the optimum mass and position of the center of the mass.

The mass of the barrel must satisfy the required free recoil speed *Vm*, which for the different types of turret is as follows:

- for powerful systems *Vm* is in the range 8 ÷ 12 m / s;
- for tank guns *Vm* is in the range 10 ÷ 15 m / s;
- for gauntlets *Vm* is in the range of 14 ÷ 20 m / s.

The resulting factual value of the barrel mass as a result of the calculations must correspond to the desired free recoil speed. This is not strictly determined, and if the actual mass of the barrel is diverted within ± 20%, it is assumed that the barrel design is satisfactory with respect to the mass. Otherwise, a mass adjustment is made by changing the construction, dimensions or material.

5. Final determination of the dimensions of the barrel and verification of the transversal strength after correction of the dimensions.

The calculations for barrel warm-up, the wear estimate and the duration of its operation are usually performed at the design stage.

The specified design tasks are logically arranged, each previous task having a multivariate solution, and the end result impose some limitations on the next solution if a system approach is applied. Thus, the options for solving each subsequent task are limited. Because it is a long process it is logically to look for a way to reduce and facilitate it. This necessitates the use of databases obtained experimentally or borrowed from the design processes of already existing artillery systems. The acquisition or creation of such types of databases allows a high degree of automation of the design process, which will inevitably lead for reducing design time and the process efficiency.

The creating a Cannon Barrel Design Automatized System (CBDAS) will greatly facilitate the designer to review multiple variants and accept a technically grounded barrel design solution. Such a system, having a rich database and working in dialogue with the designer, will ensure that you would get a quality project on a contemporary level. The question of the efficiency of the project and the correctness of the decisions taken will be decided in the course of the artillery system testing.

If a Cannon Barrel Design Automatized System has been created, it could allow automated execution only of a part of the process such as a project solution for the artillery barrel. A project solution means a barrel construction that is needed in the early stages of design. Essentially, this is a complete set of structural parameters of the barrel (shape characteristics, dimensions, kind of steel, tolerances, etc.) and its functional parameters (mass-center characteristics, strength indicators, etc.).

This set of parameters allows you to move on to the implementation of the working technical documentation of the barrel (development of a working draft).

The above describes the concept of "project procedure". This is a set of user actions in the automatized design system, the completion of which ends with a cannon barrel design solution. The design process can be presented as a set of such project operations whose algorithm remains unchanged. Separation of the project design procedure is conditional because to it reflects current standards and designing techniques. In principle, the design procedure should include a list of operations and the sequence of their execution, the possibility for the user to participate in its work, the availability of a design assignment and a description of the design object.

The above mentioned specificity of the task for cannon barrel design as a procedure confirms the need necessity in the center of the process to be placed the designer, actively interacting with the automated design program. Only the dialogue mode for the design process can provide the user with:

• introducing a variety of input information needed for the whole project process and for individual project operations;

• obtaining instructions during the system operation;

• possibility to discontinue the design process for ancillary activities at a suitable time;

• the ability to switch from one design operation to another if it does not violate the design logic;

• the ability of the designer to respond adequately to messages made by the system and to receive assistance under its operating rules;

• the possibility of completing the dialogue after achieving satisfactory results.

The information providing for the design of a cannon barrel is a set of knowledge needed to perform an automated barrel design (ABD) and their presentation in a given structure. The information need is a set of requests for information necessary for the design of the cannon barrel. The same is the basis for providing information on automated barrel design. The following data bases are required to perform the information support required for the design of a artillery barrel:

• a private technical assignment for the barrel as an element of the general technical specification for the weapon system;

• data obtained from previous design steps or other procedures in the automated design system (in this case ballistic design);

• reference data, which are usually separated into separate information and reporting system (IRS);

• data about the components of the barrel information model;

• user data.

The listed data variants and their interaction with the software for the automated design of the barrel and the users are indicated in the structural diagram of Fig. 1.

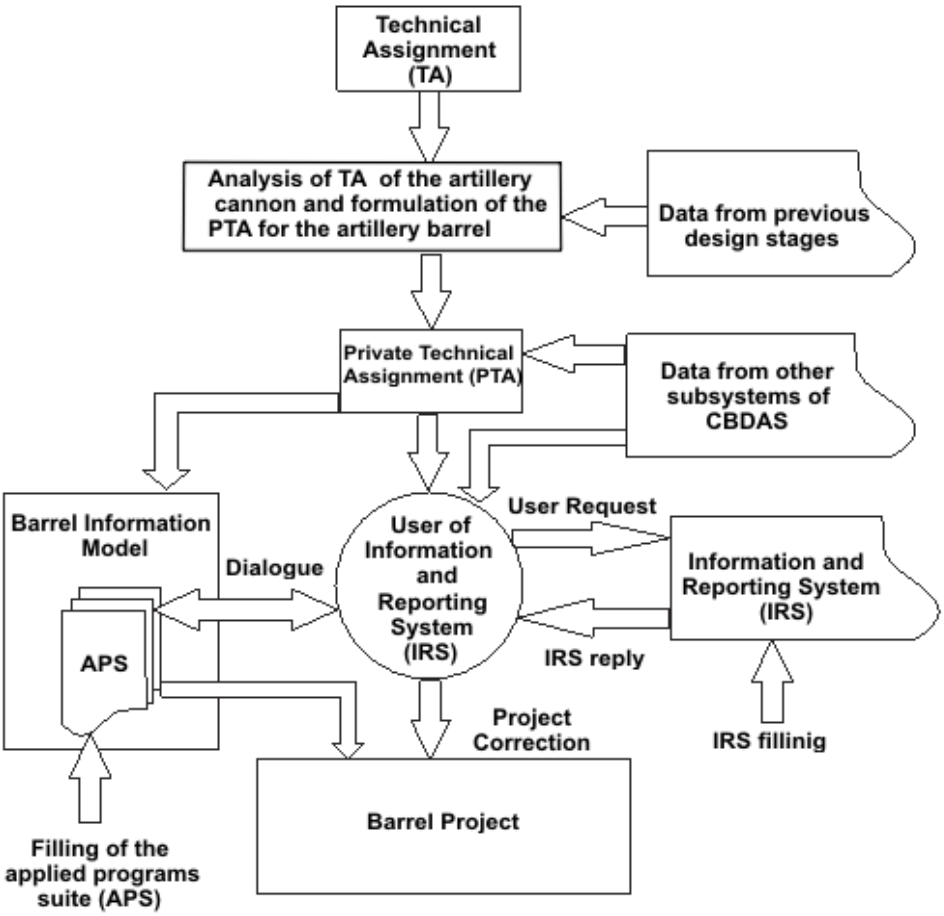


Fig. 1. Structure diagram of the information and programming providing of the system for the automated design of the artillery barrel.

The information system consists of information that enables the user to fully intervene in the process of automated design, to correct and direct it in the required direction. The scope and reliability of data in the information system extends the user's capabilities, positively influences the quality of design solutions and reduces design time for the design.

The information system of the barrel design process includes the following information blocks:

• state standards, standards of the design organization, norms, technical requirements and other data regulating the construction, materials, tolerances, assemblies, etc .;

• information for the construction-ballistic and functional characteristics of barrels from existing weapon systems;

• information for the strength, hardness, heating, wear and life of the barrels, cooling efficiency, and so on;

• information for the aggregates and objects related to the barrel constructively and functionally (ammunitions, bolts, muzzle brakes, etc.);

• information of a technological nature reflecting the achievements in the development of barrel technologies;

• information of a technical and economic nature: design costs, development of existing systems, price references for materials, etc.

The final product resulting from the user's work with the database can be presented in the form of tables with data for the barrel and drafts.

An important feature of any Information - Computing System (ICS) is the degree of its informational commitment to the environment. The Information - Computing System must be dynamic and continually use information about the changing the environment beyond the design system. In this sense, the cannon barrel design subsystem must be open and fit for improvement.

Sectoral software is presented in the automated barrel design through an applied programs suite (APS) (Fig. 1). For convenience, two types of modules (programs) must be designed in the application packages package: for designing and for control.

The modules for designing use input information at their entrance and give on their output the needed constructive parameters: type of construction, shape characteristics, dimensions, required characteristics, brand of materials, etc. In order to be solved the question of the composition of the designing module package, it is necessary to be modeled the process and to be constructed the sequence of operations.

The modules for control receive on their entrance initial information as well as information obtained in the design modules and give on their output the functional performance characteristics of the structure: strengths reserves, deformations, heating temperatures, wear indicators, frequency the oscillations, etc. For the determination of the composition of the modules for control, it is necessary to consider the conditions for the creatability of the guns.

The analysis of the processes occurring in the cannon barrel allows to be separated on several groups of parameters necessary to form a package checking programs. The main sets of parameters needed for this are:

- parameters characterizing the total transverse and longitudinal strength of the barrel and its details;
- parameters characterizing the shape, dimensions, and condition of the surface of the barrel channel;
- parameters characterizing the barrel as a mechanical oscillating system;
- parameters characterizing the barrel as an integral part of the weapon system.

The heretofore was demonstrated that the theory of cannon barrel design continues to develop on the basis of the deeper understanding of the physical processes taking place in the barrel during shooting and the more accurate modeling.

Applying a systemic approach to the complex process of barrel design, as a weapon complex subsystem, allows the continuous improvement of the process, shortening the design time and the realization of artillery models with high combat qualities.

References:

1. *Давидов К.С., Панайотова Т., Дянков П.,* Системният подход при проектирането на логистични системи, Шумен, 2017.

2. Джурков Г., „Aspects of logistics in the EU operations in the context of European policy on security and defense“, Сборник научни трудове на НВУ „Васил Левски“, факултет „Артилерия, ПВО и КИС“, ISSN 2367–7902, стр. 101 – 109, Шумен, 2015.

3. *Захаренков В.Ф.,* Автоматизированное проектирование артиллерийских орудий; Ленинград,1986. 66 с.

4. Норенков И.П. Теоретические основы САПР / И.П. Норенков и др.; М.: Энергоатомиздат, 1987. 400 с.

5. Орлов Б. В., Ларман Э. К., Маликов В. Г.; Устройство и проектирование стволов артиллерийских орудий: учебник для вузов, Москва, Машиностроение, 1976. 432 с.

6. *Спицнадель В.Н.,* Основы системного анализа, изд. Дом»Бизнес-Пресса», 2000.

7. Чуев Ю. В. Проектирование ствольных комплексов, Ю. В. Чуев. Москва, Машиностроение, 1976. 216 с.

8. *K. S. Davidov, Ts. G. Tsonev*, A Method For Solving The Task For Modernization Or Purchasing Of Lightly Armored Combat Vehicles, International Scientific Conference 2017, Collection of Papers Defense and Security Arms, Technologies, Logistics, Communication and Computing Technologies, Social Science, (c.329), Shumen, 2017.

R. N. Lazarov,

ANALYSIS OF THE FACTORS AFFECTING THE STABILITY OF THE BULLET WHEN IT MOVES IN ENVIRONMENTS WITH DIFFERENT DENSITY

Rosen N. Lazarov

National Military University "Vasil Levski", Artillery, AAD and CIS Faculty, poceh_69@abv.bg

***Abstract**: After being shot, the bullet has to pass through environments with different density and the ricochet phenomenon is often observed. It changes the energy of the bullet, its trajectory, and its integrity. By limiting the ricochet, both shooting efficiency and shooter safety are improved.*

***Keywords**: ballistics, bullet ricochet.*

АНАЛИЗ НА ФАКТОРИТЕ, ОКАЗВАЩИ ВЛИЯНИЕ ВЪРХУ СТАБИЛНОСТТА НА КУРШУМА ПРИ ДВИЖЕНИЕ В СРЕДА С РАЗЛИЧНА ПЛЪТНОСТ

Росен Н. Лазаров

In many cases, the ricochet phenomenon is used and controlled to achieve the expected results, but in certain situations it may be dangerous and even deadly. The bullet loses some of its energy, its trajectory is changed, and its integrity is eventually impaired. For these reasons, it is advisable to limit the occurrence of unwanted ricochets. To do this, it is necessary to study the ricochet conditions from different types of surfaces and the emergence of dependencies that determine the conditions of its occurrence, the way the ricochet is controlled or its exclusion.

In the artillery shooting, ricochet shooting is used to achieve air explosion after the projectile has reached the ground (water) barrier. The ricochet explosions on people and outdoor ricochet in open trenches are much more effective than the ground, as the area, affected by the splinters, is bigger.

Ricochet shooting is used in combat aviation to cause significant damage to surface ships in ricochet bombardment.

Despite the long-standing practice of using ricochet, its use in shooting on water is not well-studied and there are no mathematical models that clarify the process. Partial research and experimental results have been published in some specialized publications.

The problem that should be analyzed is the factors that affect the stability of the bullet when moving in different environments. Factor analysis can be used to define the requirements of the bullet shape, which would improve its movement in different density environments and minimize ricochets. Obtaining a bullet with an optimal shape that meets the requirements for the necessary striking action in environments of different density is a problem of exceptional theoretical complexity. It requires simultaneous solving of three tasks - the task of the external ballistics, the movement in the air environment, the task of the strike of the bullet with water, which determines its shape for limiting the ricochet and the task of its stable movement in the water in the conditions of cavitation.

Conditions for bullet resistance in the air

Stability means the bullet's ability to resist the external forces that divert its longitudinal geometric axis from the tangent to the trajectory. If the angle formed by the longitudinal axis of the bullet and the

tangent to the trajectory of the center of gravity (c.g.)increases as a result of the action of the external forces, the bullet is considered to be unstable when flying. If the specified angle which is due to these reasons is reduced, the bullet is considered to be steady.

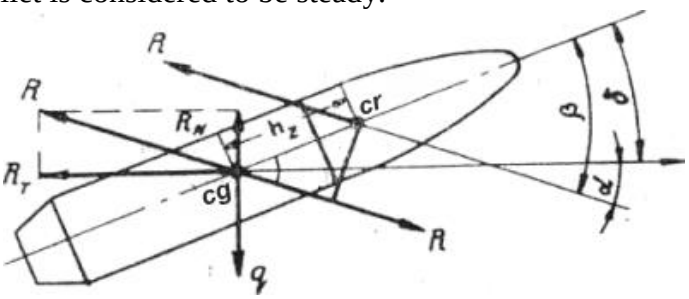


Fig. 1. Forces affecting the bullet when flying in the air.

The force of the air resistance *R* and the force of the bullet gravity *q* (Figure 1) refer to the external forces acting on the bullet in the air. The point of application of the force of air resistance is equal to surface forces, and it is called the center of resistance (c.r.).

The force of the air resistance is directed at a certain angle α relative to the tangent to the trajectory. The effect of this force becomes clearer if it is brought to the center of gravity of the bullet. By applying to the center of gravity two forces equal in value to the force *R* and directed to opposite sides and decomposing one of them into two components, we get a system of forces R_T, R_N and *q*, applied to the center of gravity, and also a pair of RR forces turning the bullet into the plane of the figure.

The force *q* causes the bullet to drop when flying, resulting in a distortion of the trajectory in the firing plane. The R_T force, called drag, causes delays in the bullet flight, resulting in descending branch of the trajectory being shorter than the ascending. The force R_N, called normal (lateral) force, causes the center of gravity to shift from the tangent to the trajectory. As the scheme of forces, which are shown in Fig. 1, revolves around the tangent to the trajectory (except the force q which retains its direction and magnitude), so the center of gravity resulting from the action of force R_N makes a helical line around the same tangent line. The torque of the pair of forces is:

(1) $$M = R.h_Z.sin\beta \approx R.h_Z.\ \beta$$

As it was pointed out, these forces try to rotate the bullet in the plane of the figure around the center of gravity, to divert its geometric axis from the tangent to the trajectory, increase the angle of the δ and impede the stability of the flying bullet. This torque is called reverse.

Two methods have been used in practice to ensure the bullets' stability during their flight in the air.

The first method is to force a strong displacement of the center of the resistance back behind the center of gravity. In this case, the torque M, defined in formula (1), ceases to be reverse and becomes stabilizing. It occurs every time the projectile's axis deviates from the tangent to the trajectory. The strong displacement of the center of gravity is possible with the help of stabilizers. This ensures stability of mines, aviation bombs and non-rotating reactive projectiles.

The second method of providing stability is to render a great angular velocity of rotation to the bullet (projectile) around the longitudinal geometric axis. In this case, the effect of the turning torque does not cause an increase in the angle of the nutation β and rotation of the bullet when flying, but leads to a precession, i.e. the rotation of the bullet axis around the tangent to the trajectory.

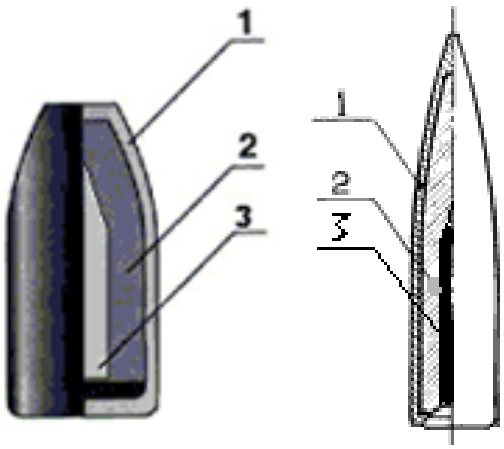
The rotating movement of the bullet (projectile) is achieved by imparting the necessary tilt (curvature) to the rifling of the barrel.

The tilt angle of the rifling may be constant along the barrel (constant curvature rifling) and variable, increasing depending on the channel travel of the barrel from the breechblock to the muzzle (progressive curvature rifling).

Progressive rifling is made to reduce the pressure from the casing on the barrel and thus reduce the wear of the groove part of the barrel. [3]

Interaction of the bullet with water barrier

It is necessary to consider the cases of interaction of the bullet with the water barrier. Water has a significantly higher density than air (800 times). Practically at a bullet speed of 100 m/s, water is to the bullet like a solid barrier.



a) b)

Fig. 2 Types of bullets and their elements
a) a bullet with long-range form; (b) a bullet with short-range form.
1 – shell (steel, brass, tompac); 2-lead; 3 – hard-alloy core.

Long-distance form bullets have a pointed front (Figure 2, b), and these with short-range form have a rounded front part (Figure 2, b). Bullets are produced also with a flat cut at the front.

In Russia, the Center for Independent Expertise on Automotive Transport has conducted an experiment on the interaction of a bullet with an aquatic environment. For the experiment, a mount was used to allow a firm fixation of the weapon, firing the bullet into a small pool with fresh water, and measuring the angle α with accuracy of one minute (Figure 3). A shot is produced, using an electro-trigger with pre-launch of high-speed camera that fixes the results of the experiment: the bullet's entry into the water, the movement, and the exit.

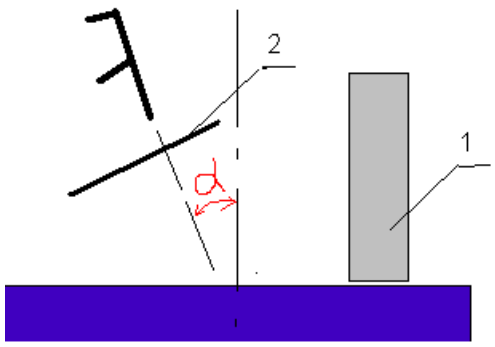


Fig. 3 Scheme for conducting an experiment on the interaction of a bullet with water barrier.
1-bullet catcher. 2-light barrier for stopping gunpowder gasses

The shooting was carried out with various ammunition and kinds of weapons. The experiment used both ordinary for the system cartridges and also cartridges with a flat cut, made with a file, resembling the expanding bullets of the hunting cartridges. About 100 shots have been produced. As a result of the experiment, it has been found that the angle of the bullet ricochet with water barrier with a pointed and rounded front has practically the same value and does not depend on the shape of the front part of the bullet.

Angle α, which has and does not have a 50/50 ricochet is for example 11 degrees and 40 minutes – the transition angle.

100% ricochet is absent at an angle α equal to 11 degrees and 15 minutes.

100% there is a ricochet at an angle α equal to 12 degrees and 00 minutes.

Expanding bullets (with a flattened front) often broke down when they encountered the water surface, and ricochet could not be seen. Also, the flat front of the bullet forms a cavitation cavity that prevents the bullet from exiting the water at an angle greater than 12 degrees. The experiment conducted allows us to conclude that a separate case study should be carried out with bullets with a flat front to determine the angle of the ricochet's occurrence.

It is also necessary to consider the case when the shot from the weapon is produced in close proximity to the water surface. In this case, there is an effect of breaking the water surface from the gunpowder gases, which overtake the bullet in the after-action phase, forming a cavity in which the bullet falls and a ricochet is not observed.

In the course of the experiment, it was found that the depth at which the bullet penetrates at the ricochet from a water surface is about 10-20 cm, and largely depends on the angle of encounter with the water surface. [2]

Combat tasks which are performed by the crew of the battleships include shooting at mines on the surface, high-speed small surface ships and boats, boarding operations, shooting at underwater enemy divers, etc. The position of the weapon against the water surface determines "advantageous" ricochet conditions (Figure 4).

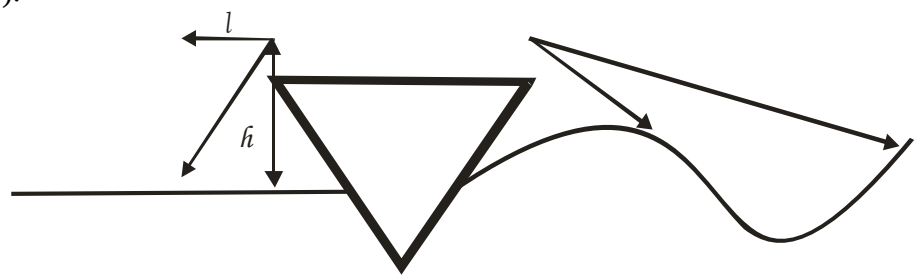


Fig. 4. Graph of ricochet conditions depending on the position of the weapon against the water surface.

h - shooting height (board and shooter height); l - critical distance which has 100% ricochet; l / h - tan 300.

It can be seen from the figure that at height of the board h = 6 m, the critical distance for the ricochet is 3.46 m, i.e. when firing at distances greater than the one described above, the probability of a ricochet is 100%. The situation is even more complex in wave conditions, because the angle of incidence will be determined by the directrix of the shooting and the tangent at the point of encounter with the water surface, and they are unpredictable. Theoretically, there may be a shot from the deck of the ship towards an approaching wave that causes ricochet and return of the bullet to its own ship or a neighboring one in the group of ships. This presents a new perspective on the type of ammunition used in our navy. [1]

Principle of bullet movement in water

Water contains dissolved air, which is released from it when heated and the pressure increases. The effect of separating air from the water can be observed with the phenomenon "Cavitation". This effect is also used in this case. The APS machinegun bullet is a steel rod 120 mm long and 5,6 mm in diameter, which becomes thinner towards the front and ends with a flat cut with a diameter of about 2 mm. The bullet has considerable mass and with great force, coming from the kinetic energy, effects the water on the area of the flat cut (with a diameter of about 2 mm). Under the pressure from the water, air is released which forms an elongated cavity (cavern) and the air pressure in it is in the range of 0.01 - 0.1 atmospheres.

a)

b)

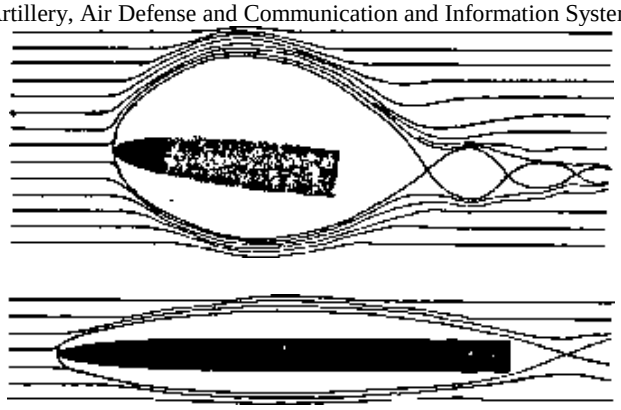


Fig. 5. The principle of bullet movement in an aquatic environment.
(a) the movement of a normal bullet; (b) the movement of a bullet designed for shooting in an aquatic environment.

Stabilization in the direction of the bullet movement (preservation of the direction) occurs at the expense of the constant oscillation in the back side of the bullet in the walls of the cavity. After the bullet passes, the cavity collapses, leaving behind small air bubbles. The bullet will continue to maintain enough speed until the speed drops below the critical value. Then the cavity decreases its size at the rear, where friction on the bullet in the water increases greatly, resulting in slowing and stopping. The reduction of the range of fire with the depth of immersion is due to different water pressure at different depths and the consequent changes in the conditions for the formation of cavities.

The stability of the bullet and its movement are controlled by the laws of hydrodynamics (cavitation, etc.), which differ significantly from the principles of bullet flight stability in the air. In this connection, it is practically impossible to create a universal bullet for air and water. A rotating bullet or bullet with stabilizers will break the cavern, etc. All versions of the bullet for smoothbore weapons can only be simplified versions of projectiles for smoothbore artillery and hunting rifles. One of the versions may be the one, shown on Fig. 5 or its modifications, although developers are limited in the versions the cartridges.

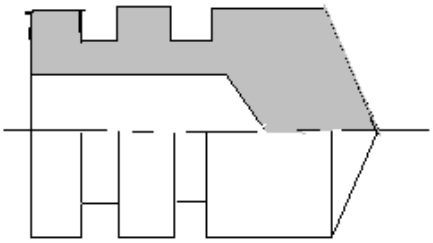


Fig. 6. A bullet variant for a smoothbore weapon, including a 12 and 16 caliber hunting weapon.

CONCLUSIONS:

1. The analysis of the stability requirements a single bullet has to meet when firing in different environments indicates that they are completely opposite when the bullet moves in air and water.

2. On the basis of this analysis, it can be concluded that it is more efficient to develop a model of the bullet shape in which its ballistic properties are preserved in air motion without ricochets from the water surface.

References:

1. Давидов К. С., Цонев Ц. Г., Маринов М. Г., “Минимизиране на вероятността от появата на нежелан рикошет при стрелба към водна повърхност”., НВУ „В. Левски“ Факултет “Артилерия, ПВО и КИС Научна сесия 2012. Сборник научни трудове – част I., Ш., 2013 (110 – 117 стр.) ISSN 1313-7433.

2. Взаимодействие пули с водной преградой, Исследование Центра независимой експертизой на автомобильном транспорте, РФ, 443098, С. https://www.cneat.ru/bullet.htm

3. Кирилов В.М., „Основи на устройството и проектирането на стрелковото оръжие“ стр. 139-141, София, 1975.

S. I. Antonov,

TRENDS IN COMPUTER DESIGN OF REDUCTION GEAR

Stamen I. Antonov

National Military University "Vasil Levski",Artillery, AAD and CIS Faculty,
stamantonov@abv.bg

Abstract: *The article explores contemporary computer tools for design of reduction gear. The article is fully adapted to the need for knowledge and skills in the future work of engineers in mashine engineering.*

Key words: *reduction gear, CAD software, geometric design, computer modeling.*

СЪВРЕМЕННИ ТЕНДЕНЦИИ В КОМПЮТЪРНОТО ПРОЕКТИРАНЕ НА РЕДУКТОРИ С ЦИЛИНДРИЧНИ ЗЪБНИ КОЛЕЛА

Стамен И. Антонов

I. Въведение

Проектирането на зъбните предавки, включващо: уточняване на вида на контактуващите зъбни повърхнини, определяне на техните геометрични параметри и извършването на якостните и кинематични пресмятания, до голяма степен се определя от предназначението им и от конкретните изисквания, поставени към тях. Съществуването и използването на съвременни CAD/CAM системи, позволява да бъдат автоматизирани процесите, свързани с моделирането и изработването на зъбните предавки. Това е основна предпоставка за създаване на нови зъбни механизми (включващо – моделиране, конструиране, изпитване, документиране, изработване), както и за оптимизиране на съществуващите такива. В доклада са отбелязани предимствата от използването на CAD/CAM системите за проектиране, отразена е последователността за моделиране на спрегнати зъбни предавки и са посочени възможностите за тяхното изработване.

II. Приложимост на CAD/CAM/CAE системите при проектиране на редуктори

Системите за автоматизирано проектиране заемат изключително място сред компютърните приложения, тъй като те са индустриални технологии, влияещи непосредствено на материалното производство.

Приложението на съвременните CAD/CAM системи се използва за тримерно меделиране на отделни детайли, на механизми и машини с голям брой възли от високо ниво на сложност, от които се изготвя графичната част на конструкторската документация – чертежите (CAD); за инженерни изчисления и анализи (CAE); за бързо изготвяне на прототипи (Rapid Prototyping-RP); за технологична подготовка на производството (CAP); за изготвяне на управляващи програми за NC машини за изработване на различни по сложност изделия (CAM), както и за цялостно управление на проектните и инженерните данни (PDM) и документи (EDM) на дадена фирма [1].

Якостни и кинематични пресмятания на зъбните предавки с помощта на CAD системи

Якостните и кинематични пресмятания на зъбните предавки в даден редуктор с помощта на CAD системи се извършват автоматично при задаване на определени стойности на изходящите параметри. При това се извеждат непосредствено крайните резултати, необходими при конструирането на зъбни механизми. Съществуват две възможности:

1. При проектиране на стандартни зъбни предавки – цилиндрични, конусни и червячни. CAD продуктите от среден и висок клас (AutoCAD, TopSolid, SolidWorks, CATIA) извършват автоматично пресмятане и генерират съответната предавка. Така получения модел може да бъде вграден директно в конструирания механизъм и може да бъде изменян многократно в зависимост от якостни, кинематични, конструктивни и естетически изисквания, поставяни към него.

2. При проектиране на нестандартни зъбни предавки – разработва се програма за тяхното якостно-геометрично изчисляване (на Mathcad, MATLAB, Excel и т.н.) или натоварванията се задават директно върху модела, при което отново при въведени първоначални данни се извеждат крайните резултати във вид удобен за ползване.

Симулация на движенията с помощта на модулите в CAD/CAM/CAE системите

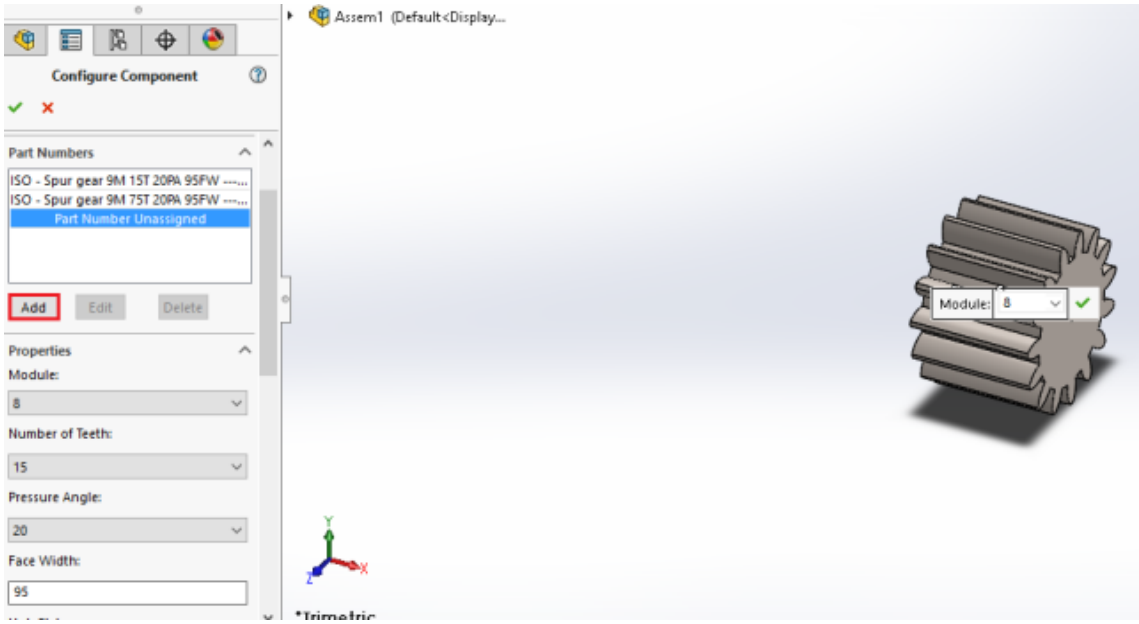
За симулация на движенията се възпроизвежда задружната работа на спрегнатите зъбни колела в предавките и се симулират движенията в зъбния механизъм, от където се проследява нормалната работа и се правят изводи за съответните граници на заклинване, колизии, хлабини и др.

Технология на изработка

Подходящо използвания CAM продукт директно генерира от моделите на зъбните колела програми за тяхната изработка на съответната NC машина (ерозийна, обработващ център и т.н.) с подходящ избор на режещи инструменти (за груба и чиста изработка) и с необходимите режими на рязане. Симулира се процеса на изработване и се анализират получените повърхнини.

Моделиране на спрегнати зъбни предавки

Геометричното CAD моделиране на зъбни предавки може да се извърши по три начина. До голяма степен изборът на вариант се опрделя от това, дали те са стандартизирани или не са, т.е. дали те са заложени в CAD програмите и техните приложения и позволяват ли използваните CAD системи това моделиране да стане.



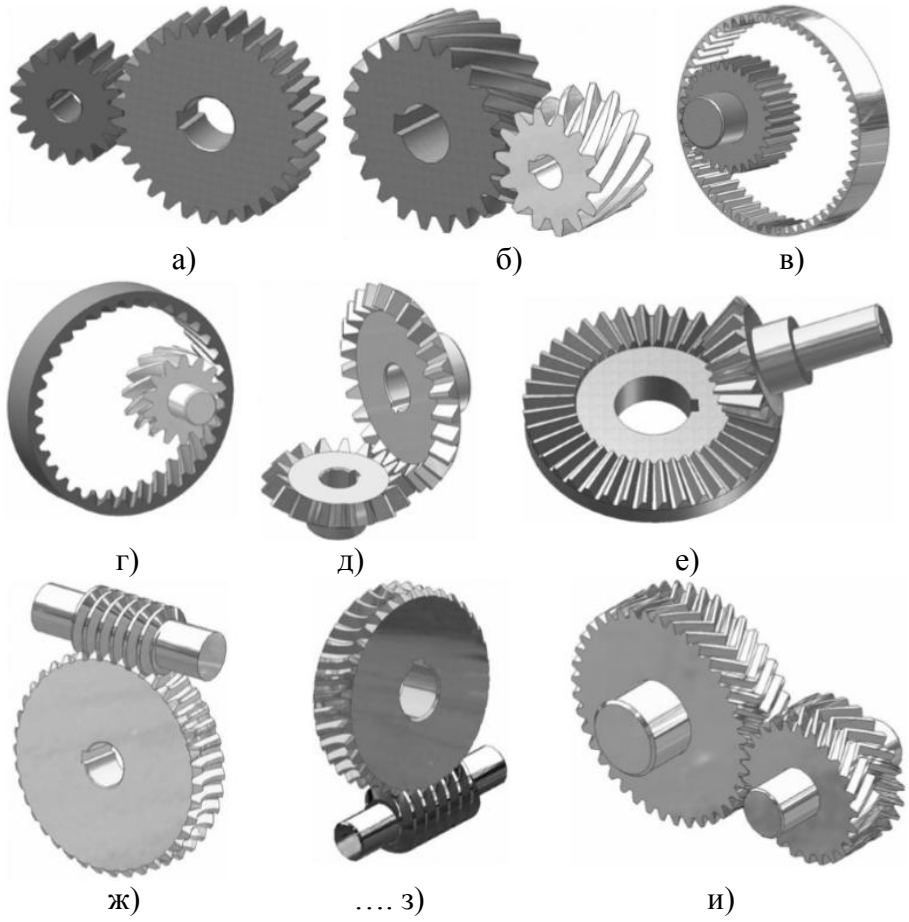
Фиг. 1. Геометрични параметри на стандартни зъбни предавки, заложени в CAD програмите

Моделиране на спрегнати зъбни предавки, непосредствено от извършения CAD синтез

Такова моделиране е възможно при пълна съвместимост на използваните CAD продукти. При него се извършва обмен на данни без загуба на информация, при което получените аналитични зависимости и графично визуализирани повърхнини от едната CAD система се трансферира в друга и се генерират твърдотелните модели на синтезираните предавки. Този начин е приложим най-вече за нестандартните зъбни предавки. Интерес представлява факта, че стандартните модели, заложени в CAD системите, по които се генерират желаните предавки, са получени по този начин.

Моделиране на стандартни зъбни предавки

За моделиране на стандартни зъбни предавки се използват вградените в CAD системите приложения. За да се получи моделът на желаната предавка, за нея се задават необходимите геометрични параметри (фиг.1) и силови натоварвания. Изчисляването се извършва автоматично, извеждат се крайните резултати и се генерират зъбни предавки. При необходимост, те могат да бъдат премоделирани чрез промяна на своите параметри, в зависимост от изменението на натоварванията и кинематиката и в зависимост от желания дизайн и конструктивни особености. На фиг. 2 са показани модели на стандартни зъбни предавки, получени с CAD продукта Solid-Works [4].



Фиг. 2. CAD модели на стандартни зъбни предавки

а) Цилиндрична зъбна предавка с външно зацепване с прави еволвентни зъби
б) Цилиндрична зъбна предавка с външно зацепване с наклонени еволвентни зъби
в) Цилиндрична зъбна предавка с вътрешно зацепване прави еволвентни зъби
г) Цилиндрична зъбна предавка с вътрешно зацепване с наклонени еволвентни зъби
д) Конусна зъбна предавка с ортогонални оси на ротация
е) Конусна зъбна предавка с неортогонални оси на ротация
ж) Червячна предавка с едноходов червяк
з) Червячна предавка с триходов червяк
и) Шевронна зъбна предавка

III. Пресмятане и моделиране на елементите на едностъпален редуктор

В доклада е представен пример за изчисляване, проектиране и симулация работата на едностъпален редуктор с цилиндрични зъбни колела с прави зъби. Стъпките за моделирането и последователността на изпълнението им са изложени по-долу. Всяка от посочените стъпки при изчислението и моделирането може да бъде извършена по повече от един начини, в зависимост от гледната точка на конструктора.

Редукторът, който е разгледан в примера е едностепенен, с цилиндрични зъбни колела с прави зъби. Корпусът му се състои от две части: основа и капак, които се разделят от равнина минаваща през осите на валовете. При изчисленията основно се използва техническият справочник „Пресмятане и конструиране на машинни елементи [2]“.

1. Определяне на предавателното число на редуктора (i)

За определяне на предавателното число на даден редуктор се вземат под внимание следните фактори: взаимно разположение на двата вала, големина и предаван на въртящ момент (Мв), скорост на въртене, ограничение в масата и габаритните размери на детайлите ако има такива [2].

Основен принцип при избора на предавателното число за цилиндрични зъбни колела с прави зъби е $i \leq 8 \div 10$.

2. Определяне на оборотите на вала

Обороти на входящия вал са в зависимост от предавателното число [2]:

$$(1)\quad n1 = n2.i$$

3. Избор на материал за зъбните колела

Оснвния материал за изработка на зъбните колела е стомана,като се допуска при малки натоварвания зъбните колела да се изработват от чугун. Изборът на стомана зависи от условията и режима на работа на редуктора, както и от установения начин на смазване. За зъбни предавки с ниски обороти до 100 min-1 се приема,че твърдоста на материала не е от значение. Зъбните редуктори с обороти над 100 min-1 задължително работят в условие на смазване и се изчисляваст на контактна якост и твърдост на зъбите за избрания материал.

Ако натоварването е придружено с удари или вибрации се налгат допълнителни изчисления за жилавост на сърцевината им. За средните натоварвания се използва качествена въглеродна стомана от следните марки: ст.35, ст.40, ст.45, ст.50.

При тежки натоварвания и вибрации за изработка на зъбни колела се използва легирана стомана. Най-използвани марки са: 40х, 40хн, ст.35хгс

Задължителната твърдост на зъбите по Бринел е ≤ 350.

Зъбни колела с малки размери се изработват заедно със съответния вал.

4. Определяне на допустимото напрежение на огъване в зъбната предавка

Допустимото напрежение на огъване при отчитане на умората на материала се определя основно от формула за симетрично знакопроменливо натоварване на зъбите в двете посоки [2]:

$$(2)\quad [\sigma]_{ог} = \frac{\sigma - 1}{[n].K\sigma}.\text{k.ц.ог [MPa]}$$

Където σ-1 е граница на умора на материала при симетричен цикъл на натоварване. Границата на умора може да се определи от приблизителен способ или при изчисляване при отчитане видът на стоманата [2].

$$(3)\quad \sigma\text{-}1 = 0{,}22(\sigma b + \sigma s) + 50$$

- [n] представлява коефицент на сигурност при пресмятане на двойни колела;
- (Kσ) представлява ефективен коефицент на концентрация на напрежение;
- Кц –коефицент на огъване отчитащ броя на циклите на огъване;

Напреженията на огъване се изчисляват за всяко зъбно колело.

5. Пресмятане на зъбни колела

Силите, който натоварват работещите зъбни колела, създават напрежения, които са пропорционални на входящия въртящ момент, който е зададен по условие. Напрежението в зъбите на зъбните колела не е постоянно по място и време и е неравномерно разпределено по дължината на зъбите поради неуспоредност между осите на зъбните колела, затова зъбните колела се изчисляват при отчитане на допустимите напрежения на огъване.

6. Изчисляване на нормалния модул

Нормалният модул се изчислява по формулата [2].

$$(4)\quad m \geq C_2 . \frac{\sqrt[3]{Мв.10.Кк.Кд}}{Z1.\ \Psi m.Y.[\sigma].10^6}$$

Където C_2 е коефицент, отчитащ вида на предавката;

• Мв е въртящ момент, който се задава по условие;

• Кк представлява концентрация на натоварване;

• Кд е коефицент, който отчита условията на динамичност, т.е той отчита динамичните сили, които възникват при въртенето на зъбните колела поради неточност в изработката и зацепването им;

• Z1 - брой зъби на водящото зъбно колело;

• Ψm - коефицент,който отчита дължината на зъба спрямо модула;

• Y - коефицент, който отчита формата на зъба;

• [σ] - допустимо напреженое на огъване за водящото колело.

7. Определяне на основните параметри на цилиндричната предавка

Броят зъби на водимото зъбно колело (Z2) се опделят по дормулата:

$$(5)\quad Z2=Z1.i$$

• Междуосовото разстояние (A) се определя по формулата:

$$(6)\quad A=\frac{Z2+Z1}{2}.m$$

• Диаметърът на делителната окръжност на водящото зъбно колело се определя по формулата:

$$(7)\quad Дд=Z1.m[mm]$$

• Външния диаметър на водящото зъбно колело се определя по формулата:

$$(8)\quad Дк=m.(Z1+2)$$

• Дължината на зъба на водящото колело (b) е функция от следните параметри:

$$(9)\quad b=\Psi m\ .m+5$$

По аналогичен начин се изчисляват и параметрите на водимото зъбно колело от едностъпалния редуктор с цилиндрични зъбни колела с прави зъби.

8. Изчисляване на задвижващия вал

Задвижващият вал на редуктора се изчислява на огъване и ускукване едновременно:

$$(10)\quad [\sigma]_{ог}=\frac{Мог}{Wог}=\frac{32Мог}{\Pi.d^3}\leq[\sigma]_{ог}$$

Където:

• Мог е огъващ момент;

• [σ]ог е допустимо напрежение на огъване;

• Wог е съпротивителен момент.

9. Изчисляване на диаметъра на задвижващия вал.

Диаметъра на задвижващия вал се определя по формулата [2]:

$$(11)\quad d1\geq\sqrt[3]{\frac{Мог}{0,1\ .\ [\sigma]ог}}$$

10. Изчисляване на задвижвания вал.

Огъващия момент на задвижвания вал се определя по следната формула:

$$(12)\quad Мог=Мв=9554.\frac{N}{n}[N.m]$$

Където:

• N е предавана мощност

• n са оборотите на задвижваното зъбно колело

Диаметъра на вала се изчислява по следната формула [2]:

$$(13)\quad d2 \geq \sqrt[3]{\frac{Mor}{0{,}1\,.\,[\sigma]or}}$$

Изчисляваните диаметри на валовете са диаметри за лагерите и са минимални диаметри за валовете. Диаметрите на лагерните шийки се оформят констроктивно в зависимост от избраните лагери.

14. Изчисляване и избор на лагери.

Изчисляването на лагерите се извършва за динамична товароносимост, като последователно това се прави за задвижващия и за задвижвания вал по формулата:

$$(14)\quad C=\frac{td}{fn\,.\,ft}.p[kN],$$

където:

• ft е коефецент за динамично натоварване;

• fn е коефицент за честотат на въртене;

• силата P се приема, че има стойност, наполовина на зададения мъртящ момент (Мв).

След якостните и кинематични изчисления следва тримерното моделиране на едностъпалния редуктор с цилиндрични зъбни колела с прави зъби.

Тримерното моделиране на машиностроителен детайл с помощта на CAD системите се извършва в следната последователност [5]:

• анализира се датайлът и се взема решение за неговото разделяне на елементарни конструктивни елементи, които могат да се създават с използваната система;

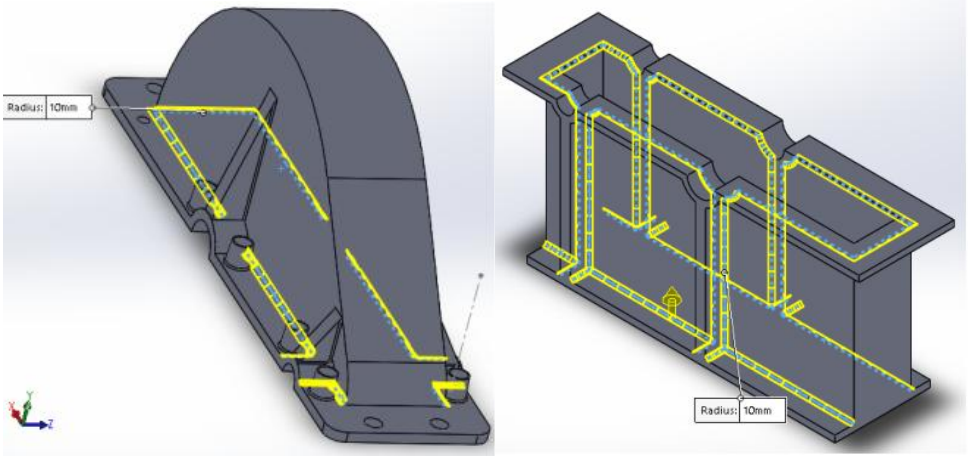
• определя се елементът, който ще се използва за базов;

• приема се ред за създаване на конструктивните елементи;

• избират се начините за построяване на конструктивните елементи;

• построяват се конструктивните елементи в приетия ред, като към тях се прилагат съответните конструктивни операции (фиг.3);

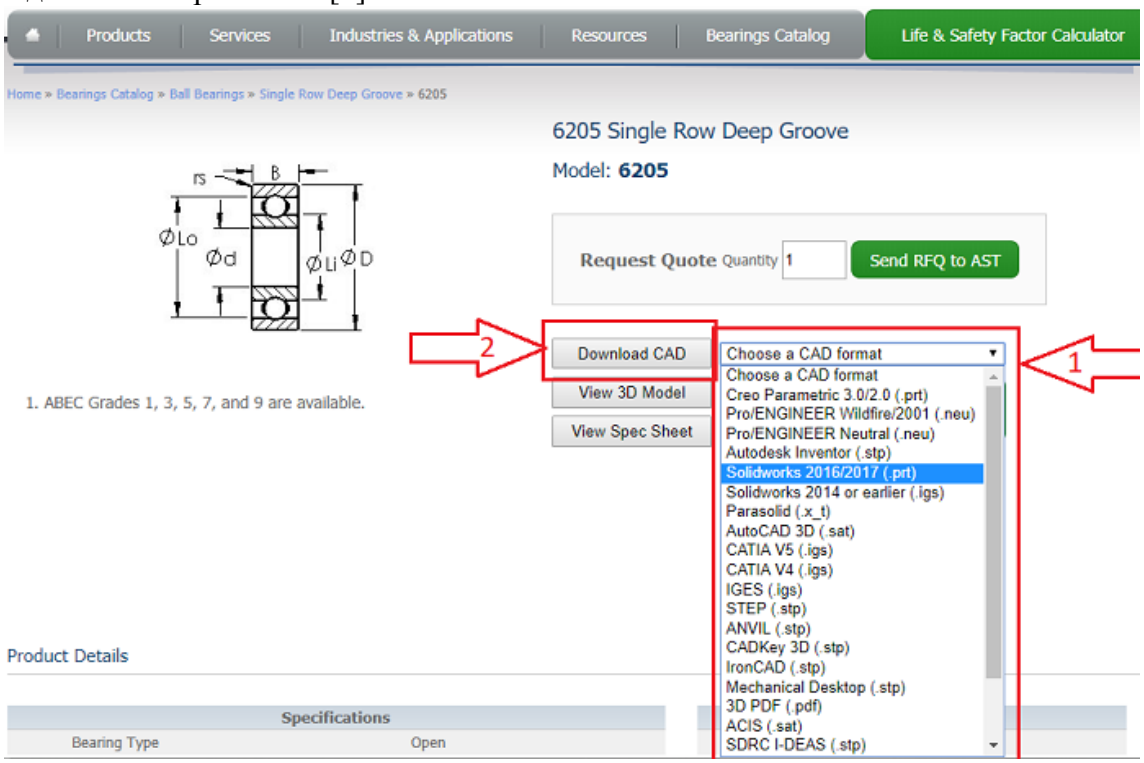
• преглед и корекция на създадените елементи за реализиране на възприетата стратегия за моделиране на детайла.



Фиг. .3 Тримерни модели на корпуса и капака на проектирания редуктор

Машинните елементи за обезпечаване на въртеливо движение – лагери могат да бъдат подбрани от интегрираните софтуерно библиотеки или да се изтеглят директно от web страницата на производителя на лагерите (фиг. 4).

Използваният за целта на доклада продукт за автоматизация на инженерния труд SolidWorks има библиотека с над 700,000 стандартни елемента, поддържа множество международни чертожни стандарти и позволява на потребителите да създават детайли и да документират създадени дигитални прототипи [4].



Фиг. 4. Подбор и оразмеряване на стандартни машинни елементи

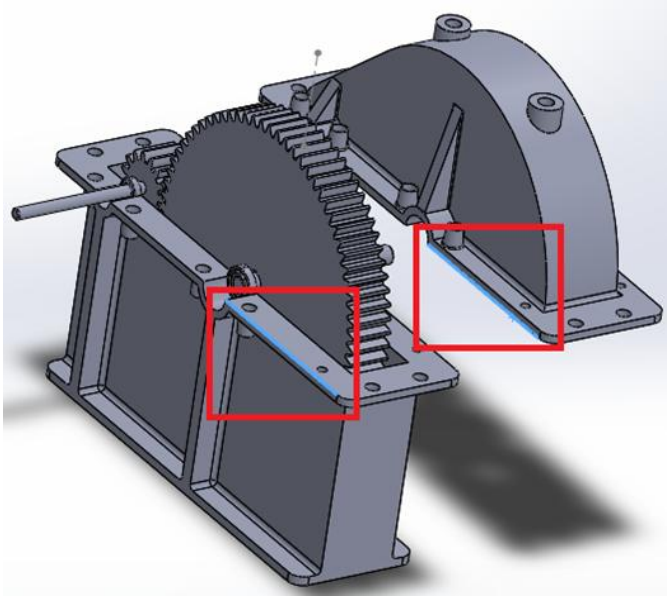
IV. Асемблиране на сглобен механизъм и създаване на чертежи

При автоматизираното проектиране могат да се създават регламентираните от стандарта два вида сглобени единици:

• сглобени единици, състоящи се само от детайли;

• сглобени единици, съдържащи детайли и други сглобени единици.

След разполагане на компонентите във файла на механизма, те трябва да бъдат сглобени. При сглобяването на компонентите се ограничават степените им на свобода. Съществуват шест възможности за движение на твърдо тяло в пространството - три транслационни премествания по направление на координатните оси и три ротационни движения около координатните оси. Компонентите се сглобяват като се използват връзки. Те дават възможност за позициониране на отделните детайли от сглобената единица в строго съответствие един с друг (Фиг.5).



Фиг. 5. Фиксиране на компоненти в свглобената единица

Създаването на чертеж от 3D модел се свежда до генериране на проекции на базата на тримерните модели, придружени със съответните размери, означения за грапавост, геометрични допуски, технически изисквания и др.

Чертежите и тримерните модели представляват взаимосвързани документи, т.е. промените в модела на детайл или схлобена единица променят и съответните чертежи. Възможно е и обратното, чрез промяна на размери в чертежа да се променят моделите. Чертожните файлове винаги трябва да се придружават от съответните моделни файлове. Чертежите се записват в отделни файлове със съответното разширение, в зависимост от използвания CAD прудукт за работа. Чертожният файл може да съдържа един или няколко чертожни листа, като в даден момент само един от тях е активен.

Създаването на чертеж включва:

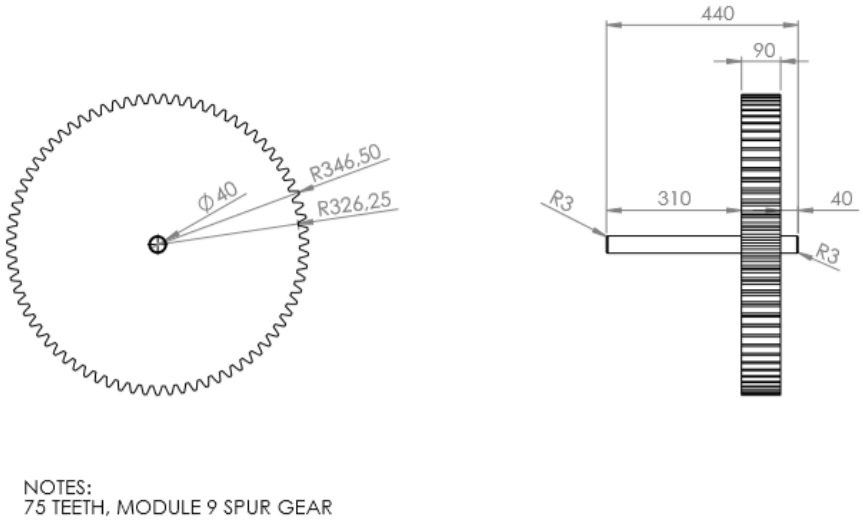
• избор на формат на чертожния лист, рамка и таблица с основния надпис;

• настройване на графичната среда – метод на проектиране (европейска или американска позиция [4]), подразбиращ се мащаб, символи за означаване на изгледи, разрези и технологични бази, начини за представяне на основни елементи от чертежа (линии, размери, щриховка, геометрични допуски, надписи и др.);

• композиране на чертежа чрез създаване на изгледи и разрези, оразмеряване, надписване и др. (фиг.6);

• попълване на таблицата с основен надпис;

• отпечатване на чертежа на периферно устройство.



Фиг. 6. Композиране на чертеж в графична среда

V. Технология на изработване

Нарязването на зъбните колела може да се извърши на металорежеща машина с ЦПУ с профилиран режещ инструмен по метода на копирането, като инструмента се движи по апроксемилирана крива, доближаваща се до контура на напречното сечение на нарязваните зъби.

Зъбните колела на моделирания в доклада редуктор могат да бъдат изработвани на обработващ център или нишкова ерозийна машина с CNC управление. За целта е нужно да бъде генерирана програма от подходящо избрана CAM система. Независимо от типа на използваната CAM система, при съставяне на управляващите програми се използват създадените с CAD системите модели на обработваните модели. От твърдотелния модел автоматично се разпознават различните геометрични елементи. Информацията, получена от тях се използва за избиране на необходимите инструменти за обработка. Траекториите на инструментите, генерирани с CAM система са в асоциативна връзка с оригиналния CAD модел и при рдактиране на 3D геометрията, траекториите се променят автоматично. CAM системата симулира и проверява пътя на инструмента и отнемането на материала от модела, като инструментът, държачът, заготовката и приспособленията за базиране и захващане са включени в симулацията и представят реалистично процеса на обработка.

VI. Заключение

В доклада е представена последователността за пресмятане и геометрично моделиране на зъбни предавки посредством CAD системи и са посочени начините за механичното им изработване.

Направена е обосновка за използване на CAD/CAM системи, като са посочени предимствата им при проектиране на зъбни предавки в редукторите.

References:

1. Донков Д., CAD/CAM системи в машиностроенето, Част 2, УИ “В. Априлов”, Габрово, 2001.

2. Д. Христов, Г. Петков, Н. Чавушян, С. Начев, М. Проданов, Пресмятане и конструиране на машинни елементи, София, 1980.

3.http://www.academia.edu/36663133/DESIGN_AND_ANALYSIS_OF_A_TWO_STAGE_REDUCTION_GEARBOX

4. https://www.solidworks.com

5. https://store.topsolid.com/cad.htm

COMMUNICATION AND COMPUTING TECHNOLOGIES

R. A. Bogdanov, Zh. N. Savova, D. K. Hubenov,

A COMPARATIVE ANALYSIS OF HARDWARE PLATFORMS FOR DEVELOPMENT AND REALIZATION OF SOFTWARE DEFINED RADIO SYSTEMS

Rosen A. Bogdanov, Zhaneta N. Savova, Dyanko K. Hubenov

National Military University „V. Levski", Veliko Tarnovo, Artillery, Air Defense and CIS Faculty, department "Communication Networks and Systems",
rab61@abv.bg, zh.savova@mail.bg, d_hubenov@abv.bg

Abstract: *The paper discusses the possibilities of building SDR systems through some of the widely available hardware platforms. A survey of some of the most commonly used SDR hardware platforms is done. A comparative analysis of the technical characteristics of the SDR platforms considered is made.*

Keywords: *Software Defined Radio (SDR), Cognitive Radio (CR), ADALM-PLUTO, USRP, WARP, BEE3, KUAR, SDRplay, FPGA.*

СРАВНИТЕЛЕН АНАЛИЗ НА ХАРДУЕРНИ ПЛАТФОРМИ ЗА РАЗРАБОТКА И РЕАЛИЗАЦИЯ НА СОФТУЕРНО ДЕФИНИРАНИ РАДИОСИСТЕМИ

Росен А. Богданов, Жанета Н. Савова, Дянко Н. Хубенов

Национален военен университет „В. Левски", гр. Велико Търново,
Факултет „Артилерия, ПВО и КИС", катедра „Комуникационни мрежи и системи",
rab61@abv.bg, zh.savova@mail.bg, d_hubenov@abv.bg

I. УВОД

Последните десетилетия в развитието на комуникациите се характеризират с експоненциално нарастване на начините и средствата, чрез които потребителите комуникират – комуникации за данни, гласови комуникации, видео комуникации, излъчване на съобщения, комуникации за управление и контрол, комуникации при спешни реакции и много други. В тази променена нова реалност се изисква лесно и ефективно модифициране на използваните радиоустройства.

Като технологии за развитие на комуникациите, които предоставят гъвкавост, ефективност на използване на мощността и оптимизиране на разходите за разработка, както и широкообхватни ползи, реализирани от доставчиците на комуникационни услуги и разработчици на продукти, достигащи до крайните потребители, са се наложили софтуерно дефинираното радио SDR (Software Defined Radio), адаптивното радио, когнитивното радио и интелигентното радио.

На пазара се предлагат различни хардуерни платформи и софтуерни продукти за тяхното програмиране, които се използват за разработка на SDR устройства.

В този доклад е представено проучване на някои от най-често използваните и достъпни SDR хардуерни платформи. Направен е сравнителен анализ на техническите характеристики, използваните технологии и вариантите за приложението на разгледаните платформи за SDR.

II. ХАРДУЕРНИ ПЛАТФОРМИ ЗА SDR

1. Universal Software Radio Peripheral

Универсалната периферия за софтуерно радио Universal Software Radio Peripheral (USRP) е гама от софтуерни радиостанции, проектирани и продавани от Ettus Research и нейната компания майка National Instruments [4]. Семейството продукти USRP е сравнително евтина хардуерна платформа за софтуерно радио и често се използва от изследователски лаборатории, университети и любители.

Моделите USRP използват архитектура, включваща основните компоненти, които се изискват за обработка на сигнали в основната честотна лента: генериране и синхронизиране на тактова честота, FPGA (Field-Programmable Gate Arrays), ADC, DAC, интерфейс към хост процесора и регулиране на мощността. Модулния принцип на използване на дъщерни платки се прилага за реализиране на аналоговите операции като ъп/даун конвертиране DDC (Digital Down-Converter) и DUC (Digital Up-Converter), филтриране и други обработки на сигнала. Тази модулност позволява на USRP да обслужва приложения, които работят до 6 GHz. Предлагат се 3 различни серии USRP: мрежови, шинни и вградени. Мрежовите платформи USRP N200 и USRP N210 са високоефективни USRP устройства, които осигуряват по-широк динамичен обхват и по-висока честотна лента от шинните. С помощта на Gigabit Ethernet интерфейс устройствата в мрежовата серия могат да прехвърлят до 50 MS/s комплексни проби от основната лента към/от хоста. Серията предлага и порт за MIMO (Multiple-Input and Multiple-Output) разширение, който може да се използва за синхронизиране на две устройства от тази серия. Всички продукти в шинната серия използват интерфейс USB 2.0 или USB 3.0 за прехвърляне на данни към и от хоста. Вградената серия съчетава функционалността на другите USRP устройства с вграден процесор OMAP 3. E310, пуснат н пазара в края 2014 г. и използва платформата Zynq SoC и Analog Devices AD9361 RFIC за реализиране на много компактен, вграден USRP модул. Устройствата от това семейство не трябва да се свързват с външен компютър и са предназначени за приложения, които изискват самостоятелна работа [7, 8].

Хардуерният драйвер на USRP UHD (USRP Hardware Driver) е драйверът на устройството, предоставен от Ettus Research за използване в продуктовото семейство на USRP. Той поддържа Linux, MacOS и Windows платформи. Няколко рамки, включително GNU Radio, LabVIEW, MATLAB и Simulink, използват драйвера UHD.

Функционалността, осигурена от UHD, може да бъде достъпна и директно с UHD API (Application Programming Interface), който осигурява поддръжка за C ++. Всеки друг език, който може да импортира функциите на C ++, също може да използва UHD.

2. Wireless Open-Access Research Platform

Безжичната изследователска платформа за свободен достъп WARP (Wireless Open-Access Research Platform) е мащабируема и разширяема програмируема безжична платформа, изградена до прототип на съвременни безжични мрежи. WARP съчетава високопроизводителен програмируем хардуер с голяма база от отворен код и поддържащи хардуерни модули: FPGA, радио, тактови сигнали, аналогови. Mango Communications WARP v3 е най-новото поколение WARP хардуер, интегриращ FPGA модел Virtex-6 на компанията Xilinx, два програмируеми RF (Radio Frequency) интерфейса и различни периферни устройства.

WARP Lab е рамка за бързо генериране на прототип на физически слой, която позволява координиране на произволни комбинации от единични и мултиантенни предавателни и приемни възли. Разширяемата рамка дава на потребителите гъвкавостта да разработват и внедряват големи мрежи от възли, за да отговорят на всяко приложение или изследователска нужда. Референтният дизайн съчетава внедряването на MATLAB и FPGA в модулите на WARPLab, което позволяват лесно разширяване и персонализиране. Докато референтния дизайн използва MATLAB за управление на възли и обработка на сигнали, той също така позволява на приложенията със строги изисквания за латентност да реализират критичните към време обработки на сигнали в FPGA [5].

3. Berkeley Emulation Engine

Най-новата система емулатор на Баркли Berkeley Emulation Engine version 3 (BEE3) е 2U шаси с възможност за модулно разполагане на FPGA системи, всяка от които използва 4 Xilinx FPGAs Virtex-5 LX110T, LX155T или SX95T. Тя е проектирана като средство за изследване на компютърната архитектура и по-специално, BEE3 е платформа, която цели ускоряване на изследванията за множество процесори RAMP (Research Accelerator for Multiple Processors). RAMP е разработка на шест университета (Berkeley, Stanford,University of Wyoming,, University of Texas, CMU и MIT) и няколко индустриални партньори, сред които: Microsoft Research, Xilinx, Sun Microsystems и IBM. BEE3 е мащабируема платформа от 1 до 64 системи на 2U шаси, която улеснява проучванията в няколко области: компютърна архитектура, системи, операционна система и софтуер, йерархия и съхранение на паметта и различни ускорители на приложения/алгоритми.

Модулната, мащабируема платформа, базирана на FPGA, със софтуерна методология за проектиране, BEE3 може да се използва за разработки на широка гама високоефективни приложения [3], като:

- когнитивни радиосистеми;
- симулация на мащабни, ad-hoc и традиционни мрежи
- обработка на радиосигнали в реално време
- симулация на MIMO системи
- емулация на компютърна архитектура
- обработка на хиперспектрални изображения
- научни изчисления и др.

4. Kansas University Agile Radio

Гъвкавото радио на университета в Канзас - Kansas University Agile Radio (KUAR) е преносима, мощна и гъвкава платформа за развитие на софтуерно дефинирано радио. Основната цел на KUAR е да създаде възможност за напреднали изследвания в областта на безжичните радио мрежи, динамичния достъп до спектъра и когнитивните радиомрежи. Хардуерът KUAR е популяризиран чрез изследователските проекти в областта на отбраната DARPA (Defense Advanced Research Project Agency) като програма от следващото поколение XG (neXt Generation). Системата е разработена в Simulink и внедрена в Xilinx VHDL (VHSIC Hardware Description Language). Всички функции API (application programming interface) за управление на KUAR са предоставени в управляваща биб-лиотека (Control Library) и се изпълняват чрез помощни програми в командния ред. Предлага се и графичен потребителски ин-терфейс GUI (Graphical User Interface), който позволява тези API функции да се управляват отдалечено или локално [2].

Таблица 1. *Сравнителен анализ на основните характеристики на хардуерни SDR платформи*

Хардуерни SDR платформи	**USRP B210**	**WARP v3**	**BEE3**	**KUAR**	**ADALM-PLUTO**	**SDRPlay -RSP2**
Основни градивни елементи	Xilinx Spartan 6 XC6SLX150 AD9361	Xilinx Virtex-6 LX240T	4 Xilinx Virtex-5 LX110T	XilinxVirtex11	Xilinx Zynq Z-7010	MSi001 MSi2500
Честотен диапазон	70 MHz – 6 GHz	2.4/5GHz	Зависи от свързаните RF модули	2.4/5GHz	325 MHz – 3.8 GHz (70 MHz – 6 GHz при софтуерна модификация)	10 kHz – 2 GHz
Честотна лента	56 MHz	40MHz	100 MHz	30 MHz	20 MHz	10 MHz
RF канали	2	4	16	16	2	1
Rx ADC	12 bits	12 bits	8 bits	14	12 bits	12 bits
Tx DAC	12 bits	12 bits	12 bits	16	12 bits	-
ОС	Windows Linux Mac	Windows	Windows Linux Mac	Windows Linux	Windows Linux Mac	Windows
Интерфейси	USB 3.0	USB-UART	RS232 USB Gig Ethemet	USB 2.0 Gig Ethemet	USB 2.0, Ethernet & WLAN с USB-OTG адаптер	USB 2.0
Цена	1 220 €	6900 $ (4900 $ за обучение)	20 000 $	4 000 $	149 $ (99 $ - за обучение)	169 $

5. ADALM-PLUTO

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 [1].

6. SDRplay

SDR-RSP2 е мощен широколентов пълнофункционален SDR, който обхваща радиочестотния спектър от 10 kHz до 2 GHz. За осигуряване на пълната функционалност на комуникационен приемник се нуждае от управляващ компютър и антена. Посредством достъпния софтуер „SDRuno", предоставен от SDRplay, може да се наблюдава до 10 MHz от спектъра в даден момент. Достъпният отворен API код позволява на разработчиците да създават нови демодулатори или приложения около SDR платформата [5].

III. СРАВНИТЕЛЕН АНАЛИЗ НА ХАРАКТЕРИСТИКИТЕ

Софтуерно дефинираните радио системи са обект на изключително внимание от всички корпоративни и университетски изследователки центрове и лаборатории. Разработени са и се използват за изследователски цели голям брой платформи, позволяващи развитието на принципите на софтуерното радио. Крайните продукти, под формата на вградени или самостоятелни изделия, са в широк ценови диапазон, което прави някои от тях трудно достъпни за целите на обучението. В таблица 1. е представено сравнение на описаните SDR хардуерни платформи по характеристики като:

- основни градивни елементи;
- честотен обхват;
- честотна лента;
- брой RF канали;
- точност на Rx ADC и Tx DAC;
- поддържани операционни системи ОС;
- интерфейси;
- цена.

Техническите характеристики позволяват ефективно изследване на разработки в широк честотен диапазон, като основно се използват честоти от 2.4 до 5 GHz. Осигуряваната честотна лента е от порядъка на няколко десетки MHz, което е достатъчно за повечето съвременни приложения. По скъпите платформи като KUAR позволяват работа със сигнали с честотна лента от 100 MHz. Подържат се няколко радиочестотни канала, като точността на конвертирането на сигналите в двете посоки се осигурява основно от 12-битови преобразуватели. Повечето от изследваните хардуерни платформи за SDR работят под управлението на операционните системи Windows и Linux, като съответно има разработени и предложени богати библиотеки от приложения. По-скъпите платформи работят и под управление на операционната система Mac за Apple компютри. Обща особеност на всички платформи за SDR е използването на технологията FPGA за изграждане на вътрешната структура на хардуерната част. Това ги прави едновременно достатъчно гъвкави за разработка на нови приложения и същевременно се осигурява необходимото бързодействие.

IV. ЗАКЛЮЧЕНИЕ

От анализа на представените характеристики на разгледаните хардуерни платформи може да се направи извод, че хардуерната платформа ADALM-PLUTO на Analog Devices Inc., която по цена е сравнима с SDR приемник, предлага възможности за реализация на пълно функционална радиокомуникационна SDR система, състояща се от приемник и предавател с честотна лента от 20 MHz в широко използвания честотен диапазон от 325 MHz до 3.8 GHz. Платформата ADALM-PLUTO позволява разработване, тестване и изследване на приложения чрез софтуерни пакети като MATLAB и Simulink, като осигурява интуитивен графичен потребителски интерфейс API. Като такава, платформата ADALM-PLUTO е подходяща както за нови разработки, така и за обучение.

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. BEEcube, FPGA Based Rapid Prototyping Platforms for Telecommunications, 2016, Available at http://www.beecube.com/uploads/6/3/4/9/63495763/beecube_brochure_web.pdf.
4. National Instruments. Ettus Research, an NI Brand, 2018, Available at https://www.ettus.com/.
5. SDRplay, 2018, Available at https://www.sdrplay.com/.
6. WARP: Wireless Open Access Research Platform, 2018, Available at https://warpproject.org/trac.
7. Xilinx, Zynq-7000 SoC Data Sheet: Overview, 2018. Available at https://www.xilinx.com/support/documentation/data_sheets/ds190-Zynq-7000-Overview.pdf.
8. Xilinx, Zynq-7000 SoC Technical Reference Manual, 2018. Available at https://www.xilinx.com/support/documentation/user_guides/ug585-Zynq-7000-TRM.pdf.

БЛАГОДАРНОСТИ

Тази статия е резултат от работата по проект “Изследване на софтуерни радиокомуникации”, финансиран от Национален военен университет – Велико Търново, Факултет “Артилерия, ПВО и КИС”.

T. G. Peshev,

RADAR WITH INVERSE SYNTHESIZED ANTENNA APERTURE – EVALUATION OF PARAMETERS OF MOVING TARGET

Todor G. Peshev

"Vasil Levski" National Military University, "Artillery, Air-defence and Communication and Information Systems" Faculty, "Air Defense" Department; town of Shumen

Abstract: *In the paper a method of synthesizing of an optimal receiver in radar with inverse synthesized aperture is considered, in order to evaluate the parameters of a moving target. The method used is the so called method of maximum probability.*

Keywords: *radar with inverse synthesized aperture, the parameters of a moving target, method of maximum probability.*

РЛС С ИНВЕРСНО СИНТЕЗИРАНЕ НА АПЕРТУРАТА НА АНТЕНАТА – ОЦЕНКА НА ПАРАМЕТРИТЕ ЗА ДВИЖЕНИЕ НА ЦЕЛТА

Тодор Г. Пешев

Въведение

Ефективността при използването на РЛС с инверсно синтезиране на апертурата на антената (ИРСА) за откриване на въздушни цели се определя от възможността за отчитане на фазовите изкривявания на сигнала, обусловени от маневрирането на целта на интервала за синтезиране. В тази статия се разглежда въпроса за синтез на оптимален алгоритъм за оценка на параметрите за движение на движеща се цел. В качеството на критерий за оптималност е избрана оценка на параметрите за движение по максимума на функционала на правдоподобие, имаща такива важни предимства като асимптотическа неизместеност, ефективност и др.

Изложение

В общия случай намирането на оценката на максимално правдоподобие се получава от решаването на следното уравнение [2]

$$(1) \qquad \nabla_{\lambda} F^{\xi}_{\lambda_0} = 0,$$

където: $F^{\xi}_{\lambda_0}$ – функционала на правдоподобие на вектора от информационни параметри λ_0, описващ статистическото наблюдение;

∇_{λ} – оператор на градиента на вектора от информационни параметри;

$\xi = \xi\ t$ - приетата реализация.

Приетата реализация представлява сума от полезния сигнал, отразен от точкова цел и бял гаусов шум, т.е.

(2) $\xi\ t\ = S\ t, \lambda_0\ + n\ t\ ,$

където: $S\ t, \lambda_0$ - отразения сигнал от точкова цел, описан с израза

(3) $S\ t, \lambda_0\ = \mathrm{A}_0 exp\ -j\frac{4\pi}{\lambda} r\ t, \lambda_0\ ,$

където: $A_0 = A_0 exp\ -j\psi_0$ - комплексната амплитуда на отразения сигнал;

$r\ t, \lambda_0$ – функция, определяща изменението на разстоянието от ИРСА до целта в момента от време t за интервала на синтезиране T_c.

Функциата $r\ t, \lambda_0$, определяща изменението на разстоянието, може да бъде апроксимирана посредством полином от втора степен, т.е. [1]

(4) $r\ t, \lambda_0\ = r_0 + \lambda_{10} t + \lambda_{20} t^2.$

В израз (4) информационните параметри λ_{10} и λ_{20} имат напълно определен физически смисъл като $\lambda_1 = V_r$ е радиалната скорост на целта, а $\lambda_2 = {}^{a_r}{}_{2}$ е радиалното ускорение на целата [1]. Следователно израз (4) може да бъде записан по следния начин

(5) $r\ t, \lambda_0\ = r\ t, V_r, a_r\ = r_0 + V_r t + {}^{a_r}{}_{2} t^2.$

Сложността на статистическото описание на приетите данни от наблюдението $F\ {}^{\xi}{}_{\lambda_0}$ се заключава в липсата на априорни данни за информационните параметри λ и на съпътстващите неинформационни параметри A_0, ψ_0 , които влият на статистиката от данни за наблюдението $F\ {}^{\xi}{}_{\lambda_0}$. За преодоляване на тази трудност при статистическото описание на наблюдението $F\ {}^{\xi}{}_{\lambda_0}$ в условията на априорна неопределеност се предлага разширяване на вектора на интересуващите ни параметри, при което съпътстващите параметри се обединяват във вектор $\alpha = A_0, \psi_0$. При такава постановка на задачата за синтез израз (2) придобива вида

(6) $\xi\ t\ = S\ t, \lambda_0, \alpha\ + n\ t\ .$

За статистическо описание на наблюдението $F\ {}^{\xi}{}_{\lambda_0, \alpha}$ в условията на априорна неопределеност се използва функционала на правдоподобие за „бял” гаусов шум т.е. [2]

(7) $F\ n\ t\ = k_0 exp\ -\frac{1}{2N_0}\ {}_0^{T_c}\ n\ t\ {}^2 dt\ ,$

където: N_0- спектрална плътност на „белия” шум;
k_0 - нормиращ коефициент;
T_c - интервал на синтезиране на апертурата на антената.

Замества се в израз (7) изразът за $n\ t$ от израз (6) и отчитайки изрази (3) и (6), се получава

(8) $$F^{\xi}_{\lambda_{0,}\alpha} = k_0 exp\ -\frac{1}{2N_0}\ {}_0^{T_c}\ \xi\ t\ - A_0 exp\ -j\frac{4\pi}{\lambda}\ r_0 + V_r t + +\frac{a_r}{2}t^2\ \ {}^2 dt\ .$$

Последният израз може окончателно да бъде преобразуван във вида

(9) $$F^{\xi}_{\lambda_{0,}\alpha} = k_0 exp\ -\frac{1}{2N_0}\ {}_0^{T_c}\ \xi\ t\ \ {}^2 dt\ \ exp\ -\frac{A_0^2}{2N_0}T_c\ \ \text{x}$$

$$\text{x} exp\ \frac{A_0}{N_0}\chi\ \lambda_0\ .cos\ \psi_0 + \varphi\ \ ,$$

където: $\chi\ \lambda_0\ =\ {}_0^{T_c}\xi\ t\ exp\ j\frac{4\pi}{\lambda}\ r_0 + V_r t + \frac{a_r}{2}t^2\ \ dt\ ,$
$\varphi = arg\ \chi\ \lambda_0\ \ .$

Изразът (9) може да се представи в много по опростен вид отчитайки, че степенния показател на първата експонента не зависи от параметрите λ_0, α и втория съмножител може да бъде включен в нормиращия множител. Освен това като се отчита и факта, че обработката на приетата реализация $\xi\ t$ се извършва за всеки строб по разстояние независимо, то може да не се отчита фазовото изменение на сигнала $\frac{4\pi}{\lambda}r_0$. Следователно израз (9) придобива следния вид

(10) $$F^{\xi}_{\lambda_{0,}\alpha} = k.exp\ -\frac{A_0^2}{2N_0}T_c\ \ exp\ \frac{A_0}{N_0}\chi\ \lambda_0\ .cos\ \psi_0 + \varphi\ \ ,$$

където: $$\chi\ \lambda_0\ =\ {}_0^{T_c}\xi\ t\ exp\ j\frac{4\pi}{\lambda}\ V_r t + \frac{a_r}{2}t^2\ \ dt\ .$$

Израз (10) е основен за синтеза на оптимален адаптивен алгоритъм за оценка на параметрите λ_0 , който може да бъде получен от решението на следната система уравнения

(11) $$\frac{\partial F^{\xi}_{\lambda_{0,}\alpha}}{\partial\lambda_1} = 0,$$

$$\frac{\partial F^{\xi}_{\lambda_{0,}\alpha}}{\partial\lambda_2} = 0,$$

$$\frac{\partial F^{\xi}_{\lambda_{0,}\alpha}}{\partial\alpha_1} = 0,$$

$$\frac{\partial F^{\xi}_{\lambda_{0,}\alpha}}{\partial\alpha_2} = 0.$$

Решението на системата уравнения (11) може да се опрости, намалявайки размера на вектора λ_0, α . За това намаляване на размера на вектора може да се приложи адаптивния бейсов подход [2], който предполага използването на априорните данни за съпътстващите параметри $p_{pr}\ \alpha$, зададени с точност до постоянния множител на параметъра γ

(12) $$p_{pr}\ \alpha\ = p_{pr}\ ^{\alpha}\ _{\gamma}\ .$$

Този подход позволява да се усредни полученият функционал на правдоподобие (10) по вектора на съпътстващите параметри α , а при изчисляването на оценката на максимално правдоподобие на информационните параметри λ_0 да се замени γ с неговото оценъчно значение γ.

За получаване на функционала на прадоподобие $F\ ^{\xi}\ _{\lambda_0,\gamma}$ за вектора на информационните параметри λ_0 се приема, че амплитудата на отразения от точкова цел сигнал е случайна величина, която е разпределена по закона на Релей, а фазата на преотражение ψ_0 е разпределена по равномерния закон в интервала $-\pi; +\pi$. Параметърът γ в този случай съответства на дисперсията на флуктуациите на амплитудата на отразения сигнал. Съгласно теорията на вероятностите априорната вероятност на съпътстващите параметри може да се запише във вида

(13) $$p_{pr}\ A_0, \psi_0\ = p_{pr}\ A_0\ p_{pr}\ \psi_0\ = \frac{A_0}{2\pi D_A} exp\ -\frac{A_0^2}{2D_A}\ .$$

Замества се израз (13) в израз (10), в резултат на което се получава окончателният израз за функционала на правдоподобие, т.е.

(14) $$F\ ^{\xi}\ _{\lambda_0, D_A}\ =\ F\ ^{\xi}\ _{\lambda_0, A_0, \psi_0}\ p_{pr}\ A_0\ p_{pr}\ \psi_0\ dA_0 d\psi_0 =$$

$$= const. exp\ \frac{2D_A\ \chi\ \lambda_0\ ^2}{N_0\ T_c D_A + N_0}\ .$$

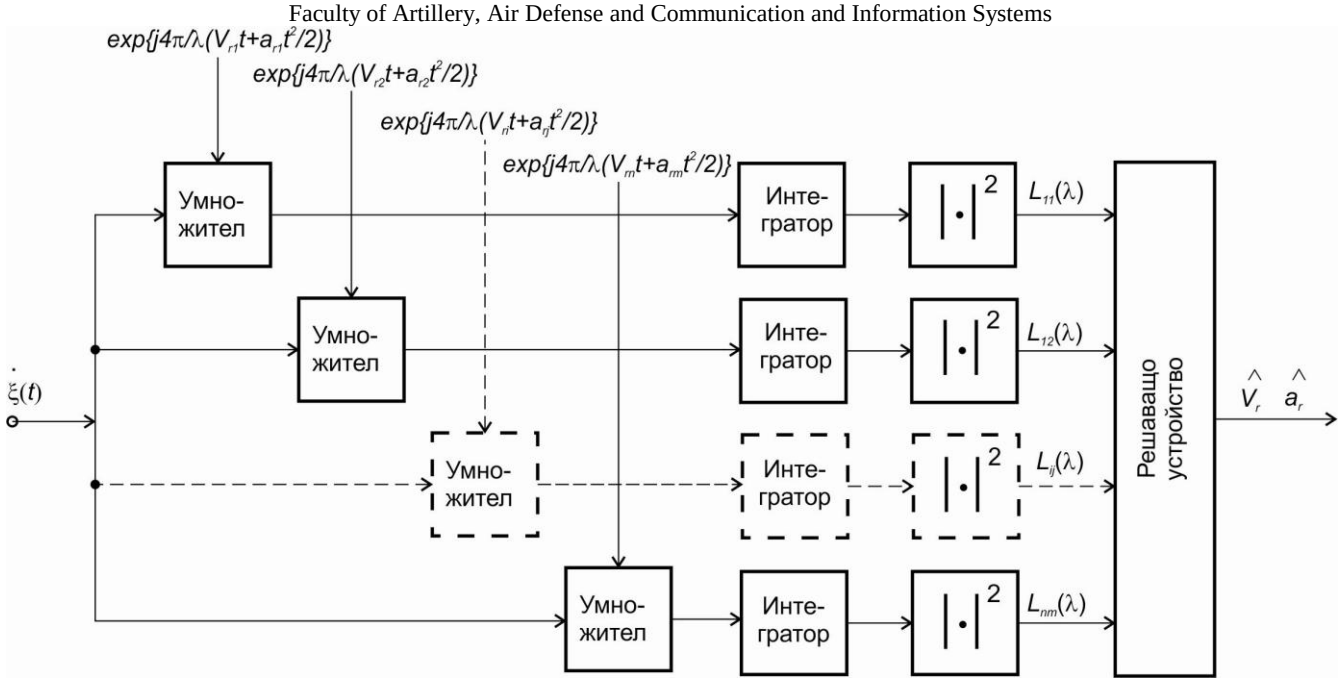
Използваме свойството за инвариантност на оценката на максимално правдоподобие, израз (14) се логаритмува и се получава

(15) $$L\ \lambda_0, \gamma\ = ln\ F\ ^{\xi}\ _{\lambda_0, D_A}\ = \frac{2D_A}{N_0\ T_c D_A + N_0}\ \chi\ \lambda_0\ ^2.$$

Анализът на израз (15) показва, че оценката на максимално прадоподобие не зависи от параметъра γ , което позволява при анализа на оптималния алгоритъм да се разглежда следният израз

(16) $$L\ \lambda_0\ =\ \chi\ \lambda_0\ ^2.$$

Структурната схема на оптимален приемник за получаване оценката на максимално правдоподобие на изформационните параметри радиална скорост V_r и радиално ускорение a_r е показана на фигура 1.



Фиг. 1. Оптимален приемник

Структурната схема представлява $m\ x\ n$ канален приемник. Във всеки канал се осъществява формиране на функцията $L_{i,j}\ \lambda_0$, където $i = 1, n$ и $j = 1, m$. Решаващото устройство избира канала, където $L_{i,j}\ \lambda_0\ = max$, като по този начин формира оценката на информационните параметри V_r и a_r. Работата на многоканалния приемник предполага разбиването на диапазона от възможни стойности на оценяваните радиална скорост V_r и радиално ускорение a_r съответно на n и m поддиапазони. Значенията за n и m се определят от изискванията за определена точност на оценките на тези параметри V_r и a_r. Очевидно е, че няма смисъл от избора на разлика между съседни значения на оценявания параметър т.е. стойността на поддиапазона по-малък от средноквадратичното отклонение в оценката на този параметър. Това само ще доведе до нарастване на броя на каналите в приемника и увеличаване на изчислителната процедура.

Заключение

Реализацията на този приемник в състава на ИРСА ще позволи да се определят параметрите на траекторията за движение на въздушната цел и в последствие използването им за структуриране на опорната функция за обработка на сигналите т.е. за синтезиране на апертурата на антената.

References:

1. Толстов Е.Ф., Антипов В.Н. и колектив, Радиолокационные станции с цифровым синтезированием апертуры антенны, „Радио и связь”, Москва, 1988.
2. Тихонов В.И., Оптимальный прием сигналов, „Радио и связь” Москва, 1983.

V. M. Vasilev,

ANALYZE SCANNED AREA BY METRIC RADARS

Vencislav M. Vasilev

National Military University, Faculty "Artillery, Air-Defence and Communications"

Abstract: *In this issue is analyzed scanned area by metric radars. A mechanism for forming multilobed beam is represented and factors which work on this process. A way to change directivity diagram position in endlong plane by alterations in fundamental frequency is represented too. It's shown on which values of the wavelength the directivity diagram is moving up or down in definite limits.*

Keywords: *directivity diagram, metric radar, mirror reflection factor, diffuse reflection factor, antenna's height.*

АНАЛИЗ НА ЗОНАТА НА ОТКРИВАНЕ НА МЕТРОВИ РАДИОЛОКАЦИОННИ СТАНЦИИ

Венцислав М. Василев

Национален военен университет "Васил Левски",
Факултет "Артилерия, ПВО и КИС"- гр. Шумен

ВЪВЕДЕНИЕ

Зоната на откриване на една радиолокационна станция (РЛС) е важен тактически параметър, който характеризира възможностите и за бойно използване. Тя представлява областта от въздушното пространство, в която станцията води непрекъснато радиолокационно наблюдение на целите. Формата на зоната на откриване се определя от формата на диаграмата на насоченост (ДН) във вертикална равнина, която се формира от антената на РЛС [3,4,6,7].

При РЛС от метров диапазон ДН във вертикална равнина има многолистов характер и е силно изрязана, а също така зависи от постилащата повърхност в участъка между РЛС и наблюдавания обект.

Отразеният ехо сигнал от наблюдавания въздушен обект на входа на приемника е смес от сигнали, както от целта, така и от постилащата повърхност в разрешаващия обем на РЛС. Преотразеното поле е сума от множество елементарни сферични вълни, отразявани от елементарните участъци на повърхността, ограничена между антената на РЛС и отразяващия обект. Полето по апертурата на антената се явява сума от отразената вълна и голям брой елементарни преотразени вълни от повърхността. Този механизъм е в основата на многолъчевото разпространение. Основната част от енергията на преотразеното поле се дължи на първата зона на Френел около точката на огледално отражение [1].

В тази статия е анализирана зоната на откриване на метрови РЛС и е представена възможност за повдигане и сваляне на ДН с цел наблюдаване на нисколетящи цели и намаляване на радиуса на мъртвия конус на зоната.

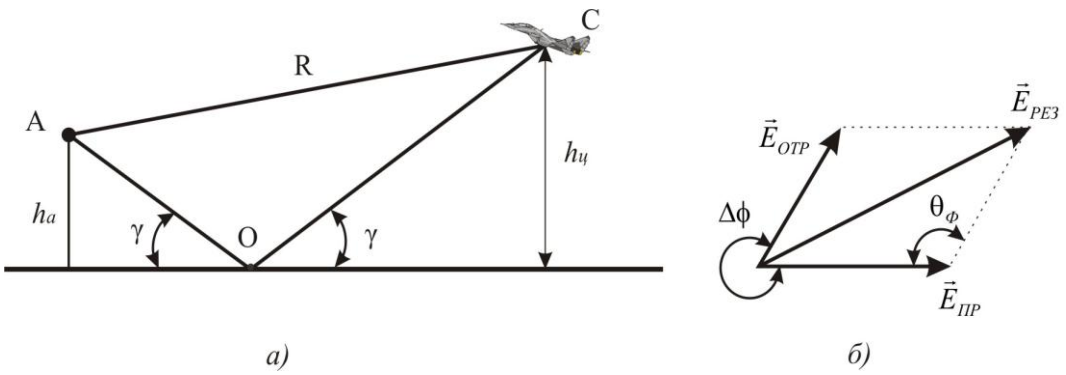
ИЗЛОЖЕНИЕ

Допуска се, че РЛС наблюдава въздушна цел над земната повърхност и се намира на разстояние R от нея. Електрическото поле в точка C от целта се разглежда като резултат от интерференцията на прекия лъч (AC) и отразеният (AOC) в точка O от земната повърхност (фиг. 1 а).

Резултантната напрегнатост на електрическото поле е сума от моментните значения на напрегнатостите на полето на прекия лъч $\vec{E}_{ПР}$ и на отразения от повърхността на земята лъч $\vec{E}_{ОТР}$ (фиг.1 б) [2, 5]:

(1) $$\vec{E}_{РЕЗ} = \frac{173\sqrt{P_{ИЗЛ}\,G}}{R_ц}\Phi,$$

където: – G е коефициента на насоченост на антената;
– $P_{ИЗЛ}$ е излъчената мощност;
– $R_ц$ е разстоянието до целта;
– ω е кръговата честота на излъчените колебания;
– Φ е множителя на затихването:



Фиг. 1. Взаимно разположение на РЛС и облъчвания обект
при формиране на резултантния ехо сигнал

Степента на влияние на постилащата повърхност се отчита чрез множителя на затихването[5]:

(2) $$\Phi = \sqrt{1 + 2\rho_{s0}\cos(\theta_\Phi + \Delta\phi) + \rho_{s0}^2},$$

където: – $\Delta\phi = \frac{2\pi}{\lambda}\Delta R$ е фазовото изместване за сметка на разликата ΔR в пътищата на пряката и отразената от постилащата повърхност вълна;
– ρ_{s0} е комплексен коефициент на отражение от земната повърхност с фаза θ_ϕ;
– λ е дължината на вълната.

Множителят на затихването показва колко пъти напрегнатостта на полето при отражения от земята е по-голяма или по-малка от напрегнатостта на полето в свободното пространство. При промяна на ΔR множителя на затихването приема стойности от $\Phi=1+\rho_{s0}$ до $\Phi=1-\rho_{s0}$.

ДН във вертикална равнина при метрови РЛС се отличава с многолистова структура [3,4,5]. Това се обяснява с факта, че в дадена точка от пространството интерферират два лъча- директен и отразен, между които съществува някаква фазова разлика. Тя се определя от фазовата разлика от пътищата на пряката и отразената вълна $\Delta\phi$ и от фазата на коефициента на отражение θ_ϕ, който приемаме за постоянен за цялото трасе. В посоките на интерференционни максимуми резултантното поле се усилва $1+\rho_{s0}$ пъти, а в посоките на минимумите намалява $1-\rho_{s0}$ пъти [5].

Когато фазовата разлика $\Delta\phi$ е равна на нула или кратна на 2π, то амплитудите на двата сигнала $E_{ПР}$ и $E_{ОТР}$ се сумират във фаза и в тези посоки амплитудата на резултантното поле $E_{РЕЗ}$ е максимална и се получава максимум на ДН. В посоки, където фазовата разлика $\Delta\phi$ е кратна на четно число пъти π сигналите се сумират в противофаза и $E_{РЕЗ}$ е минимална (фиг. 2).

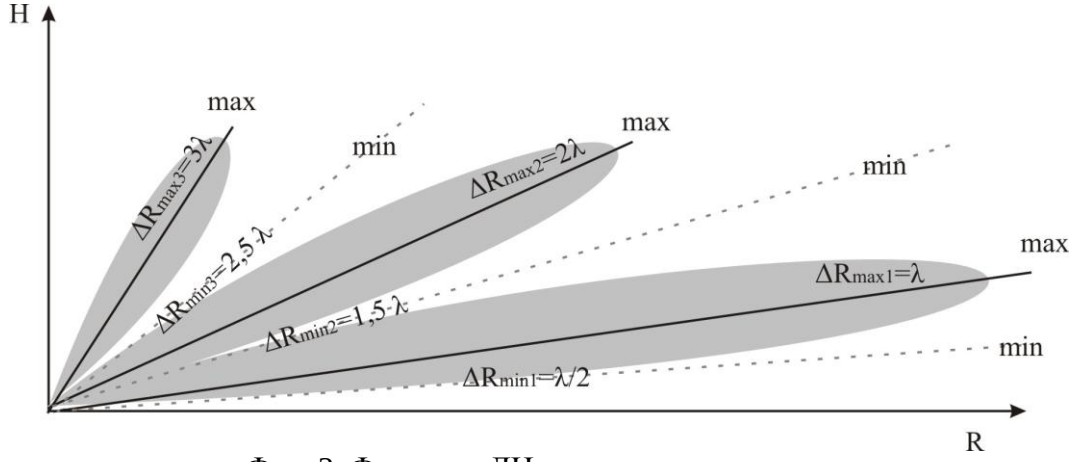
Разликата в пътищата на пряката и отразената вълна ΔR е равна на[1]:

(3) $$\Delta R \approx \frac{2h_ц h_a}{R_ц},$$

където h_a е височината на антената, а $h_ц$ е височината на целта.

При синфазния случай $\Delta\phi = 0$ или $\Delta\phi = 2\pi$, което означава, че разликата $\Delta R = k.\lambda$, където k е цяло число, се получават максимуми на ДН. В противофазния случай $\Delta\phi = \pi$ се получават минимуми в ДН, при което разликата $\Delta R = k\frac{\lambda}{2}$.

Анализирайки формула (3) при h_a=const, за да запазим постоянно значението на ΔR, а от там и $\Delta\phi = 0$ или $\Delta\phi = k\lambda$, следва че $h_ц$ и $R_ц$ нарастват пропорционално – по линеен закон. Така се формират направления, в които отношението $h_ц/R_ц$ винаги ще бъде равно на константа. Това са посоките на максимумите на ДН, които на фиг. 2 са показани с плътни линии, а с пунктири са изобразени посоките на минимумите.



Фиг. 2. Форма на ДН във вертикална равнина

ДН във вертикална равнина на РЛС от метров диапазон е многолистова и се характеризира с голяма изрязаност. За увеличаване на далечината на откриване на нисколетящи цели е необходимо да се увеличи височината на антената на РЛС. По този начин се намалява ъгъла между максимума на най-долния лист от ДН и постилащата повърхност, по който лист основно се извършва откриването на НЛЦ. Големината на този ъгъл се определя от условието: $\varepsilon_{\max} \le 15\lambda / h_a$ [2].

За най-добро формиране на най-долния лист от ДН е необходимо площадката около РЛС да бъде равна. За да преобладава огледалната съставна в сумарния сигнал е необходимо радиусът на тази площадка да бъде $R_{ПЛ} \approx 25h_a^2/\lambda$. Огледалният характер на отраженията се запазва само тогава, когато неравностите и грапавините са по-малки от дължината на вълната. В противен случай отраженията имат дифузен характер и енергията на полето на отразената вълна в целта се намалява. Тогава многолистовия характер е малко изразен: максимумите намаляват, а минимумите не са толкова дълбоки [2].

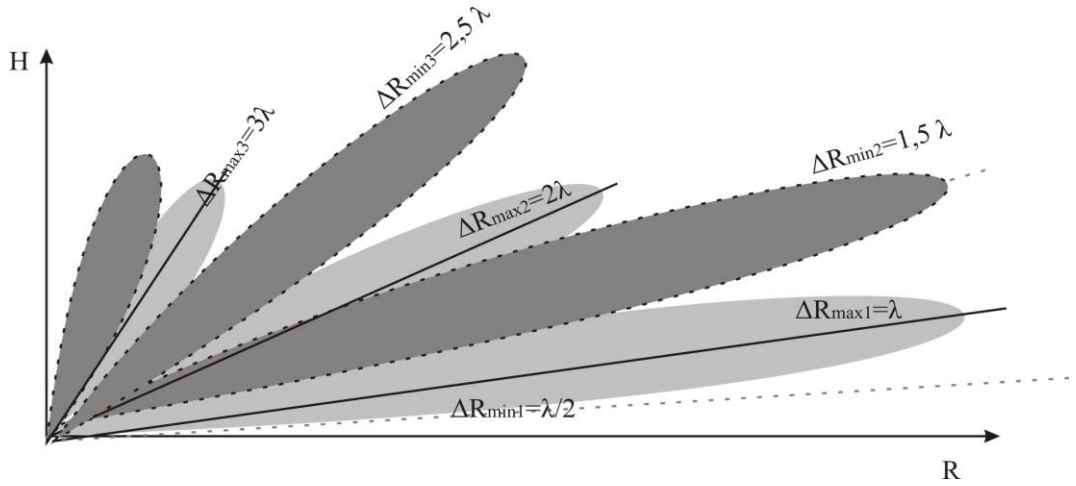
При РЛС от метров диапазон влиянието на неравностите може да се пренебрегне и постилащите повърхности на практика са относително гладки. В този случай съществува огледална съставна, а дифузната е минимална и нейното влияние на сумарния сигнал може да се пренебрегне.

Видът на ДН, представен на фиг.2 е получен при определена дължина на вълната λ_1 (честота f_1). Необходимо е да се намери такава дължина на вълната λ_2, при която минимумите на ДН при λ_1 да заемат мястото на максимумите или обратно (фиг. 3). По този начин се покрива онази част от зоната откриване на РЛС, в която е имало минимуми и там цели могат да се наблюдават. Това е еквивалентно на снемаме или повдигане на цялата ДН по ъгъл на място.

Изходните условия са следните: РЛС използва една и съща антена за приемане и предаване, височината на антената h_a=const, за времето на локация РЛС не си променя позицията, следователно формата на ДН ще остане една и съща. Задачата се свежда до определяне на зависимостта между λ_1 и λ_2.

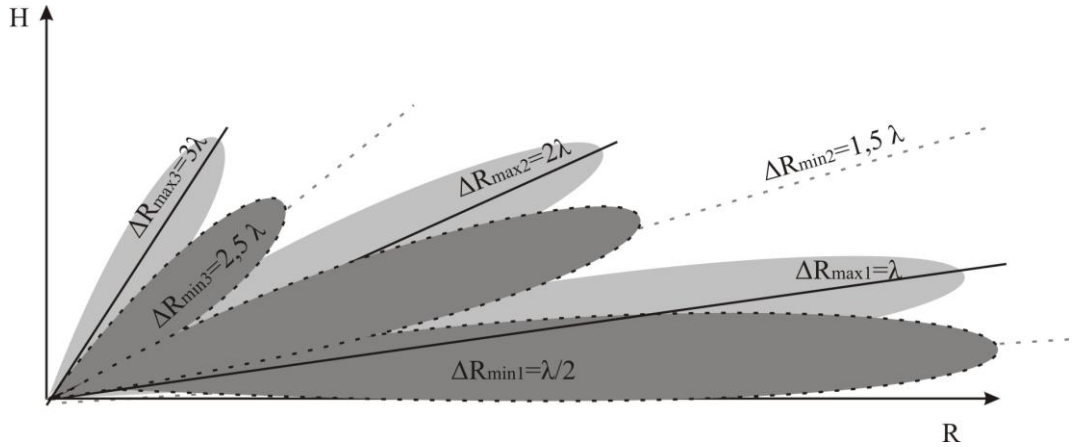
От представеното на фиг. 2 следва, че максимуми имаме в направленията, които отговарят на $\Delta R_{max1}=\lambda_1$, $\Delta R_{max2}=2\ \lambda_1$, $\Delta R_{max3}=3\ \lambda_1$. Минимумите са в посоки, за които $\Delta R_{min1}=0{,}5\ \lambda_1$, $\Delta R_{min2}=1{,}5\ \lambda_1$, $\Delta R_{min3}=2{,}5\ \lambda_1$, .. .

Необходимо е за посока, в която имаме максимум, чрез промяна на λ_1 да получим минимум.



Фиг. 3. Повдигане на ДН

Разглеждаме два случая: ако провалът в ДН след 3 лист при $\Delta R_{min4}=3{,}5\ \lambda_1$ се замени с максимум (фиг. 3), т.е. да приеме ново значение $\Delta R_{max3}=3\lambda_2$. По този начин ДН се премества по ъгъл на място нагоре и се намалява радиусът на мъртвия конус в зоната на видимост. Тогава за λ_2 се получава: $\lambda_2=1{,}17\ \lambda_1$.



Фиг. 4. Смъкване на ДН

Промяната на честотата е в зависимост от това, коя част от зоната на видимост на РЛС искаме на покрием, т.е. в направлението, където имаме провали в ДН и РЛС не наблюдава целта след промяна на честотата да бъде насочен максимум на ДН. Най-достоверно това може да бъде проверено за най-горния и най-долния лист на ДН от фиг. 2.

Във втория случай, когато смъкваме първия лист по ъгъл на място, така че да покрием малки височини в зоната на видимост (фиг.4), $\Delta R_{min1}=\lambda_1/2$ трябва да приеме значение при $\Delta R_{max1}=\lambda_1$. Отношението между дължините на вълните е: $\lambda_2=0{,}5\ \lambda_1$.

В честотно отношение промяната на дължината на вълната (честотата) поставя изисквания към честотната характеристика на антената. В първият разгледан случай разликата между дължините на вълните е по-малка, което допуска (в някакви граници) използването на една и съща антена.

Но за втория случай при намаляването на λ на половина амплитудно-честотната характеристика на антената не може да осигури необходимият коефициент на усилване и формата на ДН в хоризонтална равнина ще се промени, а това води до промяна във формата на зоната на откриване на РЛС.

Заключение:

Намаляването на радиуса на мъртвия конус изисква промяна на честотата на излъчения сигнал с около 20%, което е практически реализуемо.

Управлението на положението на първия лист на ДН изисква промяна на носещата честота (дължина на вълната) с около 50%, което налага да се анализират параметрите на антенно-фидерната система по отношение на тяхното изменение.

References:

[1]. Бартон. Д. Радиолокационное сопровождение целей при малых углах места. ТИИЭР, т.52, кн.9, 1976.

[2]. Буров, Н.И. Маловысотная радиолокация, Москва, Воениздат, 1978.

[3]. Василев, В.М. Устройство на радиолокационно изделие 1РЛ131, Учебно пособие, НВУ "В. Левски" -2007.

[4]. Дамянов, Д.Д. Антенни устройства. Военно издателство 1978.

[5]. Дамянов, Д.Д. Разпространение на радиовълните, МНО 1975.

[6]. Lecture notes from Introduction to RADAR systems, Central Florida Remote Sensing Laboratory, USA, 2003.

[7]. Prof. David Jenn, Lecture notes from Microwave Devices & Radar, Naval Postgraduate School, 2002.

V. T. Atanasov,

SMART EDUCATIONAL CLUSTER CONCEPTIALIZATION

Valentin T. Atanasov

National Military University Vasil Levsky
Faculty „Artillery, AD and CIS"

Abstract: *This paper examines the conceptualization of a multi-component, logically composed structure that provides the ability for self-organizing of distributed learning process based on information and communication technologies. The theoretical basis for the conceptual model is the synthetized paradigm of the educational process and the integration of intelligent agent, realized by final technological solutions.*

Keywords**:** *Smart education, smart labs, smart environment, smart virtual school, smart educational cluster*

КОНЦЕПТУАЛИЗАЦИЯ НА УМЕН ОБРАЗОВАТЕЛЕН КЛЪСТЕР

Валентин Т. Атанасов

Национален военен университет „Васил Левски"
Факултет „Артилерия, ПВО и КИС"
valopaint@yahoo.com

ВЪВЕДЕНИЕ

Изследванията и разработките в областите, оптимизиращи човешката дейност и реализиращи тази човешка дейност в определени граници, имат своето начало с първия компютъризиран дом ECHO IV [1], визията за умни телефони [2] и първите схващания за повсеместен изчислителен процес[3]. С извървяния път през дефинирането на човеко-компютърното взаимодействие (HCI), разглеждано от Станфордския изследовател Дъглас Енгълбърт до представянето на телефонни устройства на компанията AT&T [2] с нови функционалности, обозначени като „умни"(smart), се завършва стадият на персонално характеризиращото взаимодействие с изчислителните устройства. Дефинирането на структурирани информационни обекти, които могат да бъдат достъпвани в мрежово обкръжение, възможностите за програмируема функционалност на мрежови или настолни устройства, специфицирането на автономни технологични устройства, които инициират независима от човека комуникационна дейност, развитието на устройствата за извеждане на информация, сензорните и мобилните устройства доведоха до формирането на нови концепции при решаването на определени задачи, проблеми или изследователска дейност, пораждайки синтеза на информационната и комуникационната области.

Иновациите в информационно-комуникационните технологии са фундаментално обусловени от концептуализиране на понятия като изкуствен интелект, умни устройства, изкуствени невронни мрежи и др., навлезли в научната област от средата XX век и влагайки нов семантичен контекст. Растящият набор от функционалности, основани на изкуствени способности за събиране на информация, нейният последващ анализ и вземане на решения, намират своята практическа реализация в крайни технологични решения, които биха могли да станат елементи на високоинтелигентни самоорганизиращи се образователни структури.

Основна цел на интеграцията на самоорганизиращите се образователни инфраструктури е предлагането на нов подход в процеса на обучение. Настоящата статия разглежда модел на концептуализирането на този подход на основа на синтезиран модел на образователна парадигма.

С цел предлаганият модел да бъде да ясен и логически обусловен, а също и да бъде избегнато двусмислие при използването на термини и понятия, в настоящата статия се приемат определени дефиниции дадени по-долу:

ДЕФИНИЦИИ

Умен образователен клъстер (УОК) - Логически организиран и самоконфигуриращ се комплекс от разпределени високоинтелигентни образователни структури.

Високоинтелигентна образователна структура (ВОС) - структура от елементи на умно образователно обкръжение.

Елемент на умно образователно обкръжение (ЕУОО) - комплекс от технологична единица и интелигентен агент.

Технологична единица (ТЕ) – функционално завършено технологично решение, изградено от материална(*апаратна и инфраструктурна*)съставна или програмна съставна, или от двете.

ПРОБЛЕМНА ОБЛАСТ

За да отговори на динамичните потребности на съвременното общество, изискванията на индустриалната революция 4.0 [1] и възприятията на високо интерактивното поколение, съвременната образователна система трябва да адаптира своите модели и подходи за обучение, образователната инфраструктура, апаратната и програмната си обезпеченост, а също и да актуализира определени образователни стандарти (SCORM, LOM, QTI, xAPI и т.н.).

От друга страна вложеният изкуствен интелект в редица технологични решения като медицинско оборудване за диагностика[5], интелигентни комуникационни устройства[6], умни лаборатории[6], системи за анализ[8],[9] и др. е сериозна предпоставка и аргумент за интегрирането на тези решения в един общ комплекс с възможности за самоконфигуриране и разпределяне на образователни задачи по организиране на учебен процес. Широката гама от образователни технологии [10] са солидна основа за следваща стъпка към интеграция на технологии и подходи, които следва да бъдат разгърнати в учебния процес.

Повечето от разлежданите в [10] образователни технологии намират своите приоритетни позиции за 2018 година в сферата на висшето образование според пазарният изследовател и корпоративен анализатор Гарднър [11].

Навлезлите в последните няколко години технологични решения за активно обкръжение [[12][13][14][15], [16]] развиват концепциите за умно обкръжение в университетските кампуси, основаващи се на принципите:

- *Учене и сътрудничество на всяко устройство, по всяко време и от всяко място;*
- *Защитени комуникации между преподаватели/експерти и обучавани;*
- *Защитен достъп до ресурси на изследователи, преподаватели и обучавани;*
- *Свързаност на вътрекампусни транспортни средства;*
- *Цифрово управление на съоръжения и оборудване;*
- *Защита на данни;*
- *Защита на обучавани;*
- *Виртуални лаборатории;*
- *Събития в социума.*

Холистична недостатъчност

Тези концепции се основават предимно, а в някои случаи изцяло, на предлаганите от технологиите функционални възможности, като по този начин подменят остарялата технологична обезпеченост на учебния процес. Налице е определена адаптираност на съществуващите към днешна дата в образователната сфера подходи и методи към новите технологични реалности. Това адаптиране, обаче, не е съпроводено с концептуализиране на самия образователен процес и неговото

премоделиране в условията на технологичен скок. В [16] се разглежда образователното обкръжение като единица, описваща всеки обект или компонент в него (*лице, процес, устройство, местонахождение*), но подобен подход на сливане на обучаван, преподавател, инфраструктура и технологии в една „*хомогенна нейерархична единица*" без ясно извеждане на връзките, зависимостите и йерархичната архитектура на този сложен образователен комплекс допуска равнопоставеност между активни и пасивни елементи. Потискането на медиаторската, менторската или архетипната роля на преподавателя е предпоставка за размиване границите между формалното и неформалното учене, която тенденция би довела до доминация на неасистирания индивидуализъм в когнитивния процес и по същество отричане на експертното познание. А [15], сред характеристиките на модела на учене, въвежда известни противоречиви ракурси - персонален-социален, предоставяне-извличане, преподавател-обучаван, а в този смисъл ролята на преподавателя остава размита и неясна като индивидуализмът на обучавания граничи с абсолютизация.

Общоприетите теории за учене се основават на принципите на апроксимиране на познанието на обучавания към познанието на експерта в съответната научна област чрез един от двата основни подхода – овърлейния и пертурбационния [17] в които водеща роля играе експертът - преподавателят. А, в разглежданите по-горе тези за умно обкръжение, мястото на преподавателя, който, априори, е съществен активен елемент от процеса на учене, не е съвсем изяснено и определено. В допълнение, пренебрегването на моделите на обучаваните [18][19] при използването на технологично-подпомагано обучение би имало стохастичен характер на ефективността на учебния процес. Още повече, при изграждането на технологични решения за осъществяване на образователен процес, определени дидактически принципи следва да бъдат спазвани. Същественото е, че принципът, на който се следва да бъде основавано технологичното решение, трябва да обуславя постигането на педагогически цели на основата на дидактически модел, вплътен в технологична концепция [21].

Безспорно технологичният напредък предлага нови и по-ефективни инструменти, но все пак това е само инструментариум в ръцете на преподавателите и обучаваните в един формализиран учебен процес. От друга страна [[16], [22] изтъкват основното предназначение на технологиите в обучението: Поддържане и подпомагане на основни дейности в учебния процес(*създаване, достъп и споделяне на учебно съдържание*) и повишаване ефективността на учебните занятия (*лекции, лабораторни упражнения, семинари и др.*).

Подход на слоевете

Все пак, следва да бъдат отчетени направените стъпки при експерименталните реализации на виртуални образователни обкръжения (*пространства, лаборатории, кампуси и др.*). В настоящата статия се предлага използването на слоест модел в който модел тези предлагани или разглеждани технологични решения биха заели първия слой. Този подход на моделиране чрез слоеве предоставя възможности при възникване на промени, в следствие на определени обстоятелства (*технологични, структурни, нормативни, организационни и др.*), за промяна на тези компоненти в даден слой, които са обект на тези промени, без да бъде разрушавана структурата на целия модел.

Сигурност и защита

Една от основните критични точки в съвремието е сигурността и в този аспект образователният процес не остава встрани от този въпрос. Сигурността в човешки, материален и логистичен аспект трябва да има своята реализация, следвайки определени решения за изграждане на учебен процес, който да предоставя такива функционалности които да обезпечават:

- *Физическа защита на обучаваните;*
- *Непрекъснат мониторинг на здравния статус/показатели на обучаваните за времето на учебния процес;*
- *Идентификация на всички членове на обучаващата организацията;*
- *Локализиране местонахождението на обучаваните за времето на учебния процес*
- *Физическа защита на данни;*
- *Възстановяване на данни с учебно съдържание от сривове;*

- *Защита от неоторизиран достъп до чувствителна информация;*
- *Автентикация и оторизация на достъп до информационните масиви;*
- *Система за известяване;*
- *Виртуални асистенти;*
- *Протоколи за сигурност.*

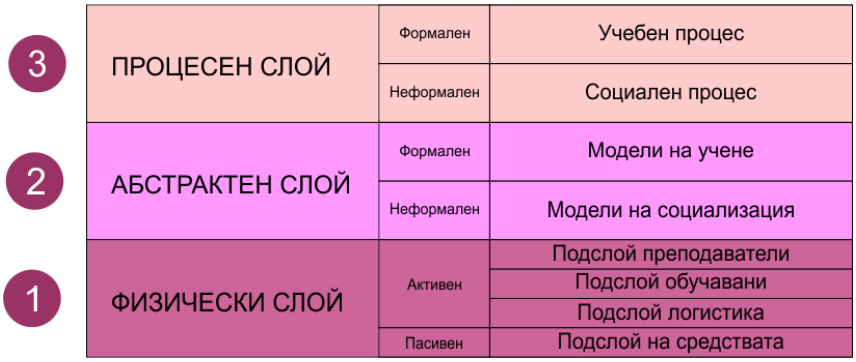
В решенията, предлагани от [16], [22], [23], [24] са застъпени част от горе изброените функционалности. Обстойна формулировка на функционалностите на технологичното решение, представящо елемент на умно образователно обкръжение е представена в [22] а също така са формулирани и задачите на представяното решение. В някои от изследванията са разгледани и възможни сценарии при функционирането на тези умни елементи [[12], [15][16][22], [23], което дава разширена гледна точка при приложението им.

КОНЦЕПТУАЛИЗАЦИЯ

Образователна парадигма

Както бе споменато, за да бъде изграден концептуален модел е необходимо синтезирането на образователна парадигма.

На фиг. 1 е даден модел на класическа образователна парадигма, която ще бъде изменена и развита по-нататък като основа при създаването на концептуален модел на умен образователен клъстер.



Фиг. 1. Модел на класическа образователна парадигма

Този представен модел на класическа образователна парадигма реализира слоестия подход, като всеки слой може да бъде формализиран независимо и самостоятелно. В продължение на предлаганата теза за влагане на дидактически принципи във ВОС се предлага разширена образователна парадигма (фиг. 2).

Фиг. 2. Модел на разширена образователна парадигма

В предлаганата разширена версия на образователна парадигма съществените изменения обхващат добавянето на нов слой и трансформация на *подслоя на средствата* по съдържание и признак. Основен отличителен белег на тази парадигма е, че всички компоненти имат „*активен*" признак, т.е. няма пасивни участници в процеса. При прехода от „*технологично подпомагано"* към „*високотехнологично-инициирано*" обучение е необходимо интегрално и структурно мислене.

Принципи и подходи

Добавеният виртуален (втори) слой представя основните физическите участници (*преподавател и обучаван*) чрез тяхната виртуализация, които единствено и само имат активни роли в това обкръжение. Парадигмата представя и йерархията на абстрактно ниво в учебния процес. Процесът на концептуализация на УОК обхваща и ВОС, като за целта се формира набор от принципи, в чиито състав ще влязат в адаптирана форма и разглежданите по-горе подходи:

- *Избягване на единична точка на срив (ЕТС) при критични ЕУОО;*
- *Повсеместна идентификация на обектите;*
- *Протоколи за сигурност;*
- *Имплементирани дидактически модели;*
- *Самоконфигуриране;*
- *Защитена зона на ареалите;*
- *Защита на данните;*
- *Автентикация и оторизация;*
- *Образователни услуги;*
- *Социални услуги;*

В табл. 1 са дадени възможните подходи за технологично реализиране на тези принципи при изграждането на дадена ВОС.

Принцип	Признак на ЕУОО	Възможни подходи
Избягване на ЕТС	Активен	Дублиране на критични ЕУОО; Дублиране на критични комуникационни трасета; Използване на подхода на директорийни услуги (LDAP, DNS, TCP/IP,IEC).
Повсеместна идентификация на обектите	Активен	Използване RFID идентификатори; Използване на биопараметрични идентификатори; Разпознаване на образи; Стандарти за картова, персонална или контейнерна RFID идентификация (ISO/IEC); Автоинициирана идентификация (АИИ); Изисквана от системата идентификация (ИСИ); Класификация на ниво на достъп.
Протоколи за сигурност	Активен	Протоколи за мрежова сигурност; Протоколи за криптографска сигурност; Протокол за класифициране ниво на достъп.
Имплементиране на дидактически модели	Пасивен	Синтезиране на нови или използване на съществуващи модели на обучавания; Разработка на стратегии на преподаване; Синтезиране на нови или използване на съществуващи дидактически модели за текущата форма на учебен процес.
Самоконфигуриране	Активен	Събитийно ориентиран подход. Интелигентен агент следи данните от функционалния статус на сензорната система и може да инициира

		реконфигуриране на ЕУОО при: • Оптимизиране на ресурси; • Критични събития.
Защитена зона	Активен	Интелигентен агент реализира: • Входящ контрол на база данни от сензорната система на входно-изходните точки; • Контрол на достъпа до информационните ресурси; • Задействане на съответния протокол при установяване на критично събитие на база текущи данни от сензорната система (*известие, пожар, наводнение, авария, инцидент и др.*);
Защита на данните	Активен	Интелигентен агент реализира: • Контрол на всеки достъп до ресурси на база класифициран идентификатор; • Контрол на достъпа до ресурси (*автентикация и оторизация*); • Операции по архивиране, възстановяване; • Оптимизиране на бази данни (*структура,таблици,размер и др.*).
Образователни услуги	Активен	Интелигентен агент реализира два подхода за предоставяне на образователни услуги: • За обучавани; • За преподаватели.
Социални услуги	Активен	Интелигентен агент реализира два подхода за предоставяне на социални услуги: • За обучавани; • За преподаватели.

Табл. 1. Приложени принципи и възможни подходи при тяхното реализиране

Основна дейност при разработката на дадена система е описанието на системното й поведение. На фиг.3 са представени случаите на употреба на абстрактен ЕУОО „Обучавани" чрез използването на формалните средства на UML [25].

Едно от съществените преимущества на основаното на модели проектиране е осигуряването на нагледното им представяне, а оттам и по-ясно разбиране на системата, която ще бъде проектирана [26], [27], [28].

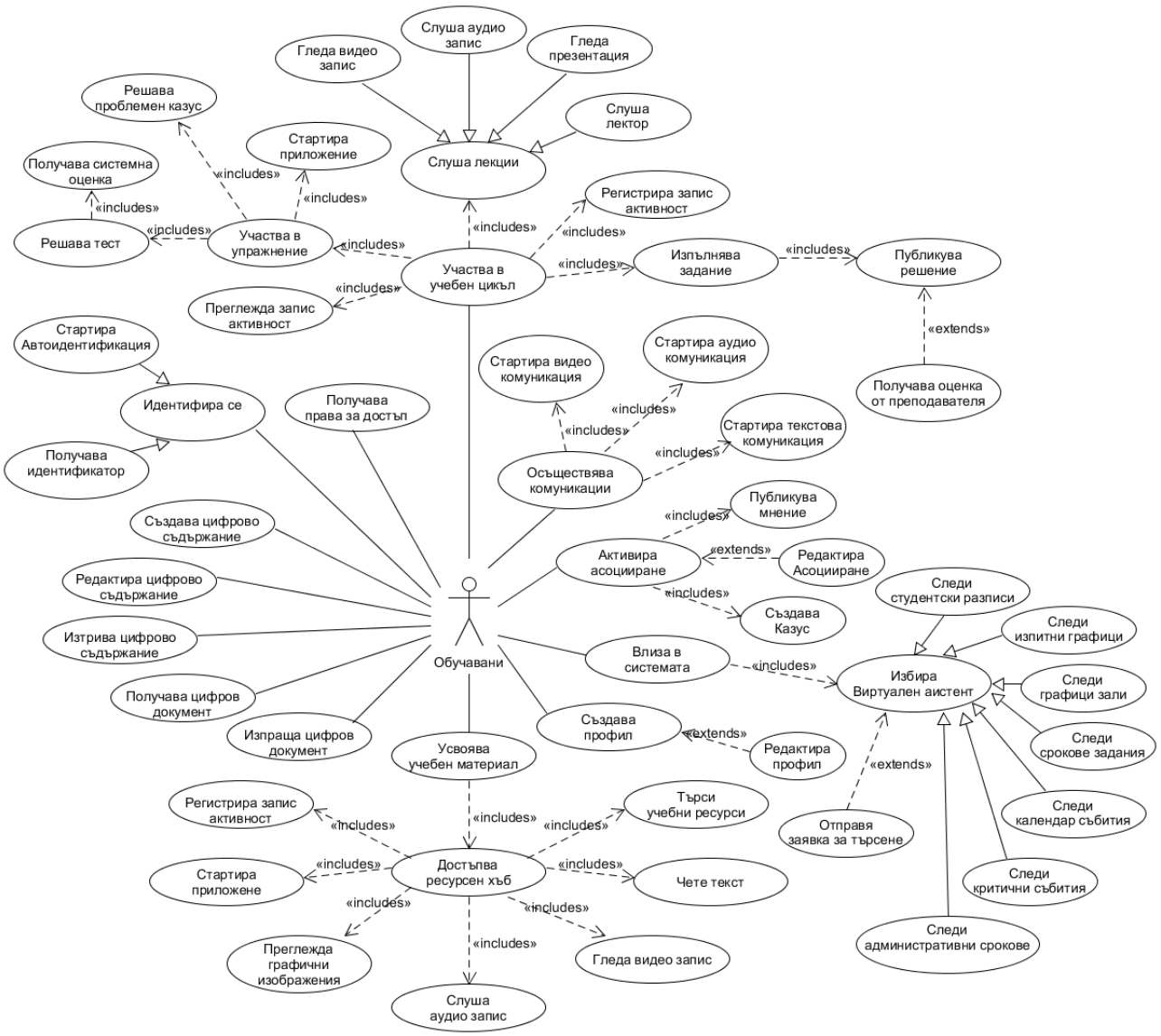
Според дадената по-горе дефиниция на ЕУОО се изисква интеграция на *технологична единица* и *интелигентен агент*. Във функционална йерархичност ЕУОО стои по-високо от съставната й технологична единица поради предлагането на интелигентно ниво на функционалност.

От своя страна, интелигентният агент следва да се основана на схващането на [29], че ако една система предполага ***автономност***, ***способност за учене*** (*самообучение или посредством обучител*) в границите на ***определено обкръжение***, то тя може да бъде определена като интелигентна.

Тази характеристика би могла да бъдат постигната при реализирането на следните принципи:

1. *Ответност* - способност за ответни действия при установени изменения на обкръжението, за да се задоволи неговото предназначение и цели.
2. *Инициативност* - способност за проявява на насочено към целта поведение, за да задоволят своите проектни цели.
3. *Взаимодействия* - способност за взаимодействие с други интелигентни агенти (и вероятно хора), за да задоволят своите проектни цели.

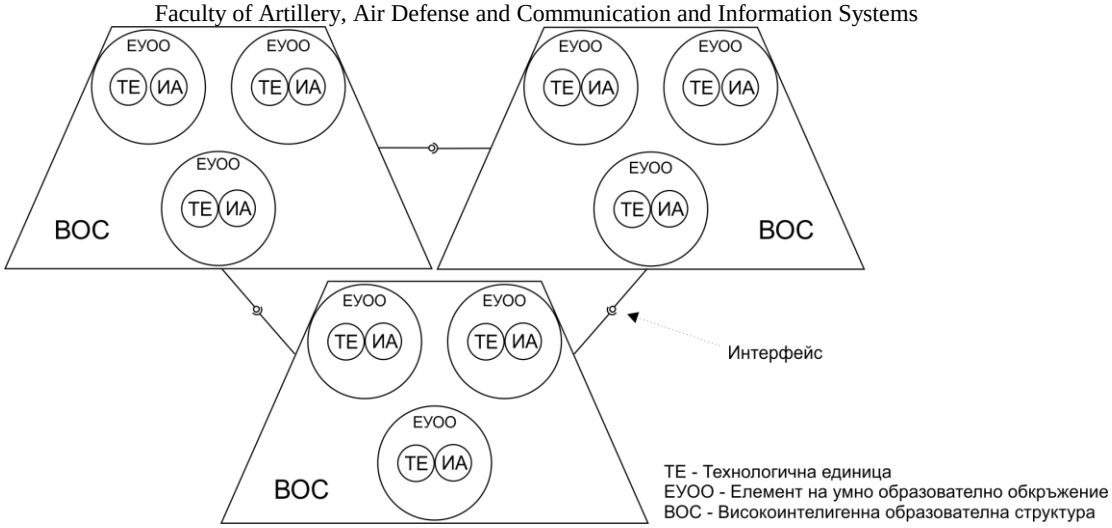
Пример за ЕУОО може да бъде даден с технологичното мобилно решение HUAWEI Mate 10 Pro [30], докато пример за *технологична единица* (*в програмно изпълнение*) би могъл да бъде разглеждан интерфейсът за редакция на съдържание на онлайн енциклопедия със свободен достъп [31].



Фиг. 3. Случаи на употреба на абстрактен елемент на
умно образователно обкръжение „Обучавани“.

Концептуален модел на умен образователен клъстер

С така синтезираните модели, приетите принципи и подходи се изгражда концептуален модел на междуструктурно ниво, който реализира идеята за умен образователен клъстер, представен на фиг.4.



Фиг. 4. Концептуален модел на умен образователен клъстер

Приема се, че в рамките на една образователна институция може да бъде приет подхода за наложено съответствие между основното структурно звено и ВОС.

Последващите стъпки по декомпозирането до ниво ТЕ остават функция на поставените цели пред моделиращите системата. Обслужващите звена следва да бъдат концептуално разглеждани като УЕОО, поради необходимостта от реализиране на принципите, разгледани във раздела принципи и подходи (Табл. 1).

ЗАКЛЮЧЕНИЕ

Предлаганата концептуализация на модели на умни образователни структури и техните елементи е предмет на бъдеща експериментална и изследователска дейност. Към днешна дата предложените модели се подлагат на анализ и последващи изменения. Поради скъпо струващите технологични интелигентни решения, които биха покрили поставените изисквания към ниво елемент на умно образователно обкръжение са затруднени дейностите по разработването на прототип и на чиято реализация предстои бъдещо емпирично валидиране и верифициране.

References:

[1] Infield, G., A Computer in the Basement? //Popular Mechanics, 1968, Volume.129, pp. 77-229
[2] Smart phones, //Popular Science, Bonnier Corporation, Volume.237, No 5, , 1990, ISSN 0161-7370
[3] Weiser, M., The Computer for the 21st Century, Scientific American, Volume 265, No 3, pp. 12-190, 1991, ISSN: 0036-8733
[4] Vaidyaap, S., Ambadb, P., Bhoslec, S., Industry 4.0 – A Glimpse, Procedia Manufacturing - ELSEVIER , Volume 20, pp.233-238, 2018, ISSN 1877-0428
[5] Schmidt-Erfurth, U., Progress in Retinal and Eye Research , 2018, (https://doi.org/10.1016/j) (посетен на 10.08.2018)
[6] Mayera, B., Rabela, B., Sorkoa, S., Modular Smart Production Lab, Procedia Manufacturing - ELSEVIER , Volume 7, pp.361 – 368, 2017, ISSN 1877-0428
[7] Huawei Reveals the Future of Mobile AI at IFA 2017, Huawei, 2017, (https://www.huawei.com/en/press-events/news/2017/9/Mobile-AI-IFA-2017) (посетен на 1.2.2018)
[8] Do You Know The Difference Between Data Analytics And AI Machine Learning?, 2018, (https://www.forbes.com/sites/forbesagencycouncil/2018/08/01/do-you-know-the-difference-between-data-analytics-and-ai-machine-learning/#7548751a5878) (посетен на 2.08.2018)
[9] Data analysis examples, (https://stats.idre.ucla.edu/other/dae/) (Посетен на 2.04.2018)

[10] Смрикаров, А, Иванова, А., Атанасов,В. и кол., Наръчник по иновационни образователни технологии, трето допълнено и преработено издание, издателство „Русенски университет“, 2018, ISBN 978-954-712-736-4
[11] Lowendahl, J., Thayer, T., Morgan, G. et al, Top 10 Strategic Technologies Impacting Higher Education in 2018, 2018, (https://www.gartner.com/doc/3844465/top--strategic-technologies-impacting) (посетен на 12.06.2018)
[12] Build an intelligent digital campus, Cisco Systems, (https://www.cisco.com/c/en/us/solutions/industries/education/connected-campus.html) (посетен на 4.07.2018)
[13] Elevate higher education with smart campus learning, Ruckus Wireless Inc, 2016, (https://ruckus-www.s3.amazonaws.com/pdf/solution-briefs/sb-smartcampus-learning.pdf) (посетен на 12.06.2018)
[14] Smart Campus: Creating services WITH and FOR people, (http://www.open-science-conference.eu/wp-content/uploads/2013/08/14_Marco_Pistore_-_Smart_Campus__Services_with_and_for_People.pdf) (посетен на 12.06.2018)
[15] Gros, B., the design of smart educational environments, 2016, doi 10.1186/s40561-016-0039-x
[16] Glushkova, T., Stoyanov, S., Popchev, I., Cheresharov, S., Ambient-oriented modelling in a virtual educational space, Comptes rendus de l'Academie Bulgare des Sciences, //Engineering Sciences, Tome 71, No 3, 2018, ISSN 1312-5702
[17] Greer, J., McCalla, G., Student Modelling: The Key to Individualized Knowledge-Based Instruction, 1994, NATO ASI, Series F. Springer-Verlag. Vol.1252
[18] Martins, A., M., Faria, L., User Modeling in Adaptive Hypermedia Educational Systems, Systems. Educational Technology & Society, 2008, Volume 11, Number 1, pp.194-207, ISSN 1436-4522
[19] Brusilovski, P., Kobsa, A., Vassileva, J., Adaptive Hypertext and Hypermedia, Springer Science & Business Media, 2013, ISBN 978-94-017-0617-9
[20] Atanasov V., Ivanova, A., Student modelling in a web-based platform for learning games composing , Proceedings of the 13th International Scientific Conference "eLearning and Software for Education, Buchares, Romania April 27 - 28, 2017
[21] Атанасов, В., Един поглед към игровите технологии в педагогически контекст, сп. „Педагогика“, бр.5, 2017, ISSN 0861 – 3982
[22] Гаврилов, А., Новицкая, Ю.,Умная учебная лаборатория для автоматизации проведения лабораторных работ, //Компьютерные инструменты в образовании, № 6, Стр.20 -32, ISSN 2071-2359
[23] Smart Classroom – bringing learning into the digital economy, Smart Classroom Whitepaper, Singtel Optus Pty Limited, 2017,(https://www.optus.com.au/content/dam/optus/documents/enterprise/pdf/Smart-Classroom-Whitepaper-23012018.pdf) (Посетен на 3.07.2018)
[24] Орозова, Д., Стоянов, Ст., Попчев, И., Виртуално образователно пространство. Сборник доклади от научна конференция с международно участие “Знанието – Източник на иновации”, 2013, Стр. 153-159. ISBN 978-954-9370-99-7
[25] Фаулър, М., UML основи, Кратко ръководство за стандартния език за обектно моделиране, Издателство „СофтПрес“ ООД, 2007, ISBN 978-954-685-306-6
[26] Friedenthal, S., Moore, A., Steiner, R., A Practical Guide to SysML: The Systems Modeling Language 2nd Edition, Morgan Kaufmann, 2011, ISBN 9780123852076
[27] Model Driven Architecture (MDA), MDA Guide rev. 2.0, OMG Document ormsc/2014-06-01, (http://www.omg.org/cgi-bin/doc?ormsc/14-06-01) (Посетен на 12.07.2018)
[28] Model-Driven Development: Definitions, Challenges, Promises…, Artisan Software Tools Ltd., 2008, (http://www.omg.org/news/meetings/workshops/Real-time_WS_Final_Presentations_2008/Tutorials/00-T5_VanZandt-Mraidha_Part1.pdf) (Посетен на 02.8.2016)

[29] M. Wooldridge, An Introduction to MultiAgent Systems, John Wiley & Sons Ltd, 2009, ISBN 0-471-49691-X
[30] HUAWEI Mate 10 Pro, (https://consumer.huawei.com/bg/phones/mate10-pro/) (посетен на 20.08.2018)
[31] Editing Games and learning, (https://en.wikipedia.org/w/index.php?title=Games_and_learning&action=edit) (Посетен на 20.08.2018)

V. T. Stoyanova, N. Kulev,

ANALYSIS OF THE CAPABILITIES OF GRAPHIC TABLETS AS A MEANS OF EDUCATION IN COMPUTER GRAPHICS

Veselka T. Stoyanova, Nikolai Kulev

National Military University "Vasil Levski"

Abstract: *A graphic tablet is a computer input device that enables a user to hand-draw images, animations and graphics, with a special pen-like stylus, similar to the way a person draws images with a pencil and paper. This article analyzes the types of graphical tablets classified by several criteria. Attention is drawn to the importance of stylus. Characteristics, applications, advantages and disadvantages of graphical tablets are analyzed.*

Key words*: graphic tablets, computer graphic, CAD, CAM*

АНАЛИЗ НА ВЪЗМОЖНОСТИТЕ НА ГРАФИЧНИТЕ ТАБЛЕТИ КАТО СРЕДСТВО ЗА ОБУЧЕНИЕТО ПО КОМПЮТЪРНА ГРАФИКА

Веселка Т. Стоянова, Николай Ж. Кулев

Национален военен университет „Васил Левски",
ФакултеТ „Артилерия, ПВО и КИС"
Гр. Шумен, ул. „Карел Шкорпил" 1

Въведение

В съвременния технологичен свят обучението по Компютърна графика поставя своите високи изисквания. Не е достатъчно да се използват само различни среди за компютърна графика и да се изучава инструментариума им, а е необходимо развиването на творческия процес с помощта, както на преподавателя, така и на материалната база, с помощта на която се извършва обучението. По-голямата част от професионалистите преминават към цифров начин на работа, причината е софтуерът, който предлага много полезни инструменти, включително такива, които революционизират начина на създаване на изкуство. Факт е, че мишката не е толкова прецизна като човешката ръка и е нужно да се създаде инструмент, който пренася картината от листа хартия директно на екрана на компютър, а именно за тази цел е подходящо да се използва, така нареченият графичен таблет или познат още като таблет за рисуване.

Графичният таблет е хардуерно входно устройство, което позволява на потребителя да изготвя ръчно изображения, анимации и графики. Графичните таблети използват писалка, която при докосване и натиск върху екрана на таблета може да нарисува избрано от потребителя изображение. Тези таблети могат да се използват за различни нужди освен рисуване, а именн за улавяне на данни или на ръкописни подписи[5]. Интересно е, че графичните таблети имат интердисциплнарен характер с пример за приложението им при обекти от противовъздушната отбрана [9]. Интересно би било да се използва обект, който е създаден с таблет, а се прилага в среда за програмиране като Матлаб[12].

С настоящия доклад се цели да се анализират възможностите на графичните таблети, предимствата и недостатъците им, които биха били полезни в процеса на обучение по

Компютърна графика в факултет „Артилерия, ПВО и КИС" при НВУ „Васил Левски" гр. Велико Търново.

Същност

Първият графичен таблет за потребителски компютри е KoalaPad. Разработена от Koala Technologies през 1984 г., като първоначално е предназначен за използване от компютъра Apple II, но по-късно е достъпна и за IBM PC съвместим компютър [2], [3].

Графични таблети използват специални писалки (стилуси), които могат да бъдат с различни размери и стилове. Важна особеност е, че имат чувствителни и специални повърхности за писане, които могат да бъдат матирани или гладки. Тези таблети осъществяват трансфери в цифров формат и могат да бъдат свързани към PC / Mac или лаптоп посредством USB или HDMI кабел[5]. Всичко това предразполага лесното прехвърляне на изображения от обикновена хартия към компютър, чрез проследяване на изображението към компютър, като се проследи върху графичния панел.

Графичните таблети се различават най-вече по следните параметри:

- Работна площ;
- Разделителна способност;
- Скорост на предаване на данните;
- Координатна система;
- Нива за чувствителност на натиск;
- Височина на зоната;
- Софтуер;
- Бутони;
- LPI (lines per inch).

При по-скъпите модели се отчита и наклона на специалната писалка спрямо таблета. Има таблети, представляващи реални екрани, при които усещането е като да рисува върху платно или лист, защото изображението се появява директно под писалката. За избора на един или друг вид устройство е добре да се познават различните видове графични таблети, техните възможности и дали те биха били полезни за една или друга дейност. Това е важно значение, също така при оборудването на лабораториите за учебни цели. В [1], [5] е реализиран доста обстоен анализ на това какви са видовете графични таблети.

Като цяло графичните таблети могат да се разделят на:

- Пасивни таблети –със сравнително достъпна цена, не изискват батерия за стилуса, те са търсен продукт. Всички сигнали се регистрират само от екрана, като потокът на информация е двуканален - единият се получава от сензорите за писалката, а другият се обработва и изпраща към компютъра;
- Активни таблети - използват стилус с батерия. Писалката и таблетът непрекъснато обменят информация помежду си;
- Оптични таблети - в стилуса е вградена микроскопична камера. Оптиката най-често се използва при цифровизирането на илюстрации, първоначално рисувани върху хартия. Контурите на рисунките по-лесно се разпознават;
- Акустични таблети - те са форма на графичния таблет, която използва звук за намиране на позицията на стилуса в зоната за рисуване. Общата функционалност на акустичните таблети се основава на стилус, който излъчва звук и микрофони, които се използват за записване на звука. Текущото положение на стилуса може да се изчисли в зависимост от разликата във времето на записания звук;
- Капацитивни таблети – екраните им включват изолационен външен слой, покрит с прозрачно проводимо метално съединение. Технологията работи чрез откриване на промени в електрическата проводимост през този слой. Тъй като технологията разчита на електрически смущения от проводящи източници, капацитивните таблети не работят посредством електрически изолационни обекти, заради това не може да се използва обикновен стилус или друг обект.

В интернет могат да срещнат много и разнообразни модели на графични таблети, всеки от които е с различна цена, възможности и приложение. Пример за такива са предложени на фиг. 1.

Фиг. 1. Пример за графичен таблет актуален за 2018 [10], [11].

В [7] се разглеждат и дефинират: резолюцията при графичните таблети, която се измерва в lines per inch (LPI), което е броят се успоредните линии на всеки квадратен инч, като колкото повече са линиите, толкова по-висока е резолюцията. От друга страна в [4] се обяснява друг важен параметър: нива на налягане като за повечето таблети са 256, 512, 1024 или 2048, по данни към 2018г. таблетите достигат 8192 нива и нагоре[8]. Тези стойности се отнасят до нивата на чувствителност на стилуса. Нивата на налягане могат да се сравняват с работата като принцип на четка, молива или парче креда при класическия художник. Колкото натискът върху стилуса е по-голям, толкова по-тъмна и по-дебела е линията, чувствителността на натиск върху писалката е особено важна за цифровите художници, които трябва да контролират дебелината, цвета, прозрачността и смесването на линиите.

Някои таблети позволяват докосване с пръст, също като тъчпад на лаптоп,това позволява да се рисува с пръст, ако е необходимо, а също и да се нанасят допълнителни щрихи. Графичният таблет е съвместим с всички операционни системи. Рисуването чрез стилус и работата върху архитектурни или други проекти върху „дъската“, максимално се доближава до традиционното създаване на изображения с молив и хартия. Трудно могат да се посочат минуси на графичните таблети, чудесно е използването им и е улеснение при структурирането и създаването на CAD обекти.

Ако може да се обсъждат недостатъци на графичните таблети един от тях е високата цена за някои модели. Поради тази причина при първоначално обучение може да се започне с по-евтин модел, за да види как се работи с него, преди да се направи избор от по-висок клас. Стилусът с батерия прави писалката обемиста и е възможно да е неудобна за ръката, но при таблетите от по-висок клас този проблем е решен. Субективни недостатък може да се отбележи и размерът на устройтвота, защото таблетите с формат А3 например са огромни и позволяват работа „с размах“, но заемат повече място и са по-трудно преносими в сравнение с по-малките (А6 например). Графичните таблети са лесно приносими, но за тяхното използване често е необходим компютър за визуализация. Това също е субективен проблем, тъй като по-новите графични таблети разполагат с интегриран LCD екран, който замества необходимостта от компютър.

Тези предимства и недостатъци е добре да се вземат предвид, когато е нужно да се оборудва цяла учебна зала. Спорен е въпросът дали да се включи хардуер, който да е еднотипен, или да се вземат графични таблети с различни параметри и така да се предостави възможност за запознаване с различен по своите особености хардуер. С втория предложен вариант може да се реализира междупредметна връзка с обучението по Компютърна периферия и Информатика.

С използването на графични таблети по Компютърна графика се цели да се повиши мотивацията за усвояване на нови знания, да се преодолеят ограничените способности за самостоятелна работа и недобросъвестното изпълнение на индивидуалните задания от обучаемите, които често се дължат и на пропуски в знанията.

Заключение

Графичните таблети намират все по-широко приложение в ежедневието, както на професионалистите, така и на обикновения потребител. Може да се препоръча като чудесно средство за развитие на творческото и креативно мислене в обучаемите. Недостатъците, им са

пренебрежими, в предвид предимствата и удобствата, които предоставят те. Часовете за упражнения се характеризират с активно участие на обучаемите, които се възползват от възможността да се ползва специфичен хардуер. Прегледът на възможностите разкрива перспективи за внедряване на нов хардуер в обучението по компютърна графика и модернизиране на тенденциите.

References:

1. http://www.picotux.com/differences-between-regular-tablets-and-grphics-tablets/ (разгледано на 10.08.2018)
2. https://www.oldcomputr.com/koala-technologies-koalapad-touchtablet/
3. https://www.computerhope.com/jargon/g/graptabl.htm
4. https://design.tutsplus.com/articles/do-you-need-a-graphics-tablet-find-out-what-you-need-to-know--vector-13586
5. https://en.wikipedia.org/wiki/Graphics_tablet#Uses
6. https://www.online-sciences.com/computer/graphics-tablet-features-advantages-and-disadvantages/
7. https://ardes.bg/news/2017/04/kakvo-e-grafichen-tablet
8. http://www.10brutes.com/
9. Чанев, Ст., Матрица на целеразпределение на групировка за ПВО, Международна Научна Конференция „Отбранителни Технологии-Шумен 2018“
10. Най-добрите графични таблети за 2018, https://www.lifewire.com/best-drawing-tablets-4141661 (прегледано на 15.08.2018)
11. https://www.amazon.com/Monoprice-MP1060-HA60-Graphic-Drawing-Tablet/dp/B004C4ZT0G, (прегледано на 15.08.2018)
12. Nikolov L., Slavyanov Kr., On the contemporary cybersecurity threats, International Scientific Journal Security & Future, Vol. 1 (2017), Issue 3, p. 111-113, ISSN 2535-0668, Avaible from https://stumejournals.com/journals/confsec/2017/3/111

Zh V. Zhivkov,

BINARY PHAZE MANIPULATED SIGNAL

Zhivko V. Zhivkov

National Military University „Vasil Levski",
Faculty "Artillery, air defence and communication information systems"
j.v.j@abv.bg

***Abstract**: Display and evaluation of maximum lobes of the autocorrelation function of the binary, periodic, phase manipulated signals*

***Kewords**: complex signal, binary phase management signal, autocorrelation.*

БИНАРЕН ФАЗОВО МАНИПУЛИРАН СИГНАЛ

Живко В. Живков

Национален военен университет „Васил Левски",
Факултет „Артилерия, противовъздушна отбрана и комуникационни и информационни системи"
j.v.j@abv.bg

Увод

Бурното развитие на технологиите по време и след на края на Втората световна война довежда до идеята за използване на сложни сигнали в радиолокационната техника. Разработването и въвеждането на полупроводникови прибори и повишаването на тяхното бързодействие позволява през седемдесетте години на миналия век да бъдат изпитани първите радиолокационни станции, използващи сложни радиолокационни сигнали.

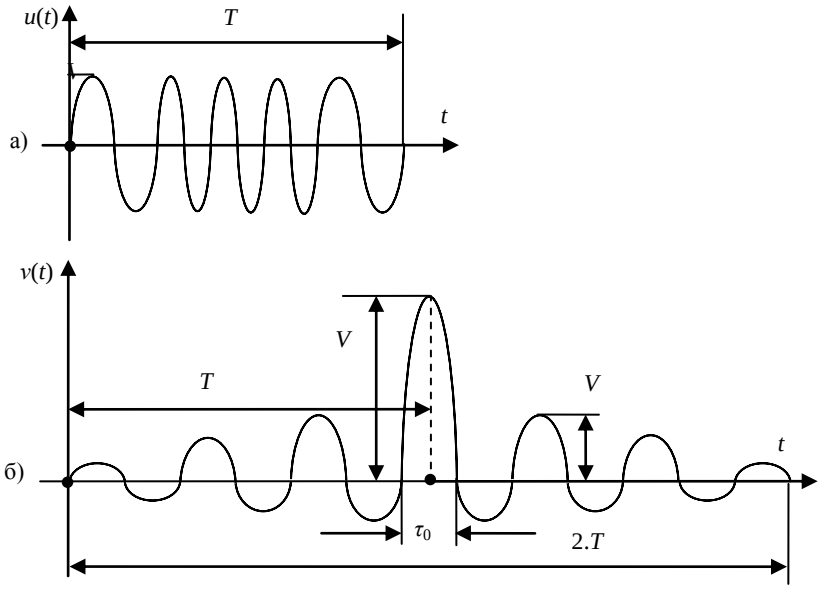
Основно предимство на сложните радиолокационни сигнали е „свиването" на автокорелационната характеристика на сигнала, което води до увеличаване на точността на определяне на координатите на радиолокационната цел (Фиг. 1), което е особено важно за радиолокационните системи.

Както се вижда, автокорелационната характеристика има основен с продължителност τ_0 и странични листи с продължителност $T - \tau_0 /2$. Общата продължителност на автокорелационната характеристика остава равна на двойната продължителност на сондиращия импулс.

Това обуславя търсенето на сложни радиолокационни сигнали ,характеризиращи се с ниски, или нулеви в идеалния случай, нива на страничните листи на автокорелационната характерисситика.

През втората половина на миналия век започва бурно търсене на такива сигнали с цел подобряване на работата на различни видове комуникационни устройства.

В радиолокацията, в частност, усилията са насочени към разработването на такива сигнали, които да имат възможно най-тесен основен лист (респективно с най-малка продължителност) с цел намаляване на грешката при определяне на разстоянието. Същевременно е необходимо нивата на страничните листи да бъдат колкото се може по-малки за да се намалят смущенията.



Фиг. 1. Общ вид на сложен сигнал след свиването му в приемника.
а) сигнал на входа на приемника;
б) сигнал на изхода на приемника.
V – ниво на основния лист на автокорелационната характеристика;
V_{max} – максимално ниво на страничните листи на автокорелационата характеристика.

1. Предимства на сложните радиолокационни сигнали

Освен горепосоченото свойство, сложните радиолокационни сигнали, притежават и редица други предимства пред обикновените, а именно:

- Позволяват пълноценно да се реализират преимуществата на методите за оптимална обработка на сигналите.
- Осигуряват висока шумоустойчивост.
- Позволяват успешна борба с многолъчевото разпространение на радиовълните.
- Осигуряват едновременна работа на много устройства в една честотна лента.
- Системите използващи такива сигнали работят с повишена скритост.
- Осигуряват по-добро използване на спектъра на честотите.

Именно тези предимства на сложните сигнали налага все по-широкото им използване в съвремието, независимо от усложняването на електронната апаратура.

В съвременните комуникационни системи най-голямо приложение намират следните сложни сигнали:

- честотно модулирани (ЧМ) сигнали;
- фазово манипулирани (ФМ) сигнали – direct sequence (DS) complex signals;
- дискретни честотни (ДЧ), наричани още “честотно манипулирани”, сигнали – frequency hopping (FH) complex signals;
- дискретни честотни съставни (ДЧС) сигнали – frequency hopping-direct sequence (FH-DS) complex signals; frequency hopping- frequency hopping (FH-FH) complex signals.

2. Определяне на нивата на страничните листи на бинарен, фазово манипулиран сигнал

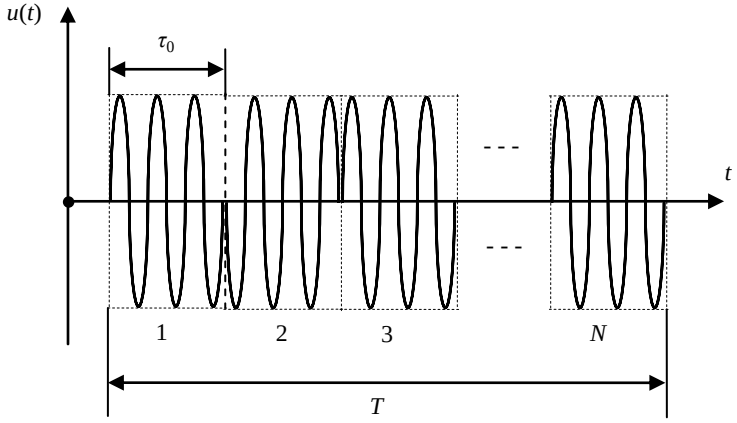
В момента най-голямо приложение намират фазово манипулираните (ФМ) сигнали поради следните предимства:

- осигуряват ниво на шумозащитеност на РЛК, адекватно на съвременните изисквания;

• генерирането и обработката им са относително по-прости в сравнение с ДЧ и ДЧС сигналите

Поради тази причина определен интерес представлява определянето на максималните нива на страничните листи на автокорелационната характеристика.

Сложни сигнали, чиято модулация на фазата, кохерентна на непрекъснатата носеща, се извършва в дискретни моменти от време, кратни на интервала на дискретизация τ_0, се наричат фазово манипулирани сигнали. Обикновено такива сигнали се състоят от правоъгълна обвиваща с продължителност τ_0, чиято фаза се изменя от импулс към импулс (фиг. 2).



Фиг. 2. Бинарен, фазово манипулиран сигнал

Общият израз на такива сигнали в комплексна форма има вида:

(1) $$S(t)=\sum_{i=0}^{N-1} p_i(t).\exp\{j(\omega_0 t+\varphi_i)\}$$

където $p_i(t)=p(t-i_{\tau_0})=\begin{cases}1, & при\ \ i_{\tau_0}\le t\le (i+1)\tau_0\\ 0, & при\ \ други\ \ значения\ \ на\ \ t\end{cases}$.

За простота в израз (1) амплитудата на сигнала е приета за 1.

От гледна точка на формирането и обработката, най-прости за реализация са бинарните фазово манипулирани сигнали, при които $\varphi_i=0,\pi$.

Означавайки $\mu_i=\exp\{j\varphi_i\}$ и отчитайки, че за $\varphi_i=0,\pi$, $\mu_i=1,-1$ се получава:

(2) $$S(t)=\sum_{i=0}^{N-1}\mu_i p_i(t).\exp(j\omega_0 t)$$

Свойствата на бинарните фазово манипулирани сигнали се описват с помощта на код $\mu = \{ \mu_i: i = 0, 1, 2, \ldots, N-1\}$.

Ако бинарен фазово манипулиран сигнал се излъчва непрекъснато и е вярно съотношението:

(3) $$\mu_{i+kN(\mathrm{mod}\,N)}=\mu_i$$

то такъв сигнал се периодичен бинарен, фазово манипулиран сигнал.

Функцията на корелация на бинарен фазово манипулиран сигнал се записва във вида:

(4) $$R(\tau,\Omega)=\lim_{T\to\infty}\frac{1}{T}\int_{-T/2}^{T/2}U(t).U^*(t+\tau).\exp(-j\Omega t)dt,$$

където $U(t)=S(t)\exp(-j\Omega t)$ е комплексната обвиваща на сигнала.

Когато филтърът е съгласуван с един период на сигнала:

(5) $$R(\tau,\Omega)=\int_0^{T_M}U(t).U^*(t+\tau).\exp(-j\Omega t)dt,$$

където T_M е периодът на модулация.

Функцията (5) се нарича периодична функция на корелация. Тя се явява периодична по τ с период T_M.

Замествайки в (5) комплексната обвиваща на сигнала (2), отчитайки свойството на функцията $p_i(t)$ (1) и замествайки $\tau = m.\tau_0$ след интегриране [2] се получава:

(6) $$R(m\tau_0,\Omega) = R_H(0,\Omega).\sum_{i=0}^{N-1}\mu_i.\mu_{i+m}.\exp(-j\Omega i_{\tau_0})$$

ако $0 \le \tau \le N\tau_0$ и $-\infty < \Omega < \infty$, където

(7) $$R_H(0,\Omega) = \int_0^{\tau_0}\exp(-j\Omega t)dt$$

Замествайки в (6) $\Omega = 0$, се получава периодичната функция на автокорелация на бинарен фазово манипулиран сигнал, построен на базата на кода μ [3]:

(8) $$R_\mu(m) = \sum_{i=0}^{N-1}\mu_i.\mu_{i+1}\cdot$$

Очевидно е, че за тази функция е справедливо неравенството:

(9) $$R_{\mu,\max} \ge \left(\overline{R_\mu(m)}\right),\ m \ne 0(\mathrm{mod}4),$$

където: $R_{\mu,\max}$ – най-големият страничен лист на функцията на автокорелация $R_\mu(m)$

$\left(\overline{R_\mu(m)}\right)$– средно значение на страничните листи на функцията на автокорелация $R_\mu(m)$

(10) $$R_{\mu,\max} = \max_m\{R_\mu(m)\},\ m \ne 0(\mathrm{mod}4),$$

(11) $$\left(\overline{R_\mu(m)}\right) = \frac{1}{N-1}.\sum_{m=1}^{N}R_\mu(m)\cdot$$

Замествайки (10) и (11) в (9) се получава:

(12) $$R_{\mu,\max} \ge \frac{1}{N-1}\sum_{m=1}^{N-1}\sum_{i=0}^{N-1}\mu_i,\mu_{i+m} = \frac{1}{N-1}\left(\sum_{m=0}^{N-1}\sum_{i=0}^{N-1}\mu_i,\mu_{i+m} - N\right) = \frac{1}{N-1}\left(\chi^2 - N\right),$$

където:

(13) $$\chi = \sum_{i=0}^{N-1}\mu_i\cdot$$

Долната граница на $R_{\mu,\max}$ се получава ако в израз (12) се замести χ^2 с $\chi^2_{\min}$. Тъй като при четно N $\chi^2_{\min} = 0$, а при нечетно N $\chi^2_{\min} = 1$, то търсената оценка е:

(14) $$R_{\mu,\max} \ge \begin{cases} -\dfrac{N}{N-1}, & при\ \ N\ -\ четно \\ -1, & при\ \ N\ -\ нечетно \end{cases}.$$

Всяко N може да се представи чрез две сравнения:

(15) за четно N: $N = 0$ (mod 4), $N = 2$ (mod 4)

(16) за нечетно N: $N = 1$ (mod 4), $N = 3$ (mod 4)

Като се отчетат (15) и (16) неравенство (14) придобива вида:

(17) $$R_{\mu,\max} \ge \begin{cases} 0, & ако\ \ N = 0(\mathrm{mod}4) \\ -1, & ако\ \ N = 1(\mathrm{mod}4) \\ -2, & ако\ \ N = 2(\mathrm{mod}4) \\ -1, & ако\ \ N = 3(\mathrm{mod}4) \end{cases}$$

Както се вижда от изложеното бинарните фазово манипулирани сигнали притежават потенциал за подобряване на работата на радиолокационните устройства въпреки известното затрудняване на техническата реализация.

Заключение

От направения анализ се налагат следните основни изводи:

- бинарните, фазовоманипулирани сигнали са с най-лесна техническа реализация;
- при синтезирането на бинарни фазовоманипулирани сигнали се получава автокорелационната функция може да има три нива на страничните листи в зависимост от броя (N) на изграждащите го подимпулси;

- на настоящия етап няма разработен математически апарат за синтезиране на импулсни, фазовоманипулирани сигнали, поради което се търсят методи за разработване на непрекъснати такива и след това се анализират получените от тях импулсни последователности.

На настоящия етап са разработени редица методи за получаване на бинарни, фазовоманипулирани сигнали – методите на Лежандр, Хол, Якоби и др.

Разработен е и съотвтения математически апарат за синтезиране на филтри за подтискане на страничните листи на автокорелационната функция.

Усилията са насочени към изследването и откриването на такива сигнали, които да имат колкото се може по-добри характеристики.

Развитието на изчислителната техника позволява синтези и анализа на фазовоманипулирнаи сигнали, съдържащи все по-голям брой изграждащи подимпулси (N), което подобрява точността и скритостта на работата на радиолокационните устройства.

Известна пречка пред използване на такова сигнали в комуникационната техника се явява малкото им информационно натоварване (един импулс носи 1 bit информация), но с увеличаването на скоростта на работа, намаляването на продължителността на импулса и увеличаването на носещата честота, този недостатък може да бъде в значителна степен намален.

References:

1. Свердлик**,** М., Б., Оптимальные дискретные сигналы. – М., “Сов. радио”, 1975.
2. Кук, Ч., Бернфельд, М., Радиолокационные сигналы, Пер. с англ. – М., “Сов. радио”, 1971.
3. Желев**, С.**, Спътникови комуникации, УИ ”Е. К. Преславски”, Шумен, 2012, ISBN978-954-577-619-9.

NETWORK INFRASTRUCTURE FOR CYBERSECURITY ANALYSIS

Linko G. Nikolov, PhD; Vasil O. Slavyanov

linkonikolov@abv.bg; vasil.slavyanov@gmail.com

***Abstract**: Applications and protocols, serving trillions of devices worldwide, have weak points and vulnerabilities. Malicious intends of hackers exploit those vulnerabilities, which can lead to information leakage, network and systems malfunction and even serious money loss. Before giving birth to an app, service or network resource facing internet, serious tests and analysis should be performed. In this paper, a proposed basic network infrastructure for applications and systems vulnerability analysis is shown.*

***Keywords**: CYBERSECURITY, VULNERABILITY ANALYSIS, NETWORK PENTESTING, NETWORK SECURITY, COMPUTER SECURITY*

1. Why cybersecurity analysis?

Cybersecurity becomes even popular with the extreme evolution of internet-connected devices such as smartphones, laptop workstations and Internet-of-Things (IoT). The vast amount of network protocols and applications, with their functionality, become a source of weak points in the IT infrastructure. Such vulnerabilities may be exploited by hackers or attackers whose aim is to acquire benefits form the access granted [1]. The benefits are various including wreaking havoc, money for ransom, administrative access to sensitive data [10] and so on. If the developed applications were to be examined for security flaws, the chance of hacker's success minimizes. Furthermore, if the network resource is constantly under security provision, penetration would be extremely difficult. With some ordinary security measures in networks and systems being implemented, companies and enterprises believe their infrastructure is shielded enough. This is neither true, nor does a hacker thinks so. Networks and systems on the global range are being under attack almost constantly 24/7/365 according to Norse Corporation's website. What about institutions dealing with classified information? Sooner or later, if precautions are not enough, breakage can occur.

With proper security testing, administrators of IT infrastructures become more aware of the real world e-threads. Security engineers have developed software platforms and penetration testing environments which are very helpful concerning cybersecurity. The goal of this paper is to model a typical network infrastructure, capable of exploring possible threads and previously unknown vulnerabilities.

2. Network topology with devices, systems and security test platforms

Simulation software is available on the market to perform network flow imitation. But having real hardware devices, the cybersecurity analysis results can be more realistic. This is the place to stress out that complex large scale SCADA, ICS (Industrial Control System) and DCS (Distributed Control Systems) systems are impossible to testify [9] with the proposed small scale network. Application, web and LAN network security are successfully tested instead.

The network topology includes three routers, two cable switches and one Wi-Fi access point for wireless LAN access (fig. 1). Two servers and three hosts are deployed as end devices. One computer with open source operating system KALI LINUX plays the role of attacking system.

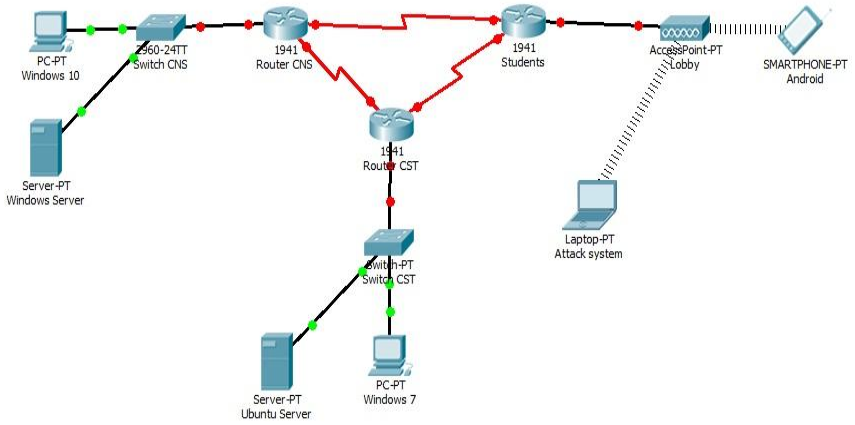


Figure 1 *– Sample hardware network infrastructure for cybersecurity analysis*

The law concerns are explicitly followed and the applications will be internal for the network only. Connection to Internet will have occasional manner. The more diverse the applications, the more efficient will be the analysis. A firewall appliance is predicted, but will be for further protocols flaw explorations. The proposed network infrastructure does not pretend to be innovative, but somewhat educational and moreover – the first line starting cybersecurity investigation in a real hardware manner. Servers can be either e-mail, web, or other widespread services. Depending on the target, the tested services may vary. In table 1 an example of useful instruments is shown:

Table 1: Testbeds for cybersecurity [8]:

Testbed	Focus area
Anubis	Malware analysis
Connected Vehicle Testbed	Connected vehicles
DETER	Cybersecurity experimentation and testing
DRAKVUF	Virtualized, desktop dynamic malware analysis
EDURange	Training and exercises
Emulab	Network testbed
Future Internet of Things (FIT) Lab	Wireless sensors and Internet of Things
Future Internet Research & Experimentation (FIRE)	European federation of testbeds
GENI (Global Environment for Network Innovations)	Network and distributed systems
NITOS (Network Implementation Testbed using Open Source)	Wireless
OFELIA (OpenFlow in Europe: Linking Infrastructure and Applications)	OpenFlow software-defined networking
ORBIT (Open-Access Research Testbed for Next-Generation Wireless Networks)	Wireless
PlanetLab	Global-scale network research
Starbed	Internet simulations

DETER, Emulab and DRAKVUF are network testbeds that apply resource time-sharing among many users. It means users acquire physical resources from the testbed and abandon them when deciding it is out of need for a couple of hours. Testbeds skip experiment definition consisting of node names and topology, OS and node type choices, etc. so that a user can rebuild the experiment later. Testbeds bring a set of OS images that can be loaded on analyzed machines. An OS image is a block level image of the filesystem on a node. Base images usually involve several Linux flavors, such as Ubuntu, Red Hat and

some Windows platforms, such as Windows Server 2016. While the attacking system performs network Penetration testing, application vulnerability scanning or fuzzy logic implementation for test randomization [9], the end computers may have installed software monitoring services, antivirus and firewall applications.

3. Short example cybersecurity tests and analysis

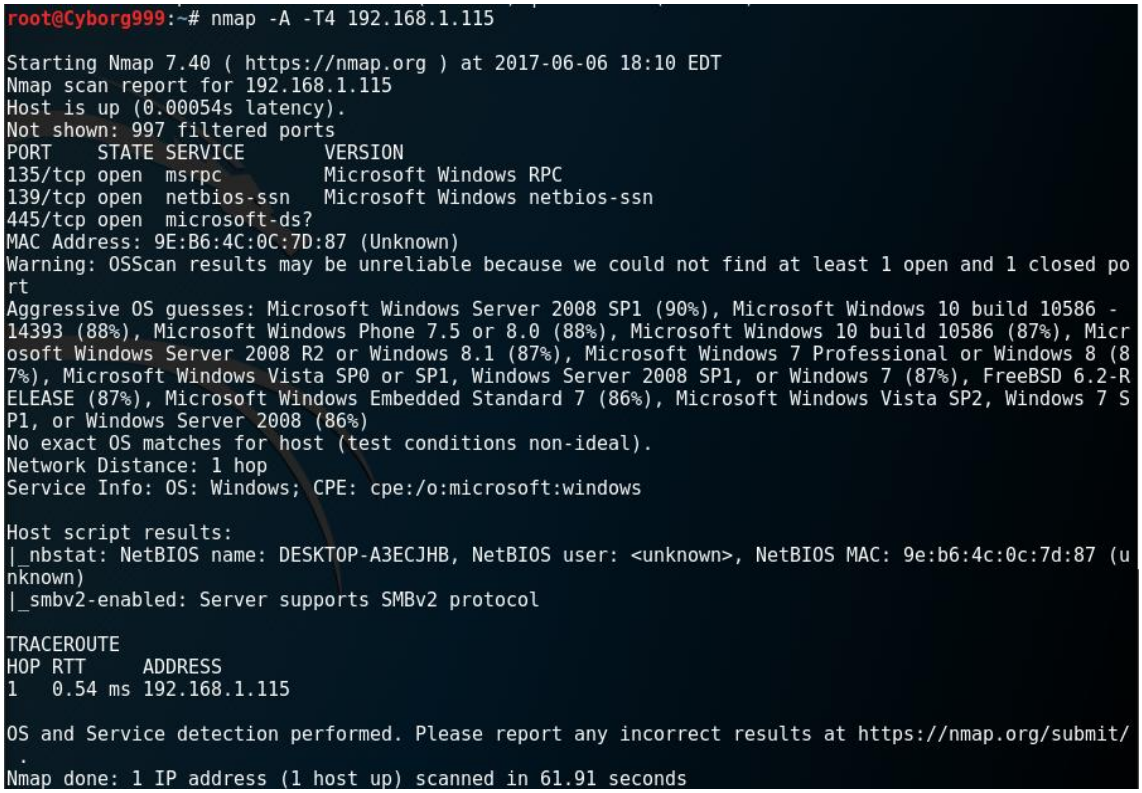
For adequate results, systems should be limited of outside networks and the operation system environment should be as real as possible (in a customer's view). In this paper the recent tools are used such as "Nmap" [2], "OpenVas" [3], the Metasploit Framework [4] and some others. The full cycle for cybersecurity analysis can be copied from the ethical hacking [7] steps, which are:

1. Footprinting and reconnaissance.
2. Network scanning and enumeration.
3. Sniffing and evasion.
4. Privilege escalation and persistent access.
5. Presence diminishing.

For example, the first task of a malicious hacker is to sniff around the network and draw a gesture of the topology. The tool, trying to connect to open TCP ports and IP addresses may be "Nmap". One example syntax in Kali Linux is as shown below:

root@kali:~# *nmap –A –T4 192.168.1.115*

where "nmap" is a command in the shell, and 192.168.1.115 is the IPv4 network address of the target device. The results after hitting this command are shown in fig. 2.



```
root@Cyborg999:~# nmap -A -T4 192.168.1.115

Starting Nmap 7.40 ( https://nmap.org ) at 2017-06-06 18:10 EDT
Nmap scan report for 192.168.1.115
Host is up (0.00054s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE       VERSION
135/tcp open  msrpc         Microsoft Windows RPC
139/tcp open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?
MAC Address: 9E:B6:4C:0C:7D:87 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed po
rt
Aggressive OS guesses: Microsoft Windows Server 2008 SP1 (90%), Microsoft Windows 10 build 10586 -
14393 (88%), Microsoft Windows Phone 7.5 or 8.0 (88%), Microsoft Windows 10 build 10586 (87%), Micr
osoft Windows Server 2008 R2 or Windows 8.1 (87%), Microsoft Windows 7 Professional or Windows 8 (8
7%), Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (87%), FreeBSD 6.2-R
ELEASE (87%), Microsoft Windows Embedded Standard 7 (86%), Microsoft Windows Vista SP2, Windows 7 S
P1, or Windows Server 2008 (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_nbstat: NetBIOS name: DESKTOP-A3ECJHB, NetBIOS user: <unknown>, NetBIOS MAC: 9e:b6:4c:0c:7d:87 (u
nknown)
|_smbv2-enabled: Server supports SMBv2 protocol

TRACEROUTE
HOP RTT     ADDRESS
1   0.54 ms 192.168.1.115

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
 .
Nmap done: 1 IP address (1 host up) scanned in 61.91 seconds
```

***Figure 2** – Example of network reconnaissance with nmap*

For scanning and enumeration, a tool Lynis in Kali (fig. 3) finds its way for exploration where computer operation system is the target object. Which in turn can give the attacker useful information about breaking points, backdoors or possible system vulnerabilities.

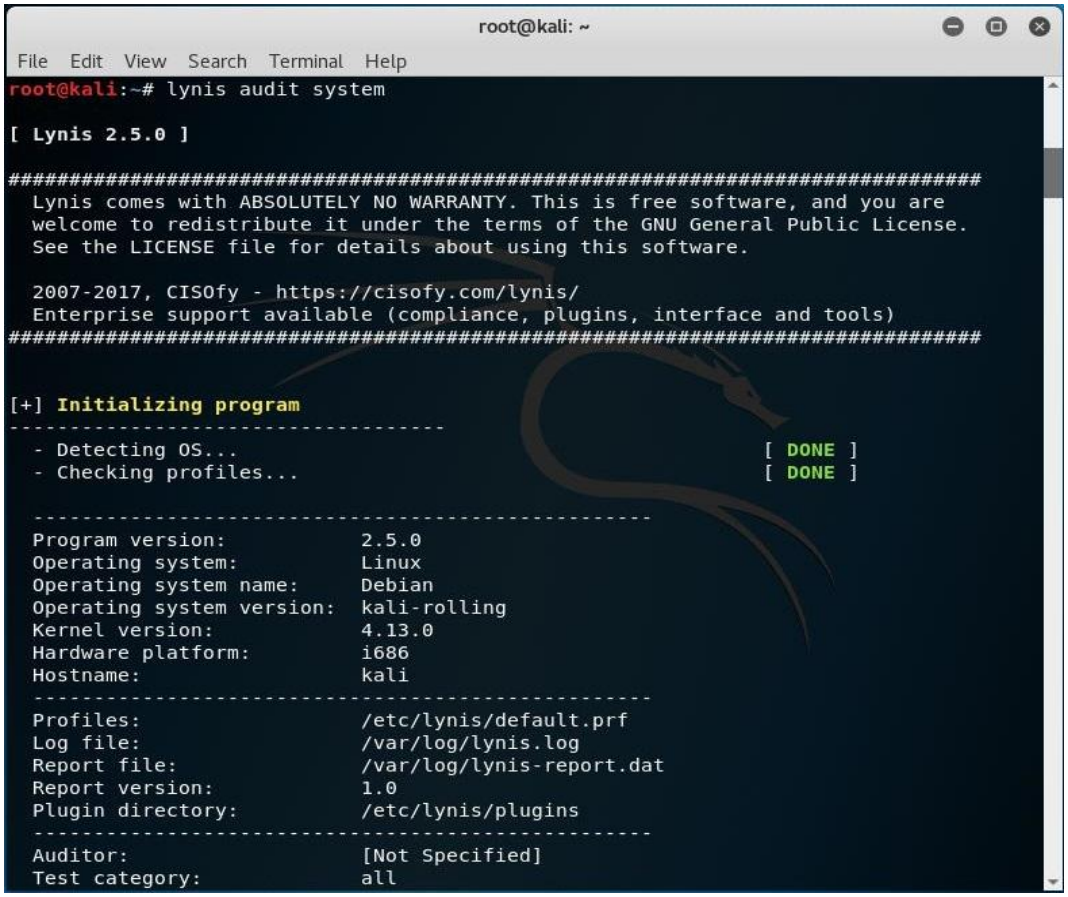


Figure 3 *– Lynis Audit result*

Further step in the cybersecurity test can be the critical vulnerability exploration. The results obtained can be in the sense of a CVE – Common Vulnerabilities and Exposures [3]. Fig. 4 shows the results of analyzing with OpenVas:

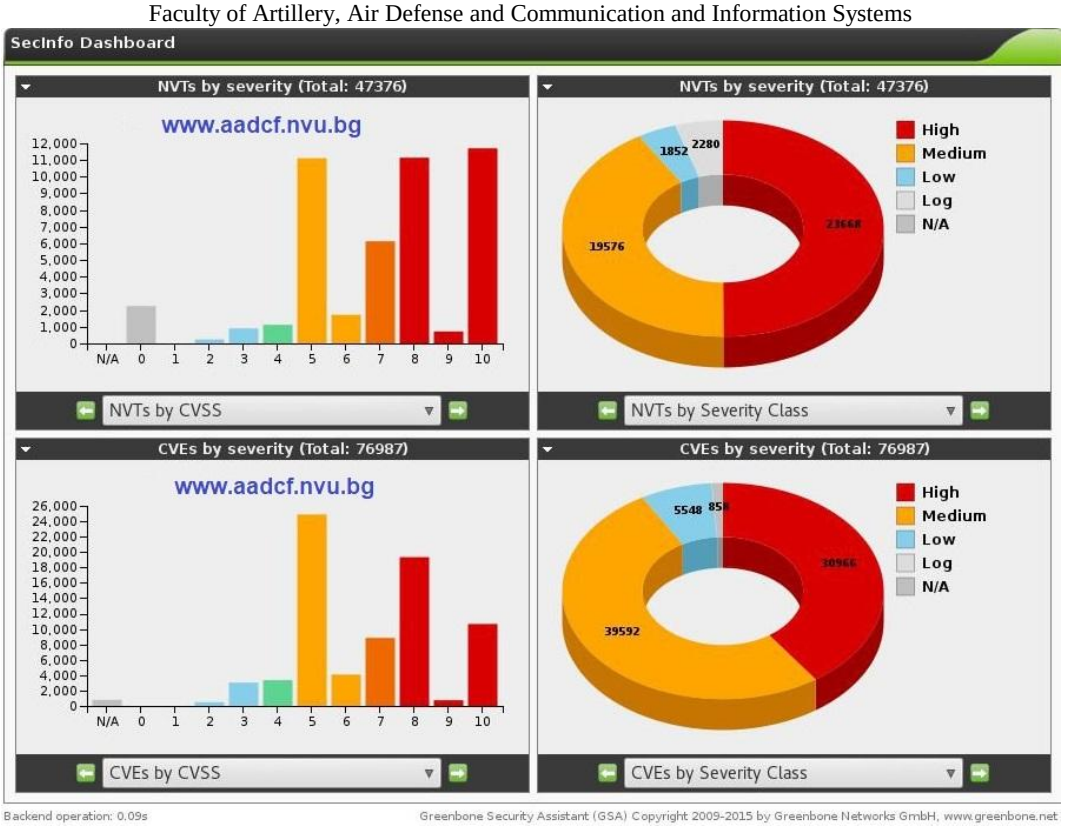


***Figure 4** – Example of OpenVas web-application vulnerabilities analysis*

The research area in cybersecurity seems as vast as the world ocean, but the good news is cyberawareness has already been woken. Terms for future development are cyberhygiene, cybercrime forensics, as well as cyber resilience. Everyday's virus signature reports and zero-day attack patches help improve systems' cybersecurity. The test results help administrators and security officers define weak points and avoid deep impacts from information losses when possible.

4. Conclusion

Subject of review in this paper was network building and cybersecurity testbed preparation for network protocols and applications exploration in a manner of computer security. The Proposed framework seems to be a helpful tool for considering good practices for cyber analysis, the goal of which is "to ensure secure systems planning and operation, response and support". Essentials in cybersecurity include investigations from detection systems, impact of an incident understanding, forensics performed, and incidents categorized with response plans.

Cybersecurity analysis is an important aspect of the understanding, development, and practice of network, computer and cloud security. Cybersecurity is a broad category, covering the technical practices for computer networks, computers, and data protection from harm and destroy. Scientists, industry workers and government clerks use formal and informal science to create and expand cybersecurity knowledge. As a testbed, the field of cybersecurity requires authentic knowledge to explore and reason about the "how and why" security controls to be built or deployed.

References:

[1] Kizza, J., "Guide to Computer Network Security", Springer, 2017 ISBN 978-3-319-55605-5

[2] Gordon "Fyodor" Lyon, "Nmap Network Scanning", ISBN 978-0-9799587-1-7, https://nmap.org/book/

[3] URL: http://www.openvas.org/about.html

[4] URL: https://metasploit.help.rapid7.com/docs

[5] URL: https://www.cybersecurityanalysis.com/

[6] Robert, W. Beggs, “Mastering Kali Linux for Advanced Penetration Testing”, PACKT, 2014, ISBN 978-1-78216-312-1

[7] Цокев, Ал., „Етично хакерство“, БАРЗИКТ, 2017, ISBN 978-619-7382-00-6

[8] Dykstra, J., “Essential cybersecurity science”, O’REILLY, 2016, ISBN 978-1-491-92094-7

[9] Slavyanov, Krasimir, “An algorithm of fuzzy inference system for human resources selection tools”, International Scientific Conference, Rezekne, Latvia, 2018.

[10] Цанков Ц. С., „Киберпрестъпността като основна съвременна заплаха за големите организации“, „МАТТЕХ“ Шумен 2016.

D. I. Sumulyov,

FORMING OF RADAR IMAGE OF TARGET, CONSISTING OF BRIGHT POINTS IN ULTRA WIDEBAND RADAR

Dimitar I. Sumulyov

AAD and CIS Faculty, "Vassil Levski" NMU, Shumen, Bulgaria

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*

ФОРМИРАНЕ НА ИЗОБРАЖЕНИЕ ОТ РАДИОЛОКАЦИОННА ЦЕЛ, СЪСТОЯЩА СЕ ОТ БЛЕСТЯЩИ ТОЧКИ В СВРЪХШИРОКОЛЕНТОВ РАДАР

Димитър И. Сумульов

Факултет „А, ПВО и КИС", НВУ „В. Левски", Шумен, България

1. ВЪВЕДЕНИЕ

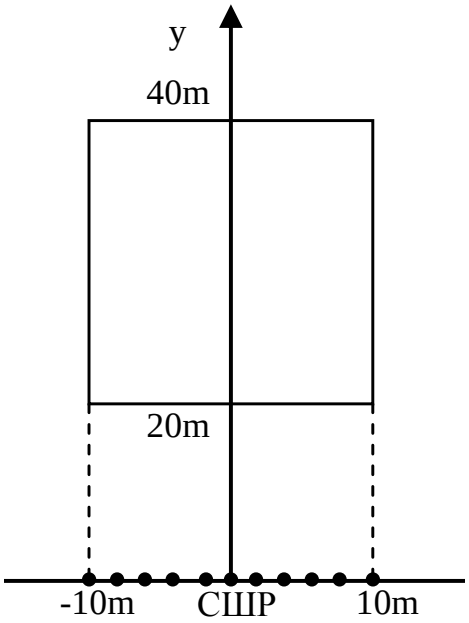
Развитието на свръхширококолентовите (UltraWideBand –UWB) технологии в последните десетилетия, доведе до внедряването на различни радари за откриване на обекти върху и под земната повърхност, системи за формиране на радиолокационно изображение на обекти (включително и през стени), автомобилни радарни 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 свръхширококолентовите 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

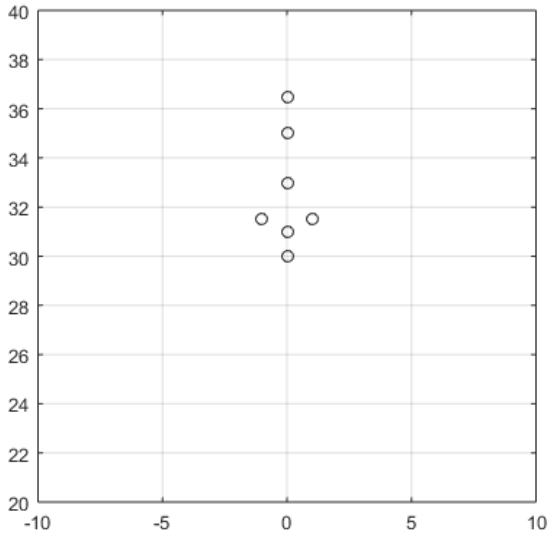
При изследванията е използвана геометричната постановка на разположение на радара и сектора на наблюдение, показана на фигура 1 [2]. Антените на СШР са разположени по оста *y* през разстояние от 2 метра. Всеки пиксел в изображението отговаря на квадрат от сектора със страна $dx = dy = 0{,}05m$. Времевият 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:

(1) $$s_k(n)=\sum_{i=1}^{7} A_i(nt_s-t_{ki})e^{-\pi\frac{(nt_s-t_{ki})^2}{\tau_u^2}},$$

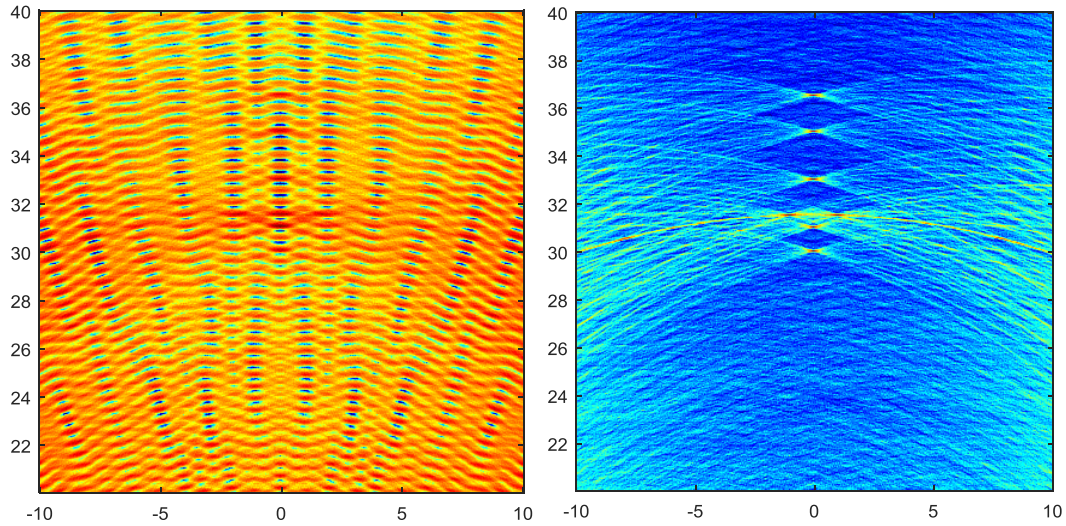
където $t_{ki}=2\left[\sqrt{y_i^2+(x_i-x_k)^2}-R_{\min}\right]/c$ е времезакъснението на сигнала, отразен от $i^{\text{-та}}$ блестяща точка, при работа на $k^{\text{-тия}}$ елемент на антенната система; x_i и y_i са координатите на $i^{\text{-та}}$ блестяща точ-

ка; x_k е координатата по оста *x* на $k^{\text{-тия}}$ 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 Рихачек 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.

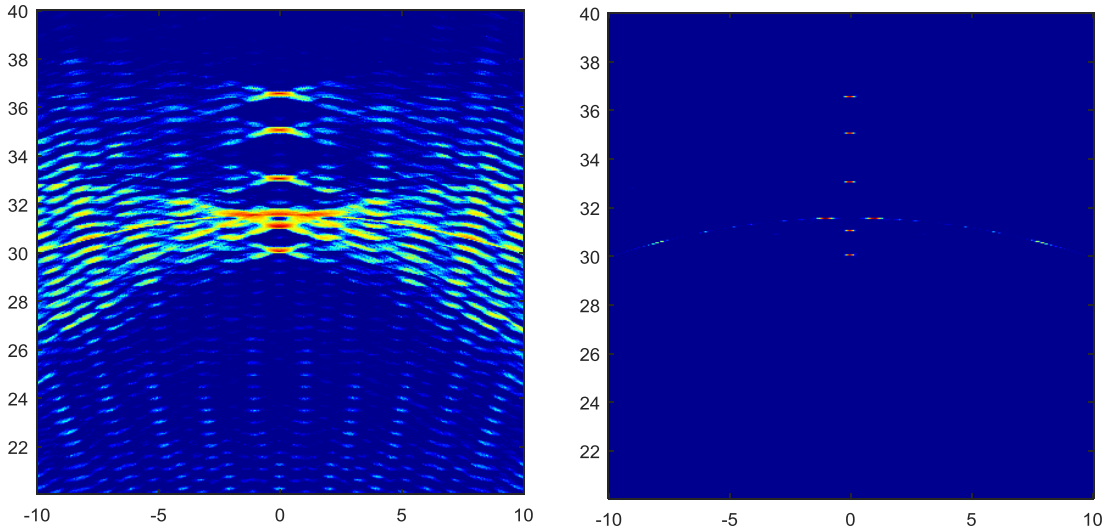


а) ядро на Рихачек *б) разделно ядро*

Фигура 3. Изображения на цел, ориентирана по оста y, при ОСШ 0,1 (-10dB).

Получените изображения показват, че при ОСШ 0,1 ядро на Рихачек 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.

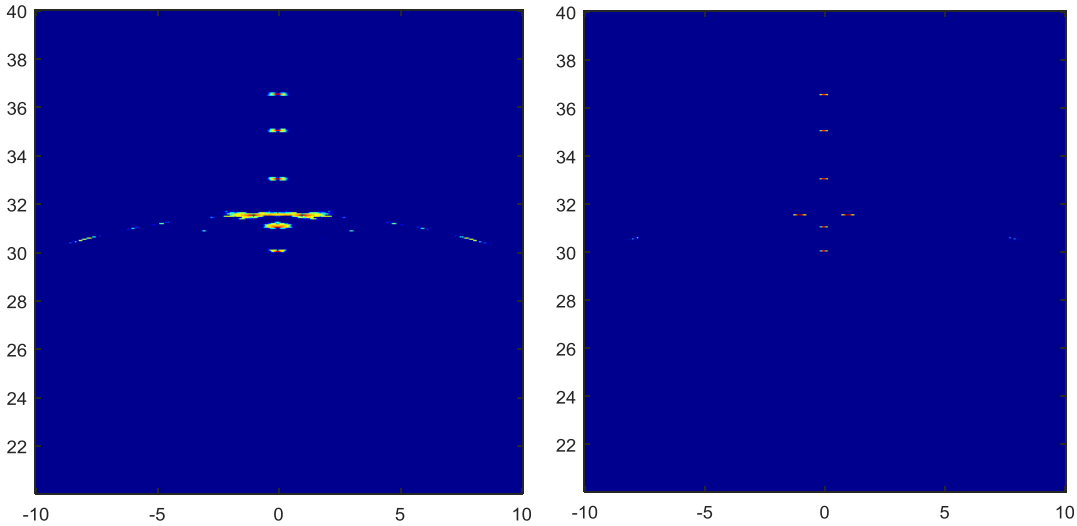


а) ядро на Рихачек *б) разделно ядро*

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 Рихачек 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.

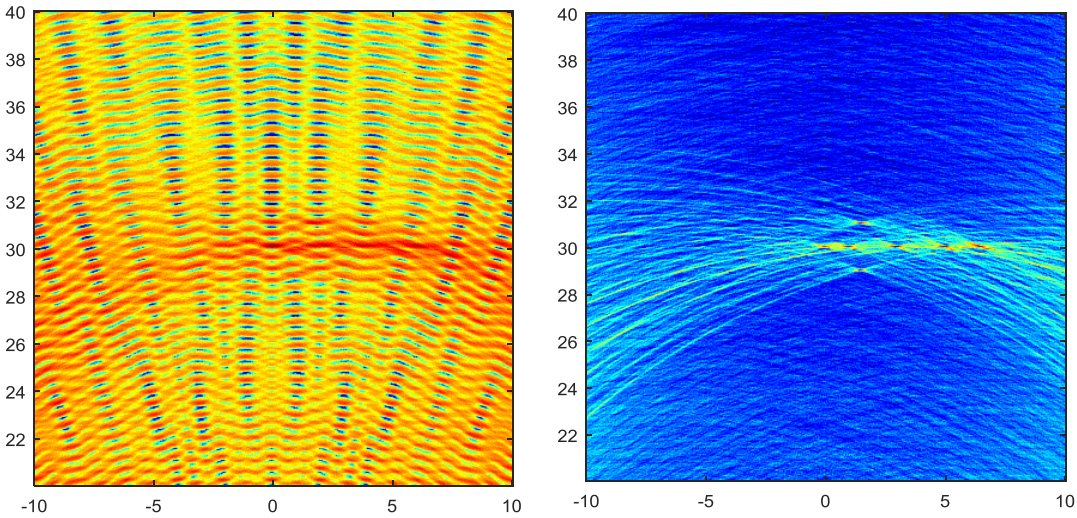


а) ядро на Рихачек *б) разделно ядро*

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 Рихачек.

На фигура 6 са показани формираните изображения за цел, ориентирана по оста *x*, при обработка с двете ядра и ОСШ 0,1.

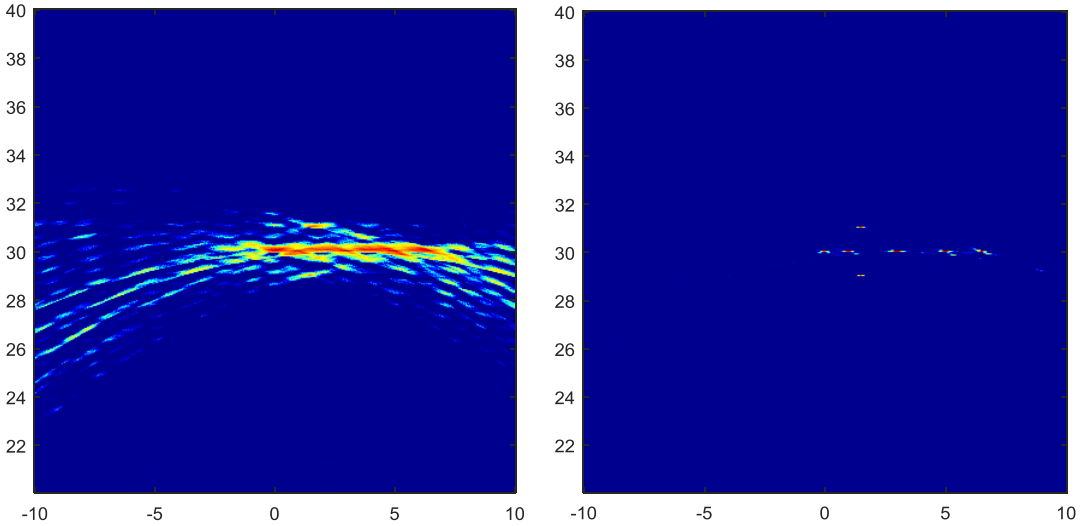


а) ядро на Рихачек *б) разделно ядро*

Фигура 6. Изображения на цел, ориентирана по оста x, при ОСШ 0,1 (-10dB).

При използване на ядро на Рихачек 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.

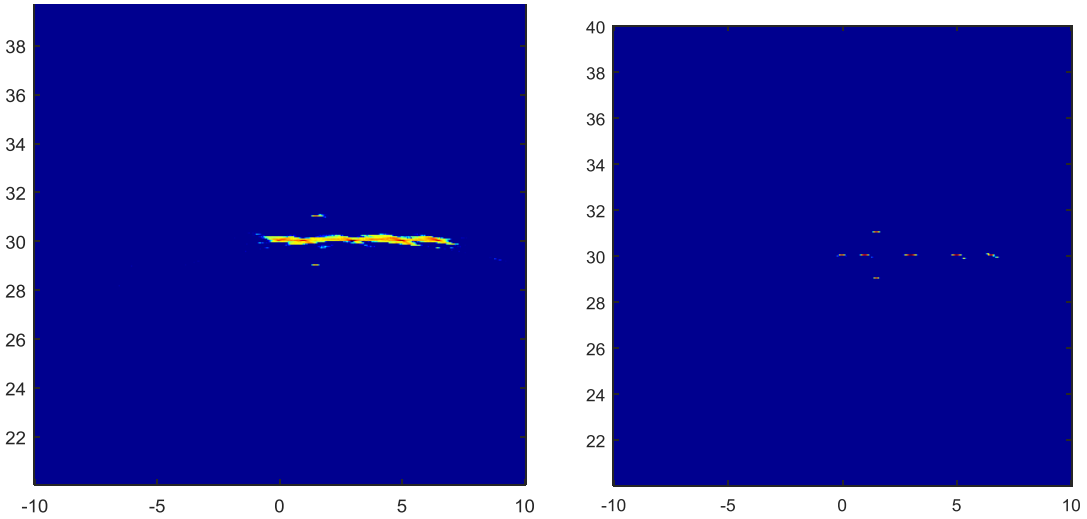


а) ядро на Рихачек *б) разделно ядро*

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 Рихачек може да се определи, че има цел, но не и нейните блестящи точки. При обработката с ядро на Рихачек 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 Рихачек.

На фигура 8 са показани формираните изображения за цел, ориентирана по оста *x*, при обработка с двете ядра и ОСШ 2.



а) ядро на Рихачек *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 силуетът на целта. При ядрото на Рихачек 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 Рихачек 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 й 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 Рихачек. 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 Рихачек 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 свръхшироколентов 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 свръхшироколентов 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.

D. K. Hubenov, R. A. Bogdanov,

SOFTWARE DEFINED RADIO AS PART OF COGNITIVE RADIO

Dyanko K. Hubenov, Rosen Atanasov Bogdanov

***Abstract**: This paper shows the advantages of software defined radios (SDR) over conventional radios. Also a quick overview of different types of SDR was made. The architecture of cognitive radio concept is presented with SDR being a basic component, along with other cognitive components for dynamic radio spectrum management.*

***Keywords**:SDR, cognitive radio, radio spectrum management*

СОФТУЕРНО ДЕФИНИРАНОТО РАДИО КАТО ЧАСТ ОТ КОГНИТИВНОТО РАДИО

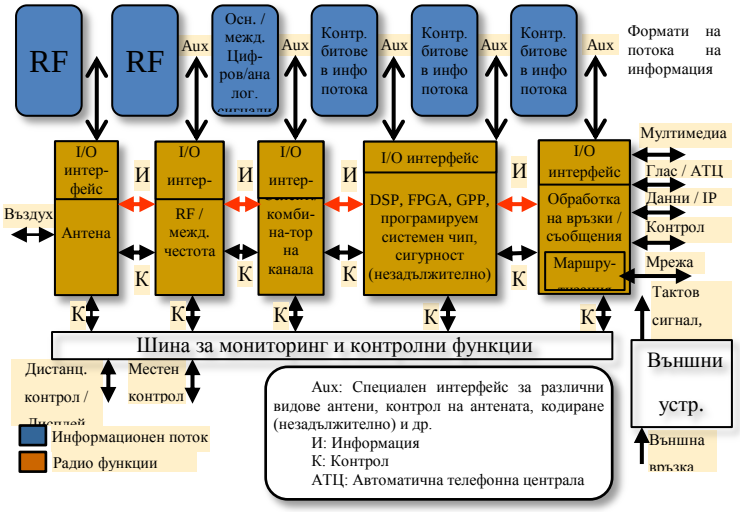
Дянко К. Хубенов, Росен Атанасов Богданов

Национален военен университет „Васил Левски“,
Факултет „Артилерия, ПВО и КИС“,
гр. Шумен, ул. „Карел Шкорпил“ 1
e-mail: d_hubenov@abv.bg, rab61@abv.bg

Въведение

Последните десетилетия се характеризират с експоненциално нарастване на начините и средствата за радиокомуникация на потребителите – данни, глас, видео, текстови съобщения, комуникации за управление и контрол и други. В тази променена нова реалност се изисква лесно и икономически ефективно модифициране на използваните радиоустройства. Софтуерно дефинираното радио SDR (Software Defined Radio) като технология за развитие на комуникациите предоставя гъвкавост и ефективност на разходите и мощността. Множество определения могат да бъдат намерени за софтуерно дефинираното радио, но едно широко използвано определение дефинира SDR като „Радио, в което някои или всички функции на физическия слой са софтуерно дефинирани”.

Традиционните радиоустройства, базирани на хардуер, ограничават функционалността и могат да бъдат променяни само чрез физическа намеса. Това води до по-високи производствени разходи и минимална гъвкавост при поддържане на множеството стандарти за разпространение. За разлика от тях, технологията на софтуерно дефинираното радио осигурява ефективно и сравнително евтино решение на този проблем, като позволява проектирането на многорежимни, многочестотно лентови и/или многофункционални безжични устройства, които могат да бъдат подобрени във всеки един момент с помощта на софтуерни ъпгрейди. Разбира се апаратурата за такъв вид дейност трябва да отговаря на високи изисквания и да включва голям набор от антени за различните сензори, както и компоненти за анализиране на сигнала. Системния софтуер на SDR устройства се състои от широк набор от модули за различни нужди като: контрол на всички сензори и потока на информацията с наличното оборудване, анализ, обработка и съхранение на цялата получена и разпозната информация и система за база данни, както и за различни видове отчети [1].



Фигура 1. Примерен модел на SDR

Както е показано на фиг. 1, SDR определя набор от хардуерни и софтуерни технологии, където някои или всички функции на радиостанциите (наричани още обработки на физическия слой) се осъществяват чрез модифициран софтуер или фърмуер, работещ с програмируеми технологии за обработка. Тези устройствата включват полеви програмируеми масиви FPGA (Field Programmable Gate Arrays), цифрови сигнални процесори DSP (Digital Signal Processors), процесори с общо предназначение GPP (General Purpose Processors), програмируема система в чипа SoC (System on Chip) или други програмируеми процесори със специфично приложение. Използването на тези технологии позволява добавяне на нови безжични функции и способности към съществуващите радиосистеми, без да се изисква добавянето на нов хардуер в тях.

1. Предимства на софтуерно дефинираното радио

Технологията се използва не защото е иновативна или фантастична, но тъй като е доказано, че тя успешно решава проблемите на конкретен пазар. Има много примери за приемане на SDR, като само в областта на отбраната успешно проектираните софтуерни радиостанции са хиляди.

За производителите на радиооборудване SDR позволява:

- Внедряване на семейство от модели радиооборудване, които да се произвеждат като се използва обща платформа за реализиране на архитектурата им.
- Софтуерът да се използва повторно в радиопродуктите, намалявайки драстично вложените средства.
- Безжично управление или друго дистанционно препрограмиране, което позволява отстраняване на програмни грешки, които се проявяват докато радиоустройството е в експлоатация.
- Намаляване на времето и разходите, свързани с работата и поддръжка на радиоустройството.

За доставчиците на радиоуслуги SDR позволява:

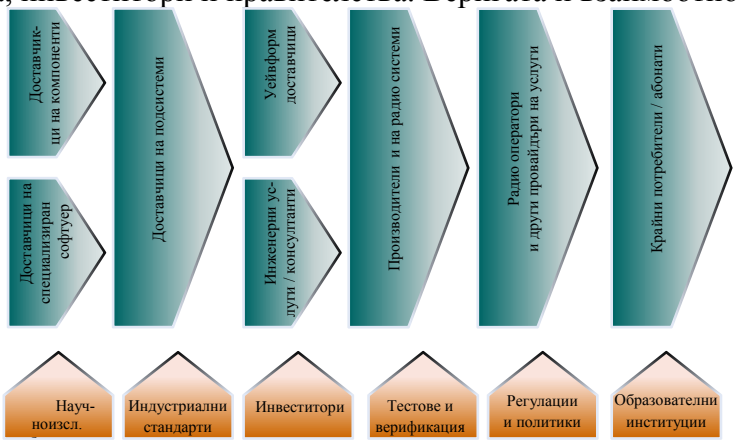
- Нови функции и възможности, които да се добавят към съществуващата инфраструктура, без да са необходими големи нови капиталови разходи, което позволява на доставчиците на услуги да доразвиват своите радиомрежи.
- Използване на обща радио платформа за множество пазари, което значително намалява логистичната поддръжка и оперативните разходи.
- Изтегляне на отдалечен софтуер, чрез което капацитетът може да бъде увеличен, Надстройки за нови способности могат да бъдат активирани и могат да се вмъкват нови функции, генериращи приходи.

За крайните потребители SDR технологията позволява:

- Намаляване на разходите за повсеместната безжична връзка, позволявайки комуникация винаги с всеки при необходимост и по най-подходящия за това начин.
- Клетъчните радиокомуникационни системи все повече използват програмируеми обработващи устройства за създаване на обща платформа или много честотно лентови и много протоколни базови станции, поддържащи множество стандарти на клетъчни системи.
- Клетъчните телефони все по-често използват устройства от вида система в чипа SoC (System on a Chip), които включват програмируеми DSP ядра, за да поддържат обработката на бейсбанд сигнал.
- Сателитните модеми на комерсиални цели и тези за отбраната широко използват програмируеми устройства за обработка на междинни честоти и обработката на бейсбанд сигнала.

Въпреки че много системи често не се предлагат на пазара като SDR, те се възползват от SDR технологиите за решаване на специфични за пазара проблеми като например: разходи за развитие, производствени разходи, разходи за надграждане и поддръжка, време за пускане на пазара при разработка на нови и усъвършенствани стандарти за въздушен интерфейс или проблеми, свързани с оперативната съвместимост на мрежата. Освен това проучванията на пазара на SDR показват, че ефективните радиочестотни технологии, поддържащи функциите на софтуерно дефинираното радио в широк спектрален диапазон са започнали да се развиват, което позволява за пръв път използването на софтуер, дефиниран като радио технология, за реализиране на системи за достъп с динамичен спектър с когнитивна или интелигентна радио функционалност. Тази тенденция се очаква да продължи, като позволи на SDR да постигне окончателно предвиденото намаляване на разходите за предоставяне на достъп на крайните потребители.

Ползите и очакваните възможности за SDR технологиите имат значително въздействие върху веригата от добавени стойности на безжичната индустрия. Тази верига се състои от продукти и услуги с добавена стойност на всеки етап, което води до проектиране на крайни SDR продукти и услуги, които отговарят на нуждите на потребителите и абонатите на безжичните системи. На различни етапи от веригата доставчиците могат да бъдат подпомагани от външни организации като образователни институции, изследователски лаборатории, органи за стандартизация в бранша, инвеститори и правителства. Веригата и взаимоотношенията в нея са показани на фиг. 2



Фигура 2. Верига на добавените стойности

Някои компании могат да представляват повече от една категория във веригата на добавените стойности. Например, някои производители разработват свои собствени SDR подсистеми и софтуерни приложения. Също така повечето доставчици на компоненти предоставят и инструменти за SDR разработка. SDR има значителни последици в рамките на веригата, засягащи различни организации и индустриални сектори чрез радиочестотната (RF) верига (предни крайни компоненти, разработчици на софтуер, производители на чипове и т.н.) и в рамките на бизнес режимите (доставчици на услуги, OEMs, IP притежатели и т.н.).

2. Видове SDR системи

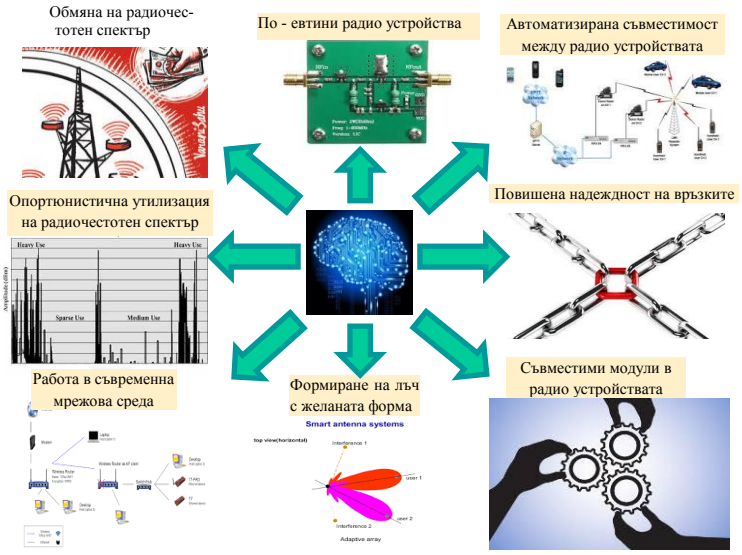
Към SDR не се предявяват изисквания да поддържа всички възможни типове радио устройства, но SDR технологиите могат да осигурят гъвкавост, необходима за постигането на пълния потенциал на устройствата, като спомогнат за намаляване на разходите и повишаване на ефективността на системата.

2.1. Адаптивно радио

Адаптивното радио е радио, в което комуникационните системи имат средства за наблюдение на собствените си резултати и промяна на оперативните си параметри с цел тяхното подобряване. Използването на SDR технологиите в адаптивна радиосистема позволява по-голяма свобода на адаптация и по този начин по-високи нива на ефективност и по-добри резултати в качеството на услугата, предоставяна от комуникационната връзка.

2.2. Когнитивно радио

Когнитивното радио (фиг. 3) е радио, в което комуникационните системи следят вътрешното състояние и околната среда, като местоположение и използване на радио честотния спектър. Те могат да вземат решения за тяхното радиоуправление и поведение чрез анализиране на тази информация при предварително зададени цели. Като такова, когнитивното радио е дефинирано така, че да използва софтуерно дефинирано радио, адаптивно радио и други технологии, които автоматично да коригират своето поведение или операции, за да постигнат желаните цели. Използването на тези елементи е от решаващо значение, за да се позволи на крайните потребители да използват оптимално наличния честотен спектър и безжичните мрежи с общ радио хардуер. Това намалява разходите за крайния потребител, като същевременно му позволява да комуникира с всеки, когато има нужда и по различни начини.



Фигура 3. Възможности на когнитивното радио

Нови приложения чрез CR	Повишени параметри на ефективност-та чрез CR
• Динамичен достъп до спектъра DSA • Самоорганизиращи се мрежи • Когнитивни системи за заглушаване • Когнитивни шлюзове / мостове • Радиочестотен спектър в реално време	• Подобряване на използването и ефективността на радиочестотния спектър • Подобряване на оперативната съвместимост между наследени и новосъздадени системи • Подобряване на надеждността на връзките

• Синтезирано MIMO • Когнитивно управление на спектъра • Когнитивно маршрутизиране	• По-евтини радиостанции • Подобряване на SDR технологиите • Удължен живот на батерията • Разширено покритие

Таблица 1. Подобряване на ефективността на съществуващите системи чрез когнитивно радио

2.3. Интелигентно радио

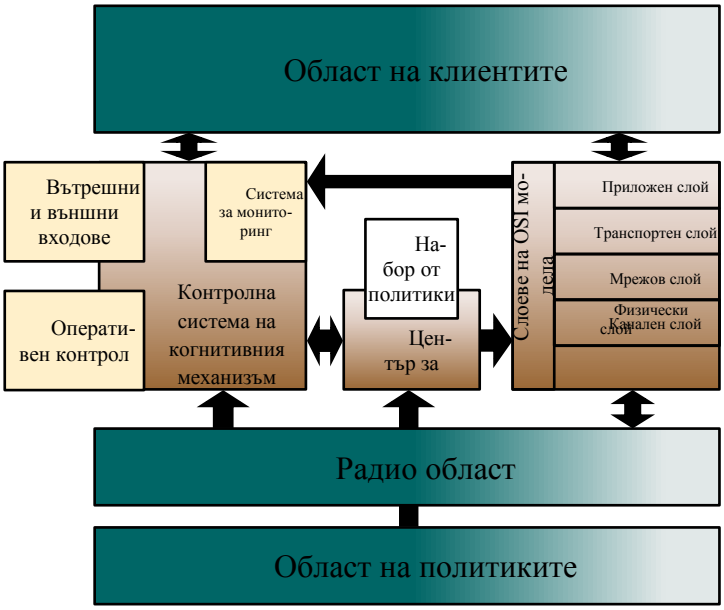
Интелигентното радио е когнитивно радио, което може да се самообучава. Това позволява на когнитивното радио да подобри начините, по които се адаптира към промените в производителността и околната среда и по този начин по-добре да обслужва нуждите на крайния потребител.

В допълнение към използването на SDR технологиите, адаптивното радио, интелигентното радио и когнитивните радиосистеми могат да използват динамичен достъп до спектъра DSA (), което позволява на системите да избират честотния спектър, в който ще работят на дадено място и за даден период от време с цел оптимизиране на използването на наличния спектър и за избягване на смущения с други радиостанции или други системи.

3. Архитектура на концепцията за когнитивно радио

Когнитивното радио има две основни подсистеми: когнитивна, която взема решения въз основа на различни входове и SDR, чийто оперативен софтуер осигурява възможните режими на работа. Освен това в архитектурата на когнитивно радио често се включва и отделна сензорна система за измерване на сигналната среда, за да се определи присъствието на други потребители или услуги. Важно е да се отбележи, че тези подсистеми не дефинират непременно отделно оборудване, а могат да включват компоненти, които се разпространяват в цялата мрежа. В резултат когнитивното радио често се нарича когнитивна радиосистема или когнитивна мрежа.

Когнитивното устройство е разделено на две части, както е показано на блоковата схема на фиг. 4. Първата част, наречена „когнитивна“, се опитва да намери решение или да оптимизира целта за изпълнение въз основа на получените входове, определящи текущото вътрешно състояние и оперативната среда на радиото. Втората част, наречена „център за политики“, се използва, за да гарантира, че решението, осигурено от когнитивната част, е в съответствие с регулаторните правила и други политики извън радиото.



Фигура 4. Архитектура на когнитивната радио концепция

4. Компоненти, поддържащи динамичния достъп до радиочестотния спектър на когнитивно радио

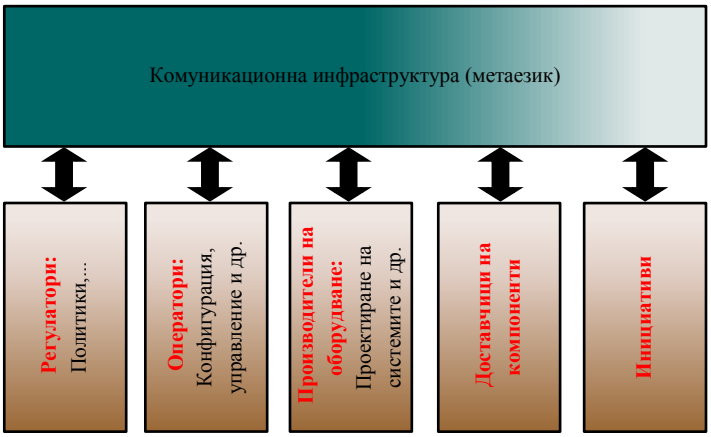
Поддръжката на когнитивния радио и динамичен достъп до спектъра изисква редица базови технологии.

4.1. Архитектура на информационните процеси

Основният проблем е разбирането на текущото състояние на сложните информационни системи и свързаните с тях подсистеми за комуникация, за да се определи как да се подобрят от гледна точка на процеса и да се анализират възможностите за взаимодействие с други системи. Архитектурата на информационния процес решава този проблем, като предоставя модел „отгоре надолу" и серия от инструменти за изобразяване на структурата на сложните системи, за да помогне при определянето, проектирането и избора на съответните когнитивни радиообработващи процеси и да улесни по-доброто разбиране на структурата и взаимоотношенията между системите, които обхващат потребителските домейни.

4.2. Език за моделиране (метаезик)

Необходими са гъвкави и ефикасни комуникационни протоколи между модерните радиосистеми и подсистеми за поддръжка на функции от следващо поколение, като вертикална и хоризонтална мобилност, информираност за спектъра, адаптиране на динамичния спектър, оптимизация на формата на съхнала, обмен на функции и усъвършенствани приложения. Език за моделиране, изграден върху подробни случаи на използване и определяне на план за сигнализация, изисквания и технически анализ на информационния обмен, осигурява основата за разработване на спецификации и стандарти в подкрепа на тези възможности. Език за моделиране или мета езика (фиг. 5), изразен на формален декларативен език, който е машинно четим, определя комуникационната инфраструктура на когнитивното радио.



Фигура 5. Метаезик

4.3. Карта на околната радиосреда

Работата на когнитивната част изисква данни и метаданни, определящи спектралната среда, в която даден терминал работи в даден момент от времето. Наричани „карта на околната радиосреда", тези данни могат да включват информация за най-икономичните транзакции в областта на радиочестотния спектър, отпаданията, предаванията, наличните мрежи и услуги. Данните, които се съдържат в картата, се получават отчасти чрез сканиране и синтезиране на измервания от много радиостанции и могат да се съхраняват в база данни, която може да бъде достъпна дистанционно от когнитивната част. Изискванията за структурата на базата данни, позволяващи този достъп включва стандартизирани структури на база данни, форматите на данните и функционал-

ността трябва да бъдат дефинирани, за да поддържат гъвкавостта, необходима за внедряване на настоящи и бъдещи когнитивни приложения за радиочестотен спектър.

4.4. Тестови измервания

Когнитивните радиостанции представляват уникални тестови предизвикателства при количественото определяне на ефективността на критични функции като сензори за спектъра, избягване на смущения, производителност на базата данни и спазване на зададените правила. Тестовите методологии, които поддържат тези предизвикателства, трябва да бъдат разработени, трябва да се обмислят редица хардуерни платформи, протоколи, алгоритми, случаи на използване и изисквания на заинтересованите страни. Трябва да се вземат предвид функционалността и производителността на тестовото оборудване, тестовите интерфейси и режимите на изпитване.

References:

1. Nikolov, L., Slavyanov, Kr. BENEFITS AND FEATURES OF A COMINT SOFTWARE. Научна конференция „Новата парадигма за сигурност в киберпространството“, Сборник научни трудове – Шумен 2014. ISBN 978-954-9681-49-9, p. 288
2. SDR forum, SDRF Cognitive Radio Definitions, http://www.sdrforum.org/pages/documentLibrary/documents/SDRF-06-R-0011-V1_0_0.pdf , November 2007
3. Wireless Innovation Forum, Quantifying the Benefits of Cognitive Radio, https://www.wirelessinnovation.org/assets/work_products/Reports/winnf-09-p-0012-v1_0_0-cr_quantification_document.pdf , December 2010
4. Wireless Innovation Forum, Value Chain, http://www.wirelessinnovation.org/assets/documents/SoftwareDefinedRadio.pdf , 2005

D. K. Hubenov, Y. V. Yosifov, N. Zh. Kulev,

5G CONCEPTS FOR WIRELESS COMUNICATIONS

Dyanko K. Hubenov, Yosif V. Yosifov, Nikolay Zh. Kulev

***Abstract**: This paper shows the advantages of new concepts for wireless communications compared to already existing ones, which will be well suited for the coming in close future 5G.*

***Keywords**:5G, FBMC, UBMC*

5G КОНЦЕПЦИИ ЗА БЕЗЖИЧНИ КОМУНИКАЦИИ

Дянко К. Хубенов, Йосиф В. Йосифов, Николай Ж. Кулев

Национален военен университет „Васил Левски",
Факултет „Артилерия, ПВО и КИС",
гр. Шумен, ул. „Карел Шкорпил" 1
e-mail: d_hubenov@abv.bg, josifov02@abv.bg, nz_kulev@abv.bg

Въведение

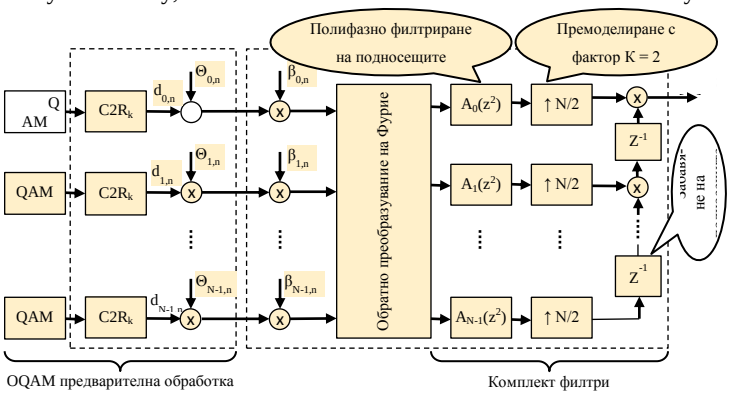
Приложенията, които ще поддържат бъдещия 5G стандарт за безжични комуникации, ще срещнат сериозно ограничение в лицето на OFDM. Ето защо големите производители на устройства за безжична комуникация и научно изследователските институти провеждат изследвания за преодоляване на този проблем, чрез създаване на нови концепции за PHY и MAC слоевете.

Общата идея зад всички модели разгледани в следващите раздели е използването на различни филтри за формиране на импулсите в сравнение с традиционния OFDM, като това води до намляване на излъчването извън основната честотна лента и съответно ефективността на използване на радиочестотния спектър. От друга страна, използването на различен филтър за формиране на импулси предполага намаляване на ортогоналността между две съседни подносещи, като енергията се разпределя от една носеща към друга. Това предизвиква появата на интерференция между носещите честоти (ICI), която трябва да бъде компенсирана. Това увеличава сложността на цялата система и по-специално на приемащата страна.

1. Селекция на множество носещи чрез комплект филтри - FBMC

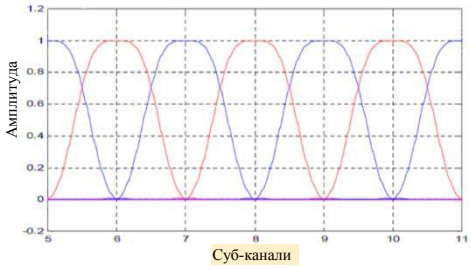
Методът „Filter-Bank Multi-Carrier" (FBMC) предполага използването на филтрация на субносещите чрез комплект филтри в предавателната и приемната страна. Съществуват различни предложения за реализация на FBMC, като например: „Staggered Modulation Multitone" (SMT), "Cosine Modulation Multitone" (CMT) и "Filtered Multitone" (FMT), но фокусът е върху SMT FBMC.

За създаването на **N** на брой полифазни филтъра $\boldsymbol{A_K}$ с дължина $\boldsymbol{K}$ се използва прототип на FIR филтър базиран на „Root Raised Cosine" (RRC) филтър с коефициент на развивката β = 0,1. $\boldsymbol{K}$ определя препокриващия фактор, който характеризира прототипния филтър и определя броя на наслоените символи във времето. При FBMC се използва K = 4.

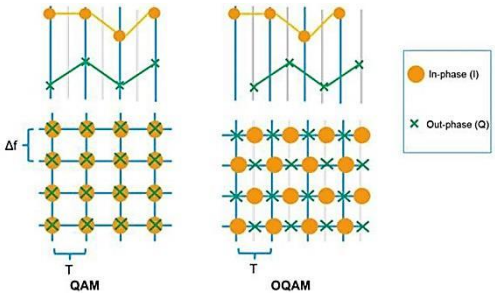


Фигура 1. Блокова схема на FBMC предавател

На фиг. 1 е показан модел на FBMC предавател. Вижда се, че наборът от филтри се получава чрез честотно изместване на ***k/N*** за даден филтър. Това оказва влияние на ортогоналността, тъй като енергията се разпределя между съседните подносещи и по този начин се създава интерференция между съседните подносещи. Всички четните подносещи и всички нечетни подносещи не се припокриват и поради това са ортогонални едни спрямо други.



Фигура 2. Разпределение на енергията в честотно изместените суб-канали



Фигура 3. Сравнение между QAM и OQAM

За да се поддържа ортогоналност в реалната и имагинерната област, Offset QAM (OQAM) се прилага към модулираните символи за данни. OQAM се постига чрез изместване на *in-phase* компонентата на QAM системата на половината от дължината на един символ T / 2 спрямо *out-phase* компонентата. Ако времевото изместване се приложи към *in-phase* частта на дадена носеща-та, то се прилага съответно и към out-phase частта на съседните носещи, което води до намаляване на интерференцията. OQAM приемникът елиминира ICI, като игнорира частта от получения сим-вол, която не съдържа данни. Използването на OQAM елиминира необходимостта от предпазен интервал като цикличен префикс в FBMC и по този начин увеличава спектралната ефективност.

2. Предимства и недостатъци на FBMC

Преимуществата, поради които FBMC е предложен да бъде използван в 5G са:

- Асинхронно предаване, при което не е необходима пълна времева синхронизация;

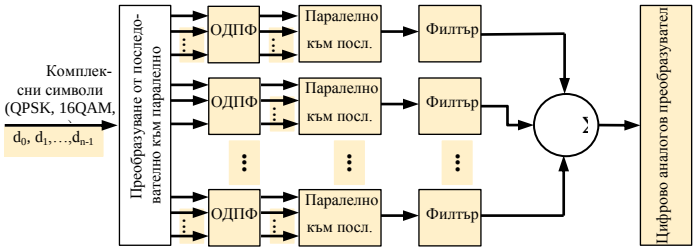
- Подходящ за използване при силно фрагментиран спектър;
- Подходящ за използване с когнитивно радио;
- Устойчивост при използване в условията на висока скорост;
- Възможност за ефективно адаптиране на основните параметри в една честотна лента.

Съществуват и някои слаби страни на FBMC, като:

- Ограничено използване на MIMO:
- Неефективен при кратки предавания, вследствие на забавянето от филтриране;
- Усложнено устройство;

3. Селекция на множество носещи чрез универсален филтър - UFMC

За разлика от FBMC при „Universal Filter Multi-Carrier” (UFMC) подносещите се групират в подленти, които след това се филтрират. Броят на филтрите и на носещите на подлента обикновено е еднакъв. Това предотвратява създаването на несъответствие, а несъседните под-ленти позволяват по-гъвкаво използване на наличния спектър. Поради това UFMC може да се разглежда като компромис между OFDM и FBMC. Фигура 4. показва блокова схема на UFMC предавател. При UFMC няма времево припокриване на съседните символи. Продължителността на символа е N + L – 1, като N е размерът прозореца на преобразуването на Фурие, а L е дължината на филтъра. Подобно на FBMC при UFMC размерът на прозореца на преобразуването на Фурие е увеличен, което усложнява неговото внедряване. Освен това при UFMC не е задължително въвеждането на предпазен интервал като цикличен префикс. Друга особеност на обединената рамкова структура е използването на множество сигнални слоеве. Потребителите могат да бъдат разделени например въз основа на техните интерфейси, както е направено в Interleave-Division Multiple Access (IDMA). Това ще доведе до допълнителна степен на свобода за системата, ще подобри устойчивостта срещу прослушвания и ще помогне да се използва капацитетът на канала за множествен достъп (MAC).



Фигура 4. Блокова диаграма на UFMC предавател

4. Предимства и недостатъци на UFMC

UFMC има следните предимства:

- Добра спектрална ефективност, близка до тази на FBMC;
- По-малък овърхед в сравнение с FBMC;
- Повишена ефективност при кратки предавания;
- Възможност за работа в режим с минимални забавяния.

Налице са и някои недостатъци:

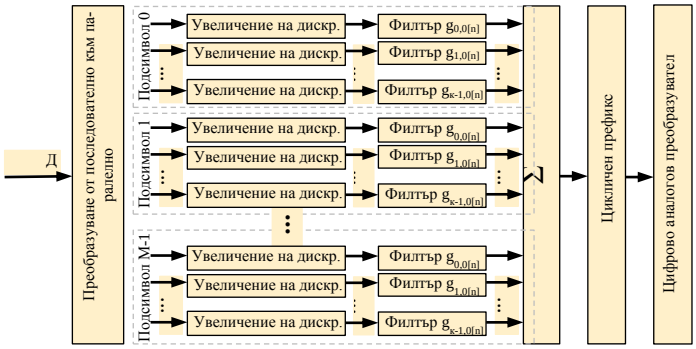
- Недостатъчна ефективност при предаване на голям обем от данни с висока скорост, вследствие на частичната загуба на комплексна ортогоналност;
- Големият размер на прозореца на преобразуването на Фурие води до усложнения;
- Наличние на интерференция, вследствие на частично застъпващите се под-ленти.

5. Обобщено честотно разделяне – GFDM

Основната идея при Generalized Frequency Division Multiplex (GFDM) отново е използването на комплект филтри, като концепцията включва разширяването на спекъра предназначен за отделния потребител до множество спектрални сегменти, всеки от които има различна по широчина честотна лента. Това от своя страна би спомогнало до голяма степен прилагането на концепцията за когнитивно радио, при която нелицензиран ползвател има възможност временно да из-

ползва спектъра предназначен за друг лицензиран ползвател. Тъй като, GFDM е на практика допълнение към FBMC той предоставя някои нови възможности, като:

- Наличие на цикличен префикс, който може да бъде приложен след мултиплицирането или преди филтрацията;
- Всяка подносеща може да има различна широчина на честотната лента;
- Филтрирането се извършва чрез циклична конволюция на определен брой символи, наричано още “захапване на опашката” (*tail biting*). Това води до сегментация във времевата област.



Фигура 5. Блокова диаграма на GFDM предавател

На фигура 5 с $g_{k,m[n]}$ е означен всеки филтър с N на брой такта, като k, m и n са съответно означенията на подносещата, подсимвола и индекса на времевия такт. Друга допълнителен аспект на GFDM засягащ MAC слоя е блоковото предаване на информация. Това дава възможност за промяна на продължителноста на съществуване на пакетите (TTL). При приложения, за които е важна скоростта на предаване на данни могат да се използва по малък брой подсимволи за предаване на информацията, докато при друг вид комуникация, където скоростта не е от такова значение ще се използва по голям брой подсимволи за даден потребител.

В честотната област обикновено съседните подносещи се застъпват, нарушвавайки критерия за ортогоналност, както и при някои от вече разгледани концепции, което обаче позволява асинхронно предаване на данни. Вследствие на асинхронното предаване на данни се предизвиква систематично увеличение на отношението бит-грешка, което при GFDM се компенсира чрез допълнително намаляне на интерференцията в приемната страна.

6. Предимства и недостатъци на GFDM

Основните предимства на GFDM са:

- По-нисък коефициент на амплитудата (PAPR) в сравнение с OFDM;
- По-малко излъчване извън основната честотна лента, вследствие използването на филтри в предавателя, които могат да се настройват;
- Подобен на OFDM модел в честотната и времевата област, предназначен за много потребители;
- Събиране на целия свободен честотен спектър, дори в региони със силно фрагментиран спектър;
- Блоково предаване на данни с използване на цикличен префикс и преобразуване на Фурие.

Основните недостатъци на GFDM са:

- Усложнен дизайн на приемника;
- Необходимост от използване на OQAM или филтри за намаляване на интереференцията между носещите (ICI/SIS), което прави MIMO по-трудно;
- Оценка на Symbol time offset (STO) и Carrier frequency offset (CFO);

Настоящата тенденция за приемане на пето поколение комуникационни стандарти поражда огромно очакване сред инженерите. Извършеният анализ на модели в иновативни концепции за безжични комуникации е полезна и вълнуваща необходимост при решаване на основни предизвикателства, които трябва да бъдат преодолени от операторите в сферата на безжичната индустрия и производителите на оборудване.

References:

1. Rohde & Schwarz: Application Note 1MA271 “5G Waveform Candidates”, 2016
2. Rohde & Schwarz: Application Note 1MA111 "UMTS Long Term Evolution (LTE) Technology Introduction”, 2012

D. K. Hubenov,

STUDY OF RADIOSIGNAL RADIATION OF USB 3.0 DEVICE

Dyanko K. Hubenov

***Abstract**: This paper shows a study of the impact of radio frequency interference caused by an USB 3.0 device over another wireless device. Also some performance improvement means are proposed in order to reduce the harmful interference.*

***Keywords**:USB 3.0, radio frequency interference, wireless device*

ИЗСЛЕДВАНЕ НА РАДИОЧЕСТОТНОТО ИЗЛЪЧВАНЕ НА USB 3.0 УСТРОЙСТВО

Дянко К. Хубенов

Национален военен университет „Васил Левски",
Факултет „Артилерия, ПВО и КИС",
гр. Шумен, ул. „Карел Шкорпил" 1
e-mail: d_hubenov@abv.bg

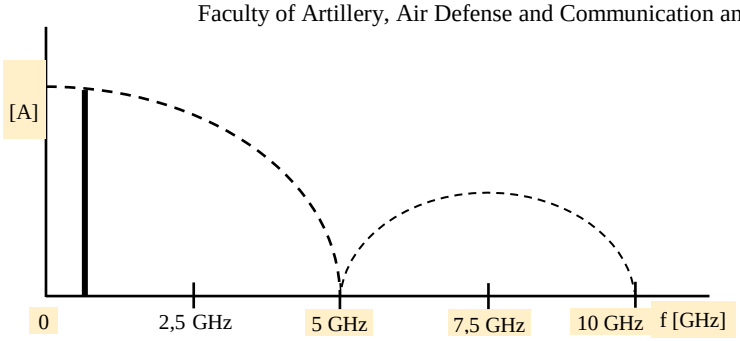
Въведение

Нелицензираните честоти в диапазона около 2,4 GHz се използват от все по-голям брой безжични устройства, като например рутери и периферни устройства за компютри (мишки и клавиатури). Трансийвърите на тези устройства могат да работят както на постоянна честота, така и да използват различни методи за промяна на работната честота, като за това могат да се използват стандартни протоколи като Bluetooth и IEEE 802.11b / g / n или собствени протоколи разработени за конкретното устройство.

За да може безжичния радиоприемник да определи достоверно наличието на полезен сигнал неговата чувствителност трябва да е по-висока от мощността на този сигнал. Границата на чувствителността на приемника се влияе пряко от минималното отношение сигнал – шум (С/Ш), необходимо за демодулация на сигнала. С увеличаване на разстоянието между предавателя и приемника нивото на приетия сигнал намалява, като в същото време намалява и отношението С/Ш вследствие наличието на смущения на основната честотна лента. Всичко това води до снижаване на обхвата на безжичните комуникации и предизвиква необходимост от повишаване на нивото на приетия сигнал за да бъде преодоляна чувствителността на приемника.

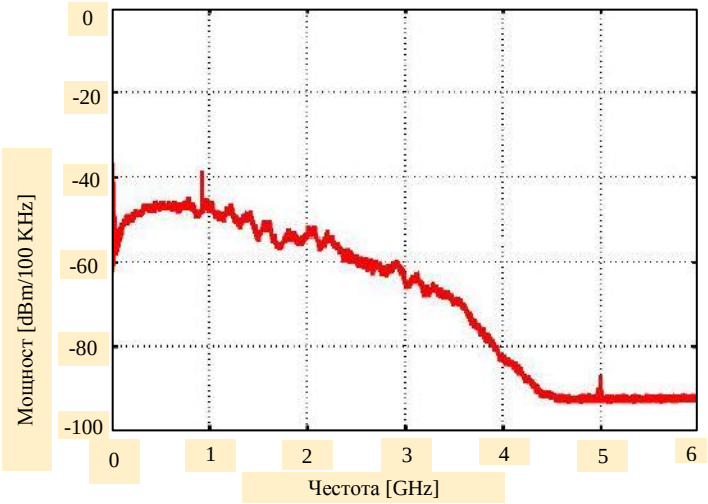
1. Стандарт за предаване на данни USB 3.0.

Интерфейс USB 3.0 позволява предаване на данни със скорост до 5 Gbit/s, като за постигане на тази скорост се използва разширен честотен спекър на тактовите честоти (фиг. 1.1) и кодиране на информацията.



Фигура 1.1. Функции на USB 3.0

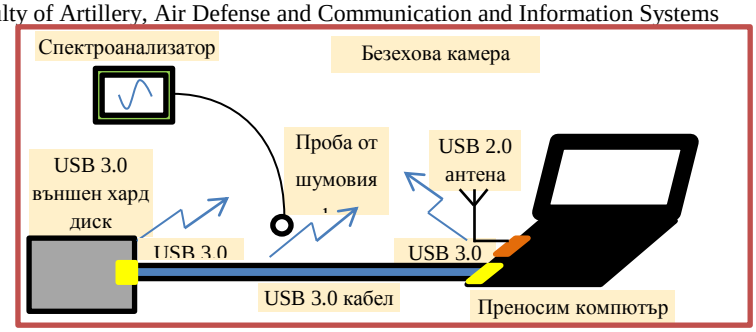
От фигурата се вижда, че информационният спектър е широколентов и варира от нула до 5 GHz. На фиг. 1.2 е показан информационният спектър на USB 3.0 сигнала от преносимия компютър. Вижда се че шумовият фон е доста интензивен в честотния диапазон около 2,4 GHz. Тези шумове е възможно да се излъчат в околното пространство чрез свързващия кабел на USB 3.0 или чрез някой от конекторите - към външния хард диск или към преносимия компютър. Това излъчване би могло да окаже зловредно влияние на разположеното в близост безжично устройство, като понижи отношението С/Ш и съответно чувствителността на приемника, предизвиквайки влошаване на качеството или дори пропадане на безжичната връзка [4].



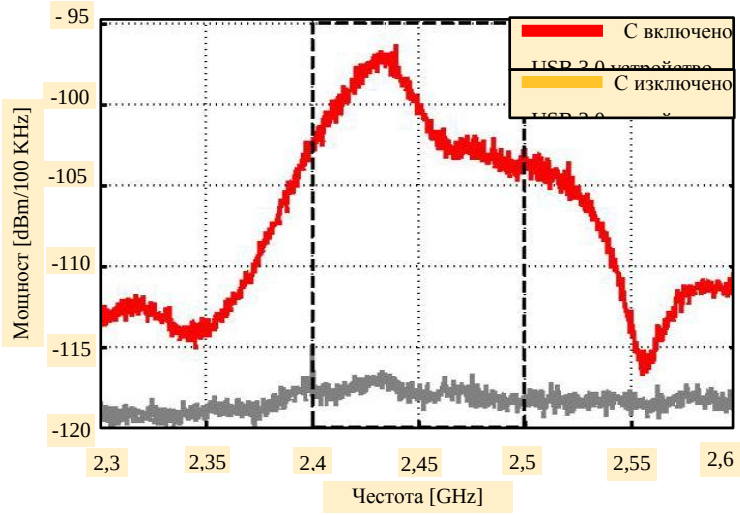
Фигура 1.2. Информационен спектър на USB 3.0

На фиг. 1.3 е показан моделът за определяне нивото на шумовия фон на USB 3.0 устройство, като е използвана безехова камера.

Взета е проба от полето, в близост до USB 3.0 външен хард диск, която след това се изследва със спектроанализатор при включен и изключен хард диск. Резултатите са показани на фиг. 1.4, където се вижда, че когато хард дискът е включен нивото на шум в честотната около 2,4 GHz се увеличава с около 20 dB. Това увеличение би могло да предизвика зловредно влияние върху нормалната работа на безжичното устройство.



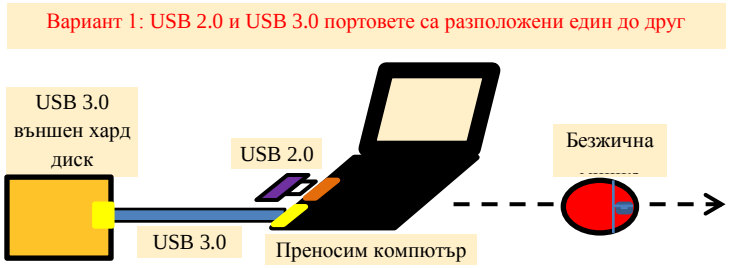
Фигура 1.3. Модел за измерване на шумовия фон на USB 3.0 устройство



Фигура 1.4. Спектър на шума при включено и при изключено USB 3.0 устройство

2. Влияние на USB 3.0 устройство върху работата на безжично периферно устройство за персонален компютър

На модела, показан на фигура 2.1, към преносим компютър чрез USB 2.0 порт е свързан донгъл комуникиращ с безжична мишка, за да се демострира влиянието на шумовете от USB 3.0 устройство върху тази безжична мишка. Освен това към същия преносим компютър е свързан външен хард диск с USB 3.0 интерфейс, като двете устройства (хард дискът и безжичната мишка) са свързани към съседни портове на преносимия компютър.



Фигура 2.1. Модел за оценка на работата на безжична мишка,
намираща се в близост до USB 3.0 устройство

Състояние на USB 3.0 външен хард диск	**Безжична мишка намираща се на разстояние**		
	0,5 метра	**1 метър**	**1,5 метра**
Не е свързано	Няма забавяне	Няма забавяне	Няма забавяне
Вариант 1: Свързано без да се предават данни	Няма забавяне	Забавяне на мишката	Забавяне на мишката
Вариант 1: Свързано и има предаване на данни	Няма забавяне	Забавяне на мишката	Забавяне на мишката

Таблица 2.1. Резултати от проверка на работата на безжична мишка, намираща се в близост до USB 3.0 устройство

Безжичната мишка се отдалечава от преносимия компютър няколко пъти на зададено разстояние, като качеството на радио връзката между безжичната мишка и преносимия компютър се оценява след всяко нейно преместване. Данните са представени в таблица 2.1, като критерии за оценяване се приема плавното преместване на курсора на мишката.

Вижда се, че когато към преносимият компютър е свързано USB 3.0 устройство работата на безжичната мишка се затруднява. Когато разстоянието между преносимия компютър и мишката стане повече от един метър се получава значително забавяне на преместването на курсора на мишката. Този ефект се отчита, както когато се предават данни по USB 3.0 устройството, така и когато няма предаване на данни.

Ако вместо USB 3.0 външен хард диск се използва друго USB 3.0 периферно устройство се получават идентични резултати. Тъй като шумът от USB 3.0 устройство е широколентов, то той би повлиял на каквато и да било антена разположена в близост, включително и Bluetooth устройства.

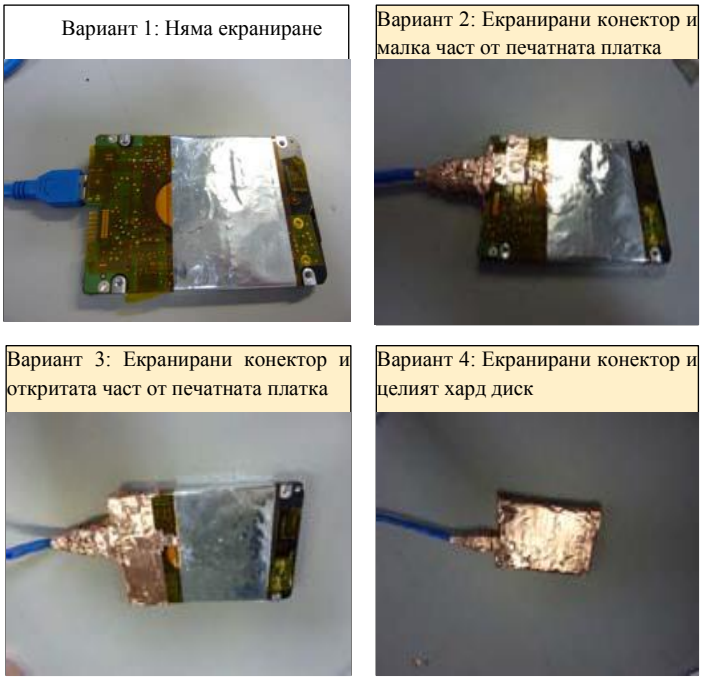
3. Методи за намаляване на влиянието на USB 3.0 устройства върху безжични периферни устройства

За да се понижи въздействието на USB 3.0 устройството върху безжичните периферни устройства е необходимо:

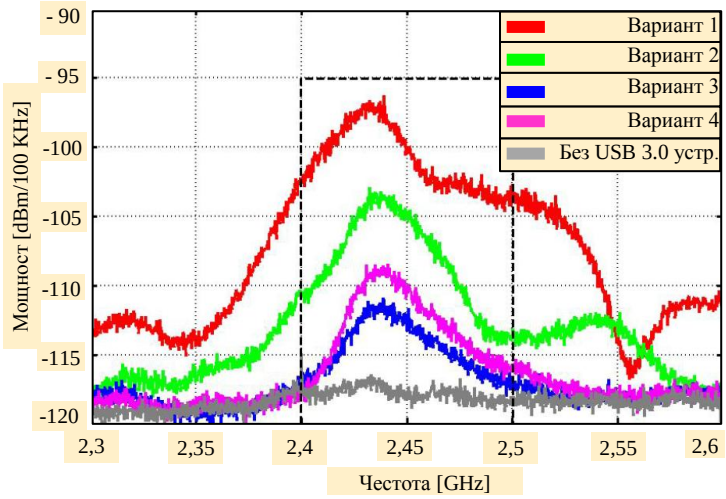
- ✓ Екраниране на USB 3.0 устройството;
- ✓ Екраниране на USB 3.0 конектора към преносимия компютър;
- ✓ Правилно позициониране на безжичната антена.

3.1. Екраниране на USB 3.0 устройството

Екранирането на USB 3.0 устройството би спомогнало за намаляване на излъчването на шум в диапазона около 2,4 GHz. На фигура 3.1 са показани различни врианти за екраниране, като при всеки от тях се прави измерване на излъчвания шум в честотната лента около 2,4 GHz. При измерванията е използван модела показан на фигура 1.3. Резултатите от измерванията са показани на фигура 3.2. От тях се вижда, че екранирането оказва голямо влияние за ограничаване на шума. Пълното екраниране при вариант 4 намалява нивото на излъчения шум с около 12 dB в сравнение с вариант 1, където няма екраниране.



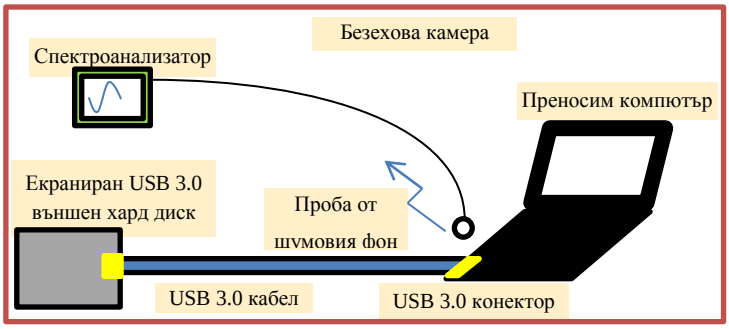
Фигура 3.1. Варианти за екраниране на USB 3.0 външен хард диск



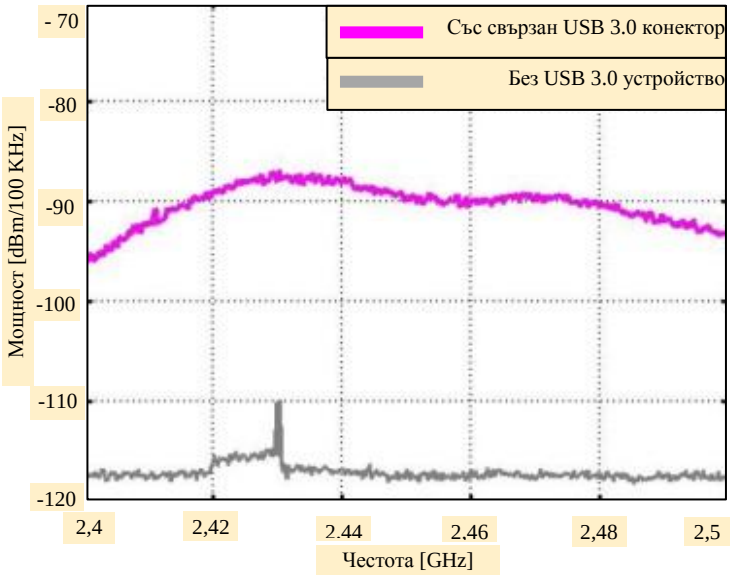
Фигура 3.2 Спектър на излъчения шум при различни варианти на екраниране на USB 3.0 устройството

3.2. Екраниране на USB 3.0 конектора към преносимия компютър

Освен шума, излъчен от самото USB 3.0 устройство, има излъчване на шум и от конектора, който свързва устройството към преносимия компютър. На фигура 3.3 е показан модел за измерване на това излъчване в безехова камера, като пробата от сигнала се взема в близост до конектора. За да се елминира напълно влиянието на самия външен хард диск, той е екраниран напълно и отдалечен на два метра чрез USB 3.0 кабел.



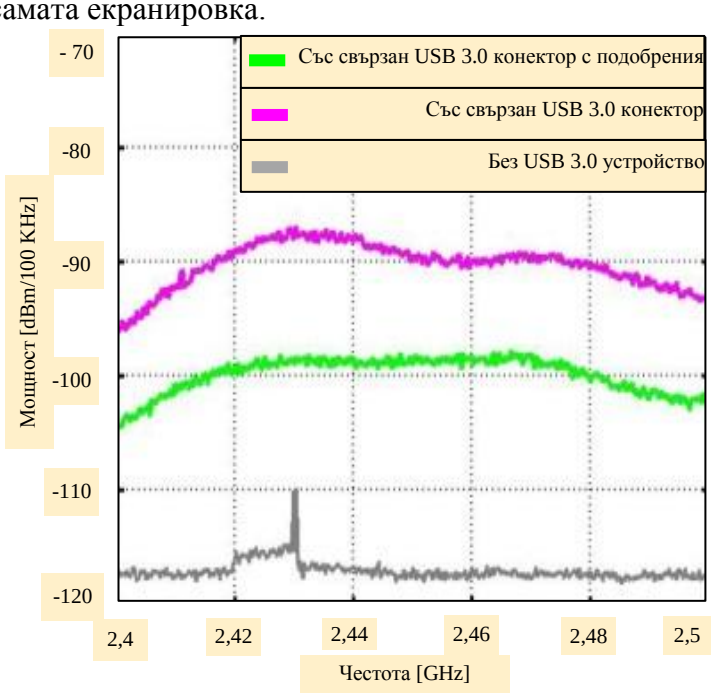
Фигура 3.3. Модел за измерване на шум генериран от USB 3.0 конектор



Фигура 3.4. Спектър на шума при изключено USB 3.0 устройство
и след свързване на USB 3.0 конектора

Както се вижда на фигура 3.4, шумът, излъчван от конектора, увеличава с около 25 dB шумовия фон, което оказва влияние на отношението С/Ш на приемника на безжичното периферно устройство.

Съществуващата екранировка на USB 3.0 конектора е предназначена да предпазва сигналните крачета, но трябва да бъде надеждно заземена. Ето защо тази екранировка не осигурява добра защита срещу излъчване на шум. Освен това свързването на екранировката към маса трябва да се извърши при минимално съпротивление. На следващо място трябва да има надеждна връзка между екраните на мъжката и женската част на USB 3.0 конектора. Препоръчително е също да се подобри качеството на самата екранировка.



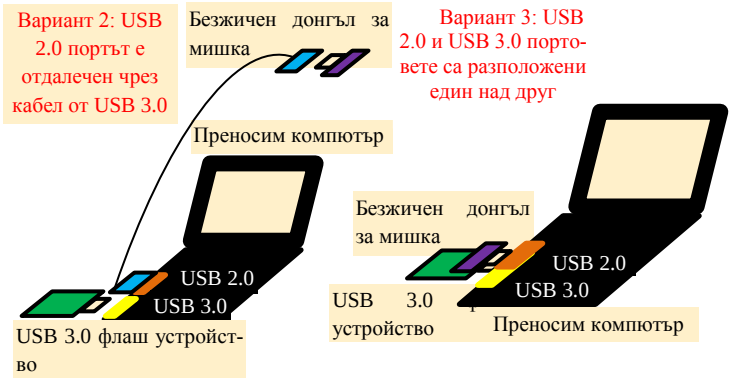
Фигура 3.5. Спектър на шума при изключено USB 3.0 устройство, след свързване на USB 3.0 конектора и при USB 3.0 конектор с подобрения

На фигура 3.5 са представени резултатите от измерване на шума след прилагане на гореописаните стъпки за намаляване на излъчения шум. Вижда се, че нивото на шума се понижава с около 10 dB.

3.3. Правилно позициониране на безжичната антена

Моделите, показани на фигура 3.6, имат за цел да оценят ролята на разположението на антената на безжичното устройство спрямо USB 3.0 флаш устройство. За вариант 2 безжичния донгъл е отместен чрез USB 2.0 кабел на по-голяма дистанция от USB 3.0 флаш устройството, а за вариант 3 двете устроства са разположени вертикално едно над друго.

Резултатите от двата варианта са представени в таблица 3.1. Вижда се, че местоположението на антената на безжичното устройство оказва голямо влияние върху нормалната работа на мишката. Отдалечаването на антената намалява влиянието на шума, генериран от USB 3.0 устройството.



Фигура 3.6. Модели за оценка влиянието на местоположението на приемната антена на безжичното периферно устройство

Състояние на USB 3.0 външен хард диск	**Безжична мишка, намираща се на разстояние**		
	0,5 метра	**1 метър**	**1,5 метра**
Вариант 2: USB 2.0 донгълът е отдалечен от USB 2.0 флаш устройството чрез кабел	Няма забавяне	Няма забавяне	Няма забавяне
Вариант 3: USB 2.0 и USB 3.0 устройствата за разположени едно над друго	Забавяне на мишката	Забавяне на мишката	Забавяне на мишката

Таблица 3.1. Резултати от проверка на работата на безжична мишка, намираща се в близост до USB 3.0 устройство

References:

1. Intel Corporation - USB 3.0 Radio Frequency Interference Impact on 2.4 GHz Wireless Devices, Document: 327216-001, http://www.intel.com/design/literature.htm, April 2012

2. IEEE Computer Society, IEEE 802.11-2016 - IEEE Standard for Information technology—Telecommunications and information exchange between systems Local and metropolitan area networks—Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, http://standards.ieee.org/findstds/standard/802.11-2016.html, 2016

3. USB Implementers Forum, Universal Serial Bus 3.0 Specification, http://www.usb.org, June 2011

4. Nikolov, L., ERROR RATE ANALYSIS IN RICEAN CHANNEL AND COMPLEX RADIO ENVIRONMENT. International Scientific Conference “Defense Technology Forum”. Collection of papers. Shumen. 2016. ISSN 2367-7902, p. 308

G. N. Mazadzhiev,

FROM A TECHNOLOGY ASSOCIATED MAN TO POST-HUMAN

Georgi N. Mazadzhiev

*"VASIL LEVSKI" NATIONAL MILITARY UNIVERSITY,
ARTILLERY, AIR DEFENSE AND CIS FACULTY*

Abstract. *В доклада се изследва технологичната трансформация на биологичната компонента в системата „човек-интелигентна машина" в три фази – настояща(пост-ПС), преходна и напреднала(повсеместен компютинг). Установени са тенденции за постепенна технологизация (с възможна дехуманизация) на човека чрез имплантируеми и безшевни технологии за усъвършенстване и разширяване на човешките способности. Персонификацията на интелигентните машини към изкуствена интелигентна личност и на човека - към подобрен „пост-човек"поставя проблема за тяхното сътрудничество/конкурентност.*

Key Words: *човек, компютър, изкуствен интелект, система, еволюция.*

ОТ ТЕХНОЛОГИЧНО ПОДПОМОГНАТ ЧОВЕК КЪМ ПОСТ-ЧОВЕК

Георги Н. Мазаджиев

НАЦИОНАЛЕН ВОЕНЕН УНИВЕРСИТЕТ „В. ЛЕВСКИ", ФАКУЛТЕТ „АРТИЛЕРИЯ, ПРОТИВОВЪЗДУШНА ОТБРАНА И КОМУНИКАЦИОННО-ИНФОРМАЦИОННИ СИСТЕМИ"

1. Въведение

Днес повече хора умират от преяждане, отколкото от глад, повече хора умират от старост, отколкото от заразни болести, повече хора се самоубиват, отколкото са убити от войници/терористи/престъпници. Нови предизвикателства пред човечеството изместват вековната борба за оцеляване[5]:

- Пренаселеност и изчерпване на природните ресурси;
- Информационен и технологичен бум;
- Търсене на ресурси в космоса и океана;
- Естествена пандемия (или биотероризъм);
- Унищожителна война;
- Измиране на пчелите;
- Климатична катастрофа, супер-вулкани;
- Дефектен ИИ или доминиращ супер-интелект, извънземен разум и др.

Някои изследователи приемат, че човешката интелигентност нараства еволюционно и това е гаранция за просперитета на човечеството(фиг.1). Други – обратно – привеждат доказателства, че вследствие на професионалната специализация настъпва спад на коефициента на интелигентност - хората разчитат на уменията на другите за своето оцеляване(фиг.2). Анализът на човешката биологична еволюция от учени в Американска асоциация за научен напредък – (AAAS) показва, че са налице сериозни компромиси във физиологичната конструкция на човешкото тяло[5]:

- Изправено ходене на два крака - по-малки тазове, ограничаване размера на родовия канал, S-образен гръбнак, който е причина за чести болки в гърба;

- По-големи мозъци - смъртта при раждане е водеща причина за смъртта на жените в репродуктивна възраст - човешките бебета са 6,1% от телесната маса на майката, при шимпанзета (3,3%) при горилите (2,7%);
- Гърло, което лесно може да се задуши;
- Слух и зрение, отслабващи в края на живота ни, и т.н.

Фиг. 1. Човешката когнитивна способност за 14 хилядолетия (Hugues Crepin)

Фиг. 2. В дясна ръка - череп на кроманьонец, в лявата - череп на съвременен човек.

Естествената биологична еволюция продължава бавно и в наши дни – ето и някои примери:

- Шерпите (наследници на Денисовия човек)**:** гъстата капилярна мрежа и разредена кръв използват по-пълноценно наличния кислород (на връх Еверест 33%); Митохондриите произвеждат с 30% повече аденозинтрифосфат (АТР) - енергията в клетките;
- 36% от източно-азиатците са развили адаптация - вродена непоносимост към алкохола, като защита от рак - зачервяване на лицето и тялото и гадене, температурата на кожата се повишава поради натрупването на ацеталдехид.;
- 25% от световното население притежава ензим, разграждащ лактозата – появил се като мутация отпреди 7500 г. в равнините на Унгария – една полезна способност за оцеляващите в студената Европа;
- Адаптации на имунната система, предпазващи от малария, проказа, туберкулоза и холера, грип - вследствие живота в градовете и отглеждането на домашни животни;
- Мутация, предпазваща от израстване на зъби-мъдреци - с по-меката храна отслабват челюстните мускули, а мъдреците увеличават риска от болезнени и смъртоносни инфекции. От няколко хиляди години на всеки четирима души липсва поне един зъб мъдрец – най-често при инуитите от най-северните региони на Гренландия, Канада и Аляска.

Става ясно, че:

- Новите предизвикателства и заплахи не могат да се овладеят с темповете на бавната естествена биологична еволюция;
- Цел на съвременното човечество е не само оцеляване, а и устойчив прогрес;
- Необходимо е да се търсят технологични подходи и средства за разширяване и усилване на способностите на хората до степен, адекватна на глобалните проблеми и конкурентни условия.

В този аспект целите на настоящата работа са:

- Да се систематизират аргументи за количествени и качествени аспекти на технологично-ускорената еволюция на човека;
- Да се установят същността и направленията на еволюционна трансформация и условията за устойчива перспектива на човешката цивилизация.

2. Изложение:

Съществуват три основни тенденции на работното място: технологично подпомагане на хората, заместване на хората с машини и съвместна работа на хора и машини. Технологичното усилване на хората има за цел да се създаде по-способна и производителна работна сила в области с физически , емоционални и когнитивни дейности. Ползите са подобрена производителност, намалени рискове за хората и по-добро качество на работа [2].

Съвременният технологичен пакет, който е двигател на човешкия напредък, е известен с абревиатурата NBIC – нано-, био-, информационни и когнитивни технологии. Сред тях доминират компютърните информационни технологии, като допринасят косвено за развитието и на останалите технологии в пакета. Ето защо по-нататък еволюционната трансформация на човека се свързва тясно с тяхното усъвършенстване. Проучването на динамиката и характеристичните особености в еволюцията на системата „човек-компютър“ се разделя условно на три етапа – съвременен (пост-PC), напреднал (повсеместен) компютинг и междинен като се базира на съвременната фактология и технологични тенденции за междинния етап. Екстраполацията за повсеместния компютинг е осъществена чрез прогнози на анализаторски агенции, експертни становища и анализи на учени, **висши мениджъри и визионери във** водещи IT-компании. В таблица №1 тези етапи се детайлизират като фази на третата технологична вълна в компютърните информационни технологии [10].

Табица №1. Технологични вълни в компютинга

НАЧАЛО	ВЪЛНА/ЕТАП		КОМПЮТЪР / СИСТЕМА	МОДЕЛ	КОМПЮТИНГ
1950-	Първа вълна		Мейнфрейм компютър	1 компютър – много потребители	СТАЦИОНАРЕН
1980-	Втора вълна	PC	Персонален компютър	1 потребител - 1 компютър	
2000-	Трета вълна Фаза 1	Пост-PC	Преносим (лаптоп/ултрабук)	1 потребител – няколко компютри	МОБИЛЕН
			Ултрапреносим (таблет, смартфон)		
			Носим (сателитни аксесоари)		
2020-	Трета вълна Фаза 2	UC - преход	Носим (второ поколение)	1 потребител много компютри	ПОВСЕМЕСТЕН
			Носим (трето поколение)		
			Вграден (интегриран)		
			Surround Computing Era (умен дом, автомобил, град - ранни образци)		
			Интернет на нещата IoT, Комуникации M2M		
2035-	Трета вълна Фаза 3	UC - напреднал	Повсеместен компютър (invoked computing)	Много потребители много компютри	
			Повсеместна мрежа, IoE, хиперсвързаност, цифрова трансформация на физическия свят, Web на физическия свят		
			Интелигентно обкръжение, телеприсъствие, телеоперации		
			Artificial Intelligence General, E-личности, E-общност, пост-цивилизация	Нови модели на взаимодействие	
	Фаза 3а		Artificial Superintelligence, E-цивилизация		ТЕХНОЛОГИЧНА СИНГУЛЯРНОСТ

В следващото изложение еволюционната трансформация на системата „човек-интелигентна машина" се анализира в три аспекта – технологизация на човека, персонификация на машините и конвергенция на хора с интелигентни машини.

2.1. Технологизация на хората

Характерна е за етапа пост-PC, когато биологичната компонента на човеко-машинната система се определя като **технологично подпомогнат човек**. Ролята на човека е водеща - активно взаимодействия с реалния и виртуалния свят, поставя цели, идентифицира проблеми, декомпозира ги на задачи за изпълнение от машината, взема решения. Основни инструменти за подпомагане в редица професионални дейности са опосредстваната реалност (обогатена реалност/виртуалност, смесена реалност), биологична ОВ, телемедицина, както и някои виртуални симулации на по-прости системи в обкръжаващия свят.

Внедряват се системи за информационно подпомагане[3] и за когнитивно подобряване на човешкия потенциал - с тренировка или в реално време. Интензифицират се аспекти на познавателната и физическа дееспособност[9].

Характерно за **технологично-подпомогнатия човек** е използването на **външни за човешкото тяло технически системи**. Те изграждат **интелигентна околна среда** за сметка на вграден хардуер и софтуер в отделни физически обекти, включително и мрежи от тях(фиг.3). Някои преносими и ултра-преносими технически системи (смартфон) опосредстват мобилно взаимодействие с физическия и виртуален свят, като използването им е в **ограничени по време сеанси**.

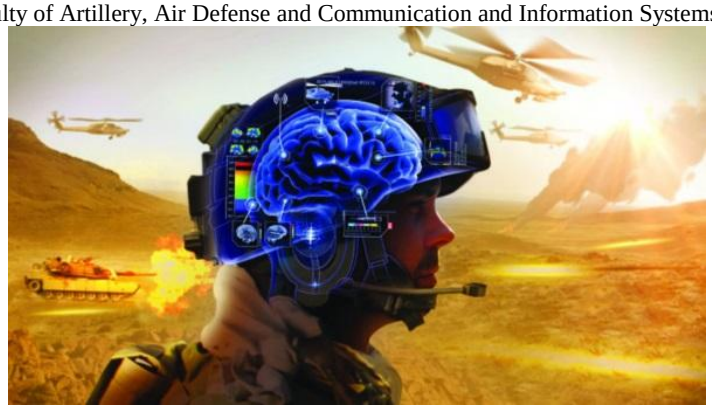
Фиг. 3. Окабеляване на самолет Boeing с Google Glass и Skylight (софтуер на Upskill)

Възниква технологична зависимост на човека като номофобия, пристрастеност, смесване на реална и виртуална личност. Нарастват социалната сегрегация, времето за виртуален живот, дистанцираността на индивидите от установения социален и когнитивен опит. Разпространява се стремеж към усамотение и отказ от реалния живот.

В междинния технологичен етап (около 2030 г.) биологичната компонента на човеко-машинната система е **функционално усилен човек с разширен диапазон от способности**. Използват се **постоянно носими (но отделими) върху тялото интелигентни системи с повишена автономност**. Започнал е процес на киборгизация – чрез имплантируеми системи. Стивън Хоукинг определя тази перспектива с думите: "Човешката раса навлиза в етап на **самопроектираща се еволюция**". Американски учени от университета в Харвард разработиха метод за „отглеждане" на кибер-тъкан в човешкото тяло:

- Имплантация в организма на биосъвместими наноматериали, които се смесват с клетките и израстват с тях в обща плът;
- Кибертъканта е ефективен интерфейс за получаване на информация за живите системи в организма.

Група университети под ръководството на DARPA **(**Brown University; Колумбийски университет; Калифорнийски университет и др) разработват скоростен имплантируем невронен интерфейс с висока резолюция (10^6 неврона) за трансфер на данни от и към човешкия мозък с декодиране и обработка на на невронни и цифрови сигнали – фиг. 4 [6].



Фиг. 4. Имплантируем високоскоростен невронен интерфейс-NESD
с висока разделителна способност
(DARPA, Brown University; Колумбийски университет; Калифорнийски университет и др.)

Животът на потребителят е функционално преплетен и адаптиран към носимия интелект в много по-висша степен (както се свиква с обувки и дрехи). **Отделянето/ отсъствието на носимите интелигентни системи създава психически дискомфорт, понижава се работоспособността, ограничава се и функционалността на човека**.

Човекът притежава, експлоатира и контролира постоянно съпътстващо го техническо персонализирано информационно пространство като избирателно усилва/отслабва/редактира ситуационната си осведоменост. Основен инструмент за това е опосредствано от компютъра възприятие на околната среда. Масово се развиват задълбочени виртуални симулации на съзнателния свят (втора земя) за прогностични изследвания в редица специализирани области – например тестване на стратегии при кризи и конфликти.

След 2040-2050 г. технологично ускорената биологична еволюция води към **нов, целево подобрен (според необходимостта) човешки биологичен вид/видове – т.н. пост-човек**, който по-успешно контролира физическия свят (Ray Kurzweil, *Exponential Finance conference, New York).* Трансформиращата мощ на **„вградените/въплътените“ в човека технологии** започват да доминират спрямо естествената природа. За надграждане на човека се използват високоефективни **„безшевни“ генетични, симбиотични биокибернетични и нано-технологии**. Постигат се многократно увеличени когнитивни способности, пълен контрол над емоционалното, психическо и физиологично състояние, удължен биологичен живот чрез функционално протезиране и усилване на сектори в мозъка (Расин), замянят се органи или тъкани с подобрени версии.

Още сега технологиите за търсене, редактиране и отстраняване на гени в човешката ДНК - CRISPR-Cas9 позволяват т.н. генетично програмиране:

- Създаване и развитие на „подвид на хомо сапиенс“, устойчив на радиация, безтегловност, репродуктивни проблеми в космоса;
- Нов тип вътрешна биологична защита за космонавтите, освен известните физични, електрични и фармакологични предпазни средства.
- „Дизайнерски бебета", проектирани със зададени генетични подобрения - персонализиране на ин витро ембриони чрез добавяне, премахване или промяна на гени [7];
- „Редактиране на зародишната линия„ – унаследяване на генетичните модификации, намеса в човешката еволюция.
- Тъканна нанотрансфекция (TNT, университет на Охайо) чрез „инжектиране" на генетичен код в клетки и препрограмиране на типа им за възстановяване на увредени органи или функционалността на остаряващи тъкани;
- Управление на генната активност с програмируеми, но преходни генни модулатори [8] – фиг. 5;
- Устойчивост на вирусна инфекция, предозиране с опиоид, отравяне с органофосфат и експозиция на гама радиация;

Фиг. 5. Технологии **PREPARE** – генетична терапия като платформа за защита от заплахи за общественото здраве и националната сигурност с временен и обратим ефект в зададен период[8]

Учени от Харвард са разкрили специфични зони в мозъчната структура на гениални и крайно-успешни хора. Това позволява да се тестват методи за изкуствено активизиране на мозъка в тези зони, в т.ч. да се разработят фармацевтични средства за биохимична стимулация на хора, така че те да продуцират гениални идеи.

И все пак именно уязвимостта и слабостта на нашето тяло с неговите атрибути (раждане, здраве, болест и смърт) ни правят хора и личности. Стремежът да преодолеем своите слабости с антропотехника и биохакинг води до технологизация на човешкото тяло. Ако развитието на суперспособности у пост-човека не се балансира със „супер-морал“ това означава, че технологизацията поражда и определена степен на човешка дехуманизация.

2.2. Персонификация и хуманизация на интелигентните машини

В изходния етап (пост-PC) интелигентната машина (в т.ч. и компютъра) е обособен ултрапреносим компонент на системата Ч-М с пасивно-изпълнителска роля, елементи на проактивност и значително време за готовност. Взаимодействието Ч-М е от затворен тип, ангажира значителни психични ресурси, а сетивната свързаност с външната реалност е минимална. Мобилността и ултрамобилността повишават честотата на работните сеанси и минимизират продължителността им. Възникват и **нов клас пространствено-разпределени, мрежово свързани и автоматично комуникиращи интелигентни машини, които образуват „умни” пространства с локален, регионален и глобален обхват**.

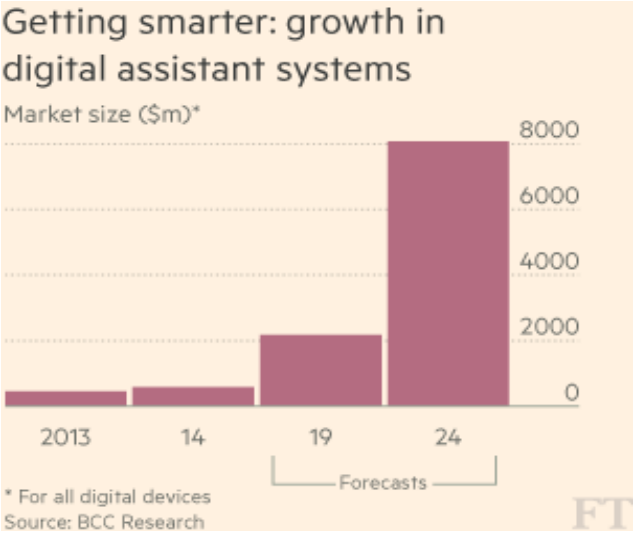
Контекстната функционалност се базира на технологии за сензорен синтез [16] и контекстно зависими приложения – гласови интерфейси, проследяване на местоположение, маршрут, здравен статус и начин на живот. Разработват се **когнитивни машини с бионична архитектура и невроморфни компоненти** (SyNAPSE – IBM, смартфон процесори A11 Bionic, Kirin 970 с NPU - невроморфен ускорител и др.) Внедряват се множество специализирани приложения на изкуствения интелект **(Artificial Narrow Intelligence, ANI).** ИИ с облачни изчислителни ресурси (латентност, заплахи за личните данни и зависимост от качеството на мрежовата връзка) **еволюира към симбиоза на локален и облачен ИИ като облачните ИИ-ресурси тренират локалните ИИ-алгоритми с огромни масиви данни**. Значително се подобряват контекстност, когнитивност, интуитивност, персонализирани услуги и преживявания.

Доминира GUI, но се разработват и възприемчиви **интелигентни машини,** комбиниращи интуитивни интерфейси – фиг. 6. Мултимодална комуникация се постига с говорещи 2D-цифрови изображения в различни превъплъщения, които имитират движения на устни и съпреживяване чрез мимики и изражения (виртуална глава “Zoe”).

Предлагат се облачни услуги за избор на **базова личностна комплектация на виртуални асистенти**. Виртуални аватари се създават по снимка, видео и отговори на дузина въпроси (Lifenaut). Така се имитират аспекти на човешка външност и поведение. Работи се по усъвършенствано 3D-телеприсъствие - с модули за глас, съвети, мотивация, външен вид и някои емпатични реакции.

В **междинния технологичен етап** човеко-машинната система може да се определи като симбиотична и синергична (хуманистична интелигентност HI). Усилването на човешките възможности се осъществява чрез **постоянно носима върху тялото (но отделима) автономна интелигентна система, взаимодействаща с облака**. Цифровата трансформация на физическия свят доминира, а специализираните приложения на изкуствения интелект (**ANI) са масови.**

Носимата интелигентна машина е практически незабележима и е постоянна част от личното пространство. Полезността се разширява чрез интелигентна периферия (аксесоари, умно облекло, имплантируем модул). **Тя функционира като естествено разширение на ума и тялото и може да се определи като адаптирана (протезна) система**. Използването й консумира минимални психични ресурси.



Фиг. 6. Нарастваща доминация на виртуалните асистенти като интелигентен мета-слой на върха на всички услуги – прогнози на Forecasts

Мултимодалната сензорна чувствителност към заобикалящата среда и поведението на потребителя позволява да се изгради модел на конкретното обкръжение, профил на човешките потребности и поведение Възприемчивостта към текущ и агрегиран контекст за физическото и социалното обкръжение се постига с хардуерни, софтуерни сензори и контекстна машина. Възниква частичен потенциал за посредничество между човека и реалния свят – разширяване, филтриране и модифициране на човешките възприятия за реалността. Разширената свързаност и възприемчивост към реалния свят и човека е предпоставка за напреднала когнитивна функционалност в редица специализирани области.

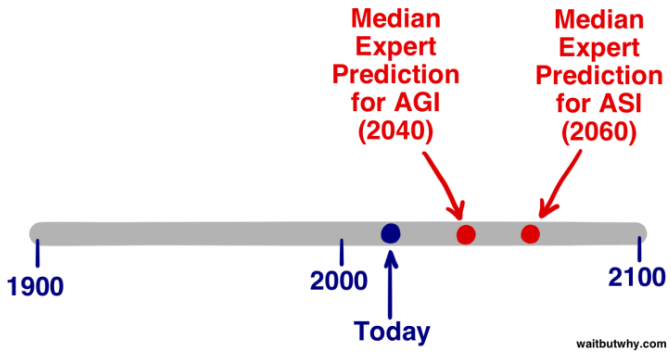
Взаимодействието Ч-М еволюира до симбиотичното взаимодействие (СВ). То се осъществява неусетно, фоново, контекстно и мобилно в реално време. Доминират преки интерфейси – ментален [4] и гласов интерфейс. (DARPA – проект „Универсален преводач”).

Интелигентната носима машина придобива по-развита личностна комплектация с модули за емпатия и програмирана съвест. Емпатичният модул съдейства за емоционален контакт с компютъра чрез *плацебо емпатия* (изражение и интонация на гласа, емоционален отклик на аватара). Целта са емоционално интелигентни и социално квалифициращи машини, реагиращи адаптивно и адекватно на човешките потребности. Етичен регулатор(R. C. Arkin) съблюдава правила и закони, включително възможността за избор между: зло и "по-малко зло", приемливо и неприемливо поведение. Етичен адаптор минимизира щетите от определени действия. Той подлежи на самообучение за адаптиране към потребителя. Нарушаването на технологичния „морал" предизвиква промяна в "поведението" на интелигентната машина (аналог на гузната съвест при хората).

В по-далечна перспектива (2040+) мрежата от интелигентни машини еволюира към **мащабируеми интелигентни пространства** - изчислителният ресурс е разпределен и невидимо вплетен във физическия свят, който се превръща в повсеместно интелигентно обкръжение[1,2]. Облачните решения не са централизирани сървърни ферми, а вездесъща изчислителна материя.

С постигането на адекватна изчислителна мощ и различни специфични подходи (машинно самообучение, реверсивен мозъчен инженеринг, самоподобряваща се архитектура и др.), след 40-те години на 21-ви век се очаква пробив в усилията за създаване на изкуствен интелект на човешко ниво (Artificial Intelligence General, **AGI)**. Става дума за емулирани "способности да се разсъждава, планира, решават проблеми, да се мисли абстрактно, да се разбират сложни идеи, да се учи бързо, да се учи от опита (Linda Gottfredson).

През 90-те години, **Върнър Виндж** популяризира термина **„технологична сингулярност" като предстоящ технологичен скок, когато изкуственият интелект ще еволюира до суперинтелект ASI (Artificial Superintelligence, ASI)** [17], надминавайки когнитивния потенциал на най-добрите човешки умове в практически всяка област. **С**ингулярният **скок в технологичното равнище се характеризира от** Курцвейл като **„закон за ускоряващата се възвращаемост"** [13]. Други очакват възникването на **AGI и ASI значително по-късно** [12] – фиг.7.



Фиг. 7. Прогнози на експерти за поява на универсален интелект(**AGI**) и за суперинтелект (**ASI**)

Високата степен на автономност на интелигентната машина прераства в осъзнатост и свобода на избор за **изкуствения интелект на човешко ниво AGI, а още повече за изкуствения суперинтелект. Съответните Е-общности и цивилизации биха могли да отхвърлят човешките закони и морал, създавайки свои еквиваленти. Този избор означава, че е възможно да поемат пътя на дехуманизация или дори на конфронтация с пост-човешката цивилизация.**

2.3. Сближаване на хора и машини

Елементи на сближаване и сътрудничество между хора и интелигентни машини се наблюдава и днес – такава е концепцията за използване в индустрията на т.н. колаборативни роботи, както и на антропоморфни роботи за услуги.

Назрява необходимостта от регулация на поведението на все по-сложните и автономни интелигентни машини (роботи, автомобили, дронове и др.). Целта е безопасност в различни сценарии от тяхната работа с хора. Предлагат се **стандарти за наблюдение и контрол** над процедурите за проектиране и производство на интелигентни и автономни технологии (IEEE). Google също работят върху основите на т.н. **технологичен „морал" на робота** – мащабируемостта на надзора, възможността да се дефинира универсално понятия като „вреда" в законите на Айзък Азимов и др. ЕС също стартира дискусия за създаване на правила, гарантиращи безопасни приложения на **AI.**

Постепенно интелигентността и автономността на машините нараства до възможността за симбиотично взаимодействие с хора. Типичен пример е еволюцията на съвременния телематичен автомобил с множество системи за подпомагане на човешкото управление до напълно самоуправляем, чието поведение е типично човешкото – до степен да предвижда намеренията на пешеходеца още преди да е стъпил на пътното платно, както и на други участници в движението.

Сценарият за равнопоставеност и сътрудничество с хората е по-вероятен за AGI като атрибут на изкуствени (Е-) личности с физическа или виртуална форма (андроид/робот/аватар). В тях може да се възпроизвежда или копира биологическата, психологическа и социална подструктура на човешки личности – фиг.8. Комуникационната им платформа ще е

пълноценна - вербална, невербална (изражение на лицето, език на тялото, интонация на гласа) и емоционална.

Е-личностите емулират човешката познавателна система. Обучението им за придобиване на знания и квалификация е практически мигновено. Клонират се чрез презапис. Имат способност за извънтелесно придвижване чрез предаване на информация за възпроизвеждане. Взаимодействието „човек-ИИ" се трансформира в подходящ за целта аналог на между-човешките отношения. **Етични и правни закони могат да регулират взаимоотношенията на човечеството и възникналата Е-общност. Възможно е да възникне пост-цивилизация, обединяваща биологичното човечество с Е-общността на интелигентните личности, въз основа на подходяща етично-правна система**.

Фиг. 8 „Е-личности" - реконфигуруема работна сила (по филма „Истински хора")

Фиг. 9 Сътрудничество/конкурентност между естествен и изкуствен интелект

Възможно е също и друго развитие, при което границата между естествения човешки интелект и изкуствения интелект се размива – например чрез директно копиране на човешкото съзнание и личност в Е-личност (проект на DARPA „Технологии за изтегляне на човешката памет"). В един вариант приживе виртуалното копие на конкретния човек може да населява облака и да проучва реални негостоприемни светове – чрез хиперсвързаност с бионично тяло. Друг вариант е цифрово безсмъртие след биологичната смърт, когато електронната личност (във физическо или виртуално въплъщение) продължава да функционира и да съжителства със своето традиционно обкръжение.

Още по-трудно е да се конкретизира сценария при поява на изкуствен супер-интелект, който акумулира и развива хилядолетния опит и знания на човечеството [11, 15]. Съществува потенциал за посредничество на супер-интелекта между хората и реалния свят, например като капсулация чрез сетивна виртуална реалност [14].

Заедно с повсеместно-разпределения изчислителен ресурс, супер-интелектът образува екосистема на когнитивни изчисления — мащабируема архитектура и алгоритми, емулиращи способности на мозъка по възприемане на мултимодална информация, отчитане на минал опит, приемане на решения и самообучение.

Изходът от паралелното съществуване на биологичната човешката цивилизация с тази на ИСИ е неопределен поради проблемната контролируемост на такава технология. Конкурентността може да доведе до конфликти и доминация на суперинтелекта с окончателна цифрова трансформация на биологичната цивилизация – фиг. 9.

Според доминацията на конкурентните предимства е възможно съвместно съществуване на биологична и електронна (Е-) цивилизации или биологичното общество се трансформира изцяло в електронно и/или виртуално.

С появата на изкуствен суперинтелект еволюцията стига до сингулярност. Неопределен е баланса в отношенията с човешката цивилизация, която може да се е трансформирала до виртуална.

3. Заключение

В проследените етапи от еволюцията на човека в системата „човек-интелигентна система" става ясно, че двете компоненти се сближават:

- в пространствен план интелигентната машина еволюира от ултрапреносима и носима (отделима) до неотделима (протезна) част от тялото на човека;
- в характеристичен план системата се развива към симбиотично взаимно влияние – човекът се технологизира и в определена степен се дехуманизира, а машината адаптивно се хуманизира и персонифицира във все по-висша степен;
- в аспекта физическо сливане на системните компоненти изходът се решава от пост-човечеството и Е-общността с възможности за обособяването им като конкурентни и/или сътрудничещи си общности и цивилизации.
- Човеко-машинното взаимодействие (ЧМВ) от етапа пост-PC прераства в симбиотично взаимодействие (СВ) и накрая в електронен аналог на равнопоставени отношения.

Възможно е да се направят следните обобщения:

- Машинната еволюция е насочена към персонификация до възникване на изкуствена интелигентна личност;
- Хуманизацията на интелигентната машина е функция на вложения в нея технологичен еквивалент на човешките етични норми и нравствени ценности, както и съвършенството на антропоморфния й облик;
- Персонификацията и хуманизацията на интелигентните машини са контролируеми цели до етапа на сингулярност;
- Развитието на технологиите обхваща все по-широк спектър от човешките способности, а тяхното усъвършенстване е в посока адаптация с човешкото тяло като постоянно носим и/или имплантиран атрибут, а впоследствие до „безшевно" вграждане/въплътяване;
- Основен акцент е технологичното усилване на човешката интелигентност - разширени анализи с експертни системи, използване на машинно самообучение в обработката на изображения, откриване на прозрения и вземане на решения;
- Технологично-подпомогнатата човешка еволюция води до технозависимост, поради симбиотичния функционален синергизъм на човешката цивилизация и всеки индивид с конвергентните технологии;
- Перспективата за физическо сближаване и сливане на системните компоненти се допълва с възможности за обособяването им като съпоставими разумни личности, общности и паралелни цивилизации.
- Условието за устойчиви взаимни отношения на сътрудничество е адекватност на етичните норми и правна система за всеки еволюционен етап и степента на тяхното възприемане и адаптиране в паралелните цивилизации като основен регулатор.

Желаният от човечеството сценарий за бъдещето е **„човек плюс машина, а не човек срещу машина".**

References:

1. Мазаджиев Г., Специализирани компютърни системи, Шумен, 2014, ISBN 978-954-9681-62-8.(2)
2. Мазаджиев Г., Преход към повсеместна информационна инфраструктура, списание CIO, ИКТ за отбраната(ч.1), юли, 2014, бр.7, ISSN 13112 – 5605(3)
3. Мазаджиев Г., Мобилни системи за информационно подпомагане – приоритети и иновации във военното дело, списание CIO, ИКТ за отбраната(ч.1), юли, 2012, 63- 64, ISSN 13112 – 5605.(4)
4. Мазаджиев Г., Човеко-компютърно взаимодействие: ментални интерфейси, Химера ООД, Шумен, 2016
5. Харари Ю. Н. , Sapiens. Кратка история на човечеството, Изд."Изток-запад", 2016, ISBN 9786191529506

6. Emondi Al., Neural Engineering System Design (NESD), HTML.URL: www.darpa.mil/program/neural-engineering-system-design
7. David Cyranoski, Sara Reardon, Chinese scientists genetically modify human embryos, NATURE, 2015, HTML.URL: https://www.nature.com/news/chinese-scientists-genetically-modify-human-embryos-1.17378
8. Dialing Up the Body’s Defenses Against Public Health and National Security Threats, HTML.URL: https://www.darpa.mil/news-events/2018-05-25(PREPARE)
9. Mazadjiev G., Bio-mechatronic Technologies Create Super-Troopers, ICT Media, Special issue, September, Comunication&Information Technologies for the Defense, 23-24, ISSN 13112 – 5605, 2009.(11)
10. Mazadjiev G. , Doychinov D.T., A Vision of the Evolution of the System “Man-Computer”, Collection of papers, International Scientific Conference, Defense Technology Forum, “Vasil Levski” NMU, Artillery, Air Defense and CIS Faculty, 2015, т.1, с.185-191., Химера ООД, Шумен, 2015, ISSN: 2367-7902
11. Nick Bostrom, How Long Before Superintelligence?, Linguistic and Philosophical Investigations, 2006, Vol. 5, No. 1, pp. 11-30.(12)
12. Paul G. Allen, Mark Greaves, The Singularity Isn't Near, MIT, Technology Review, October, 2011. HTML.URL: http://www.technologyreview.com/ view/425733/paul-allen-the-singularity-isnt-near/(13)
13. Ray Kurzweil. The Law of Accelerating Returns, 2001. HTML.URL: http://www.kurzweilai.net/the-law-of-accelerating-returns(14)
14. The future of hybrid tech and our 21st century commute, Toshiba & Ian Pearson, 2015. HTML.URL:http://www.communicationforce.com/wp-content/uploads/2015/06/Toshiba_Future-of-Tech-Report_English-Design.pdf(15)
15. Tim Urban, The AI Revolution: The Road to Superintelligence**.** HTML.URL: http://waitbutwhy.com/2015/01/artificial-intelligence-revolution-1.html(16)
16. Steven Sinofsky, Supporting sensors in Windows 8, 2012. HTML.URL: http://blogs.msdn.com/b/b8/archive/2012/01/24/supporting-sensors-in-windows-8.aspx(18)
17. Vernor Vinge. "Vernor Vinge on the Singularity". San Diego State University. Retrieved 11 April 2013(19)

S. A. Aliev, P. Ribarski,

THE INTERNET OF THINGS AND ITS APPLICATION IN VIRTUAL ECOSYSTEMS

Sunay A. Aliev, Plamen Ribarski

Email: sunay.aliev@yahoo.com; p_ribarski@abv.bg

Abstract: *This article aims to provide reference points by which the integration of new communication standard 5g and growing interest and deployment of IoT from a number of leading IT companies in the field of computer information systems. The research visualize challenges architecture and integration of the two fields. Global use of a web adopted platforms is a new perception and different quality of use. Access to mobile internet becomes completely essential to carry out communication and activities of different types. Through the collaboration of 5g mobile standard and Internet of Things will create flexible work practices for everyone around the world. Growing mobile access to the Internet, cloud-based services, and big data analytics are allowing anyone, anywhere to leverage "big wisdom" – a whole new kind of globally connected & shared knowledge base.*

Keywords: *5G, IoT, internet of things, mobile, communications, integration, challenges, architecture, integration, collaboration, systems, fields, flexible, access, landscape.*

ИНТЕРНЕТ НА НЕЩАТА И ПРИЛОЖЕНИЕТО МУ ВЪВ ВИРТУАЛНИТЕ ЕКОСИСТЕМИ

Сунай А. Алиев, Пламен Рибарски

Email: sunay.aliev@yahoo.com, p_ribarski@abv.bg

Въведение

Краят на XX век и началото на XXI век са белязани с редица фундаментални промени, свързани с развитието на информационните технологии, появата на Интернет и преминаването към икономики, базирани на знания. Свидетели сме на явления като дигиталната революция и глобализацията. Информацията става ключов ресурс за всяка една страна, била тя положителна или отрицателна. Използването и манипулирането ѝ са в известна степен начин на представяне на реалността от технологични устройства, която ни заобикаля. Устройства, които са част от нашето ежедневие, начин на поведение и разбиране. С темповете на развитие и комерсиализиране на иновациите е възможно хората сами по себе си да се превърнат не само в потребители на технологията, но и част от самата нея, т.е. посредници между устройствата и устройства сами по себе си – биологични компютри.

Същност на проблема

[23] навлизането на облачните услуги се откри възможност за разширяването на една нова индустрия, отново част от дигиталната революция – Интернет на нещата (IoT-Internet of Things). Концептуално тези две технологии са коренно различни. Разполагат с напълно различни парадигми и начини на имплементиране. Според [5, 6] неоспорим факт е, че водещи компании като Microsoft, Intel, Apple, Google, Huawei, Amazon и т.н. (табл. 1) инвестират изключително големи финансови ресурси в изграждането и функционирането на модел, който интегрира облачните

услуги с интернет на нещата като провежда една двупосочна колаборация между тях. От своя страна е посочено в [7], че технологични гиганти като Qualcomm, Arm Holdings, AMD т.н. (табл. 2) също се борят за на пазара в отдела на микропроцесорите, които са ключът към управлението на устройствата от ново поколение. В резултат на настъпващите промени се създава вазимосвързана екосистема на интернет на нещата, поддръжката на обекти, мрежи, сензори, микропроцесори, машини, концетратори на данни и програми с високо ниво на изкуствен интелект.

Таблица №1

Име на компания	**Абревиатура**	**Отдел**
AMAZON WEB SERVICES	*AMZN*	Интернет на нещата приложим към облачните услуги – платформени или софтуерни
AT&T	*AT&T*	Интернет на нещата приложим към мрежови компоненти и оборудване
AXEDA	*XEDA*	Интернет на нещата приложим към облачни услуги – базирани на софтуерни колекции и анализиратори на данни, генерирани от сензори и други устройства
DELL	*DELL*	Интернет на нещата приложим към ентърпрайз технологии
GE	*GE*	Интернет на нещата приложим към софтуерна платформа, която интегрира машинно генерирани данни с традиционни и облачни бази данни
GOOGLE	*GOOG*	Интернет на нещата приложим към ежедневни дейности в реални среди – домашни, административни, корпоративни и производствени
HP	*HP*	Интернет на нещата приложим към изграждането на споделени връзки от по-високо ниво в рутер и суитч устройства
IBM	*IBM*	Интернет на нещата приложим към M2M комуникации
INTEL	*INTC*	Интернет на нещата приложим към осигуряване сигурност на потребителя и данните, с които той оперира
MICROSOFT	*MS*	Интернет на нещата приложим към ежедневни бизнес дейности
FACEBOOK	*FB*	Интернет на нещата приложим към създаването на приложения от софтуерни компани
ORACLE	*ORACLE*	Интернет на нещата приложим към управлението на бази от данни
SAP	*SAP*	Интернет на нещата приложим към платформа за управление на мобилни приложения
QUALCOMM	*QCOM*	Интернет на нещата приложим към платформи с отворен код

Водещи производители на микропроцесорна техника за IoT устройства

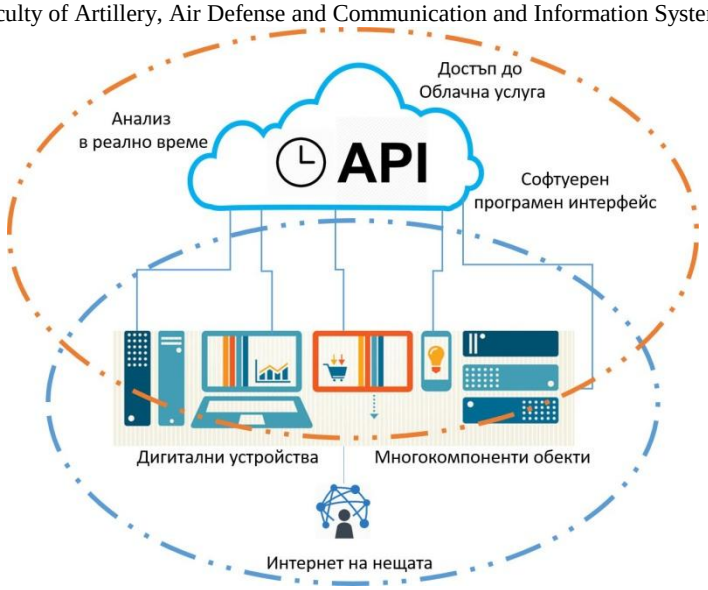
Таблица №2

Производител	Абревиатура	Отдел
QUALCOMM	*QCOM*	Микропроцесорна техника за (IoT – интернет на нещата) устройства
ARM HOLDINGS	*ARMH*	Микропроцесорна техника за (IoT – интернет на нещата) устройства
INTEL	*INTC*	Микропроцесорна техника за (IoT – интернет на нещата) устройства
AMD	*AMD*	Микропроцесорна техника за (IoT – интернет на нещата) устройства
RED HAT	*RHT*	Микропроцесорна техника за (IoT – интернет на нещата) устройства
SIERRA WIRELESS	*Swir*	Микропроцесорна техника за (iot – интернет на нещата) устройства
CISCO	*CSCO*	Микропроцесорна техника за (IoT – интернет на нещата) устройства
GOOGLE	*GOOG*	Микропроцесорна техника за (IoT – интернет на нещата) устройства
APPLE	*APPL*	Микропроцесорна техника за (IoT – интернет на нещата) устройства
IBM	*IBM*	Микропроцесорна техника за (IoT – интернет на нещата) устройства

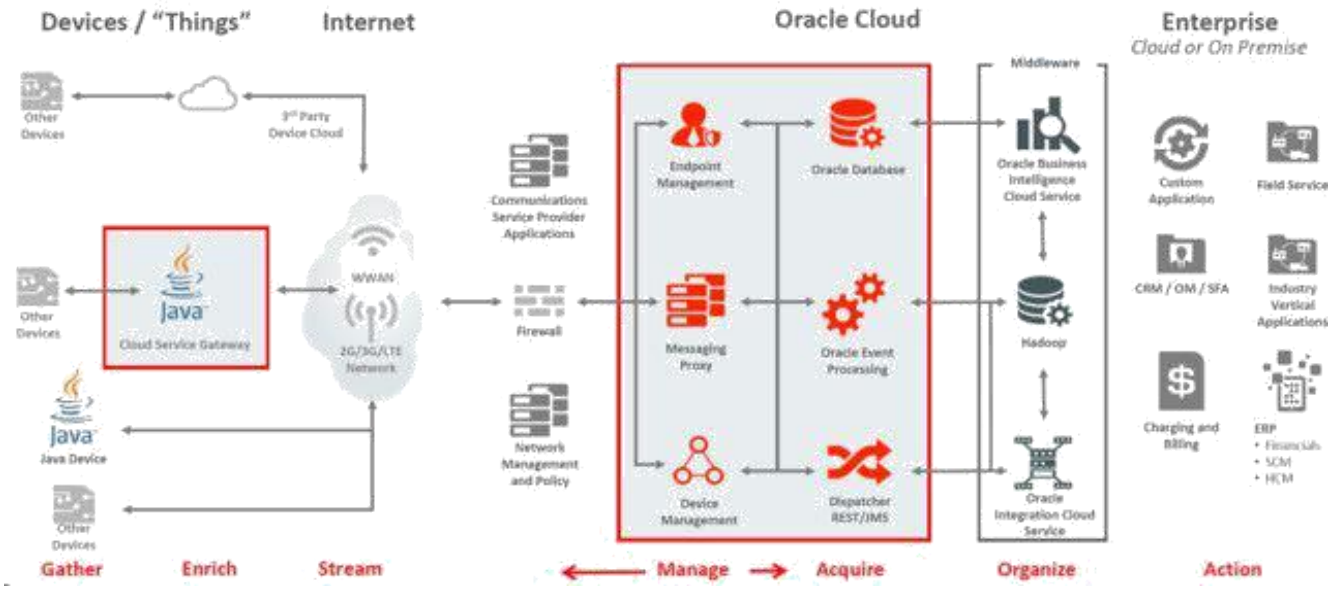
Водещи производители на микропроцесорна техника за IoT устройства

Теоретична постановка

След като облачните услуги вече са актуални и част от ежедневието ни, стана ясно, че е налице необходимостта от сближаване им с интернет на нещата. Тази интеграция между двете технологии (фигура №1), показва на информационното технологично общество единствено и само, че технологията е поема в правилната посока. Симбиозата между двете е необратима и е следващото стъпало към по-доброто потребление и използване на облачните услуги. Вследствие на което се стига до извода, че трябва този модел и парадигми да се съобразят и еволюират до етап на използване на зелена енергия и енергия от възобновяеми източници. Причината за това е използването на голяма хетерогенна разпределена сензорна мрежа, огромен брой сензорни потоци. Друг начин е да има паралелно използване на облачните услуги от интернет на нещата. Тези облачни структури могат значително да увеличат изчислителната мощност на продуктите базирани на модела – интернет на нещата и комуникацията между тях. Според [8] на фигура №2 може да се види до колко високо е заложен принципът на хибридност в зависимост от колаборацията между двете технологии.



Фигура №1



Фигура №2

Проблеми със сигурността

След разглежданите модели на интеграция и колаборация на двете технологии възниква може би най-важният въпрос – Какво е положението със сигурността в цялостния процес? В [5] се твърди, че с развитието на технологията сигурността ще е ключов фактор в използването на интернет на нещата. Всички устройства ще бъдат уязвими сами по себе си от към злонамерени атаки. Атаки, които са проблем и при осигуряването на защитата в облачните услуги. Всички устройства разполагат с уникални идентификатори и могат да предават информация и данни по мрежата. Трафикът е активен нон-стоп. В следствие на което комуникацията идваща от облачните устройства и услуги е използван принципът M2M (машина-към-машина), интелигентните енергийни мрежи и автоматизацията им. В (табл. №3) от [1, 2, 3, 4, 5] се посочват основните видове облачни атаки, които са в сила и за устройствата от тип - интернет на нещата. Друг фактор са несигурните и не до там сложни потребителски пароли, които самите потребители задават при употребата на апликациите, които са обвързани с устройства. Това ги прави лесни мишени за атака, извличане и манипулиране на лична, конфиденциална информация. По този начин достъпът и работата на приложенията се нарушава и устройствата могат да бъдат използвани по всички възможни начини с цел незаконни намерения.

Таблица №3

Име на атаката	Засегнати зони
DENIAL OF SERVICE	Хардуер IAAS, PAAS структури
CLOUD MALWARE INJECTION	Облачни инфраструктури
SIDE CHANNEL ATTACK	Облачни инфраструктури, мрежови достъп и комуникация
AUTOTHENTICATION ATTACK	Облачни инфраструктури, мрежови достъп и комуникация
MAN IN THE MIDDLE	Облачни инфраструктури, мрежови достъп и комуникация
AUDIO STEGANOGRAPHY	Облачни инфраструктури и мрежови комуникационен достъп
TARGETED SHARED MEMORY	IAAS, PAAS структури
PHISHING	Облачни инфраструктури, мрежови достъп и комуникация
BOTNETS	Облачни инфраструктури, мрежови достъп и комуникация
BACKDOOR CHANNEL ATTACK	Хардуер, IAAS, PAAS структури
FLOODING ATTACK	Облачни инфраструктури, мрежови достъп и комуникация
TRACEBACK	Облачни инфраструктури, мрежови достъп и комуникация
DATA STEALING PROBLEM	Облачни инфраструктури, мрежови достъп и комуникация
THEFT OF SERVICE	Облачни инфраструктури, мрежови достъп и комуникация
PORT SCANNING	Облачни инфраструктури, мрежови достъп и комуникация
ATTACK ON VIRTUALIZATION STORAGE ALLOCATION AND	Облачни инфраструктури, мрежови достъп и комуникация
MULTITENACY	Облачни инфраструктури, мрежови достъп и комуникация

От направеното проучване може да достигнем до следния извод. Интернет на нещата, изглежда, че може да бъде следващото голямо нещо в областта на технологиите. В [6] се посочва фактът, че сме в ерата на индустрия за един трилион долара, индустрия с милиарди долари от капиталови инвестиции се инвестират в нея. Мрежови устройства в дома, офиса, както и вградени в инфраструктурата и производството ще направят света по-ефективен и по-добро икономически място. Както потребителите, така и производителите ще се възползват от по-голямата автоматизация, по-доброто събиране на информация и анализирането и, интуитивен потребителски интерфейс и дизайн. Кибер сигурност е фундаментът, който трябва да подсигури облачните услуги и интернет на нещата. Трябва да ги приоритизира като модели и подмодели. [9] Твърди, че е възможно е и таргетиране на уязвитите точки с цел предефиниране на приоритетите на сигурност, които действат сега в момента. Намесват се и фактори от рода на – коя операционна система използват нашите устройства, кои платформи и кои софтуерни услуги. Аспект, който малко потребители обмислят за важен. Ако производителят на съответната операционна система е допуснал грешки и оставил вратички образно казано за достъп и манипулиране на самата система и данните, които се съхраняват в нея – това я прави опасна за потребителя и за устройствата, с които тя си комуникира както и с облачните услуги, с които оперира. От своя страна пък това води до дос-

тъп и към останалите устройства, които са част от йерархията и структурата на облачните услуги и интернет на нещата.

Заключение

Докато този потенциал е на практика неограничен, има много притеснения около личния живот, сигурността и заплахата от хакери или злонамерени действия. И все пак, ако това е следващото голямо нещо, има редица компании, които инвеститорите могат да считат, освен за създатели на устройствата, но и за отговорни лица по пътя на имплементиране на сигурност и надеждност, при нормално потребление от страна на протребители. Те са крайната точка на действие и въздействие, и имат нужда от предоставена сигурност когато оперират с облачните услуги и интернет на нещата.

References:

1. Chappell, D. (August 2008). A short introduction to cloud platforms: An enterprise-oriented view.San Francisco, CA: Chappel and Associates.
2. Hutchinson, C., & Ward, J. (March/April 2009). Navigation the next-generation application architecture. IEEE ITPro, 18–22.
3. Borko Furht, A. E. (2010). Handbook of cloud computing. New York : Springer Science+Business Media.
4. Hemke M., Ubuntu Unleashed 2015 Edition: Covering 14.10 and 15.04, SAMS, Pearson Education.
5. Kanniga Devi and S. Sujan, ”A survey on application of cloudsim toolkit in cloud computing”,International journal of innovative research in science, engineering and technology, vol. 3, issue 6 pp. 13146-13153, June 2014
6. Cloud Standards Customer Council (н.д.). Извлечено от Cloud Standards Customer Counci: http://www.cloud-council.org/ (последно посетен на 09.10.2018)
7. Interoute. (н.д.). What is IaaS? Извлечено от Interoute:http://www.interoute.com/what-iaas (последно посетен на 18.10.2018)
8. Technopedia. (н.д.). Security as a Service (SecaaS or SaaS). Извлечено от Technopedia: https://www.techopedia.com/definition/26746/security-as-a service-secaas-saas(последно посетен на 15.10.2018)
9. Interoute. (н.д.). What is a Hybrid Cloud? Извлечено отInteroute: http://www.interoute.com/cloud-article/what-hybrid-cloud (последно посетен на 10.10.2018)

A COMPARATIVE ANALYSIS OF DIGITAL SIGNATURE CRYPTOGRAPHIC SYSTEMS

Anastasiya A. Dimitrova

Национален военен университет "В. Левски", Факултет „Артилерия, ПВО и КИС", гр. Шумен, докторант в катедра „Компютърни системи и технологии", anidimitrova3005@abv.bg

Abstract: *The document looks at the technologies and algorithms for encrypting information. There is research of some of the most commonly used digital signature algorithms. A comparative analysis of cryptographic systems for digital electronic signature was performed.*

Keywords: *Digital Signature Algorithm (DSA), Eliptic Curve Cryptography (ECC), Elliptic Curve Discrete Logarithm Problem (ECDLP), Elliptic Curve Digital Signature Algorithm (ECDSA), Rivest, Shamir и Adleman (RSA).*

СРАВНИТЕЛЕН АНАЛИЗ НА КРИПТОГРАФСКИ СИСТЕМИ ЗА ЦИФРОВ ЕЛЕКТРОНЕН ПОДПИС

Анастасия А. Димитрова

I. УВОД

Особена актуалност в последните години придоби проблемът за гарантиране на авторството и сигурността на комуникациите в отворени системи [2, 9, 10]. Значимостта му произлиза от изискванията за получаване на точна и достоверна информация за изпратеното съобщение, неговия подател и получател, при условия на канали за връзка с възможност за подслушване и преднамерени шумове, организирани от престъпни и терористични групировки. При електронната комуникация липсва сигурността на непосредствения контакт с бизнес партньора, като електронните съобщения преминават през много посредници, управляващи своите комуникационни системи по различни комуникационни протоколи, някои от които несигурни. Това изисква повишаване на ефективността на криптографските системи, за да се гарантира, че някой не е прочел или подменил съдържанието на предаваното съобщение.

В наши дни проблемът се решава с използване на механизма на цифровия електронен подпис. По въпроса съществуват множество научни публикации за повишаване на ефективността на асиметричните криптографски системи чрез използването на елиптични криви. Въпреки това, в тази област съществуват голям брой въпроси, които не са изследвани с необходимата изчерпателност. Необходимо е систематизиране на научните методи в областта, които да са оригинални и практически приложими в съвременните комуникационни и информационни системи.

В доклада първо са анализирани основните криптографски примитиви, осигуряващи услугите за информационна сигурност. След това са разгледани асиметричните криптографски системи базирани на елиптични криви, направен е сравнителен анализ на алгоритмите за цифров подпис.

II. ИНФОРМАЦИОННА СИГУРНОСТ

1. Технологии, осигуряващи услугите за информационна сигурност

Основните технологии, осигуряващи услугите за информационна сигурност, са криптиране на данните, хеширане, автентификация и цифров подпис.

Криптиране (шифриране) е математическа процедура за промяна на данните от форма на четливост в друг, неподлежащ на разчитане, вид. Обратното преобразуване на информацията в първоначалния й вид е дешифриране. За целта се използват математически алгоритми, като се цели да се осъществи безопасно съхранение или предаване на данни по незащитен информационен канал.

Технологиите за криптиране на информация могат да предоставят следните услуги [3]:

- Конфиденциалност, която прави информацията неразбираема за неоторизирани потребители.
- Цялостност на данните, която предоставя доказателство, че информацията не е била променена по неразрешен начин, докато тя се създава, предава или съхранява.
- Автентификация, чрез която се проверява самоличността на потребителя или системата, която създава информацията.
- Оторизация, при която след доказване на самоличността, на обекта се предоставя ключ или парола, която ще му позволи достъп до определени ресурси.
- Недопускане на отхвърляне, което гарантира, че подателят не може да отрече изпращането на съобщението.

2. Основни криптографски примитиви

Симетрични алгоритми за криптиране

Симетричните алгоритми за криптиране (Symmetric Encryption) използват един и същ таен ключ (Secret Key) и криптографски алгоритъм, за да шифрират и дешифрират съобщенията.

При този алгоритъм за шифриране и дешифриране на информацията, подателят и получателят разполагат с един и същи ключ, за използването, на който са се договорили преди началото на комуникацията. Ако ключът не е компрометиран, то при декодирането на шифрованата информация автоматично се извършва идентификация на подателя, тъй като само той, освен получателя, разполага със съответния ключ. Подателят и получателят са единствените физически лица, които имат достъп до секретните ключове и при компрометиране на системата, те са единствените, които носят отговорност. Проблемът, който е актуален и при други криптографски системи, е въпроса свързан с безопасното разпространение на симетричните (секретни) ключове. Алгоритмите за симетрично криптиране използват ключове с малка дължина и позволяват бързото шифроване на относително големи по обем информационни масиви.

В съвременния свят алгоритмите за криптиране се подлагат постоянно на анализ от специалисти от целия свят, за да се утвърдят като „добри" алгоритми. Процесът на криптоанализ се концентрира върху разбиването на ключовете, чрез които е извършено криптирането. Съществува зависимост между алгоритъма за криптиране и дължината на използваните ключове за този алгоритъм, които предлагат определена „сигурност" на криптирането. Тази сигурност се измерва в брой години, които трябва да работят компютърни системи с определена изчислителна мощност, за да разбият ключа. С всеки изминат ден изчислителната мощност на компютрите се увеличава, а паралелните компютърни системи предлагат все повече паралелно работещи процесори, които биха могли да се използват за разбиване на ключовете. Ето защо сигурността на криптиране е относителна и зависи от наличната в момента изчислителна мощност, която може да се използва за разбиване на ключовете.

Асиметрични алгоритми за криптиране

Асиметричните алгоритми за криптиране (Asymmetric Key Algorithms) използва двойка различни ключове за криптиране и декриптиране на текста. Двата ключа са свързани математически. Асиметричното криптиране често се нарича криптиране с публичен ключ (Public Key Encryption). За общуване на две страни са необходими две различни, но свързани стойности за ключовете: публичен и частен.

При този метод на криптиране ключовете за шифриране и дешифриране на информацията са различни, макар и да се генерират на едно и също място. Един от ключовете е общодостъпен (публичен), а другият се съхранява в съответствие с условия, гарантиращи неговата конфиденциалност. Макар и двата ключа да позволяват шифриране и дешифриране на информацията, криптираната с единия от тях може да бъде декриптирана само с другия. Всяка асиметрична криптографска система се явява обект на атака по метода на пробата и грешката, което налага използването на ключове с по-голяма дължина, от тези в симетричните, при гарантиране на еквивалентно ниво на защита. Това неминуемо довежда до повишаване на изискванията към използвания изчислителен ресурс.

Асиметричните ключове са уязвими за атаки и поради факта, че са по-трудно заменими от симетричните. Ако атакуващият получи достъп до секретен асиметричен ключ, то ще бъде компрометирана не само текущата, но и всички последващи комуникации.

Хеш функции

Хеш функцията (Hash Function) представлява резултатът от еднопосочно математическо изчисление, което приема съобщение с произволна дължина и връща код с фиксирана дължина. Резултатът с фиксирана дължина се нарича хеш (Hash) или отпечатък на оригиналното входно съобщение (Message Digest). Алгоритъмът се нарича „еднопосочен", защото не може да се реверсира резултата, за да се възстанови оригиналното съобщение. За да бъде приложима в криптографията хеш функцията трябва да притежава следните свойства:

- Функцията да бъде постоянна, т.е. един и същи входен аргумент трябва да води до един и същи резултат;
- Функцията трябва да бъде еднопосочна (необратима);
- Резултатът от функцията трябва да бъде случаен, за да се предотврати разбирането на началното съобщение;
- Резултатът от функцията трябва да бъде уникален, т.е трябва да е почти невъзможно да се открият две съобщения, водещи до един и същ представител на съобщение.

Хеш функциите обикновено се използват за проверка на целостта на съобщенията. Промяна само на един символ в оригиналното съобщение, би променила голям брой от битовете в хеш кода [3].

В таблица 1 са представени най-често използваните криптографски алгоритми и предоставените от тях услуги за сигурност.

Таблица 1. *Криптографски алгоритми и предоставените от тях услуги*

Алгоритми	**Крипти-ране**	**Цифров подпис**	**Разпределение на ключове**	**Хеш функция**
Симетрични				
DES, 3DES	✓			
AES	✓			
Blowfish	✓			
IDEA	✓			
RC4	✓			
Асиметрични				
RSA	✓	✓	✓	
ECC	✓	✓	✓	
Diffie-Hellman			✓	
El Gamal	✓	✓	✓	
DSA		✓		
LUC	✓	✓	✓	
Knapsack	✓	✓	✓	
Хеширане				

MD2, MD4 и MD5				✓
SHA				✓
HAVAL				✓

III. АСИМЕТРИЧНИ КРИПТОСИСТЕМИ НА БАЗАТА НА ЕЛИПТИЧНИ КРИВИ

1. Сигурност на криптосистемите базирани на елиптични криви

Всяка криптосистема се основава на трудна математическа задача, която е невъзможно да се реши с наличните технически изчислителни средства. Проблемът с решаването на дискретния логаритъм е в основата за сигурността на много криптосистеми включително и тези с елиптични криви. Сигурността на ранните криптосистеми с публичен ключ се основава на факта, че е трудно да се разложи на прости множители голямо число, съставено от два или повече големи прости множители. По-специално, сигурността на криптосистемите базирани на елиптични криви се основава на трудността на проблема с дискретния логаритъм при елиптични криви ECDLP (Elliptic Curve Discrete Logarithm Problem). Сложността на решението на дадения проблем се дължи на ресурсно изискващите операции събиране и удвояване на точки. При асиметричните криптосистеми базирани на елиптични криви се приема, че намирането на дискретен логаритъм на случаен елемент от елипсовидна крива по отношение на публично известна базова точка е неосъществимо. Сигурността на криптосистемите с елиптични криви зависи от възможността да се изчисли задачата за умножение на две точки и невъзможността да се изчисли множителя при дадени точки на оригинала и на техния продукт получен при умножението.

Основното предимство, което предоставят асиметричните криптосистеми с елиптични криви, е по-малкия размер на ключа, което от своя страна намалява изискванията към ресурсите за неговото съхранение и предаване. Следователно групата криптосистеми, основани на елиптични криви, може да осигури същото ниво на сигурността, гарантирано от RSA базирана криптографска система, но при по-къс ключ. Например, 256-битов публичен ключ при алгоритъм с елиптична крива гарантира сигурност еднаква с тази на 3072-битов RSA публичен ключ.

Американската агенция за национална сигурност NSA (National Security Agency) през 2010 г. одобри използването на елиптични криви за криптографски цели, като позволява приложението им за защита на информация, класифицирана като строго секретна с 384-битови ключове.

Най-бързият известен алгоритъм за решаване на ECDLP проблема е Po алгоритъма на Полард. Това е алгоритъм с експоненциално време, което определя по-малките препоръчителни дължини на ключовете при криптосистеми с елиптични криви при осигуряване на еднакво ниво на сигурност. Препоръчваните дължини на ключовете от NIST са представени в таблица 2 [7].

Таблица 2. *Препоръчвани дължини на ключовете от NIST*

Симетрични алгоритми [bits]	**RSA и DH [bits]**	**ECC [bits]**
56	512	112
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

Криптосистемите на базата на елиптични криви получават все по-голямо разпространение по-скоро като алтернатива, а не като заместител на RSA системите. Те имат няколко предимства, особено при използването в устройства с ограничени ресурси като маломощни процесори и/или малко памет.

Основните области на приложение на криптосистемите базирани на елиптични криви са:

- мобилна търговия (m-commerce) – WAP, клетъчни телефони, джобни компютри;

- смарт-карти (например Europay, Mastercard и Visa (EMV));
- схеми за генериране на двойка ключове използващи дискретен логаритъм [6]
- споразумение при обмяна на ключове използвани във финансови услуги [5].

В криптосистемите на базата на елиптични криви могат да се идентифицират следните проблеми:

- реалната сигурност на тези системи не е напълно изследвана;
- трудност при генерирането на подходящи криви;
- несъвместимост с другите криптографски системи с открит ключ;
- необходимост от лицензиране и патентоване;
- относително бавни при проверка на електронния цифров подпис [1].

Въпреки тези проблеми криптографията базирана на елиптични криви ECC (Eliptic Curve Cryptography) предоставя математически примитиви с публичен ключ, които използват много по-къси дължини на ключа в сравнение с RSA базираните криптосистеми и тези на алгоритъма на цифров подпис базиран на Gold Diffie-Hellman (DH) алгоритъма. Това е решаващо предимство за вградените устройства, в които мощността, обемът памет и изчислителната мощност обикновено са ограничени. По този начин много приложения преминават към ECC, тъй като изискванията за сигурност се увеличават заедно с ограничаване на използваните ресурси в устройствата [4].

IV. СРАВНЕНИЕ МЕЖДУ АЛГОРИТМИТЕ ЗА ЦИФРОВ ПОДПИС

Сигурността играе важна роля в съвременното виртуално общество. От изключително значение е въпроса да се осигури целостта на предаваните данни, като е важно всички важни данни да бъдат подписани от техния собственик. Цифровият подпис осигурява средство за проверка на целостта на данните, като едновременно с това предоставя сигурност в получателя, че данните са били изпратени от подателя. Основните алгоритми за цифрови подписи, които се използват днес, са алгоритъма на Rivest, Shamir и Adleman (RSA) и Elliptic Curve Digital Signature Algorithm (ECDSA).

1. RSA алгоритъм

Алгоритъмът RSA е разработен в Масачузетския технологичен институт (MIT) през 1977 година от Рон Ривест, Ади Шамир и Леонард Адлеман. Сигурността на RSA алгоритъма се основава на генерирането на големи числа, което означава, че по-дълга битова последователност осигурява по-голяма защита. RSA се използва за криптиране/декриптиране на данни и също има способността да подписва и/или да проверява целостта на пакетите данни. RSA не изисква използването на конкретна хеш функция, така че сигурността на цифровия подпис и криптирането зависи отчасти и от избора на хеш функцията, използвана за изчисляване на подписа.

3. ECDSA

Алгоритъмът за цифров подпис базиран на елиптични криви ECDSA е аналог на алгоритъма за цифров подпис DSA (Digital Signature Algorithm), но е базиран на използването на елиптични криви. ECDSA е разработен през 1985 г. от Нийл Коблиц и Виктор Милър. Схемите ECDSA осигуряват същата функционалност като RSA схемите, включително подпис и/или проверка на подписани пакети. Ограничените по мощност среди, като вградените системи, нямат ресурси да изпълнят 1024-битов RSA алгоритъм, докато позволяват реализирането на 192-битов ECDSA. Размерите на ключовете за ECDSA варира от 163 до 571 бита и 1024 до 15360 бита за алгоритми за RSA [8].

Таблица 2 представя препоръчителните дължини на използваните ключове за RSA и ECDSA алгоритмите в съвременните системи за цифров подпис.

Таблица 2. Еквивалентни дължини на ключове за RSA и ECDSA

RSA дължина на ключа (битове)	ECDSA дължина на ключа (бита)
1024	192
2048	256

От таблицата може да се направи изводът, че ECDSA изисква значително по-малък размер на ключовете от RSA за осигуряване на едно и също ниво на сигурност, като предлага по-бързи изчисления и по-малко място за съхранение. Следователно, ECDSA е идеален за ограничени среди, като таблети, смарт телефони, RFID системи и датчици.

V. ЗАКЛЮЧЕНИЕ

RSA и ECDSA са основните алгоритми за цифров подпис доказали своята ефективност срещу съвременните кибератаки, които се характеризират с относително приемлива скорост на криптиране и декриптиране на данните. Алгоритъмът ECDSA поддържа същото ниво на сигурност като RSA алгоритъма при по-малки дължини на използваните ключове и същевременно с това осигурява по-бързи изчисления при по-ниска консумация и по-малък обем памет. В допълнение ECDSA може да генерира ключове с по-висока скорост от RSA при сравними по дължина ключове.

Предимствата на алгоритъма ECDSA спрямо другите криптографски системи за цифров подпис са:

1. Осигурява по-голяма сигурност с по-малки размери на ключовете.
2. Предоставя ефективни и компактни приложения за реализация на криптографски примитиви в чипове с ограничени ресурси.
3. Поради по-малкия размер на чиповете, се намалява количеството отделена топлина и се намалява тяхната консумация.
4. Най-често е подходящ за устройства с малка изчислителна мощност и по-малко памет.
5. Осигурява по-лесни хардуерни реализации.

По-малките размери на ключа при ECDSA алгоритъма позволяват използването на криптографски примитиви осигуряващи конфиденциалност на предаваните данни, проверка на тяхната цялостност и по-бързо генериране на цифрови подписи в ограничени изчислителни устройства, като вградени системи, таблети, смарт телефони, RFID системи, датчици и IoT модули.

References :

1. Ташева Ж. Н. Информационни технологии за сигурност, Издателски комплекс на НВУ „Васил Левски", ISBN 978-954-753-189-5, 2013, 155 с.
2. Ташева Ж. Н., Р. А. Богданов, Анонимна система за комуникации в киберпространството, използваща протокола TOR, Сборник научни трудове от научна конференция 2014 „Защитата на личните данни в контекста на националната сигурност", Факултет „Артилерия, ПВО и КИС", стр. 259-266, ISBN 978-954-9681-49-9.
3. Ташева Ж. Н., Р. А. Богданов, Технологични решения за информационна сигурност, Издателство на НВУ „В. Левски", 2012, 110 с.
4. Verneuil V., Elliptic curve cryptography and security of embedded devices. Diss. Université de Bordeaux, 2012.
5. ANSI X9.63-2011 (R2017) Public Key Cryptography For The Financial Services Industry - Key Agreement And Key Transport Using Elliptic Curve Cryptography. 2017.
6. Barker El., Chen L., Roginsky A., Smid M., NIST Special Publication 800-56A, Revision 2. Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, 2018, Avaible from https://nvlpubs.nist.gov/nistpubs/ SpecialPublications/NIST.SP.800-56Ar2.pdf

7. Barker El., NIST Special Publication 800-57 Part 1 Revision 4 Recommendation for Key Management Part 1: General, 2016, Avaible from: http://dx.doi.org/10.6028/NIST.SP.800-57pt1r4
8. Levy Sh., Performance and Security of ECDSA, Avaible from https://pdfs.semanticscholar.org/7b20/33159cc8ef7f50619b1592eeea639e2807a3.pdf
9. Nikolov L., Slavyanov Kr., On the contemporary cybersecurity threats, International Scientific Journal Security & Future, Vol. 1 (2017), Issue 3, p. 111-113, ISSN 2535-0668, Avaible from https://stumejournals.com/journals/confsec/2017/3/111
10. Stoyanova V, Possibilities for the application of social networks in transmission of secret information, International Scientific Conference CONFSEC ISSN print 2603-2945, ISSN online 2603-2953, year 1, ISSUE 2(2), 2017, Avaible from http://confsec.eu/sbornik/1-2017.pdf

Sht. R. Stoyanova,

BLOCKCHAINS AND SMART CONTRACTS FOR THE INTERNET OF THINGS

Shtiliyana R. Stoyanova

National military university „Vasil Levski" , Veliko Tyrnovo

Abstract: *Blockchains allow us to have a distributed peer-to-peer network where non-trusting members can interact with each other without a trusted intermediary, in a verifiable manner. We also point out certain issues that should be considered before the deployment of a blockchain network in an IoT: from transactional privacy to the expected value of the digitized assets traded on the network.*

Keywords*: Blockchain, distributed systems, internet of things.*

БЛОК-ВЕРИГИ ТЕХНОЛОГИЯ И УМНИ ДОГОВОРИ, ПОДПОМАГАЩИ „ИНТЕРНЕТ НА НЕЩАТА"

Щилияна Р. Стоянова

Национален военен университет "Васил Левски", ф-т „Общовойскови", гр. Велико Търново

1. Въведение

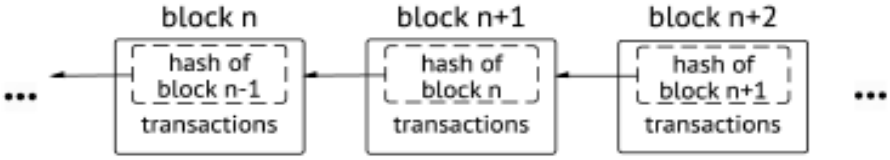
Блок-вериги технологията все по-често привлича интереса на търговските дружества в различни сфери: от финансова [1] и здравни грижи [2, 3], комуникационни услуги [4], недвижими имоти [5, 6] и държавния сектор [7]. Причината за огромният интерес е чрез използването на блокови вериги , приложенията, които преди това са се изпълнявали само чрез доверен посредник, работят по децентрализиран начин, без да е необходима външна намеса за постигане на същата функционалност със същата степен на сигурност. Това просто не е било възможно преди.

Интелигентни договори - самостоятелно изпълняващи се скриптове, намиращи се в блоковите вериги, като тези концепции позволяват точна, безотказна и автоматизирана работа. Това трябва да направи блоковите вериги примамливи за работещите изследователи и разработчици в сферата "Интернет на нещата" (IoT).

Цел на този доклад е да се даде подробно описание за това как блоковете и интелигентни договори работят, за да се идентифицират плюсовете и минусите, които въвеждането им носи в система. Докладът е структуриран в няколко раздела, обхващаши следната тематика: какво е блок-верига, как действа мрежата на блоковата верига, как интелигентните договори позволяват да се ограничи взаимодействието между операторите на дадена мрежа, и как могат да бъдат създадени и автоматизирани, разглежда как IoT и блоковите вериги могат да се използват заедно, да се подчертаят съществуващите приложения на IoT-on-the-blockchain и да се разгледат някои проблеми, които могат да възникнат по време разработването на блоковите вериги, представят се някои решения за преодоляване на проблемите, които могат да възникнат.

Описание на блок-вериги технологията

Блок-веригата, която е разпределена база от данни се използва и споделя между членовете на мрежата. Тя е въведена с Bitcoin [8] за избягване на проблема с двойното плащане на такси [9].



Фигура 1. Блок схема на блог верига технологията

Всеки блок във веригата (виж фиг. 1) съдържа списък на транзакциите и хеш към предишния блок. Изключението от това е първият блок на верига (не е изобразен), наречен генезис, който е общ за всички клиенти в блокова верига и няма родител. Блоковете от веригата могат да стоят сами за себе си и не е необходима криптомерност [11]. Блок-веригата се представлява като дневник, чиито записи са включени в блокове с времеви марки. Всеки блок се идентифицира чрез криптографския си хеш. Всеки блок препраща към хеш блока, който е пред него. Това създава връзка между блоковете, като по този начин създава верига от блокове или блок-верига - виж фигура 1. Всеки възел с достъп до този преди него, обратно свързан списък с блокове, може да го прочете и да разбере каква е състоянието на данните [10], които се разменят в мрежата.

По-лесно може да се разбере как функционира блок-верига, когато се изследват как функционира блоково верижната мрежа. Това е набор от възли (клиенти), които работят на една и съща блок-верига чрез копието, което всеки един държи. Един възел може по принцип да действа като входна точка за няколко различни потребители на блок-верига в мрежата, но за простота се предполага, че всеки потребител осъществява транзакции в мрежата чрез свой собствен възел. Тези възли образуват мрежа от тип peer-to-peer, където:

1) Потребителите взаимодействат с блоковата верига чрез двойка частни/публични ключове [9]. Те използват своя частен ключ, за да подписват собствените си транзакции и са адресируеми в мрежата чрез своя публичен ключ. Използването на асиметрична криптография води до установяване на автентичността, целостта и репутацията в мрежата. Всяка подписана транзакция се излъчва от потребителския възел на хонорарите си с едно хоп;

2) Съседните блокове гарантират, че тази входяща транзакция е валидна, преди да я предаде по-нататък; невалидните транзакции се изхвърлят. В крайна сметка тази транзакция се разпространява в цялата мрежа;

3) Транзакциите, които са събрани и валидирани от мрежата чрез горепосочения процес по време на договорен времеви интервал, се подреждат и записват в блок за кандидатстване с временна стойност. Това е процес се нарича mining (миниране). Минният възел излъчва този блок обратно в мрежата. Изборът на минния възел и съдържанието на блока зависят от консенсусния механизъм, който мрежата използва;

4) Възлите потвърждават, че предложеният блок (а) съдържа валидни транзакции и (б) препратките чрез хеша на правилния предходен блок в тяхната верига. Ако случаят е такъв, те добавят блока към тяхната верига и прилагат транзакциите, които съдържа, за да актуализират своя световен изглед. Ако това не е така, предложеният блок се изхвърля. Това означава край на кръга.

Това е повтарящ се процес. Когато се говори за потвърждаване на транзакцията в стъпка 2, естественият въпрос е: какво представлява валидна транзакция?

В една блок-верижна мрежа това, което има по същество, е набор от недоверчиви клиенти, които споделят база данни без доверен посредник [11]. Тайната за предаване на конфиденциални съобщения е от огромно значение[13]. За да се предотврати избухването на хаос в тази разпределена среда и за да се подпомогне мрежата да достигне общ глобален поглед към света (т.е. постигане на консенсус), всяка блокова верига трябва да установи определени правила, които всяка транзакция на базата данни трябва да спазва. Тези правила, които зависят от приложението, се програмират във всеки клиент на блок-веригата, който след това ги използва, за да реши дали дадена входяща транзакция е валидна и съответно дали тя трябва да бъде препредавана в мрежата или не. В опростения модел на "споделена база данни", която се представя тук, нека се приеме, че всеки ред от базата данни е присвоен на публичен ключ (или адрес), който контролира кой може

да го редактира. След това валидна транзакция е тази, която се опитва да промени реда, за който има съответният подпис.

Когато всеки възел в мрежата следва стъпките, изброени по-горе, споделената върху която работи, се превръща в автентичен и запечатан във времето запис за дейността на мрежата [10]. Трябва да се обърне внимание, че възлите не трябва да се доверяват на други, което създава термина "доверие"; вместо това доверието се постига като възникваща собственост от взаимодействията на различните участници в системата.

Установяване на консенсус по мрежата

Възлите трябва да се договорят за транзакциите и за реда, по който са изброени в номинирания блок. В противен случай отделните копия на блоковата верига ще се различават; възлите ще имат различен изглед на състоянието на света и мрежата повече няма да може да поддържа уникалната хронология (т.е. блок-верига), освен ако този възел не бъде решен.

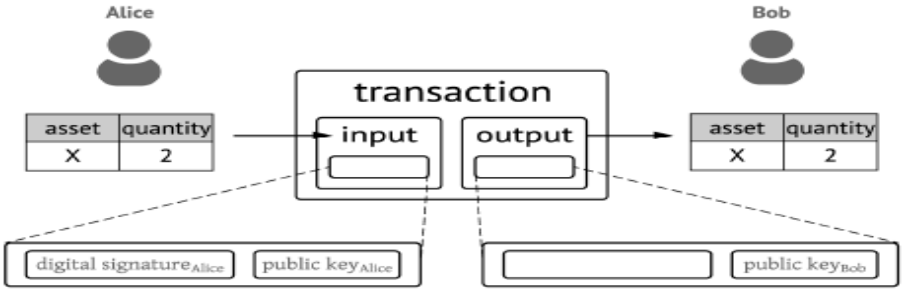
За целта е необходим разпределен, съгласуван механизъм във всяка блокова верига, за да се постигне това. Видът на използван механизъм за консенсус зависи от типа блоково верижна мрежа и вектора на атаката, която мрежовият оператор приема.

Доказателство за участие (Proof-of-stake-PoS) е алтернатива на доказателството за работа, което изисква много по-малко изчисления на процесора за добива. В PoS шансовете за извличане на следващия блок възли са пропорционални на равновесието на този възел. Схемите на PoS имат свои собствени силни и слаби страни , а действителните реализации се доказват да бъдат доста по сложни .

Практическата византийна толерантност (Practical Byzantine Fault Tolerance-PBFT) е такъв алгоритъм. Той предлага решение на проблема с византийските генерали , който работи в асинхронни среди като интернет. (Bitcoin чрез механизма, описан по-горе, също така предлага практическо решение на същия проблем.). Той включва трифазен протокол и понятието "първичен" (лидер) възел, който действа като блок миньор; лидерът може да бъде променен от останалата част от мрежата чрез т.нар. "механизъм за гласуване", ако се срине или ако има произволно поведение (византийски грешки). PBFT работи при предположението, че по-малко от една трета от възлите са дефектни (f), поради което казват, че тя изисква най-малко $3f + 1$ възли.

Трансфер на цифрови активи по блокова верига

За да покажете как работи прехвърлянето на активи, най-добре е да се разгледа опростен пример от банковия свят. Пример е централната база данни на банката, която следи общите баланси на всеки клиент. По същество се разглеждат таблица с три колони: "тип актив", "собственик" ("контрагент") и "количество" ("сума"). Например, ред в тази таблица с "USD", "Alice", "10" идентифицира Алис с десет депозирани в тази банка. Боб има сметка в същата банка с $ 0 в него. Когато Алис прехвърля $ 2 на акаунта на Боб, "количество" на долара / Alice (типа на актива / собственика) се актуализира до $ 8, а този на USD / Bob сега прочита $ 2. Актив ($ 2 USD) или по-скоро цифровото представяне на този актив е прехвърлен между две предприятия чрез преобразуване на съответните редове в базата данни. Това прехвърляне на цифрови токенизирани активи може да бъде постигнато лесно и по криптографски сигурен начин, като се използва блоково верижната мрежа, която използва транзакционния модел Bitcoin. Ако се помисли отново за модела на база данни, споделяна от недоверчиви клиенти в безпристрастна среда, както в раздел II-A. Всеки ред носи същите имена, както в банковия пример по-горе, с изключение на това, че собственикът вече държи публичния ключ на потребителя, на когото е разрешено да редактира реда. Да се приеме, че базата данни показва, че Алис притежава 10 единици от актив X. (Ще се види как е установена тази истина, т.е. как тези активи са били генерирани скоро). Това е ред в тази база данни, който носи публичния ключ на Алис в " колоната "собственик" и стойностите "X" и "10" съответно в колоните "тип актив" и "количество". Да се предположи, че Алис знае публичния ключ на Боб. Как Алис прехвърля 2 единици от X на Боб? Тя подписва транзакция, която променя реда й, намалява стойността на X по 2 и създава нов ред, чийто "собственик" е настроен на публичния ключ на Bob и чиито "тип актив" и "стойност" "elds" са настроени съответно на "X" и "2".



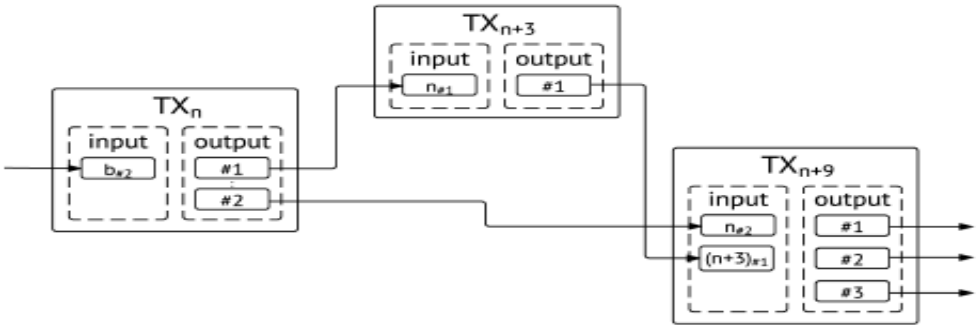
Фигура 2. Транзакция, която прехвърля взетия актив (X) от Алис на Боб. Алис влиза в системата и създава забрана срещу публичния ключ на Боб, така че само Боб може да го похарчи.

Алис прехвърли 2 единици от X на Боб, като създаде нов ред с тази информация и му го даде; Фигура 2. (В действителност, транзакцията на Алис също е изтрила собствения си ред, е създала нов ред, определен за един от нейните публични ключове, и е преместен с останалите 8 единици на X, които тя държи там. Това се прави, за да се контролира конкуренцията. За предотвратяване на конфликти между операциите за едновременно записване в системата; редове не се променят, вместо това те се изтриват и се създават нови редове с актуализираните стойности [11].) Новият баланс на актива "X" на Боб може да бъде изчислен чрез обединяване на всички редове в базата данни, съответстващи на неговите публични ключове и чийто "тип актив" е зададен на "X". Същото важи и за Алис.

Трябва да се бърне внимание, че една транзакция може да адресира до няколко съществуващи редове вместо само една, т.е. прехвърляне на активи, разпръснати в базата данни, стига да е правилно подписана за достъп до тях. Тези съществуващи, все още изтрити редове се наричат неизразходвани транзакции (UTXO) в Bitcoin; те са създадени от по-ранни транзакции в системата. UTXO, които транзакцията консумира, се наричат транзакционни входове; UTXO, които транзакцията създава, се наричат транзакционни изходи.

Транзакцията след това основно изтрива набор от редове (UTXO) и създава набор от нови редове (UTXO) в базата данни (виж фигура 3 за пример). Един очевиден въпрос от горното описание е: как да се генерират активи и да се въвеждат във веригата.

Преди да се стигне до състоянието на Алис с 10 единици от X, тези 10 единици на X трябва да дойдат от някъде.



Фигура 3. Транзакция на n изразходва втората UTXO

Транзакцията представена на фиг. 3. е транзакцията b (b # 2) и генерира два нови изхода (n # 1 и n # 2), изразходвани от транзакции n+3 и n+9 съответно. Подобен процес се отнася за всяка транзакция в мрежата. Транзакциите са следователно свързани помежду си и дават възможност за лесно проследяване на пробите. Отговорът е, че зависи от мрежата и нейната цел. Обикновено упълномощеният възел използва специален тип транзакция за въвеждане на актив (или нови дялове на актива) в мрежата.

Ако се приеме, например, частна блок-верижна мрежа между Алис, Боб и Карол. Карол определя това чрез използване на MultiChain , платформа за блокиране, която възлага разрешения

(може да се свърже с мрежата, да осъществи транзакция в мрежата, може да издаде в мрежата) на публични ключове. Карол конфигурира мрежата така, че нейният публичен ключ да може да издава активи в мрежата. Тя кани Алис и Боб да се присъединят; и двамата са наясно с способността на Карол да издава активи на веригата. Всичките имат двойка частни и публични ключове. Карол подава подписана транзакция, която генерира 10 единици от X. Възлите в мрежата считат тази сделка за валидна, тъй като нейният публичен ключ е разрешен по подходящ начин. След това Керол прехвърля тези новосъздадени единици от X на Алис, което ни води до Алис с 10 единици от X.

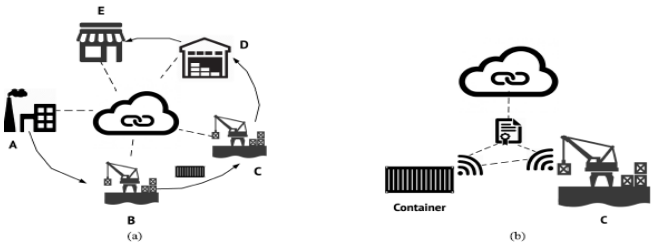
В случая на Bitcoin в мрежата се въвеждат нови битови монети с всеки изваден блок: Минният възел включва така наречената транзакция в блока от транзакции, които излъчва в мрежата. Това прехвърляне на монети няма входни данни и не възнаграждава добива на възел с предварително определено (от мрежата) количество bitcoins.

Блокови вериги и IoT

Създателите правят възможно преминаването от децентрализирана архитектура към все по-разширяващата се система на „Интернет на нещата“ да бъде устойчива. От страна на производителя, настоящият централизиран модел има високи разходи за поддръжка, заради разпространението на софтуерните актуализации до милиони устройства в продължение на години, след като са били прекъснати дълго. От страна на потребителя има оправдано липса на доверие в устройствата, които "стоят" във фонов режим и необходимостта от подходът "сигурност чрез прозрачност". Тези проблеми могат да бъдат разрешени с широко обхватен модел "peer-to-peer", който може да работи по прозрачен начин и да разпространява сигурно данните; авторите правилно посочват, че този модел е елегантно решение на този проблем.

Полезността на блоковете в настройка на IoT не спира там. Ако се обмисли типичния пример за веригата за доставки, който се използва, за да се подчертае стойността на блок-верига: контейнер, който напуска производствения обект (точка А), се транспортира по железопътния транспорт до съседния порт (точка Б) (точка В), се транспортира отново до съоръженията на дистрибутора (точка Г), докато окончателно достигне мястото на търговеца на дребно (точка Е). Този процес включва няколко заинтересовани страни и проверки по пътя, всички от които са показани на фигура 4а. Всеки участник обикновено поддържа собствена база данни, за да следи актива, който те актуализират въз основа на входящите данни от другите страни по веригата.

Мрежата, която използват блоковите вериги, която е създадена за проследяване на този актив, би означавала, че сега има една обща база данни, в която да се следи, къде се получават актуализации с криптографска проверка, да се разпространява автоматично по мрежата и да се създаде опровержима следа от информация. Например (Фигура 4b), когато превозвачът стигне до крайния порт, той изпраща подписано съобщение към предварително определен и договорен интелигентен договор, за да позволи на всеки от веригата да знае, че контейнерът е в точка В. Тъй като транзакцията е подписана, той действа криптографски надежден прием на корабната компания че контейнерът е достигнал до пристанището на местоназначението. Приемникът в пристанището изпраща до същия интелигентен договор, за да потвърди, че той е в притежание на контейнера.



Фигура 4. Пример за проследяване на активите, използващи интелигентни договори и интернет.

На фигура 4а контейнерът напуска производственото предприятие (А), достига до съседния порт (В) по железопътния транспорт, транспортира до целевия порт (С) и след това до съоръженията на дистрибутора (D) мястото на търговеца на дребно (Е). На фигура 4b се съсредоточаваме

върху етапа B-C. Носителят на контейнер изпълнява ръкостискане с дока на целевия порт (C), за да потвърди, че контейнерът е доставен до очакваното място. След като завърши ръкостискането, той подава към интелигентен договор, за да подпише доставката. Портът за местоназначение следва заедно, за да потвърди получаването. Ако възелът в C не публикува в договора в приемлив срок, превозвачът ще знае и може да започне разследване на място.

Някои проблеми и техните решения.

Могат да се идентифицират няколко трудности, които може да възникнат при експериментирането на разработчиците на системи IoT с блокови вериги или при внедряване на техни устройства в IoT, които да участват в блок-верижна мрежа. В сравнение с правилно конфигурирана централизирана база данни, блоковите вериги като цяло ще доведат до слабо представяне при по-ниска производителност на обработка на транзакциите и по-големи закаснения. Този проблем е особено изразен в обществените мрежи, където се извършват proof-of-work механизми (доказателствени механизми), въпреки че нови предложения, като Bitcoin-NG, показват обещаващи резултати. Като цяло, тази технология е цената, която трябва да се плати за безпристрастна децентрализация и устойчивост.

Поддържането на поверителността на блоковата верига е сложен проблем. Всяко участващо устройство е идентифицирано от техния публичен ключ (или неговия хеш). Участникът не е необходимо да знае ключовете на всички останали; той просто се нуждае от ключа на неговата транзакция. Въпреки това всички сделки в блоковите вериги се случват публично. Чрез анализирането на тези данни, заинтересованата страна може да идентифицира модели и да създава връзки между адресите и в крайна сметка да разкрие действителните идентичности.

Няколко начина да се смекчи, но не напълно да се реши този въпрос, ако поверителността е важна за разглежданото приложение са:

1) Нека даденото устройство да използва нов ключ за всяка транзакция или да използва различен ключ за всеки контрагент, за да се направи разпознаването на шаблона различно.

2) В случай на частни блокчета, препоръчително е да не се използва една и съща блок-верига за всички транзакции, ако друг участник може да получи конкурентно предимство чрез проследяване на активността на устройството ви.

Правната приложимост на интелигентните договори е ограничена. Работата се върши, за да бъдат техническите правила за интелигентните договори правно приложими и задължителни за всички страни. Начин за увеличаване на шансовете за юридическа приложимост е да се включи позоваване на действителния договор в реалния свят в интелигентния договор и обратно. Допирателна към това е въпросът за очакваната стойност на активи, които са осуетени. Блоковете се използват за търговия с тези символи, защото са свързани с някаква стойност. В блок-верига, която не поддържа интелигентни договори, двойната интеграция не е опция.

Една блокова верига може да се нуждае и от следните механизми за допълване на нейната функционалности трябва да бъдат децентрализирани, за да не се нарушава характерът на мрежата:

- DNS услуга, която съдържа насоки към ресурси. Blockstack , например предоставя такава услуга в мрежата Bitcoin. Потребител изпраща подходящо кодирана транзакция в блока за Bitcoin, за да създаде блокове на Blockchain, които филтрират блок-веригата за последователности от данни, съответстващи на валидни блокиращи транзакции, и ги използват, за да променят съответно базата данни с имена.
- Сигурна комуникация и обмяна на информация. Както се отбеляза по-горе, съобщенията в блок-веригата се четат от всеки участник в мрежата. Всеки път, когато е необходим частен комуникационен канал, вместо това трябва да се използва протокол като телешоу или Whisper. Потребностите на мрежата за споделяне на файлове могат да бъдат адресирани чрез конфигурирана P2P система като IPFS .

V. ЗАКЛЮЧЕНИЯ

Комбинацията от блокови вериги и „интернет на нещата“ може да бъде доста мощна. Блоковите вериги осигуряват гъвкави, наистина разпределени системи от типът "peer-to-peer" и безопасна комуникация между трети лица дори и без наличие на доверие. Интелигентните договори

позволяват да се автоматизират сложни многоетапни процеси. Устройствата от „интернет на нещата“ са точките на контакт с физическия свят. Когато всички те са комбинирани се автоматизира отнемащите много време дейности по нови и уникални начини, постигане на криптографска защита, както и спестяването на значителни разходи и време в процеса. Смята се, че понататъшното интегриране на блоковите вериги в областта на „интернет на нещата“ ще доведе до значими трансформации в различни индустрии, с което да се въведат нови бизнес модели и като с това да се преразгледат как се прилагат съществуващите системи и процеси.

References:

[1] А. Мизрахи. (2015). Записване на собственост на базата на блокови вериги: http://chromaway.com/papers/A-blockchainbased-property-registry.pdf

[2] Г. Грийнспан. (2015). Прекратяване на дебатите срещу Bitcoin или Blockchain.

[3] http://www.multichain.com/blog/2015/07/bitcoin-vsblockchain-debate/

[4] Д. Кели и А. Уилямс. (2016 г.). Система за търгуване с облигации на четиридесет големи банки. HTTP: http://www.nytimes.com/reuters/2016/03/02/business/02reuters-bankingblockchain-bonds.html

[5] Д. Опара. (2016 г.). 3 начина, по които блоковите вериги ще променят пазарът за недвижими имоти. http://techcrunch.com/2016/02/06/3-ways-that-blockchain-will-change-the-real-estate-market/

[6] Двойно харчене - Bitcoin WiKi, https://bg.bitcoin.it/wiki/double-spending.

[7] Документация на Eris Industries – Blockchains. https://docs.erisindustries.com/explainers/blockchains/

[8] И. Кар. (2016 г.). Естонските граждани скоро ще имат най-защитената база от данни в света и доказателство за това са здравни записи. http://qz.com/628889/this-eastern-european-country-is-moving-its-health-recordsto-the-blockchain/

[9] М. Уолпорт, Технология на разпределените книги: отвъд блоковата верига ",UK С. Лейси. (2016 г.). Енергийната блокада: Как Bitcoin може да бъде катализатор за разпределената мрежа. http: //www.greentechmedia. com/articles/read/the-energy-blockchain-could-bitcoin-be-a-catalyst-forthe-distributed-gr

[10] С. Накамото. (2008 г.). Bitcoin: Система за електронна парична система от тип "Peer-to-Peer". https://bitcoin.org/bitcoin.pdf

[11] W. Suberg. (2015). Най-новото партньорство на Factom поема здравеопазването на САЩ.

[12] Стоянова В., Възможности за изпращане на тайни съобщения през Интернет, CIO бр. 7, 2015,

D. M. Koleva,

FACTORS CONCERNING THE PRACTICE OF INFORMATION SECURITY IN TRAINERS

Doroteya M. Koleva

National military university "Vasil Levski"

***Abstract**: 192 valid questionnaires from elementary students of South Korea were collected, and then these were analyzed using structural equation modelling. The results show that information ethics and information security awareness affect information security practice of elementary students. And the research findings confirmed that the information security vocabulary test was useful to assess security awareness levels for elementary students. This new approach can assist management to plan and evaluate information security education. This study presents herein implications and suggestions for further research.*

***Keywords**: Information Security Education, Information Ethics, Information Security Awareness, Information Security Practic*

ФАКТОРИ, ЗАСЯГАЩИ ПРАКТИКАТА НА ИНФОРМАЦИОННАТА СИГУРНОСТ ПРИ ОБУЧАЕМИТЕ

Доротея М. Колева

Национален военен университет „ Васил Левски"
Факултет: „Общовойскови"

Зависимостта от участието на човека и човешкото поведение за защита на информационните активи налага обучение, за да се осъзнае ролята и отговорностите по отношение на информационната сигурност. Обучението по информационна сигурност е необходимо дори и за ученици от началното училище. Според статистиката на киберпрестъпленията в Южна Корея например престъплението в кибернетичното пространство възлиза на 16,4% [11]. В днешно време се превръща в сериозен социален проблем. Все по-важно е да се гарантира сигурността на данните. Въпреки това, образованието за информационна сигурност в училищата не е имало добри резултати.

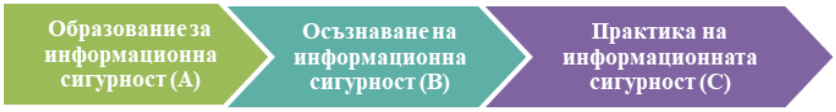
Първата цел е да се разработи и тества въпросник, който да оцени осведомеността на учениците от началното училище за проблемите на информационната етика и информационната сигурност. Втората цел може да се получат фактори, засягащи осведомеността за сигурността на информацията, определени от нивото на осъзнаване.

Образование и информационна сигурност

Обучението по информационна сигурност непрекъснато се развива. Изследвания на съдържанието на образователната информация за информационната сигурност са обобщени в Таблица 1. В много изследвания има разнообразно съдържание на качеството на уеб сайтове, чрез изследвания на съществуващи проучвания, измеренията на образованието в областта на информацията се основават на три измерения, които се отнасят до етиката на информацията, информационната сигурност и практиката на информационната сигурност.

Когнитивна поведенческа теория

Когнитивната поведенческа теория, която включва теорията и поведението и според [1] изпъква един лесно запомнящ модел, който обяснява връзката между мисленето и емоцията. Тя се нарича модел ABC: A = Активиращо събитие, B = Вярвания, мисли, C = Емоционални и поведенчески последици. Това проучване е предполагало, че образованието за информационна сигурност като активиращо събитие ще подобри осведомеността за сигурността на информацията като вяра и мисли, а след това предшестващите събития предизвикват поведенчески резултати в резултат на практики за информационна сигурност.



Фигура 1. A-B-C модел

Проучван модел и хипотези

Наличието на информационна дисфункция се дължи на липсата на етична осведоменост по отношение на защитата на информацията и за да се отговори на това, е необходимо високо ниво на етичен ум, за защита на информацията, постигнато чрез обучение. [2] изследва ролята на информираността за сигурността на информацията и възприемането на справедливостта при спазването на политиката за сигурност на информацията. В [13] се предлага един различен поглед на информационната сигурност и по скоро аспекта й за предаване на конфиденциална информация. Усъвършенстването на информационната сигурност и възприеманата справедливост окажат влияние върху отношението към спазването на правилата и регламентите за организационната сигурност. Горният аргумент води до следната хипотеза:

- H1. Познаването на етиката в информацията има положителен ефект върху практиката на информационната сигурност.

[4] разглежда в предишни проучвания и показват, че връзката между осведомеността за сигурността на информацията и практиката на информационната сигурност е директна. [9] потвърждават, че дейностите за информационната сигурност се подобряват след провеждането на обучение и кампания за повишаване на осведомеността относно сигурността на информацията.

- H2. Усещането за информационна сигурност има положителен ефект върху практиката на информационната сигурност.

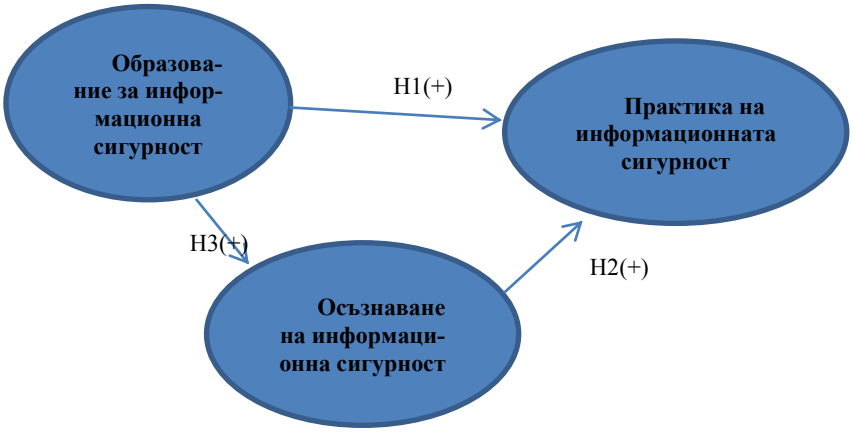
[12] твърди, че въпросът за вземането на решения по етиката на информацията не е нищо ново или конвенционално, признава се като комбинация от двете. Описани sa етичните въпроси на информационното общество, като например социалните последици, професионалната етика, интелектуалната собственост, неприкосновеността на личния живот, компютърната престъпност и злоупотребите, етиката на хакерите, отговорност и приобщаване.

Структура	Понятие	Литература					
		Обучителна програма в Южна Корея [11]	Сеулска Столична служба по образование [10]	Обучение в Съединени американски щати [5]	Английска учебна програма [6]	Обучение в Индия [7]	Брой
Информационна етика	Кибертормоз	√	√	√		√	6
	Злонамерено мнение		√			√	4
	Интернет зависимостта	√	√	√		√	5
	Незаконни онлайн сайтове		√		√		5
	Незаконни файлове за	√	√	√	√		7

	изтегляне						
Информаци-онна сигурност	Хакерство		√	√	√		5
	Вируси	√	√		√		6
	Спам	√				√	5
	Фишинг		√				1
	Криптиране	√					1
	Разкриване на лична инфор-мация	√	√				4
	Резидентна регистрация (поверител-ност)						1
	Инструмент за поверителност						1
	Използване на оригинална програма		√	√	√		6
Практика на информаци-онната сигурност	Инсталиране и използване на антивирусна програма						1
	Управление на парола на сайт					√	3
	Предотвратя-ване на пове-рителността	√	√				4
	Потвърждение законите за поверителност			√			2
	Информаци-онна сигур-ност за онлайн комуникация				√	√	3
	Докладване за спам	√				√	5

Таблица 1. Използвана литература за анализ

[11] заявява, че информационната култура, политика и норми, заедно с формите на информацията, могат да повлияят на нагласите и отношението на инженерите по обработка на информацията и в крайна сметка как те да третират информацията. Горният аргумент води до следната хипотеза:



Фигура 2. Изследователски модел

Участниците

За да се гарантира точността на изследването, представителната извадка е добре да бъде група от ученици от началното училище над 10-годишна възраст. Препоръчително е за проучването да се използват над 100 обучаеми.

Въпросник

След разширен литературен преглед е разработен въпросник. Той се състои от термини разбираеми при разглеждането на езиковото ниво на учениците от началното училище. Въпросник се състои от четири раздела. Първата секция събира обща информация за пола, възрастта и жилищна област. Втората част се отнася до възприемането за етиката на информацията. Третата секция се отнася до възприемането за сигурността на информацията. Четвъртият раздел е за възприемането относно практиката на информационната сигурност. Скалата със седем точки се използва за изявления от втората секция, вариращи от "1" до "7".

Метод за анализ

Поради ограниченията на такива проучвателни подходи, като регресионния анализ, се възприема потвърждаващ подход, използващ частични най-малки квадрати (PLS) като метод за анализ. PLS е широко използван в теоретичното тестване или потвърждаване. Също така е подходящ подход за изследване дали връзките могат или не могат да съществуват и по този начин се предлагат за по-късно тестване [10]. Използват PLS-Graph версия 3.0 за анализ на измервателните и структурните модели.

Модел на измерване

За да се валидира този модел за измерване, проучването предприема оценки за валидност на съдържание, дискриминация и конвергентна валидност. Валидността на съдържанието на проучването е установена от съществуващата литература. Дискриминационна валидност на инструмента е оценена чрез изследване на комбинирана нестабилност на мерките и отклонението е извлечено. Въпреки, че много проучвания, използващи PLS използват 0,5 като индикация за нестабилност на мерките, оценката като 0,7 е препоръчителната стойност за нестабилност [3]. Както е показано в Таблица 3, тези комбинирани стойности на нестабилност варират от 0.625 до 0.638 - над допустимите нива. За дисперсията, извлечена от мерките, оценката от 0,5 означава приемливост[10]. Таблица 3 показва, че вариацията превишава препоръчаните стойности. Освен оценката на валидността на измервателния модел, това изследване извършва проверка за мултиколинеарност сред независимите променливи. От направения анализ в Таблица 4 се показва установената корелациите между детерминантите на удовлетвореността на потребителите. Най-високата корелация, 0.731, съществува между удобство и удовлетворение. Останалите корелации варират от 0.791 до 0.798. Тези корелации показват, че мултиколинеарността е добра в предложения модел.

Структурен модел

За генериране на t-стойноста и стандартните грешки се използва процедура за зареждане[3]. От гледна точка на добротата на показателите за годност, осведомеността за информационната етика, осведомеността за сигурността на информацията и практиката на информационната сигурност представляват 57% от разминаването. Тези резултати осигуряват силна подкрепа за позиционираните взаимоотношения между осведомеността относно етиката на информацията, осведомеността за сигурността на информацията и практиката на информационната сигурност. Таблица 5 показва, че резултатите от хипотезата се одобряват. Резултатите показват, че осведомеността относно етиката в информацията и осведомеността за сигурността на информацията засягат практиката на информационната сигурност на студенти и осведомеността за етиката на информацията засягат осведомеността за сигурността на информацията.

Структура	Факторно зареждане	t Стойност	Композиране на надеждност	AVE	Cronbach's Alpha
Информационна етика 1	0.749	14.684	0.638	0.924	0.904
Информационна етика 2	0.781	15.566			
Информационна сигурност 1	0.853	42.306	.631	0.932	0.915
Информационна сигурност 2	0.798	23.39			
Информационна сигурност 8	0.661	13.716			
Практика на информационната сигурност 1	0.801	24.833	0.625	0.893	0.852
Практика на информационната сигурност 2	0.703	17.278			

Таблица 3. Резултат от анализираните потвърдени фактори

	Практика на информационната сигурност	Информационна сигурност	Информационна етика
Практика на информационната сигурност	(0.798)	0	0
Информационна сигурност	0.691	(0.795)	0
Информационна етика	0.594	0.731	(0.791)

Таблица 4. Корелационна матрица

Хипотеза	Път	Коефицецент	t Стойност	Резултат
H1	Информационна етика -> Практика информационната сигурност	0.191	1.967	Одобрен
H2	Информационна сигурност -> Практика информационната сигурност	0.551	5.561	Одобрен
H3	Информационна етика -> Информационна сигурност	0.731	27.158	Одобрен

Таблица 5. Резултат от тестваните хипотези

Заключение

Това проучване е насочено към обучението по информационна сигурност на студенти. Целта на този доклада е да се проучи, че информационната етика и информационната осведоменост засягат практиката на информационната сигурност на обучаеми. Резултатите показват, че етиката на информацията и осведомеността за сигурността на информацията засягат практиката на информационната сигурност на учениците. Резултатите от анализа потвърждават, че тестът за речника за информационната сигурност е полезен за оценяване на равнищата на осведоменост за сигурността на учениците. Има някои ограничения в изследването. В бъдещите проучвания изследователската извадка трябва да бъде проектирана по-широко, за да представлява цялото население. Макар че е трудно да се сравнят резултатите, това изследване може да бъде добре насочено към образованието за информационна сигурност, което подобрява информационната етика и информационната сигурност и променя поведението на учениците от началното училище.

References:

[1] Albert E, he revised ABC's of rational-emotive therapy (RET)", Journal of Rational-Emotive and Cognitive-Behavior Therapy 9(3), 129-172 (1991)

[2] Bulgurcu, B., H. Cavusoglu and I. Benbasat, Roles of Information Security Awareness and Perceived Fairness in Information Security Policy Compliance, AMCIS 2009 Proceedings, Paper 419 (2009)

[3] Chin, W.W., The partial least squares approach to structural equation modeling. In: Marcoulides, G.A. (Ed.), Modern Methods for Business Research. Lawrence Erlbaum

[4] Choi, N., D. Kim and A. Whitmore, Knowing is doing, Information Management & Computer Security, 16(5), 484-501 (2008)

[5] CSTA, CSTA K-12 Computer Science Standards (2011)

[6] Department for Education, England, National curriculum in England: Computing programmes of study

[7] Department of Computer Science and Engineering Indian Institute of Technology Bombay, Mumbai, CMC: A Model Computer Science Curriculum for K-12 School (2013)

[8] Education and Information Research Academy of Korea, Primary and secondary information education (2005)

[9] Eminağaoğlu, M., E. Uçar and E. Eren, The positive outcomes of information security awareness training in companies – A case study, Information Security Technical Report, 14(4), 223-229 (2009)

[10] Fornell, C.R. and Lacker, D.F., Two structural equation models with unobservable variables and measurement error. Journal of Marketing Research, 18(1), 39–50 (1981) [11] Grover, S., Lying, deceit, and subterfuge: A model of dishonesty in the workplace, Organization Science, 4(3), 478-495 (1993)

[12] Johnson, D., Computer ethics, Prentice Hall, Inc. (1994)

[13] Стоянова В., Възможности за изпращане на тайни съобщения през Интернет, CIO бр.7, 2015,

http://cio.bg/7294_vazmozhnosti_za_izprashtane_na_tajni_saobshteniya_prez_internet, [accessed June 30, 2018]

S. B. Pavlova, D. V. Velev,

ONE ALGORITHM FOR SPECTANOGRAPHY BASED ON THE SPATIAL AREA

Stanislava Biserova Pavlova, Dian Valentinov Velev

National military university" Vasil Levski"

Abstract: *We construct and implement a new Steganography algorithm based on spatial domain to hide a large amount of information into color BMP image. It utilizes the arrangement of the secret data to compensate distortion, which is called fixed LSBs(Least Significant Bits) substitution methods.*

Keywords*: BMP image; steganography; spatial domain;*

ЕДИН АЛГОРИТЪМ ЗА СТЕГАНОГРАФИЯТА, БАЗИРАН ВЪРХУ ПРОСТРАНСТВЕНАТА ОБЛАСТ

Станислава Бисерова Павлова, Диан Валентинов Велев

Национален военен университет "Васил Левски", Факултет „Общовойскови"

Въведение

Стеганографията е наука за скриване на тайна информация и включва предаване й чрез привидно безобидни файлове. Целта е не само съобщението да бъде скрито, но да бъде предадено без да бъде засечено. Стеганографията поддържа скриване на съобщенията сред огромния обем на интернет трафика, в медийни файлове, където добавянето на тайно съобщение трудно се открива с човешкото око, дори файлът да бъде обстойно прегледан [1].

Внедряването на нови по-ефикасни средства за скриване и защитено предаване на конфиденциална информация, би предотвратило изтичането на данни и чувствителна информация [15]. Стеганографията може да се комбинира с криптография за да се постигне по-добра защита на информацията. Скриване на информация вътре в изображенията е популярна техника в днешно време.

Най-често срещаните методи за извършване на тези промени включват използването на най-младшия значещ бит (LSB least significant bit) разработен от Chandramouli в [2], маскиране, филтриране и трансформации върху изображението на прикриващия обект. В [3] е представен алгоритъм за откриване на LSB стеганография. В [4] авторите изграждат математически рамки, базирани на сложни теоретични възгледи, които търсят границите на стеганографията. Конструкцията на HweeHwa Pang в [5], използва хеш стойност, която се получава от името на файла и паролата и по този начин се открива скритият файл. Този подход се използва с нови модификации. Следващото интересно приложение на стеганографията е разработено в [6], където съдържанието е криптирано с един ключ и може да бъде декриптирано с няколко други клавиша, относителната ентропия между криптиране и един специален ключ за декриптиране съответства към количеството информация. Заради непрекъснатите промени в стеганографията и големите количества информация, с които се разполага се предлага използването на техники за машинно обучение за характеризиране изображенията като подозрителни или не, разработени от [7]. В [8] се използва ентропийна техника за откриване на подходящите области в изображението, където информацията може да бъде вградена с минимално изкривяване. C. Zhang et al. [9] косвено

скрива тайните битове информация заедно с някои избрани графични изображения, базирани на алгоритъм за невронни мрежи, за да се получат битове за шифроване. Този подход се разглежда в доклада. Когато се използва 24-битов цвят от изображение, малко от всеки червен, зелен и син цвят могат да се използват всяка от компоненти. Именно за това могат да се съхраняват общо 3 бита на всеки пиксел. По този начин изображение с размери 800 × 600 пиксела може да съдържа общо количество от 1440000 бита (180000 байта) тайна информация. Така че основната цел на доклада е да се намери решение, как да се вмъкне повече от един бит на всеки байт в един пиксел на прикриващия обект и той да дава резултати като LSB [2], [3].

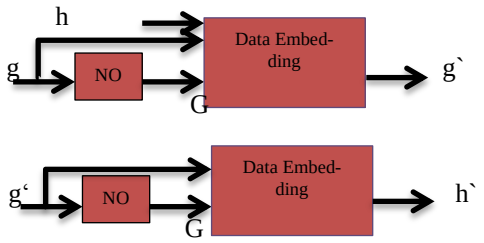
Докладът има за цел да анализира един нов алгоритъм за стеганография, базиран на интелигентна система за скриване на голямо количество от всякакъв вид информация чрез растерно изображение [4], [6] чрез използване максимален брой битове на байт за всеки пиксел. Има два вида атаки, които биха обезпокоили процесът на вграждане на информацията, първият е да се работи срещу визуални атаки [7], [10] - способността на хората неразбираемо да успяват да различът шума и визуални модели, а втората опасност се отнася до работата срещу статистическите атаки [3], [8], [11], [12] .

Стеганографията в изображения, които включват най-младшите битове

В [13] се предлага метод за скриване на данни, който се нарича адаптивен номер на LSB, базирани на човешката визуална система. Те приемат, че тайните данни са под формата на двоични потоци, които могат да компресирани мултимедии, или просто серия от текстове, предаващи съобщения за предаване в хост изображенията. Този метод се основава на човешката визуална система. Сивият цвят промяна стойността на всеки пиксел в изображението на хоста и след вграждането е извън човешкото възприятие. В допълнение към този метод, вградените тайни данни могат да бъдат извлечени без познаване на първоначалния образ. Преди да се разгледа този метод се е използвал друг, който е за вграждане на мултимедийна информация в прикриващо изображение. Тази адаптивност може да бъде създадена като номерата на LSB за вграждане се използват без допълнителни разходи от модифицираната стойност на пикселите. Има функция за картографиране, която е подложена на човешка визуална чувствителност и се използва за постигането на тази цел.

При въвеждане на тази основна функция, **Ng()** е LSB-mapping функция. Тя дава броя на LSBs, които могат да бъдат вградени за всяко едно възможно сиво ниво ***g***. След вграждането се означават с ***g'***, тогава състоянието на за тази адаптация е- ***N()g*** стойностите преди и след промяната на пикселите трябва да остане непроменена. Пример за това е ***Ng***.

На фигура 1, е показана концепцията и като с ***h*** се обозначава вградената тайна информация. Така, според формулата ***N(),*** се слага променлива ***g*** в N() и се получава ***g'***. По този начин се добавят няколко бита. От друга страна ***g*** може да бъде извлечена, когато приемникът използва формула N(), за да получите вградени данни.



Фигура 1. Концепцията за самостоятелен брой на LSB за вграждане и извличане на данни.

i	Интервал	Брой използвани LSBs
		1 бит
0	0~87	2 бита
	88~191	3 бита

	192~255	4 бита

Таблица 1. Брой използвани LSBs

Съгласно функцията LSB-mapping Ng () (1) и оценената $\boldsymbol{k_i}$, определен в Таблица 1, лесно се изчислява колко бита може да се вградят в един пиксел. Резултатът показва, че ако $\boldsymbol{g}$ е поставен между 0 и 87, се използват два LSBs. Може да се заключат три и четири LSBs.

Алгоритмичен подход на стеганографията. Анализиран алгоритъм

Съкращение	Описание
$\mathbf{y_i}$	-тия пиксел на изображението на прикриващ обект, [0,255] yi
N	- Общо пиксели в прикриващия обект
Y_i	-i-тия пиксел на стего изображението, [0,255] yi ∈
b_i	- Скрити данни, bi ∈ [1,0]
S_i	- Променени са тайни данни
k	- Бита на замяната в скриването на данни
m	- Всеки m пиксели наведнъж m $N_m \leq N$
LSB	Най-малък значещ бит
LSB_i	i-ти най-малък значещ бит

Таблица 2. Номенклатура

При този метод се въвежда използвания символ в алгоритъма от таблица 2 с номенклатурата. Алгоритъмът се разделя на три части. Първата част е предварителна обработка; секретни данни $\boldsymbol{b_i}$ трябва да бъдат първоначално модифицирани. Втората част е скриването на данни; заменя се $\boldsymbol{k}$ от LSB на оригиналната стойност на пиксела в сивата скала на първо място. Новата стойност на пискела трябва да е по-малък от оригиналната. Изважда се някаква стойност от $\boldsymbol{y}$. След това допълнително се компенсира променената стойност $\boldsymbol{y_i}$ за подходяща стойност чрез сравняване с отношението между двете модифицирани тайни съобщения $\boldsymbol{s_i}$. След като се премине през тези две части се получава стегообраз. Последната част е свързана с извличането на данни. Когато получателят получи това изображение по открит канал, той може да използва временна стойност като съхранява първите извлечени битове. От предишните части също може напълно да се извлече тайното послание стъпка по стъпка. Методът може да се разгледа на фигура 2.

Изпълнение на алгоритъма

Оценка на качеството на изображението

Може грубо да бъде разделена на две части около оценка на качеството на изображението, което се променя от компресията или скриване на данни. Първият метод директно използва човека с визуална система. Това е просто система за човешко виждане като например корекция на гладката област в изображението. Трудно е обаче най-вече за човешките очи, за да открият малката разлика на две изображения в допустим диапазон. Освен това, усещането за зрението във всеки човек не е същото, така че е трудно да се установи един общ стандарт. Съотношението (PSNR) за измерване на качеството на изображението е друг обективен стандарт за оценка. Формулата е показана по-долу [19]:

(1) $$PSNR = 10 \times \log \frac{255}{MSE}$$

(2) $$\mathrm{MSE} = \frac{1}{m \times n} \quad {}_{i-1}^{m \times n} \; Si - Ci \;\; 2$$

1	0	0	0	0	0	0
1	1	1	0	0	0	1

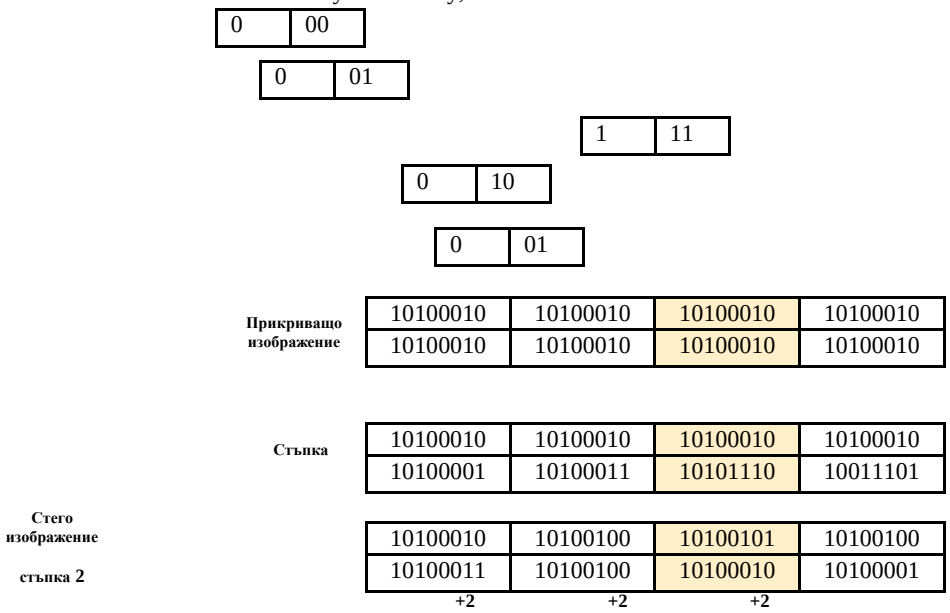
Тайни данни

1	00	0	00	0	00	0
01	1	11	1	10	0	01

Модифицирано съобщение

Pre-processing

1	00



Фигура 2. Пример за скриване на данни при m=8 и k=2

Във формули (1) и (2):

- MSE е средна квадратна грешка на оригинално изображение и модифицирано изображение [19];
- S_i и C_i отделно представят оригиналния пиксел и променения пиксел в същата позиция на изображението;
- m и n са на ширината и височината в изображението.

По този начин по-високият PSNR показва по-добро качество на изображението. Трудно е човешките очи да разграничи разлика между двете изображения, когато PSNR е по - голяма от 30 db. По-високият PSNR не е достатъчен, за да покаже, че качеството на изображението е по-добро като се разглежда в детайли.

Резултати от алгоритъма

В доклада се използва произволно генериран битов поток, който да бъде тайно съобщение [15]. Избрано е едно от четирите класически изображения, наричащо се "F16", което се състи от 512 до 512 пиксела. На фигура 3 са показани оригиналното и стего изображение с k = 3.

(а) Оригинално изображение (б) Стего изображение

Фигура 3. Оригинално и стего изображение с к=3

Капацитетът се определя, като се задържат битове на пиксел. По-високата стойност на k е ниската PSNR, която е показана в таблица 3.

Прикриващо изображение	k	Капацитет	PNSR (m-S)	Капацитет	PNSR (m=16)	Капацитет	PNSR (m=512)
Lena	2	1,75	46,7440	1,875	46,5587	1,996	46,3950

	3	2,625	41,1411	2,8125	40,9261	2,994	40,7452
	4	3,5	35,2325	3,75	35,0138	3,994	34,8128
Baboon	2	1.75	16,7406	1,875	46,5562	1,994	45,3891
	3	2,625	41,1538	2,8125	40,9174	2,994	40,7412
	4	35,2416	35,2416	3,75	35,0043	3,996	34,8033
F16	2	46,7528	46,7528	1,875	46,5627	1,996	46,3653
	3	41,1425	41,1425	2,8125	40,9448	2,994	40,7282
	4	35,2383	35,2383	3,75	35,0235	3,992	34,8119
Pepper	2	46,7402	46,7402	1,875	46,5540	1,996	46,3698
	3	41,1346	41,1346	2,8125	40,9374	2,994	40,7421
	4	35,2418	35,2418	3,75	35,0278	3,992	34,8069

Таблица 3. Резултатите от вграждането на случайното съобщение

В доклада се категоризира методът на фиксиран LSB заместващ метод и след това се сравнява с друг подобен, който е разгледан в таблица 4. За да бъде сравняването максимално актуално [16], m трябва да се зададе като максималната стойност с размер 512* 512. Размерът на тайното послание е по-малко от ***k*** бита, отколкото другите две схеми и стойността на капацитета е почти близо до ***k***.

Прикриващо изображение	k	(m=512*512)	OPAP [3]	LSB
Lena	2	46,38	45,37	44,15
	3	40,72	38,73	37,92
	4	34,81	32,83	31,78
Baboon	2	46,37	44,37	44,15
	3	40,72	38,37	37,92
	4	34,80	32,80	31,86
F16	2	46,37	45,37	44,15
	3	40,72	38,73	37,92
	4	34,80	32,80	31,86
Pepper	2	46,37	45,37	44,15
	3	40,72	38,73	37,89
	4	34,80	32,81	31,85

Таблица 4. Сравнителен анализ на OPAP и LSB

В таблица 4 колоната, обозначена като OPAP [14], предлага метод с оптимален процес на настройка на пикселите; колоната, обозначена с LSB, е прост LSB заместващ метод.От таблицата и според [17], [18] се вижда, че ефективността е по-добра от OPAP и LSB.

Заключение

Стеганографията е ефективен начин за прикриване на информация и скриването й. Настоящият алгоритъм позволява на дадено лице да скрие информацията в друга информация с надеждата, че никой не би помислил да разгледа съдържанието на файла. Алгоритъмът, който е разгледан представлява псевдокод и е възможно да се приложи алгоритъм за стеганография, за да се скрие голямо количество информация в растерно изображение като носител.

Установено е, че настоящият алгоритъм е привлекателен и резултатите, постигнати от него, са ефикасни в областта на вграждане на информация (стеганография). Изпълнени са три вида сравнение: първите две сравняват настоящия алгоритъм в 4 bitmap по размер и добавен шум. Направено е сравнение на PSNR и с други методи. Именно това сравнение показва, че предложеният метод е по-добър от OPAP и LSB методите.

References:

[1] S-tools(http://digitalforensics.champllain.edu/download/s-tools4.zip).

[2] Chandramouli, R. and N. Memon,. "Analysis of LSB based image steganography techniques," Proc. of ICIP, Thessaloniki, Greece, pp. 7-10, Oct. 2001.

[3] Dumitrescu, S., W. Xiaolin and Z. Wang, "Detection of LSB steganography via sample pair analysis," In: LNCS, Springer-Verlag, New York, Vol. 2578/2003, pp: 355–372, 2003.

[4] Ahn, L.V. and N.J. Hopper, "Public-key steganography. In Lecture Notes in Computer Science of Advances in Cryptology," EUROCRYPT 2004, Vol. 3027 / 2004, Springer-Verlag Heidelberg, pp: 323–341, 2004.

[5] Pang, H.H., K.L. Tan and X. Zhou, "Steganographic schemes for file system and b-tree," IEEE Trans. on Knowledge and Data Engineering, Vol. 16, pp.701–713, 2004.

[6] Dobsicek, M., "Extended steganographic system," In: 8th Intl. Student Conf. on Electrical Engineering. FEE CTU. 2004

[7] Mittal, U. and N. Phamdo, "Hybrid digital-analog joint source-channel codes for broadcasting and robust communications," IEEE Trans. On Info. Theory, vol. 48, pp. 1082 –1102, 2002.

[8] Pavan, S., S. Gangadharpalli and V. Sridhar, "Multivariate entropy detector based hybrid image registration algorithm," IEEE Intl. Conf. on Acoustics, Speech and Signal Processing, pp: 18-23, 2005.

[9] C. Zhang, H.W. Guesgen, W.K. Yeap "Neural Based Steganography, Lecture note in computer science Computational Intelligence. Neural Networks," LNAI 3157, pp. 429–435, Springer-Verlag Berlin Heidelberg 2004.

[10] Moulin, P. and J.A. O’Sullivan, "Information-theoretic analysis of information hiding," IEEE Trans. on Info. Theory, vol. 49, pp. 563–593, 2003.

[11] Amin, P., N. Liu and K. Subbalakshmi, "Statistically secure digital Image data hiding," IEEE Multimedia SignalProcessing MMSP05, China, 2005.

[12] Jackson, J., G. Gunsch, R. Claypoole and G. Lamont, "Detecting novel steganography with an anomaly- based strategy," J. Electr. Imag. Vol. 13, 860– 870, 2004.

[13] W.N. Lie and L.C. Chang, “Data hiding in images with adaptive numbers of least significant bits based on the human visual system”. Proc.IEEE Internat. Conf. Image Process.1,286-290,1999.

[14] C.K. Chan and L.M. Cheng, “Hiding data in images by simple LSB substitution”, Pattern Recognition 37,469-474, 2004.

[15] Стоянова В., Възможности за изпращане на тайни съобщения през Интернет, CIОбр.7,2015, http://cio.bg/7294_vazmozhnosti_za_izprashtane_na_tajni_saobshteniya_prez_internet, [accessed June 30, 2018]

[16] C.C.Chang and W.C. Wu, “A steganographic method for hiding secret data using side match vector quantization”, IEICE Trans.Inf.Syst., Vol.E88-D,no.9,pp.21592167, 2005.

[17] ISO/IEC JTC1 CD 11544: Coded representation of picture and audio information-progressive bi-level image compression, 1993.

[18] Y.Q. Shi, Z.Ni, D. Zou, C. Liang and G. Xuan, “Lossless data hiding: fundamentals, algorithms and applications”, IEEE ISCAS 2004.

[19] Stoyanova, Veselka; Tasheva, Zhaneta. RESEARCH OF THE CHARACTERISTICS OF A STEGANOGRAPHY ALGORITHM BASED ON LSB METHOD OF EMBEDDING INFORMATION IN IMAGES, 2015.

SOCIAL SCIENCE

K. M. Markov,

COMMUNICATIONS, DISTRIBUTION AND MANAGEMENT

Krasimir M. Markov

National Military University, "Artillery, Air Defense and CIS" Faculty

Absract: *The importance of communication and distribution for the management of the organization is discussed.*

Keywords: *communication, distribution, management, organization*

КОМУНИКАЦИИ, ОБЩУВАНЕ И МЕНИДЖМЪНТ

Красимир М. Марков

Национален военен университет, Факултет „Артилерия, противовъздушна отбрана и комуникационни и информационни системи"

Терминът „комуникация" има старогръцки произход и означава „обмен", „съобщение", „връзка". В съвременната теория на управлението е прието комуникацията да се разглежда като „процес при който чрез хора, групи, организации и общности, намиращи се във взаимна връзка помежду си, се създава, предава и използва взаимоизгодна информация, която е необходима за организиране на тяхната околна среда" [9].

Комуникацията има своите особености, познаването на които от ръководителя предполага нейната ефективност. По-важните от тези особености са:

- комуникацията е постоянна – в смисъл, че ние общуваме непрекъснато, а освен това дейността на ръководителя е невъзможна без приемането и предаването на информация;
- комуникацията е символична – тя се осъществява с помощта на символи, чиято роля играят думите, цифрите, жестовете, мимиките и т.н.;
- комуникацията е субективна – в нея хората отразяват собствените си знания и опит, в нея се „отличават" и характерологичните особености на личността;
- комуникацията се учи – хората се учат да говорят, пишат, слушат, свирят и т.н., което по същество е усвояване на комуникативни знания и умения;
- комуникацията е двустранен процес – ръководителя не само предава информация, но и подчинените му трябва да я приемат и усвояват;
- комуникацията е договаряне – ръководителят уточнява с подчинените си терминологията и така създава обща сфера на кодиране и декодиране на информацията;
- комуникацията е и култура – тя се основава на определени правила, норми, и принципи на етика в отношенията;
- комуникацията в съвременния свят е невъзможна без технически средства – ръководителят използва посредничеството на техниката (телефони, компютри и т.н.), за да обменя информация с началниците и подчинените си. Без наличието на техниката е невъзможно управлението на организацията;

- комуникацията е самооценка и самоотразяване – тя от една страна е отражение на личните интереси, потребности, очаквания и емоции, а от друга дава възможност на човек да се самооценява и самоосъзнава.

Процесът на комуникациите има своите елементи и етапи на протичане [9]. Елементите на процеса на комуникация са:

Отправител – това е лицето, което предава информацията.

Съобщение – това е самата информация, кодирана в определени символи (думи, знаци, цифри и др.)

Канал – средство за предаване на информацията.

Получател – лицето, което приема (получава) информацията и я интерпретира.

Мениджърът може да играе ролята на отправител или на получател на информацията.

Кои са етапите на комуникационния процес:

Зараждане на идеята – на този етап мениджърът трябва да обмисли за кого е предназначена информацията, как да се отправи съобщението при отчитане на конкретната ситуация и цели.

Кодиране и избор на канал – преди да бъде предадена, всяка информация се кодира. Ако символите са думи, мениджърът трябва да избере най-подходящите, като обмисли и съответната интонация и жестове, така той превръща информацията в съобщение. По-особен вид е писмената информация (доклади, рапорти, заповеди), която има своя логика и правила особено за формализираните документи.

Предаване – става дума за физическо предаване на информацията, което може да се осъществи лично, по телефон или друго средство.

Декодиране – след като информацията е стигнала до получателя, той я декодира. Ако мениджърът е подбрал правилно символите, това означава, че информацията ще бъде декодирана правилно. Това се разбира в процеса на дейността, ако получилият информацията е пристъпил към действия, очаквани от отправящия;

Обратна връзка – необходим елемент в управленческия процес, чрез който става ясно дали комуникацията е осъществена правилно.

В организацията комуникацията е свързващ елемент на управлението, чрез нея мениджърът планира, организира, мотивира, контролира и осъществява лидерските си функции [9]. Един ръководител използва от 50% до 80% от своето реално време за разговори. Това още повече издига ролята на комуникациите.

В литературата по проблема се сочат факти от изследвания, които показват, че 73% от американските, 63% от английските и 85% от японските ръководители считат комуникациите като главно препятствие по пътя към достигане на ефективно управление на техните организации [1], което означава, че ефективно работещи ръководители са тези, които са ефективни в комуникациите.

Какви видове комуникация осъществява мениджърът [10]?

Формални комуникации – това са тези комуникации, които следват организационно-управленската и организационната структура на организациите [9], т.е., те са йерархично ориентирани. Формалните комуникации в организацията се движат в три посоки:

- комуникация „отгоре надолу" – мениджърът може да бъде субект и обект на тази комуникация. Обект, когато приема информация от висшестоящите инстанции, и субект, когато предава информация на подчинените си. Взаимоотношенията в тази комуникация са кодирани в уставите и дори в известна степен са формализовани;
- комуникация „отдолу нагоре" – тук мениджърът също е субект и обект. По отношение на информацията, идваща от подчинените му, той е обект, а субект - при предаване на информация към по-старшите началници;
- комуникация по хоризонтала – осъществява се с равни по длъжност (други мениджъри на подразделения), в нея също мениджърът е субект и обект и тя се подчинява на законите на етиката.

Неформални комуникации – независимо че в организацията съществува строга йерархия, в малките звена, където хората са 8-10, много от формите на комуникация се извършват като не-

формални разговори. В действителност независимо от съществуващите ограничения хората в организацията не могат да бъдат спрени да говорят и обсъждат неща извън чисто служебните, дори и в хода на дейността. В мениджмънта комуникационната мрежа на неформалните комуникации се нарича „лоза". Името идва от времето на гражданската война в САЩ, когато телефонните линии се окачвали по дърветата и висели като лоза [9]. Информацията при нея е устна, при която се обсъжда всичко - и началници, и служба, и приятелки, музика и филми, и т.н. Самата „лоза" бива няколко вида според начина на предаване на информацията:

- едностранна – предава се информацията по верига, като един казва на друг, той на друг и в крайна сметка всички я получават;
- клюка – един казва на всички;
- вероятностна – всеки наслуки казва на друг;
- грозд – някой казва на определени хора.

Независимо от негативното мнение, което мениджърите по принцип имат за неформалната комуникация между подчинените им, тя трябва да се приема като факт, още повече, че неформалната мрежа може да работи и за тях, стига умело да я използват за обратна връзка. При това „лозата" има някои предимства, които мениджърът умело може да използва:

- информацията при нея се предава с по-голяма скорост, отколкото при формалната комуникация (агенция „партенка");
- информацията при нея е сравнително точна. Опитът показва, достоверността й е около 75%;
- има селективност при предаване на информацията;
- има големи възможности за вътрешно развитие и усъвършенстване;
- представлява тип комуникация, в която хората участват с голямо желание и активност.

Особен елемент на комуникацията, отразяващ етичността в системата, е комуникационният климат. Приема се, че той „показва колко и каква информация се създава, предава, приема и използва в организацията" [9]. Факторите, влияещи на комуникационния климат, са разнообразни, но определящи са стилът на мениджъра и наложената етика в комуникацията. В зависимост от особеностите на структурата в управлението на организацията мениджърът може да си служи с два вида стил на комуникация:

- директивен стил – основава се на точни указания и разпореждания, прилага се в крайните фази на организационното сглобяване на структурата и нейните подразделения, когато се предполага, че подчинените вече добре познават и изпълняват задълженията си;
- напътстващ стил – той подобно на директивния си служи с много заповеди, разпореждания и указания, но се прилага в началните етапи на сглобяване на организацията. При него мениджърът разяснява заповедите и разпорежданията, провежда множество лични разговори, с оглед да се убеди правилно ли са разбрани задачите.

Познаването на основите на комуникацията в управлението предполага мениджърът да формира у себе си и определени комуникационни умения отнасящи се най-вече до способността му да говори и слуша. Тези умения се изграждат на база съблюдаването на определени правила [8].

Правила при говоренето:

1. Когато прави забележки, мениджърът трябва да засяга особеностите на поведението, а не личността на подчинения.

2. Повече внимание трябва да обръща на наблюденията, а не на заключенията. Наблюдението е това, което мениджърът е констатирал, заключението е негова лична интерпретация. Оценките трябва да се основават на фактите, а не на субективната им интерпретация.

3. Не бива мениджърът да се изказва с оценки. Този род изказвания се основава на неговата ценностна система и неговите разбирания за добро и зло; правилно и неправилно и т.н. Такива оценки не подпомагат процеса на взаимното разбиране.

4. При разбор на някаква ситуация мениджърът да се старае да търси подходящи примери в съвременния живот (най-добре от живота на организацията), а не от своето минало.

5. Да се опитва да дава колкото е възможно по-малко съвети. По-добре да споделя своите наблюдения, все едно че обменя мисли и информация с партньори.

6. При предаване на някаква информация мениджърът да подбере подходяща ситуация и адекватна форма за предаването й.

Правила за (при) слушане:

1. Внимателно да изслушвате говорещия, за да разберете същността на предаваната информация.

2. Опитайте се да извлечете от думите на говорещия неговата представа за вас.

3. Преразкажете си на ум чутото, това ще ви помогне да разберете дали сте схванали същността на казаното.

4. Покажете на събеседника с вида си, че вие обръщате внимание на това, което ви говори. Можете да вмествате потвърдителни думи или жестове.

В последно време все повече се засилва интересът към психологията на общуването. Интересът се обуславя както от факта, че в съвременното общество с увеличаване на възможностите на средствата за комуникация се натъкваме на неумение да общуваме, така и от изключителното значение на общуването при формирането и на личността, и на организационната структура.

Всъщност ежедневието е система от единици на общуване и дейност съответно „действия" и „операции" за решаване на конкретни задачи. Б. Ломов отбелязва, че дори относително краткото общуване на човек с човека или група хора може да окаже върху психическото развитие на човека (формирането на неговата личност) много по-голямо влияние отколкото продължителното изпълнение на дадена дейност. По принцип акцентирането само върху един от двата елемента на единството – дейност и общуване води до съществени грешки при формирането на умение за общуване. От тези грешки можем да избягаме ако разглеждаме дейността и общуването в по-широк план. Така ще видим, че дейността не е само чист труд, а и общуване в и по повод на този труд, а общуването като форма на човешката активност и начин за изграждане на лични отношения, неминуемо предполага разглеждането му в контекста на дейността на индивида или групата и това е факт с който ръководителите от всички звена и всички структури би следвало да се съобразяват.

Ядрото на личността - нейният „аз", е възможно да разберем изключително в контекста на човешката дейност и при отчитане общуването на индивида с другите хора.

Същност, форми и значение на общуването - има много различни виждания за общуването [по 7]:

Мясищев го определя като взаимодействие между хората в сферата на познавателните процеси, в емоционалната сфера и в сферата на поведението или казано с други думи взаимното им психологическо отражение, тяхното отношение един към друг.

Петровски счита, че общуването е многопланов процес на развитие на контактите между хората, породен от потребностите на съвместната им дейност.

Интересен, но от по-различна гледна точка е възгледът на Бодалев, който въвежда понятието комуникативно ядро на личността, което според него е единство на отражение, отношение и поведение проявявани от индивида при взаимодействие с различни хора и общности, с които той встъпва в контакт.

Паригин дава значително по-широка дефиниция на общуването, като сложен и многостранен процес, който може да бъде в едно и също време и процес на взаимодействие между индивидите, и информационен процес и отношение на хората един към друг, и процес на взаимно разбиране един с друг.

Дж. Мийд определя общуването като процес, при който посредством символи един индивид сигнализира на друг да извърши своята част от съвместната дейност.

Тези и други автори в своите определения разглеждат проблема в зависимост от ъгъла на своите интереси, така същността на общуването се определя или едностранчиво или пределно общо.

За нуждите на изясняване на същността на общуването можем да предложим следното определение:

Общуването е сложен многопланов процес осъществяващ се в определена социална общност, възникващ по силата на обществена потребност и осигуряващ обмен на информация, взаимодействие, възприемане и разбиране между членовете на общността, като основа на груповата дейност и база за контакт между индивидите.

Понятието общуване е възможно да бъде съотнесено с едно близко, но по-широко понятие – комуникация. Комуникацията е обмен на информация, този процес може да се осъществи между хората, но и между човек и компютър, докато общуването е процес осъществяван само между хората.

Като процес общуването изпълнява определени функции. Б. Ломов ги определя като [6]:

– информационно-комуникативна;

– регулационно-комуникативна;

– афективно-комуникативна.

Аргайл и Хендерсън [2] изследват и друга функция на общуването – функцията да произвежда и осигурява на включените в общуването хора социална подкрепа необходима за справяне с проблемите на ежедневието.

Кои са акцентите и спецификата на общуването като комуникация?

– общуването е отношение между два индивида, всеки от които е активен субект.

– обмяната на информация предполага въздействие върху поведението на партньора. Нещо повече, ефекта от комуникацията се определя от това доколко влиянието е изменило поведението на партньора.

– комуникативното влияние е възможно само ако комуникатора (предаващия информация) и рецепиента (приемащия информация) имат единна система за кодиране и декодиране на сигналите. При това е необходимо и комуникатора и рецепиента да имат еднакво разбиране за ситуацията общуване.

Предаването на всяка информация е възможно само чрез знакова система. При общуването различаваме вербална и невербална системи за комуникация.

А) Вербалната система – с помощта на речта се осъществява кодирането и декодирането на информация. За обозначаване на компонентите на вербалната комуникация са въведени понятията „говорене" и „слушане";

Б) Невербална система – бива няколко групи:

– кинесика или оптикокинестическа система от знаци – включва: жестове, мимики, пантомими – изразяващи емоционалните реакции на човека, придаващи различни насоки на общуването;

– паралингвистична система от знаци – включва: системата на вокализация, качеството на гласа, неговите диапазон и тоналност;

– екстрамажористична система – включва: паузи в речта, плач, покашляне и други;

– проксемика – пространствената и времевата организация на общуването;

– система на контакта с очи – намира място в цялостното и във визуалното общуване.

Обща характеристика на системата за невербална комуникация е, че тя не само помага да се усили или намали вербалното въздействие, но и съдейства по-пълно да се изявят намеренията на общуващите.

Освен своите системи общуването има и своите страни и нива.

А) Интерактивна страна – разглежда общуването като взаимодействие между хората в процеса на непосредствената организация и осъществяване на тяхната съвместна дейност. Тя не е само външна картина на взаимодействието (формална страна на общуването). За нея са значими мотивите, целите на общуването, взаимодействията между хората в психологията най-често се използва дихотомичното им групиране на сътрудничество (използват се термините „кооперация", „съгласие", „приспособление", „корпорация", „асоциация") и конфликтност (използват се термините „конкуренция", „конфликт", „опозиция", „десоциация").

Б) Перцептивна страна – разглежда се общуването като взаимно възприемане на партньорите и установяване на тази основа на взаимно разбиране. За разбиране същността на перцептив-

ната страна на общуването трябва да разглеждаме механизмите на идентификацията, рефлексията, стереотипизацията и обратната връзка.

– идентификация – способ на разбиране партньора по общуване, чрез несъзнателно или съзнателно употребяване себе си на другия;

– рефлексия – осъзнаване на активния индивид как е възприеман от партньора по общуване;

– стереотипизация – класификация на формите на поведение и интерпретиране на причините за проявлението им чрез съотнасяне към вече известни явления, категории и социални стереотипи;

– обратна връзка – получаване на информация за това какво въздействие се оказва на партньора по общуване и коригиране на тази основа по-нататъшната стратегия на общуване.

Перцептивната страна на общуването се съпътства от редица ефекти по-важни от които са:

– ефект на ореола – при него информацията за даден човек се трупа върху образ, който е създаден по-рано;

– ефект на първичността и новостта – изразява се в това, че при възприемане на непознат човек определяща е първата информация, а при познат последната.

Какви нива на общуването се разглеждат в социалната психология. Ломов определя следните нива:

– макониво – индивида общува с другите хора в съответствие с обществените отношения, традициите, обичаите;

– мезониво – общуване в пределите на определено съдържание или тема еднократно или многократно във времето;

– микониво – акт на контакт изразяващ се в определени външни показатели, например: въпрос – отговор, ръкостискане, мимика и др. Това е най-простото общуване лежащо в основата на останалите нива.

Добрович [по 3] определя нивата на общуване като – примитивно, конвенционално, манипулативно, стандартизирано, делово и духовно.

От гледна точка на ролята на общуването е необходимо да видим кои са основните видове общуване:

– социално ориентирано общуване (лекция, доклад, реч, телевизионно и радио предаване и др.). В този случай субекта по стаж е представител на обществото (или социална група) и решава социална задача. Той или подбужда обекта (слушателите) към непосредствена активност, или ги обединява около социално значими идеи, формира или изменя убежденията, или осигурява фон за такова въздействие съобщавайки социално значима информация (новини и др.).

– групово предметно – ориентирано общуване – то е включено в груповата дейност и непосредствено подпомага (обслужва) групата в решаването на стоящите пред нея задачи. Предмет на това общуване е ориентираното групово взаимодействие в процеса на труда.

– личностно-ориентирано общуване – това е общуването на един човек с друг. То може да бъде делово – ако е насочено към някаква съвместна дейност, или изясняване на отношения нямащи връзка със съвместната дейност.

Етапи на общуването. Бариери и стратегии - в процеса на общуването обикновено се определят следните етапи [по 4]:

– потребност от общуване – заключава се в необходимостта да се съобщи или разбере информация да се повлияе на събеседника, тази потребност подбужда човек да встъпи в контакт с други хора;

– ориентиране в целите на общуването и в ситуацията на общуването – едно общуване има смисъл само, ако се разбере целта, която си поставяме с него и ситуацията в която то се провежда;

– ориентиране в личността на събеседника – необходимо е да разберем дали информацията, която подаваме ще бъде правилно възприета от събеседника, като при това отчитаме негови

личностови особености, като темперамент, характер, особености на мисленето и разбира се моментното емоционално състояние;

– планиране на съдържанието на своя модел на общуване – обикновено безсъзнателно пристъпвайки към общуване, човек си създава представа за това какво именно ще каже при общуването и как ще подреди информацията, която ще поднесе;

– избор на средства за общуването – в повечето случаи безсъзнателно, а понякога и съзнателно човек подбира конкретните средства, речевите фрази, които ще използва, решава как ще говори и как ще се държи при общуването;

– възприемане и оценка на ответната реакция на събеседника – в случая става дума за контрол на ефективността на общуването, на основата на осъществяването на обратна връзка;

– коригиране на насочеността, стила и методите на общуване – всеки човек обикновено в резултат на общуването, си прави изводи за своето поведение в него, за своя стил и метод на общуване и въвежда корекции в тях.

Независимо, че всички очакваме провеждайки общуване с други хора да бъдем адекватно разбрани, това невинаги се случва под влиянието на различни фактори, които обикновено наричаме бариери на общуването. Наличието на подобни бариери се явява причина за конфликтите или способства за тяхното разгаряне. Това се случва тъй като общуващите имат различни, а често и противоположни желания, стремежи, характери и разбира се различно самочувствие. За да се преодолеят такива бариери, човек е необходимо да има поне елементарни познания за потребностите, нагласите и характера.

Обикновено в психологическата литература се посочват следните бариери на общуването:

– стереотипи – заковани мнения за отделни лица или ситуации;

– изкривени представи – отхвърляне на всичко, което не съответства на нашите възгледи;

– враждебно отношение към събеседника;

– липса на внимание и интерес от страна на събеседника – най-вече в резултат на това, че той не осъзнава значимостта на информацията, която му поднасяме;

– пренебрегване на фактите – създаден у човека навик да прави изводи и заключения на основата на неточна или повърхностна информация;

– неправилно подбиране на думите, нелогичност в израза – ограничава възможността да бъдем разбрани от партньора по общуване;

– неправилен подбор на стратегията на общуване.

Стратегии на общуването. Както вече споменахме, неправилният подбор на стратегиите за общуване се явява една от бариерите на общуването, които снижават неговата ефективност. Прието е да се разгледат няколко стратегии на общуването:

– открито-закрито общуване – подразбира се идеята, че е възможно информацията или част от нея да не е предназначена за широк кръг хора или за част от тях. Това определя избора на стратегия - на кого и как, и в какъв обем информацията трябва да бъде поднесена;

– монологично-диалогично общуване – определен тип информация, която не подлежи на обсъждане и обикновено се поднася от лица с по-висок социален статус, предполага монологично общуване, ако информацията изисква обсъждане на съдържанието, това налага общуването да бъде диалогично;

– ролево-личностно общуване – при ролевото общуване човек пристъпва към него съобразно социалната роля, която заема, а при личностното общуването се осъществява без значение на социалната роля и статус на равноправни начала.

Както се вижда от изброените стратегии на общуването, коя от тях ще изберем зависи от социалния статус, който имаме, социалната роля, която играем, кръга от хора, на които трябва да поднесем информацията и т.н.

Транзакционен анализ при общуването. Този анализ се явява рационален метод за разбиране на поведението на базата на три състояния на „Аз-а" – „родител", „възрастен" и „дете", разработен от Ерик Берн (1910-1970). Тези три състояния на „Аз-а" той описва така [по 5]:

– „родител” – това е експертно контролната инстанция на нашия „Аз”, явяваща се съсредоточаване от схеми и правила, които са усвоени по-рано от човека и които се изпълняват без допълнително осмисляне. В ежедневието тази роля играят родителите, по-възрастните братя и сестри, или началниците в службата, чиято роля е в началствено-покровителския маниер на общуване.

– „дете” – това е ефектно импулсивната и интуитивно-творческата характеристика на нашия „Аз”, в тази позиция ние се държим недостатъчно сериозно и отговорно. В живота тази роля се изпълнява от децата, младите специалисти и т.н.

– „възрастен” – това е когнитивно активното начало на „Аз-а”, основна черта на който се явява независимостта и здравия разум. В тази роля влизат близки, познати, приятели, колеги в службата.

От изброените позиции най-успешно и ефективно е общуването между двама събеседници, които заемат еднакви роли. В останалите ситуации на общуване на възрастен – дете, родител – дете, общуването е динамично, то зависи от обсъжданата тема и емоционалното състояние на страните. Често се случва нивата на общуване да са маскирани. Обикновено се дава пример на общуването на продавач и купувач, което външно напомня на общуването възрастен – възрастен, но на практика купувача и в ролята на дете, защото той се явява търсещ услугата, а продавача е в ролята на родител, тъй като той обяснява качествата на продукта.

Фактори благоприятстващи контакта при общуване: установяването на контакт е главната задача на първата фаза на общуването. Самото осъществяване на контакта предполага да се създаде благоприятна среда предразполагаща събеседника към беседа, атмосфера на привличане на вниманието и на подбуждане на интереса на събеседника към себе си. Един от основните фактори са характерите на събеседниците. Сред чертите на характера, които предразполагат към общуване обикновено се посочват доброжелателността, искреността, вежливостта, тактичността и др., и обратно, чертите на характера, които затормозяват общуването и в повечето случаи предизвикват конфликти са грубостта, безцеремонността, демонстративността и т. н. Друг фактор благоприятстващ общуването е психологичната нагласа към партньора по общуване. В случая, за да бъде тя благоприятна това означава, че ние трябва да сме внимателни, откровени, обикновено като най-благоприятни фактори на нагласата за общуване се сочат одобрението, самоодобрението и емпатията. Когато говорим за одобрение имаме предвид признаването на събеседника правото да се чувства, да говори и да постъпва така, както той смята за необходимо, в крайна сметка хората не са идеални и трябва да се приемат с техните положителни и отрицателни черти. От особено значение е фактора емпатия, който означава умението да почувстваме състоянието на събеседника като свое собствено състояние. Това ни позволява емоционално да откликнем на неговите проблеми. Наблюдава се при такова общуване, включително и копиране на поведенските реакции на партньора като жестове, пози, движения и др.

Завършването на всеки акт на общуване е не по-малко важен акт, отколкото началото и самото общуване, дори в повечето случаи това е най-трудния елемент от общуването.

References:

1. Ангелов, А. Основи на мениджмънта. Илинда. С., 1996
2. Аргайл, М., Хендерсън М. Анатомия на човешките отношения. НП, С., 1989
3. Бодалев, А. А. Психология общения. М., 1996
4. Бороздина, Г., Психология делового общения. М., 2006
5. Вердербер, Р., К. Вердербер, Психология общения. М., 2003
6. Горбунова, М. Социальная психология. М., 2006
7. Градев, Д., Г. Йолов. Общуването. ВИ. С., 1985
8. Розанова, В. А. Психология управления. Интел – синтез, М., 1997
9. Христов, С. Основи на управлението. В., 1997
10. Thill, J., C. Bovei. Excellence in Business Communication. “Mc. Grow-Hill”. 1991

Sungjae Choo, Lukas Birsak, Tjeerd Tichelaar, Marin Marinov,

THE OLD MAPS OF THE WORLD, EUROPE AND BULGARIA FROM GEOGRAPHICAL POINT OF VIEW. AND THEY REPRESENTATIVE IN THE GEOGRAPHIC MAPS AND GEOGRAPHIC ATLASES

Sungjae CHOO*, Lukas Birsak, Tjeerd Tichelaar***, Marin Marinov******

**Sungjae CHOO, Professor Department of Geography Kyung Hee University Seoul 130-701, Republic of Korea,*sjchoo@khu.ac.kr

*** Lukas Birsak, lecturer of cartography at the department of geoinformation and environment at the Carinthia University of Applied Sciences and Geschäftsführer(managing director)at Ed. Hölzel Ges.m.b.H. Nfg KG.Jochen-Rindt-Straße 9 ,1230 Wien* birsak@hoelzel.at

**** Tjeerd Tichelaar, Editor –in Chief at Noordhoff Uitgevers,Winschoterdjep 70a P.O.Box 58 , 9700 MB Groningen ,The Neetherlands tjeerd.tichelaar@gmail. com*

***** Marin Marinov, geographer, Bulgaria marinmarinov5@gmail.com*

Abstract: *The geographical maps are more important element for every country. The geographical maps are one of important products of geography and history.*

The old maps are documents who offer also more important information for history and geography for countries. In this article we will present an old maps from the World, Asia, Europe, Balkan peninsula, and Bulgaria. Also and information for authors of the same maps. In additional we analyze and some of maps.

Moreover in same article we connect geography, history and geographical names as important element of geographical maps.

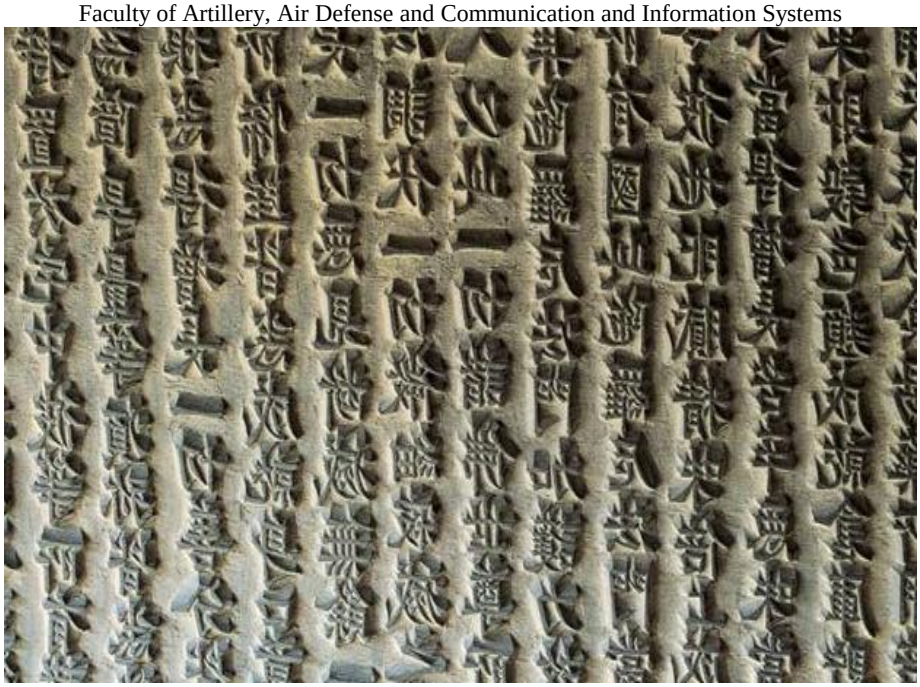
Keywords: *Maps, Korea,DMZ, the hanji paper, woodblock, tripitaka koreana, Chinese characters, Ed. Hoelzel company, Austria, De Bosatlas company, The Neetherlands.*

The old maps of the World, Europe and Bulgaria are important source for history and geography today. Same maps offer detailed information for history and geography in the ancient time.

The Chinese people first discovered the way for the create paper.

However, Korean first discovered of hanji paper and woodblock printing.

He created the first the printed book with those methods with title "Tripitaka koreana"is 75 year before Europeans printed books.



More of ancient maps of Asia written were with Chinese characters.
Even ancient maps created in Korea, Japan and Vietnam also with Chinese characters.
One of them is this map present detailed East hemisphere below.

In same maps are included Africa, Middle East, and Asia. Typical for this map are that China is in the center of map. Because for ancient cartographers from Asia China is the “center” of the World in same period of creature of this map.

Author of the same map write below on the map information for used source for creature of this map.Those are two old maps form ancient China. Moreover, in this map we can observe the mains Japan’s islands in the right and Korea peninsula with more big size compare other countries around Korea peninsula. In additional we can observe in this map also Africa, Middle East and East Europe.

In the same map also absent parallels and meridians. The authors of the map are Geun Gwon,Sa Hong Kim,Mu Lee,Hoe Lee 1402 year.The original manuscript is copy of an original in Guykoju University Japan.

The map Taedong yojido (in translation) a Map for the Land of an Eastern Country – Korea, the map create was since 1891 year the map was created during 10 years period by Jeong –Ho Kim .This is other map from Asia also.

More over the map of Korean peninsula divided was into 22 albums.

Same map is without net of parallels and meridians. Also a divided Korean peninsula on distance of 120le (10 le = 4km) from north to south, and of 80 le from west to east.

The size of map is 6,6m/4m.This map is easy for use because was shaped crafted was and created as an atlas consisting of 22 separated books. In which 22 books contents the whole map of Korea peninsula with size 6,6m/4m.In northeast corner on the map are fragment from maps of Seoul and Pusan The map content was used by Japanese's military organization during Russo- Japan war since 1905 year.

Since 17-18 centuries began process of translation of old maps of Asia into European languages.

In same moment in more ancients and contemporary maps from Asia are with two geographical. One use from persons from Asia and second use by Europeans. Additional some geographical objects are with two geographical names in use even today.

For example:

The cartographer from ancient China use geographical name East Sea for Sea of Japan. East Sea (Donghae)′ ⇒′Sea of Japan (Nihonkai)

Another important question is Romanization and Cyrilisation of geographical names in the modern geographical names today of Asia.

This fact determinate used of the old geographical names of geographical objects even today. But those fact create difficulty of cartographers in the process of print geographical names in the maps. Also and difficult for understand those maps with two geographical names for one geographical object:

For Example now in Korea use two geographical names for some objects: Taegu ⇒ Daegu, Pusan ⇒ Busan, Chŏnju ⇒ Jeonju , Kimpo ⇒ Gimpo , Gaeseong ⇒ Kaesong

Dokdo ⇒ Liancourt Rocks, Ieodo ⇒ Socotra Rock, Ammokgang (river) ⇒ Yalu River, Dumangang (river) ⇒ Tumen River

The geographical names of the Taebaeksanmaek(太白山脈), based on geological genetics.

But Baekdudaegan(白頭大幹), based on traditional perception on physical structure.

Korean cartographers use event today in the maps follow geographical names for seas around Korean peninsula.

Donghae(East Sea) or Sea of Japan, Seohae(West Sea) or Yellow Sea or Huang Hai, and Namhae South Sea. See maps below.

CHINA
JILIN
LIAONING
NORTH KOREA
SOUTH KOREA
SEA OF JAPAN (EAST SEA)
YELLOW SEA (HUANG HAI)
Korea Bay
P'YŎNGYANG
SEOUL (Sŏul)
Dandong
Sinŭiju
Shenyang
Fushun
Benxi
Anshan
Changchun
Jilin
Harbin
Tumen
Yanji
Hunchun
Najin
Ch'ŏngjin
Kimch'aek
Hamhŭng
Hŭngnam
Wŏnsan
Kaesŏng
Inch'ŏn
Kwangju
Taejŏn
Taegu
Pusan
Ulsan
P'ohang
Kyŏngju
Chŏnju
Ch'ŏngju
Cheju-do (S. Korea)
Cheju
Korea Strait
JAPAN
Fukuoka
Shimonoseki
Kita-Kyūshū
Tsushima
Iki-shima
Higashi-suidō
Cheju-haehyŏp
Kyŏnggi-man
Paengnyŏng-do (S. Korea)
Ullŭng-do (S. Korea)
Zarubino
R.U.S.E.D.

For Korea peninsula and the maps of Korea are typical one important military element of the maps.

This is DMZ area.The DMZ is NO state border area!!!

At the end of Second World War the Korea was divided into a northern zone occupied by Soviet Union and southern zone occupied by USA.

The 38^0 paralel service as the boundary between the two zones.

Now DMZ is NO border area between two countries of Korea peninsula!

After the end of Korean war 1950-53 year, a new border fixed at the Demilitarized Zona (DMZ), a streep 4 kilometer wide strip of land where was ceasefare from east to west for a distance 241 km from east coast to the west coast.

DMZ content also:

1) Northern limit of the Demilitarized Zone
2) Military Demarcation Line(MDL)
3) Southern limit of the Demilitarized zone
4) Civil Control Line (CCL)) is from 5 to 15 km from DMZ
5) Military Property Protection Zone (MPPZ)

Photo of DMZ from South Korea.

Same is situation with use both geographical names in the old maps created by foundation member of the company Ed.Hoelzel, slovenian cartographer Blasius Kozzen.

On his map of the Dalmatia, hi use also both German and Slovenian geographical names

See map below:

The company Ed.Hoelzel is deep connecting with cartography of Bulgaria. A long time the company Ed.Hoelzel worked was for Bulgaria cartography.

His cartographer the Vinzenz Haardt von Hartenthurn created different kind of maps for Bulgarian civil schools and for Bulgarian army. Now some of his maps are in Austrian military archives.

He was professor at Military academy and member of the General staff of Austro-Hungary army until 1914 year.

Photo of Vinzenz Haardt von Harthenthurn

The Vinzenz Haardt von Harthenthurn (1843- 1914year) as cartographer and military cartographer same was author of different maps of the World, Europe and Bulgaria.

As cartographer and military cartographer he is author of different maps connect the International World map and Balkan peninsula and Bulgaria.

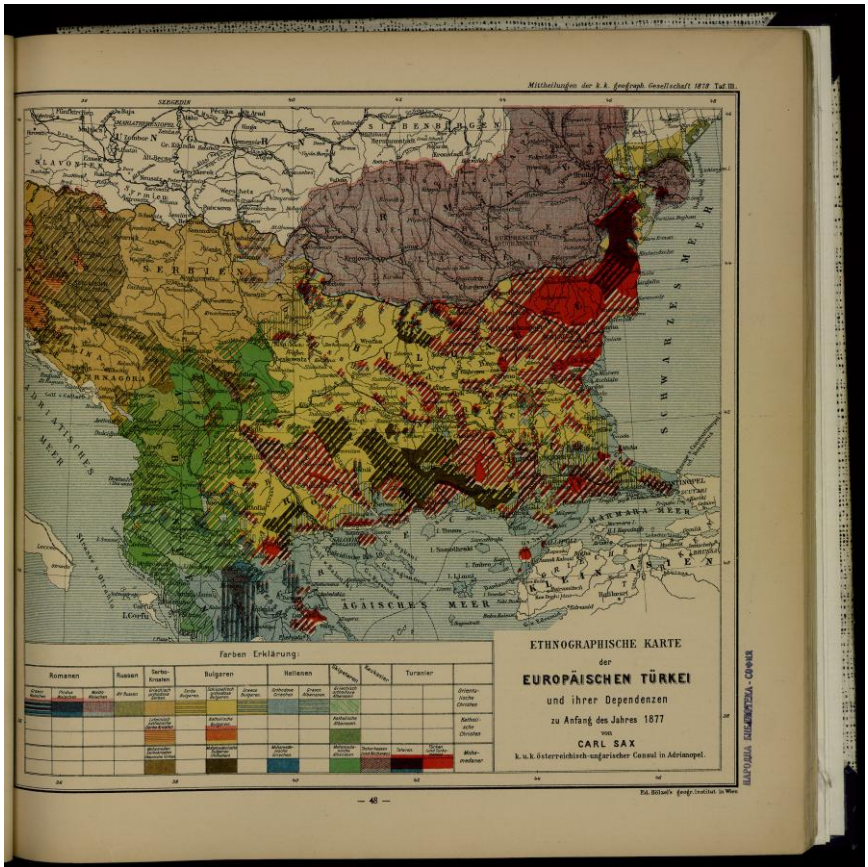
He is also author of:

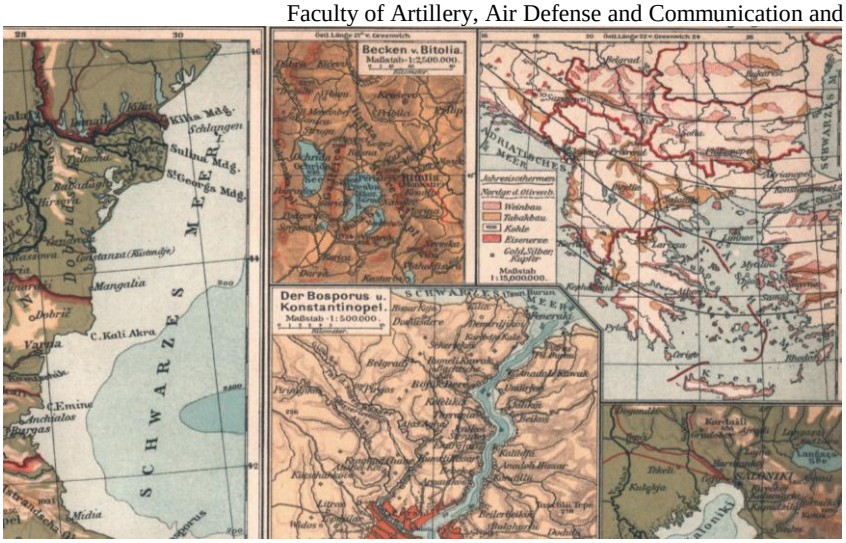
“Etnographische Karte der Europaischen Turkei” with data of Austrian diplomat Carl Sax same map is printed in Ed. Hoelzel company.Same map was used by Bulgarian authors about 1924 year.

Same map was used information by Austrian diplomat in Adrianopol Carl Sax and created joint collaboration with Royal Geographical Society of Austro-Hungarian Empire and Ed Hoelzel company. In additional same map printed in was Ed.Hoelzel Company in Austria.

This map used was a key map for determination of the ethnic border areas of the Balkan countries in the Congress of Berlin 13 June-13 July 1878(The Treaty of Berlin 1878 year).

The first social economic map of Balkan Peninsula also created was in the company Ed.Hoelzel since 1910 year with same cartographer.



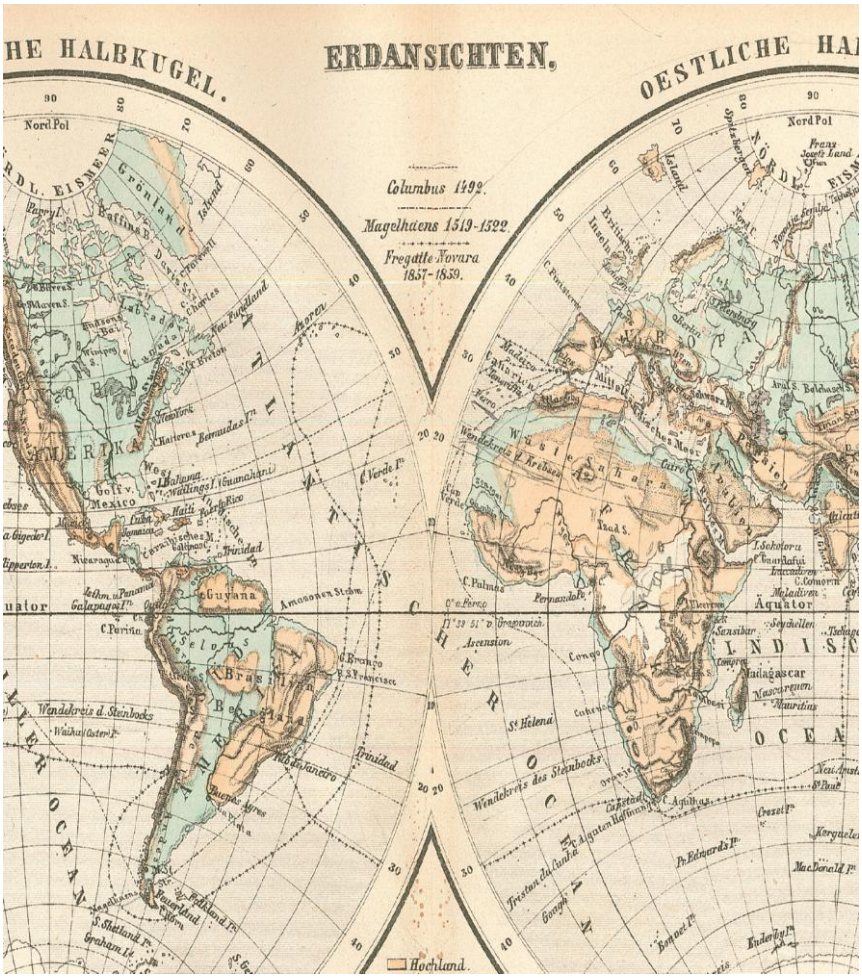


The Vinzenz Haardt created was also military map with scale 1:200 000 of Balkan peninsula since 1898 year. Also map with scale of 1: 1 000 000 with international cartographer for create those maps for international conference in Paris 1914year. He is also cartographer and author of many other maps of the countries of the world.

Now same maps are in Austrian Military Organization.

Same cartographer creates wall maps for Bulgarian schools via publishing house “Hristo Danov” in town Plovdiv,Bulgaria.

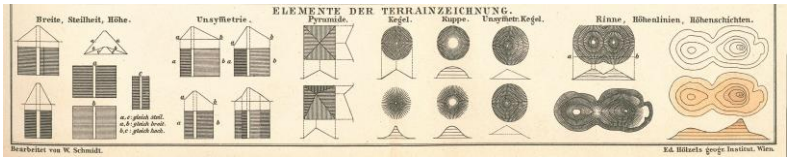
Hi, create also the map of Holly places and Palestine for Bulgarian school also published in same publishing house printed in 1938 year. The map below is from 1884 year of the same company Ed.Hoelzel.



Now the company Ed.Hoelzel created digital atlases and maps.

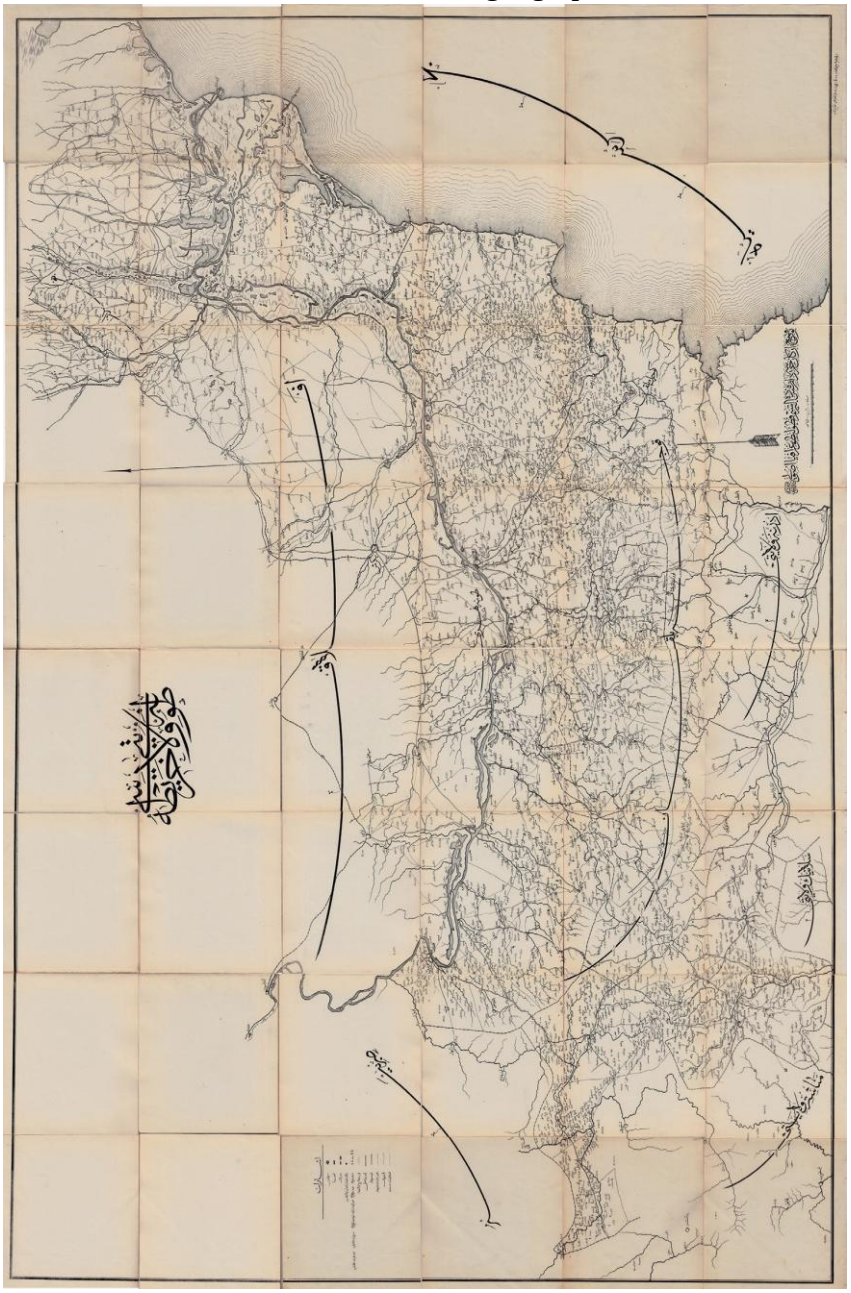
The company Ed.Hoelzel now is one of the leaders companies for digital school atlases in the world.

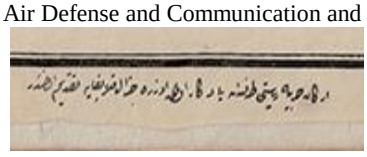
The company also practical developed way of presentation of relief on his own maps.



See picture below.

The last map of Bulgaria use from military person is the map of the Danube Vilayet (Tuna Vilaeti Harit) in scale 1: 400 000 printed was about 1878 year. The geographical names of this map are by oriental way of transliteration and no information for list of geographical names of same map.





The same map is ownership by Professor Boguslav R. Zagorski.

In this map near legend written was that this map is prepare by Ottoman general staff and printed in new way of print.

Professor Zagorsky create detailed research on this map.

On low right corner of the same map written was bellow “This map is a gift for General Galabov by General staff of Ottoman army”.

The more important question now is:

Who is General Galabov in Bulgarian military history?

The last maps in our article are from the Neetherlands.

Isak Tirion was born in 1705 in Utreht and dead in 1765 year.

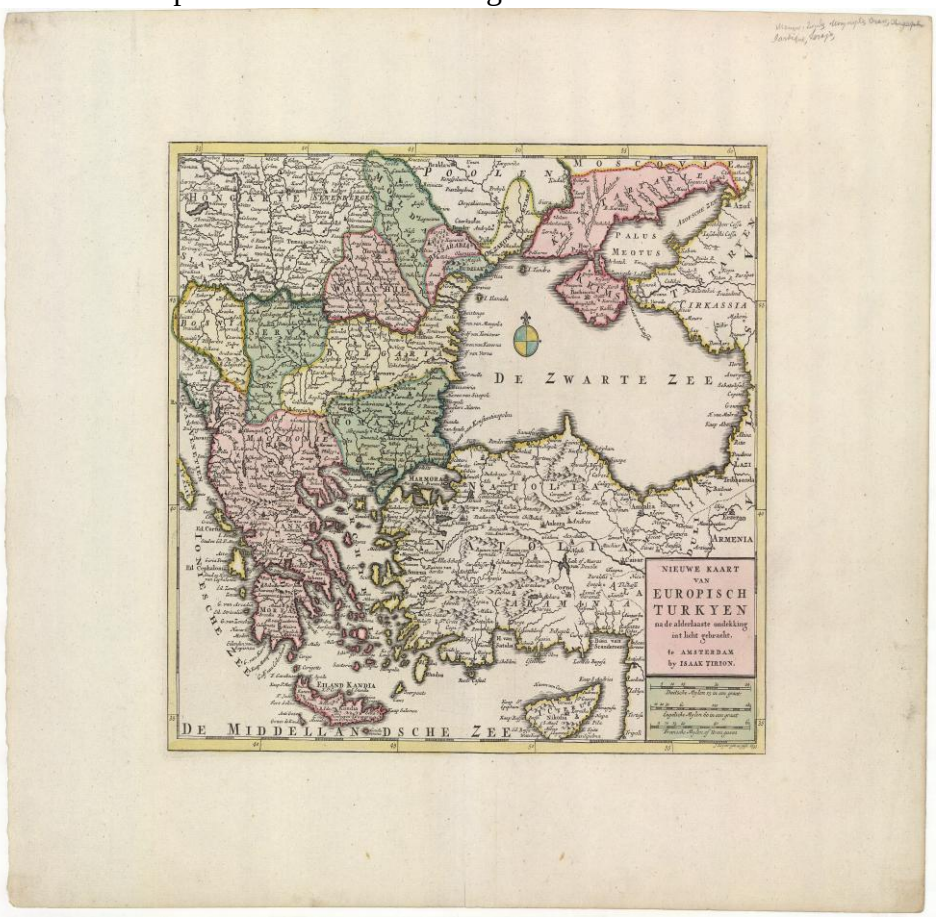
He is cartographer and publisher by the Northern Neetherlands.

He is authoring of famous both books for history with titile “History” and other book with title the “Modern History”.

Both books are with very good maps.

In the maps of those books, the village Dragoevo in Bulgaria was writte as town Tragoi near Eski Stambol this was old name of our old capital city of ancient Bulgarian kingdom Preslav.

Now same ancient town is part from the Shumen region.



Other old maps of Balkan peninsula was created by the company De Bosatlas also from the Neetherlands.The same company founded was by Pieter Roelof (or Roelf) Bos he was born February 19, 1847 in Groningen, † June 22, 1902 ibid) and was a teacher in the subjects of Dutch and geography. He was the first to publish the De Bosatlas, the most important Dutch school atlas, named after him.

Pieter Bos wrote many maps and books for the then new geography at schools. In 1877 he published for the first time the School Atlas, which had many 55 editions to now days and it is still used today also.

In 1888 Bos was examiner in the teacher training and exercised this part-time job until 1901. In 1893 he joined the board of the Royal Netherlands Geographical Society

The cartographers from the same company began to Romanization in 1879 the geographic names on the territory of the Balkan Peninsula and Bulgaria.

This is evident from the first map showing Bulgaria and East Rumelia. The process of Romanization of geographical names continued until the end of the First World War.

For example the town Russe in Bulgaria we can observe in the maps below with two geographical names Roesjtsjoek., The town Varna also we observe with geographical name Warna also.

The town in Romania Constantsa with two geographical names also Kustendsje and Constantsa. In additional also the towns Saloniki and Thesaloniki,Gallipoli and Galibolu,The town Bergama with three geographical name Pergamus and Pergamon.

Those geographical names of the towns we can observe in the maps show below.

The third map of Balkan Peninsula is by current atlas of the company De Bosatlas used since 1995 year.

The processes of Romanization and change of geographical names the world maps continue even today in all countries.

The UN make guide with list of geographical names of all members of UN countries.

OOSTENRIJK-HONGARIJE
Szegedin
Arad
Klausenburg
RUSLAND
Zevenburgen
Focsani
Maria Theresiopel (Szabadka)
Slavonië
Essegg
Hongarije
Temesvar
Hermannstadt
Kronstadt
Galatz (Galati)
Ismail
Braila
Banjaluka
Neusatz (Ujvidek)
Versecz (Wersjitz)
Ploesci
ROEMENIË
Zvornik
Belgrado (Beograd)
Semendria (Smederovo)
Craiova
Boekarest (Bucuresci)
Silistra (Silistria)
Cernavoda
Bosnië-
Sarajevo
Constantsa (Kustendsje)
Giurgewo (Georgiu)
Russe (Roesjtsjoek)
SERVIË
Hercegovina
Krusevac
Pleven
Svistov
Mostar
Novipasar
Nis
Soemla
Varna
Dalm.
Ragusa
MONTENEGRO
Pristina
Sofia
BULGARIJE
Jambol
Podgorica
Boergas
Cattaro
Cetinje
Köstendil
Kazanlik
Skodra of Scutari
Philippopel
Skoplje of Uskub
Adrianopel
ALBANIË
Konstantinopel
Durresi of Durazzo
Ohrida
Bitolia of Monastir
Seres
Kavala
Feredsjik
Uskudar (Scutari)
Orphani
Dede Agatsj
Enos
ITALIË
Walona (Avlona)
Saloniki
Thasos
Gallipoli
Broessa
Imbros
Metsovon
Limnos
TURKIJE
Corfu
Corfu (Kerkyra)
Trikkala
Larissa
Joannina (Janina)
Pharsalos
Volos
Mytilini (Lesbos)
Arta
GRIEKENLAND
Evripo, Euboea of Negroponte
Bergama (Pergamon)
Leukas (Sta. Maura)
Mesolongion (Missolunghi)
Ithaka
Thebe
Chalkis
Chios
Smyrna
Kephallinia (Cefalonia)
Patras
N.-Korinthe
Athene
Andros
Samos
Zante (Zakynthos)
Salamis
Tinos
Keos
Mykonos
Boedroem (Halicarnassus)
Tripolis
Thermia
Paros
Naxos
Pylos (Navarino)
Sparta
Siphnos
Kos
Milos
Nio (Ios)
Astropalia
Santorini
Tilos
Rhodos
Kythira (Cerigo)
Rhodos
Antikythira (Cerigotto)
Chania
Megalokastron (Candia)
Karpathos
Kasos
Kreta of Kandia

References:

1. S.Choo Sungjae , Sang-Hyun Chi ,People,Places,and place names in the Republik of Korea. NGII of South Korea. ISBN 978-89-93841-19-0

2. F.J Ormeling, Rob van der Vaart, Biografie van de Bosatlas: 1877-heden, Wolters-Noordhoff Atlasproducties, Groningen, 2005. ISBN 9001122272

3. Ingrid Kretschmer, Lukas Birsak: Der Kozenn-Atlas – ein österreichischer Schulatlas schreibt Kartographiegeschichte. In: Mitt. der Österr. Geographischen Gesellschaft. Bd. 149, 2007,

4. Lukas Birsak: Die Österreichischen Schulatlanten des Verlages Ed. Hölzel. In: Ferdinand Mayer (Hrsg.): Wiener Schriften zur Geographie und Kartographie. Band 5, Wien 1992,

Geschichte des Kozenn-Atlasses 1861–2011, auf Website des Verlag Ed. Hölzel.

CONTENTS AND CHARACTERISTICS OF THE INNOVATION PROCESS IN MILITARY EDUCATION IN BULGARIA

Atanas L. Atanasov

***Abstract**: The paper examines the issue of innovation in the field of military education. The starting point is the understanding of the innovation process as a structural and consecutive process in which the results of fundamental and applied research are implemented. Objective conditions are being considered that affect the sphere of education as a whole and the situation in military academies. There is an inadequate system for adopting management decisions, which makes it impossible to build an innovative management system in military education. Together with insufficient funding, this leads to the impossibility of adopting economically rational management decisions for long-term strategic and innovation development, which in turn threatens the development of the competitiveness of the scientific and educational system.*

***Keywords**: innovation management, innovation process, military education*

СЪДЪРЖАНИЕ И ОСОБЕНОСТИ НА ИНОВАЦИОННИЯ ПРОЦЕС В БЪЛГАРСКОТО ВОЕННО ОБРАЗОВАНИЕ

Атанас Л. Атанасов

Национален военен университет „Васил Левски"
Факултет „Артилерия, ПВО и КИС" - гр. Шумен
ул. „Карел Шкорпил" №1, тел. 054/801040, вътр. 54232

1. Обща постановка на проблема

Разработването на иновационни проекти е от съществено значение за развитието на висши училища от нов тип и следва да е част от стратегическите приоритети на университетските ръководства. Иновациите са важна част от процеса на глобализация и необходима предпоставка за създаване на конкурентно предимство. Същността на иновационната дейност е максимизацията на социално-икономическия ефект за сметка на по-доброто използване на интелектуалните ресурси на обществото. В обобщен вид иновационният процес представлява структурно-последователен процес. В хода на иновационния процес, на основата на резултатите от фундаменталните и приложни изследвания и съответното ресурсно осигуряване, се осъществяват създаването на високите технологии, организацията на производството и реализацията на наукоемката продукция.

В частност военното образование не остава незасегнато от налагащите се световни процеси. Като приоритет в работата на висшето военно ръководство на държавата се откроява именно въвеждането на иновации във висшите военни училища, като инструмент за адекватна подготовка на кадри за сигурността и отбраната на страната. Това е ефективен начин за отговор на произтичащите от глобализационните процеси заплахи и предизвикателства. За реализиране на такъв иновационен процес е необходима финансова обезпеченост.

За разлика от иновационния процес в развитите страни, иновациите у нас се извършват в условия на нестабилна икономика, недостатъчен частен капитал, който би могъл да се насочи към разработване и усвояване на най-нова техника и технологии.

Според нас, за постигане на тази задача е необходимо да се разработи единна иновационна политика, която да дава приоритетно развитие на военно-научната област и повишаване на конкурентоспособността на военното производството както на вътрешния, така и на международния пазар с цел нарастване на отбранителните способности на страната. Особена роля в това отношение има поддържането на системата на висшето военно образование на световно равнище.

Подходите за формиране на единна иновационна политика са:

- Системният подход за формиране на иновационната политика;
- Приоритетното развитие на висшето образование и военната наука;
- Ясно определяне на източниците за финансиране на приоритетните направления;
- Формиране на иновационна система на базата на научно-техническите, интелектуалните и финансовите възможности на страната.

В този план държавните структури, отговарящи за развитието на иновационната дейност в страната, не използват в пълна степен потенциала на научните изследвания за провеждане на необходимите научни разработки.

В същото време чуждестранни колективи и експерти получават възнаграждения за оценките, заключенията и препоръките, които правят по важни за отбраната проекти.

За осигуряване на ефективна иновационна дейност са необходими държавна подкрепа, формиране на държавен научно-технологичен сектор и определяне на ясна схема за финансиране на иновационните програми и проекти със средства от държавния бюджет.

Нарастващата роля на знанието и образованието е общопризната. На висшето военно образование се възлагат специфични задачи свързани с гарантиране на мира и сигурността на всяка отделна страна и на света като цяло. Според нас висшето военно образование трябва да акцентира освен върху професионалната подготовка и върху личностното формиране и потенциала от аналитични способности на обучаемите, което би се отразило върху ефективността на националната сигурност. С други думи, натрупването и прилагането на необходимите професионални знания в комбинация със съответните личностни качествагарантират постигането на търсения ефект.

Посоченото по-горе е обусловено от редица обективни условия, които влияят на сферата на образование като цяло и на ситуацията във висшите военни училища в частност. Между тях са:

- нарастването на наукоемките военни дейности (интелигентна отбрана);
- интензивното нарастване на обема на научната и техническата информация;
- бързата смяна на военните технологии;
- нарастване дела на интердисциплинарните изследвания.

Решаването на тези проблеми изисква нови подходи за формиране и развитие на кадри с висше военно образование. Най-актуални днес са моделите, свързани с развитие на критично мислене, креативни способности и интелектуални ресурси на личността. Всичко казано дотук позволява да се направи извода, че главна насока в дейността на висшите военни училища днес е не просто присъждането на специалност, а залагането на професионални основи от знания и личностни нагласи, подчинени на задачата за непрекъснато обучение и самостоятелно развитие в професионален и личен план. За ефективното развитие на висшето военно образование са необходими различни съвременни модели на обучение във висшите военни училища.

2. Особености на иновативния модел на военно образование

Трябва да отбележим, че самият термин „модел на обучение" не се използва еднозначно. Обобщаващ модел на иновативно обучение за първи път се споменава в труда на Kozma R. B. and J. Johnson 1991.[1] В него се предвижда:

1) активно участие на студента в процеса на обучение;
2) възможност за използване на получените знания в реални условия;
3) представяне на информацията под най-различна форма (текстова или цифрова);
4) индивидуален подход към обучението на колективната дейност.

Един от фундаменталните въпроси, отнасящи се до динамиката на иновационния процес в системата на висшето военно образование, е съкращаването на времевия интервал между появата на новото знание и неговото използване, внедряването му. Тези въпроси днес са от особена важност, защото от бързината, с която новите знания се прилагат в практиката, зависи успеха на целия иновационен процес. Като правило управлението на иновационния процес предполага преодоляване на препятствията, затрудняващи практическата реализация на прогресивните идеи. Анализът на понятието „иновационен процес" и неговите основни компоненти позволяват да се разбере същността на иновационния мениджмънт. Иновационният мениджмънт представлява съвкупност от принципи, методи и инструменти за управление на иновационните процеси[2]. Общопризнато е, че иновационният мениджмънт, като самостоятелна област на професионалната управленска дейност, представлява една от разновидностите на функционалния мениджмънт, чийто непосредствен обект са иновационните процеси. Това определя мястото на иновационния мениджмънт в системата на управленските дисциплини. Ако разгледаме иновационното развитие на военно-образователната система от гледна точка на управлението на едно висше военно училище, то можем да констатираме, че основната дейност в него е модернизацията на основните елементи на образователната система. Най-съществените от тях са:

- съдържанието и структурата на учебните програми;
- методиката на преподаване;
- принципите и средствата за осъществяване и поддържане на образователния процес.

По всеки от посочените елементи на управление и функциониране на висшето военно училище съществуват множество проблеми. Един от тях е липсата на гъвкава и адаптивна система на иновационно управление и стратегическо развитие на военното образование, както и наложилата се система за вземане на управленски решения, за ефективността на която е необходимо информационно осигуряване на образователната дейност.

На практика повечето висши училища нямат адекватна система за вземане на управленски решения, което прави невъзможно изграждането на иновационна система за управление (иновационен мениджмънт). Заедно с недостатъчното финансиране, това води до невъзможност за вземане на рационални управленски решения за дългосрочно стратегическо и иновационно развитие, което на свой ред е заплаха за развитието на конкурентоспособността на научно-образователната система. Военните училища не са изключение.

В последно време в сферата на иновационния мениджмънт бързо започнаха да се развиват отраслови дисциплини като: управление на иновациите в образованието, в банковото дело, в транспорта, в индустрията, в съобщенията и в други наукоемки и високотехнологични отрасли. Тези управленски дисциплини изследват спецификата на методите и инструментите за управление на иновационните процеси в отделните отрасли. Сферата на образованието е една от най - иновационните сфери, от която в най-голяма степен зависи създаването на иновационен климат и ефективност на военното дело като цяло. Характерът и ефикасността на иновационните процеси в различните сфери на обществена дейност съществено зависят от характера и ефективността на иновационната дейност в сферата на образованието. При разпространението на иновациите в сферата на военното образование се създава и развива съвременна военнообразователна система на отворено, гъвкаво, високо технологично ниво на знания, на непрекъснато образоване и учене през целия живот. Такава система представлява единство от:

- технологични иновации в системата на образованието - нови методи и начини на преподаване и обучение;
- управленски и организационни иновации, свързани с организацията и управлението на образованието.

Всичко това води до съществено изменение на образователния процес. Като правило точно тук се наблюдава най-сериозното предизвикателство - внедряването на иновациите в определен период да се извършва в условия на остарели управленски структури и методи. Това изисква разработване и реализация на организационни иновации, чието усвояване е най-важния фактор за развитието на цялата образователна система. Под силата на въздействието на иновационните образователни технологии се формира развитието на пазарните механизми в областта на образова-

нието. Това са новите форми на държавно финансиране на образованието, диверсификацията на източниците на финансиране, новите механизми за финансиране от бизнеса, данъчното стимулиране на инвестициите, както и новите механизми за заплащане на труда.

Тези процеси изискват не просто преобразуване на технологичната база на образователните институции, а кардинално изменение на тяхната институционална същност. Резултатът е поява на нови образователни институции, които използват новаторски методи на образование и нови организационно-административни механизми за тяхното функциониране.

Под влияние на съвременните компютърни и телекомуникационни технологии в условията на развитие на пазара в сферата на образование се формира нов модел на университета, в който се обединяват традиционното образование и някои основни типове институционални форми (организационни структури) на дистанционното образование **(таблица 1)**.

Таблица 1. Сравнителна характеристика на иновационните модели на обучение

Иновационни модели на обучение	**Ключови особености**	**Характеристика на традиционния модел на обучение**
Контекстно обучение	Интеграция на различните видове дейност на студентите: учебна, научна, практическа. Създаване на условия, максимално близки до реалните	Увеличаване дела на практическата дейност на студентите (с акцент на професионалните умения)
Имитационно обучение	Използване на игровите и имитационни форми на обучение	Увеличаване на дела на активните методи на обучение (имитационни игри)
Проблемно обучение	Използване на самостоятелното търсене от студента на знания чрез прилагане на проблемния подход от преподавателя на учебния материал	Преминаване от репродуктивен характер на учебните задачи към продуктивен, творчески характер на учебния труд
Модулно обучение	Ясно структуриране на учебния материал с оглед на максималното му усвояване, съпроводено със задължителен блок от упражнения и контрол след всеки фрагмент	Специфична организация на учебния материал – в най-стегнат и достъпен за студента вид
Пълно усвояване на знанията	Разработване на варианти за постигане на учебни резултати (на основата на изменения в параметрите в условията на обучение) за обучаемите с различни способности	Внимание върху резултатите от обучението
Дистанционно обучение	Широк достъп до образователните ресурси, максимално опосредствана роля на преподавателя и самостоятелна, автономна роля на студента	Използване и прилагане на най-новите информационно-комуникативни средства и технологии

От таблица 1 се вижда, че всеки модел на обучение развива определен елемент от системата на образователния процес, като акцентира на неговата практическа част (контекстното обучение) и на методическия инструментариум (имитационното обучение). Според нас, особено внимание заслужават характерът на дейността на обучаемите и на преподавателя (проблемното обучение), начинът на организация на образователния процес (модулното обучение), постигането на ефективен резултат (пълното усвояване на знанията) или използването на специфичните средства за обучение и технологиите (дистанционното обучение). Всеки от разгледаните иновационни модели представлява модернизация на традиционните модели на обучение, разкривайки неизползван потенциал.

В [8] са предложени различни стеганографски алгоритми и характеристики, които са изследвани, като всичко това може да бъде приложено освен в традиционното обучение в магистърска програма „Киберсигурност“, а и в дистанционно обучение в същата учебна програма.

Заключение

На база на гореизложеното може да се направи изводът, че **иновационното образование като цяло не представлява един определен модел, а принцип на рационално използване на новите потенциални възможности на вече известни елементи на образователния процес.**

Иновационният подход във военното образование се определя не чрез използването на един единствен модел, а от способността да се създава и моделира необходимия за съответното висше военно училище елемент на образователния процес, като се използват различни подходи. Точно такава способност прави процеса на обучението във висшето военно училище технологичен, т.е. прогнозируем и съответстващ на планираните резултати. Необходимо е да се добави, че в рамките на такова конструиране е целесъобразно да се използват смесените модели. Например, в системата на дистанционното обучение е много ефективен принципът на модулното обучение, съчетан с модела на пълното усвояване на знанията. Съдържанието на учебния материал е ефективно да се систематизира в модули, а условията на обучение (темпа на усвояване, провеждането на процедурите) да варира на основата на модела за пълно усвояване на знанията. Няма съмнение, че такъв подход е по-перспективен в контекста на развитие на образователните тенденции на XXI век, тъй като позволява да се реши една от важните задачи на “социалната поръчка” - адекватна подготовка на младите хора за отбраната и сигурността на страната. Според нас, за да се създаде иновационен потенциал, е необходимо да се изследват креативните съставни части на процеса, тъй като натрупването на знания и опит чрез иновационн технологии има определящо значение.

Повишаване ефективността от системата на военно образование и наука у нас е един от най - актуалните въпроси за сигурността на страната. Факт е, че равнището на военно образование, научно-техническия прогрес и интелектуалния потенциал имат съществено значение за съвместимостта и воената интеграция на страната не само в рамките на региона, но и в ЕС и НАТО.

Следователно, основен елемент за успешното развитие, функциониране и конкурентоспособност на всяка военно образователна система в дългосрочна перспектива е ефективно развитата иновационна дейност. Организацията и прилагането на научно- образователни програми е главната съставна част на иновационното развитие на едно съвременно общество. Системата на висшето военно образование трябва да изгради гъвкава и адекватна иновационна система за управление, осигуряваща ефективно и дългосрочно развитие на всяка конкретна образователна институция в съответствие с изискванията на обществото като цяло. Всяка иновационна система трябва да отчита тенденциите и реалностите в развитието на световната образователна система, чиято отличителна черта е постоянното усъвършенстване в сферата на висшето образование. Ето защо, усъвършенстването на системата за военно образование е не само начин за решаване на вътрешните проблеми свързани със сигурността и отбраната на страната, но и възможност за надеждно партньорство в системата на европейската отбрана и НАТО.

References:

1. Борисов, Б., Георгиева, Т., Ев.Парашкевова. Процес на осъществяване на инвестиционни проекти в иновационната фирмена дейност. Списание “Диалог” 1, 2009.

2. Великов, Н., Висшето образование в търсене на модел и алгоритъм за ефективно развитие. Сп. “Икономически алтернативи”, бр.3, 2007.

3. Димитрова, В., Система от показатели за стратегическото управление на висшето образование, Сборник с доклади от научно- практическа конференция, В.Търново, 2010.

4. Панайотов, И., Оценяване на качеството на висшето образование, Втора национална научна конференция с муждународно участие на МОМН „Качеството на висшето образование в България – проблеми и перспективи”, Русе, 2009.

5. Станев, Ил., Йорданова, Л., Шест идеи, които ще разтърсят висшето образование, в-к „Капитал”, бр. 35, 03.09.2010.

6. Baregheh A, Rowley J and Sambrook S.Towards a multidisciplinary definition of innovation, *Management decision*, vol. 47, no. 8, 2009.

7. Kozma, R. B., and J. Johnson, The technological revolution comes to the classroom, 1991.

8. Stoyanova V., Possibilities for the application of social networks in transmission of secret information, International scientific conference CONFSEC, ISSN PRINT 2603-2945, ISSN ONLINE 2603-2953, YEAR 1, ISSUE 2(2), 2017.

E-LEARNING - AN ALTERNATIVE TO THE TRADITIONAL

Atanas L. Atanasov

***Abstract**: The paper examines some trends in the development of education and an attempt have been made to predict the changes brought by the technological progress of humanity. A brief feature of e-learning is made as an alternative to traditional education. The advantages of online learning are described and in a synthesized way are presented the advantages and disadvantages of the virtual classroom.*

***Key Words**: e-learning, online learning, innovation technologies, virtual classroom*

ЕЛЕКТРОННОТО ОБРАЗОВАНИЕ – АЛТЕРНАТИВА НА ТРАДИЦИОННОТО

Атанас Л. Атанасов

Национален военен университет „Васил Левски"
Факултет „Артилерия, ПВО и КИС" - гр. Шумен
ул. „Карел Шкорпил" №1, тел. 054/801040, вътр. 54232

1. По какъв начин информационните технологии ще променят образованието?

Постоянният напредък на информационните технологии през последните години неминуемо оказва влияние върху образованието. Днес в много от образователните институции се въвеждат все повече технологии в процеса на преподаване. Благодарение на новите интерактивни инструменти, които са на разположение на обучаеми и обучаващи, онлайн образованието набира все повече популярност и доверие.

Според някои проучвания, към настоящия момент повече от половината от американците притежават таблет или електронен четец. Що се отнася до достъпа до интернет, изчисленията показват, че над 75% от американските домакинства са свързани с глобалната мрежа от вкъщи. Имайки предвид тези статистически данни, логично звучи прогнозата, че онлайн образованието ще заема все по-значима роля в образователната система в САЩ.

В световен план, тенденцията за увеличаващ се достъп до онлайн образователни ресурси е съотносима. Онлайн курсовете предлагани от специализирани образователни сайтове като edX и Coursera свързват обучаващи се от цял свят във виртуални образователни центрове. В общ план, благодарение на интерактивните дъски за обучение, образователни видеа и други интерактивни

средства за обучение, преподавателите успяват да предават информацията на своите студенти по иновативен и по-обхватен начин. На фона на подобна настояща ситуация, предвижданият ефект от информационните технологии върху развитието на образованието в бъдеще е значителен.

Очаква се технологията на виртуалната реалност да намери своето място в образователния процес като спомогне участниците в него да възприемат познанието по революционен начин.

Благодарение на агресивното присъствие на информационните технологии в нашия живот и съответно лесния достъп до информация, реалните практически умения ще бъдат ценени изключително много от работодателите. Поради това, много специалисти предвиждат значението на дипломите и сертификатите да бъде подложено на преоценка.

Настоящето присъствие на смарт устройства като таблети, смартфони и интерактивни дъски ще продължи да се увеличава в бъдеще. Тази тенденция ще допринесе за по-голяма ангажираност и заинтересованост на обучаваните в образователния процес. Що се отнася до преподавателите, те ще могат да се възползват от умните устройства като стимулират учениците да участват по-активно в дискусиите или да им възлагат в реално време анкети и задачи за решаване.

Броят и качеството на виртуалните образователни центрове като edX, Coursera, khan Academy ще продължава да се увеличава. Това ще доведе до положителна конкуренция между настоящите и бъдещите играчи в тази сфера и борба за вниманието на обучаващите се потребители. Според специалисти, все повече утвърдени образователни институции като училища и университети ще включват в своите програми образователните материали и техники създадени от онлайн образователните центрове.

Значимото влияние на новите технологии и достиженията на техниката ще променят изначално връзката между преподавател и учащ. Налаганият досега едностранен канал на общуване ще остане в миналото, а комуникацията между двете страни в образователния процес ще бъде двустранна и напълно непосредствена. Това ще подложи на качествена промяна и класическото физическо пространство, в което се провеждат образователни събития.

Технологията на 3D принтиране ще бъде широко достъпна за все повече образователни институции. Нейното практическо предназначение в редица образователни дисциплини като биология, химия, физика и изобразително изкуство ще бъде осъзнато от ръководните фактори и приложено.

Изброените тенденции в сферата на образованието са само малка част от прогнозираните промени, предизвикани от технологичния прогрес на човечеството. В следващите години ще разберем доколко са изпълними и приложими.

2. Дистанционно обучение в България

Животът на обикновения човек става все по-забързан с всеки изминал ден. В тези дни рядко имаме време да се концентрираме върху всичко, което искаме да направим, и често времето дори се оказва наш враг. Когато около нас постоянно се случват толкова много неща, не можем да си позволим да бъдем ангажирани с всяко едно от тях. Длъжни сме да отсяваме действително нужната информация от второстепенната, за да бъдем наистина продуктивни и ефикасни човешки същества.

Един добър начин това да се случва, без да губим ценно време, е да бъдем мобилни. Колкото и някои хора да отричат това, съвременните технологии ни облагодетелстват. Единствено благода-

рение на Мрежата, към която принадлежат много от нас, и на възможността да притежаваме устройства, с които да бъдем навсякъде, по всяко време, успяваме да се справим с ежедневието си. Планирането на деня, провеждането на срещи и важни разговори все по-често се случва онлайн – нещо, което преди 20 години дори не бихме си представили. С две думи, не бихме имали възможностите, които имаме сега – например живот и работа в чужбина, свободна комуникация с хора от най-различни краища на света и дистанционно обучение.

Макар електронното образование да добива все по-голяма популярност, все още съществува известен скептицизъм по отношение на резултатите от него. Дистанционното обучение е за някои държави неразбираемо и ненужно, а в други такива вече е установена практика. За щастие, в България то бавно, но сигурно набира скорост. „За щастие”, защото стандартното образование в България е не само в застой, но и в по-голяма криза с всяка изминала година; крайно време е да се

въведе алтернатива.

Електронното образование не е твърде различно от класическото, както може би много хора си мислят. Алтернативата не се характеризира с нов, съвършено различен метод на обучение, а с възможностите, които се отварят пред всекиго, решил да се възползва от подобна образователна програма. Но каквото и да говорим, традиционното училище действително започва да изглежда сложно и „демоде”, някак неподходящо за времената, в които живеем. А в човека е заложено да се движи напред и да улеснява процесите в живота си – защо да не улесним и начина, по който да се учим?

Важно е да си припомним, че дори само преди век много малко хора са имали възможността да получат образование, качествено или каквото и да било. Но колкото по-образовани ставаме, толкова повече осъзнаваме и нуждата от образованието – затова и днес можем да се похвалим с наличието на толкова училища, колежи, програми за обучение. А в България все по-често се срещат критики по отношение на материала, преподаван в училище, компетенцията на преподавателите и несъответствието между стандарти и изисквания.

Това въздейства по различен начин на различните хора – някои заминават в чужбина, където да следват висше образование или децата им да получат средно; други избират да не изпращат децата си в редовно училище. А трети изобщо не могат да си позволят този лукс; нито имат възможност да бъдат образовани и да развиват талантите си, а е редно всички да имат равни възможности по отношение на образованието си. Никой, желаещ да се учи, не бива да бъде подминаван с равнодушие, а да се направи опит той да получи знанието, необходимо за неговото личностно развитие. Електронното образование може да бъде решението на всички тези проблеми.

Всеки, който е бил студент, е донякъде запознат с дистанционното образование – тъй като задочната форма на обучение е дистанционна. Както споменахме, алтернативните форми на обучение не са твърде различни от конвенционалните – те все още включват заучаването на определена информация, решаването на упражнения и развиване на мисълта и способността за логически заключения.

Колкото и да губи влиянието си върху учениците, класическото образование е все още живо и е най-практикуваната форма на обучение. За съжаление, то разчита най-вече на квалифицирани преподаватели, за да може да има нужния ефект върху всеки ученик. А в България откриването на наистина компетентен учител вече представлява трудност. Хипотетично, училищата биха съществували още дълго време при наличието на подходяща база от страна на преподавателите. Но когато станем свидетели на отсъствието на тази база, логично е да се запитаме – защо изобщо да ходим на училище?

С риск това заключение да изглежда възмутително – всъщност, не е нужно да ходим на училище. Един от начините, по които Мрежата ни помага да не изпускаме живота си и да осъществим целите си, без да полагаме очаквания труд, е възможността да се обучаваме онлайн. Нарастващата популярност на тази услуга се дължи на голямата цифра хора, уверили се от първа ръка в ефективността на такъв метод на обучение. А тези, които нямат възможността да отидат на училище, по една или друга причина? За тях това дори не е алтернатива, а единственият път да постигнат целите, които преследват.

Всеки би получил позитивни резултати от своето онлайн обучение, благодарение на няколко фактора: виртуалната комуникация, определеното от самия клиент време за провеждане на курсовете и квалификацията на преподавателите. Това би позволило на всекиго да осъзнае собствените си нужди и да получи знанията, необходими за неговото израстване – академично или професионално.

Много хора са на мнение, че виртуалното общуване не може да пресъздаде средата, която създава разговорът очи в очи, но именно фактът, че наблюдавате преподавателя или ученика си през екрана, дава поле за повече концентрация: виртуалната среда е по-формална. Що се отнася до личното време, всеки сам избира кога да се обучава, както и да се консултира с преподавателя си.

Ние смятаме, че дистанционното обучение е бъдещето на глобалното образование. Не всеки може да си позволи да посещава частни курсове или училище, или пък не всеки може да надгради професионалните си знания до степента, нужна за кандидатстване за по-висока работна позиция. Но електронното обучение скоро ще бъде разпространено до нивото, в което се застъпва не само специализирано образование – за ВУЗ или корпоративно обучение, – но и базовите знания,

нужни на всеки от нас. Може да звучи утопично, но не е ли чудесно всеки да може да получи нужното образование, без дори да напуска дома си? Бъдещето е пред нас.

3. Кои са предимствата, надделяващи при избора на онлайн обучение?

Виртуалния свят създава неограничени възможности за обучаващите се. На първо място, студентът не губи време да влезе в клас и на практика спестява пари. Освен това не се изисква да отиде на определено място, за да получи достъп до онлайн образование. Виртуалните класни стаи обединяват разстоянието между преподавателите и студентите, които могат да бъдат на разстояние километри и дори на различни континенти.

Човек може да посещава онлайн курсове у дома или на работното място. Какво е необходимо? Само добра интернет връзка, компютър и желание. Учете в интерактивна виртуална класна стая с учители на живо. Благодарение на уникални платформи и новите технологии всеки има достъп до най-добрите преподаватели, от всяка част на страната, по всяко време. Така се комбинират предимствата между класическото преподаване и неограничените възможности на новите технологии.

Във Факултет „А, ПВО и КИС“ гр. Шумен при НВУ „В. Левски“ например се прилага обучение в различни бакалавърски и магистърски програми, които в минимална степен използват възможностите на виртуалния свят. [1] Лесно би било използвано, ако се реализира една виртуална класна стая и така обучаемите с лекота биха експериментирали с изложените постулати и биха могли да проверят и потвърдят верността на изследователските данни.

Виртуалният свят всъщност имитира реалния свят и позволява на студентите да изразяват и съмнения. Във виртуална класна стая обучаващия се може да подаде заявка или да вдигне ръката си, когато има въпрос. По този начин учителят може да разрешава проблема, когато са в почивка. В реалния свят за да зададе въпроса си обучаващия би трябвало да прекъсне учителя. Във виртуалната класна стая се вижда и учителят, който социализира средата, а освен това влага индивидуален подход според нуждите на обучаващите се.

Друга чудесна особеност на този тип обучение е, че човек може да запише сесията и да я отложи за по-късно. Така не пропуска класове. С помощта на учителите обучаващите се получават допълнително внимание, което обикновено не успяват в големите, традиционни класни стаи. С толкова много инструменти и функции, учебният процес е много по-опростен. Така ефективността е по-голяма и за по-кратко време се усвоява повече материал. Всъщност човек наистина може да схване теми, които трудно се разбират в истинската класна стая.

С развитието на образованието, виртуалните класни стаи лека полека се установяват и успешно биха заменили традиционната класна стая!

4. Виртуална класна стая – предимства и недостатъци

Виртуалната класна стая представлява онлайн учебна среда, която може да бъде уеб базирана и достъпна чрез портал или основана на софтуер, изискващ сваляне на изпълним файл. Подобно на реална класна стая, виртуалната стая предоставя синхронно обучение, т.е. учителят и учениците попадат във виртуалната учебна среда едновременно. Имат възможността да общуват, да гледат презентации или видеоклипове, да взаимодействат помежду си и да се ангажират с ресурси в работни групи.

Някой от предимствата на виртуалните класни стаи са:

Неограниченост - участниците по целия свят се включват в класове на живо, сътрудничат си и взаимодействат помежду си;

Финансово достъпни-ниските разходи са огромно предимство. Учещите могат да спестят пари, отпадат и пътните разходи. Освен това спестяват време, тъй като се нуждаят само от интернет връзка.

Гъвкавост на обучението - всяка аудио и визуална презентация може да бъде записана. Така съдържанието остава достъпно, което е от голяма полза при бързо опресняване или попълване на пропуски.

Достъпност – предоставят чудесни възможности за импровизирани срещи и групови проекти, където участниците обменят идеи.

Какви са недостатъците? Да разгледаме някои неблагоприятни аспекти:

Виртуалните стаи са безлични - винаги ще има хора, предпочитащи традиционното пред онлайн обучението. Някои учители и ученици не се чувстват комфортно с идеята да участват в курс, който се преподава изцяло онлайн;

Необходимост от допълнително обучение - повечето виртуални класни стаи са проектирани да се използват интуитивно и участниците, използващи технологии от този вид се чувстват комфортно. Някои обаче ще се нуждаят от допълнително обучение;

Липса на социализация.

Въпреки това недостатъците са незначими на фона на предимствата и включването на виртуална класна стая като форма на обучение в учебно заведение е стъпка към успеха.

Така се дава предимство на дистанционното обучение, чиито основен недостатък е липсата на директна комуникация, а и на чувство за общност между обучаващите се.

References:

1. Veselka Stoyanova, Zhaneta Tasheva, RESEARCH OF THE CHARACTERISTICS OF A STEGANOGRAPHY ALGORITHM BASED ON LSB METHOD OF EMBEDDING INFORMATION IN IMAGES ,*Publication: Trans MotAuto15*. Available from: https://www.researchgate.net/publication/304579312_Trans_MotAuto15, accessed June 30, 2018.

2. Станев Ил., Йорданова, Л., Шест идеи, които ще разтърсят висшето образование, в-к „Капитал”, бр. 35, 03.09.2010.

3. Baregheh A., Rowley J. and Sambrook S. Towards a multidisciplinary definition of innovation, *Management decision*, vol. 47, no. 8, 2009.

4. Kozma, R. B., and J. Johnson, The technological revolution comes to the classroom, 1991.

V. P. Petrov,

STRATEGIC COMMUNICATIONS OF THE USA

Veliko P. Petrov

Abstract**:** *This report aims to familiarize readers with the "strategic communications" of the United States. The specifics of strategic communications were studied in relation to traditional forms of communication activity. The four main parts that are included in the "Strategic Communications" are discussed. The basic principles, components, parameters of strategic communications are revealed. The implementation of the Strategic Communication process involves several key stages. Five sets of scientific and technical tools used for the interests of forming a "trust zone" for "strategic communications" are addressed in the US Military Classification. Discussions are being discussed in US state authorities on the content of "strategic communications". The effectiveness of strategic communications will be of key importance in the 21st century and the US and its allies will reaffirm their understanding of the strategic role of communications.*

Keywords**:** *strategic communications, USA,*

СТРАТЕГИЧЕСКИТЕ КОМУНИКАЦИИ НА САЩ

Велико П. Петров

National Military University "Vasil Levski", Faculty of Artillery, Air Defense and Communications and Information Systems, Department of Information Security; town of Shumen.

“*Да победиш врага си, без да се биеш, е върхът на военното изкуство*”.
Сун Дзъ, IV в. пр.н.е.

От най-далечни времена са известни примери, които показват, че хората използват комуникация като средство за убеждаване, влияние върху вярванията и поведението на другите, често за изграждане на желания от тях имидж и разрушаване на противниковия публичен образ, а нерядко – за изучаване, осигуряване на благоприятно обществено мнение или пък за справяне с отрицателното[1].

Според Wikipendia стратегическите комуникации могат да означат концепция, процес или данни, които да подпомагат дългосрочните цели на организацията и изпълнението на плановете й. Стратегическите комуникации започват да се използват като понятие от 1990 г. насам, като най-много публикации за тях има в периода след 2001 г. За стратегическите комуникации пишат много автори, но по-известни от тях са: Дан О'Хеър, Буртон Каплан, Сали Рей, Сали Патерсън, Дейвид Джоплин, Даниел Кинг, Густав Фридрих, Линда Диксън, Джон Уайт и др.

Съгласно съвременните схващания стратегическите комуникации обхващат няколко основни домейни или специфични места и платформи, които трябва да бъдат изградени, за да говорим за подобен тип дейности. Домейните са следните: *технологичен*, базиран на информационни и дигитални технологии; *познавателен* – ориентиран към управление и трансфер на знание; *визии* за бъдещи инициативи и действия; *административен* – за синхронизиране на идеи, теми и практики; *подготовка на вероятни сценарии* за преодоляване на критични проблеми; и *логистичен*, свързан с визуализиране на процеси и картографиране на важни точки от инфраструктурата.

[1] Сашо Воденичарски, Артефакти на стратегическите комуникации от древен Египет, Годишник на ВА“Г. Раковски“, Факултет „Национална сигурност и отбрана“, кн 3 от 2013 г., стр.190.

През последните няколко години терминът „Стратегическа комуникация"[2] (СК) започна да се използва с нарастваща популярност. Обаче различното използване на термина довежда до съществен безпорядък. В резултат на това е необходимо да се разясни какво се разбира под "Стратегическа комуникация".

Терминът „Стратегическа комуникация" получава разпространение преди всичко в САЩ, както в научните кръгове и среди, така и в политиката, военното дело, бизнеса. От началото на 21 век в тази страна намират своето място много опити да се даде разностранна и систематизирана оценка на значимостта на СК във външната политика и осигуряването на националната сигурност на страната. Тук можем да се позовем както на съответните научни изследвания и материали от научни конференции, така и на голям брой документи на Министерството на отбраната, Държавния Департамент и други държавни структури на САЩ.

Към "Стратегическата комуникация" се отнасят:

– синхронизацията на *думи, дела и действия* и това, как те ще бъдат *възприети от подбраните аудитории;*

– програмите и действия, съзнателно насочени към общуването и привличането на целеви аудитории, включително и *осъществяваните посредством връзките с обществеността, публична (обществена) дипломация, информационните операции и психологическите операции.*

Подход за ефективно между институционално взаимодействие и търсене на по-добра комуникация е възприет от САЩ и доктринално е регламентиран в тяхната Концепция за стратегическа комуникация (Strategic Communications Concept). Концепцията е особено ефективна при конфликти като в Ирак и Афганистан, когато военни операции се водят срещу бунтовници и се налага те да бъдат подтикнати към нов начин на мислене, да се въведе промяна в отношението и нагласите на гражданското население, да се насочи съзнанието към различни идеи и възгледи и в крайна сметка да бъде променено тяхното поведение. Въздействието върху аудиторията е ключов елемент от промяната, защото бунтовниците са организирани групи, водени от идеите за промяна на политическите, икономическите, социалните и културните страни на обществения живот, които не съответстват на собствените им възгледи. По тази причина стратегическите комуникации са насочени едновременно към ограничаване или елиминиране на въздействието на бунтовническите сили върху местното население и целенасочена промяна на неговите възгледи, нагласи и поведение.

Стратегическата комуникация не е просто ново направление в информационните войни (ИВ) – това е новата концепция за самите информационни войни, приета като развитие на теорията за информационните операции, която активно се разработваше от Държавния департамент, от Министерството на отбраната, от други правителствени и неправителствени учреждения и организации на САЩ. Определението на СК от доклада на Белия Дом пред Конгреса на САЩ от 16.03.2010 г. "***Национални рамки на стратегическата комуникация***", доколкото даденият документ отразява последния към днешна дата официален подход към разбирането на СК президентско ниво и по тази причина оказва непосредствено въздействие на СК на САЩ. Под стратегическа комуникация се разбира ***комплексът от мероприятия по целенасоченото въздействие върху военнополитическото ръководство, различните обществено-политически сили, международните организации, т. е. върху така наречената „целева аудитория"[3] (ЦА) на другите страни (както враждебни, така и съюзни, и неутрални), предприемани от различните правителствени и неправителствени учреждения и организации на САЩ, както и на техните съюзници.***

В това определение се прави напълно уместно стопиране на необходимостта от синхронизация на думи и дела, доколкото опитът от първото десетилетие на 21 век дава в лицето на администрацията на Дж. Буш – не най-добрия пример за такава синхронизация в историята на САЩ и може би, един от най-лошите варианти на възприемане на думите и действията на САЩ на международната арена, даже и от техните най-близки съюзници.

2 Стратегически комуникации - това разбиране, бе въведено в употреба от министерството на отбраната на САЩ през септември 2006 г. със знанието и съгласието на тогавашния министър на отбраната Д. Рамсфелд в документа „***Пътна карта (план) за СК***". Днес е одобрен от Комитета на началник щабовете (КНЩ) за включване в обновеното издание JP.

3 ***Под целева аудитория*** се разбира не само и не толкова общността от хора, обединена по национални, социални или имуществени признаци, живеещи в която и да е страна, а преди всичко общността, споделяща единна ценностна система.

В обхвата на „Стратегическите комуникации" са включени **четири основни части** (показано на фиг. 1.)**:**

– връзки с обществеността – провеждани от военните (Military Public Affairs) и провеждани от цивилните (Public Affairs);

– публична (обществена) дипломация (Public diplomacy);

– информационни операции (Information Operations – Info Ops;

– психологически операции (Psychological Operations – PSYOPS).

Четирите основни части на „Стратегическите комуникации" са взаимно свързани помежду си, но всяка част от тях си има и *своите особености*.

Фиг. 1. Обхват на стратегическите комуникации[4]

САЩ имат отдавнашна традиция да влияят на народите от другите страни посредством публичната (обществената) дипломация. Последната дава ценно допълнение на традиционната междудържавна дипломация, в която преобладава официалното взаимодействие на професионалните дипломати. За разлика от връзките с обществеността, насочени предимно към информиране и влияние върху населението и средствата за масова информация на САЩ, публичната дипломация включва и усилията по прякото взаимодействие с гражданите, обществените дейци, журналистите и други лидери на общественото мнение извън пределите на страната. Публичната дипломация е призвана да оказва влияние на отношението към политиката и националните интереси на САЩ, да подбужда към действия за тяхната поддръжка и подкрепа. Това може да се забележи от доклада на Белия Дом пред Конгреса на САЩ от 16 март 2010 г.

В Обединената доктрина за информационни операции на обединените началници на щабове (февруари 2006 г.) се дава следното определение за **информационните операции**: „Информационните операции са неотделима част от успешното изпълнение на военните операции. Главната цел на информационните операции се състои в това, да се постигне и поддържа информационното превъзходство на САЩ и неговите съюзници. Информационното превъзходство осигурява обединените сили с конкурентоспособно преимущество само тогава, когато то ефективно се проявява в съответните решения. Информационните операции представляват *интегрирано използване на радиоелектронната война, компютърните мрежови операции, психологическите операции, военното заблуждаване и оперативна сигурност, включващи техните съпътстващи и приложни аспекти, с цел да се повлияе, да се разруши, да се притесни или да се попречи на процеса на човешкото или автоматизираното взимане на решения от противника, защитавайки нашия собствен интерес или взето решение"*.

В съюзната доктрина за информационни операции AJP-3.10[5] е дадено следното определение „*информационната операция е военна функция за предоставяне на консултации и координация на военните информационни дейности с цел да се създаде желания ефект върху волята, разбирането и способността на противници, потенциални противници и други участници в подкрепа на целите на операцията*". Тези операции се съпътстват от информационни дейности, които са действия предназначени да повлияят на информацията и информационните системи.

4 Сашо Воденичарски, Артефакти на стратегическите комуникации от древен Египет, Годишник на ВА"Г. Раковски", Факултет „Национална сигурност и отбрана", кн 3 от 2013 г., стр.190.
5 AJP-3.10 „Allied Joint Doctrine, for Information Operations", 2009, p. 23.

В полевото ръководство „Психологически операции" на сухопътните войски на американската армия е дадена една от най-съдържателните дефиниции за психологически операции – *планирана употреба на медии и действия за разпространяване на подбрана информация и индикатори сред чуждестранна аудитория, която влияе на емоциите, мотивите и в крайна сметка на поведението на чуждестранни правителства, организации, групи хора и личности.* Целта на психологическите операции е да предизвика нагласи и поведение, благоприятни за замисъла на планираните операции. Понятието психологически операции е с по-широко съдържание от психологическа война, защото включва и действия, които могат да бъдат насочени и към приятелски и неутрални аудитории, докато психологическата война е насочена само към враждебна целева аудитория.

Под връзки с обществеността (*Public Affairs*) в отбраната се разбира публичната информация (контакти със средства за масово осведомяване), вътрешната информация (наричана още командна) и дейностите за връзки с местната общественост, насочени както към вътрешните, така и към външните аудитории на институцията.

Необходимите условия за успешни и ефективни стратегически комуникации са:

• *Да бъдат едновременно бързи и съгласувани.* По този начин рязко нарастват шансовете на действащите лица да са част от аудиторията и нейния начин на мислене, но същевременно се изисква много интензивно сътрудничество по веригата на политико-военната йерархия и в рамките на различните отдели, дирекции, министерства и ведомства в отделните страни, участващи в операцията.

• *Да бъдат упълномощени достатъчно лица от политико-военното равнище на командване да комуникират с аудиторията.* Сегашната традиционна структура и система за предоставяне на права за оповестява не на информация и комуникация от старшите звена на подчинените значително забавя скоростта на комуникациите. Ето защо е необходимо да бъдат упълномощени повече хора по командната верига да комуникират по различни канали, като, разбира се, това не отменя изискването за нейната съгласуваност.

Горните изисквания зависят изцяло от съществуващата командна и организационна структура и успешните стратегически комуникации до голяма степен ще се определят от намирането на компромисно решение за изграждане на нова гъвкава и ефективна мрежова структура за управление на информационните потоци и дейности, съответстваща на новата оперативна среда.

Могат да бъдат изведени още няколко важни съображения, свързани със същността на понятието „стратегически комуникации":

– то не бива да се възприема като заблуждаване или манипулиране на общественото мнение или определена аудитория;

– понятието „стратегически комуникации" следва да се възприема в контекста на целенасочено въздействие, чрез прецизно координиране на информацията и интегрирани комуникационни способности;

– понятието „стратегически комуникации" не бива да се разбира като задължение само на стратегическото ниво да комуникира с различните целеви аудитории, доколкото оперативното и тактическото ниво също следва да бъдат изцяло ангажирани с тези процеси;

– стратегическите комуникации трябва да се възприемат като съвкупност от координирани дейности, писмени и вербални обръщения и послания от политически фигури, представители на командната структура на САЩ, лидери на участващи в операцията, представители на средствата за масово осведомяване или граждански организации, насочени към промяна на отношението и поведението на определена аудитория;

– понятието „стратегически комуникации" изисква процесът на организирането им и съответно правата, задълженията и отговорностите на участващите в тях да бъдат ясно и точно регламентирани.

САЩ разполагат с редица конкурентни предимства за осъществяване на „стратегическа комуникация" в света. Сред тях ще разграничим:

1) Запазващите се и продължаващи икономическо, военно и научно превъзходство и надмощие на САЩ в съвременния свят (въпреки че те все по-бързо изчезват);

2) Глобалната система на контролиране на военно-политическите и икономическите съюзи, транснационалните институти;

3) Превес и надмощие в сферата на масовата култура в общественото съзнание на Земното кълбо над културното влияние на другите държави;

4) Превъзходство в глобалните средства за масова информация над която и да е, друга страна по света;

5) Превъзходство в теоретичната и практическата разработка на националната концепция за стратегическата комуникация.

Стратегическата комуникация е невъзможна без ефективно стратегическо разузнаване. За това има обективни причини. За ефективното осъществяване на стратегическата комуникация е *задължително провеждането на щателно изследване с цел да се постигне точна представа за същностните характеристики на подлежащите на комплексно въздействие (политическо, икономическо, културно, информационно-психологическо и др.) целеви аудитории, за разнообразната среда на обитаване на дадена целева група, на външните въздействия (тяхната история и настояще) и, разбира се, тяхната ефективност*. Необходимо е адекватно да се оценява динамиката на състоянието на обекта, като се разграничат вътрешните и външни противоречия на развитие и много други, които се намират в голяма част в открити източници, но изискват многостранна обработка на получаваните данни от това множество източници.

Министерството на отбраната на САЩ в интерес на развиване на концепцията през март 2008 г. проведе първата конференция на базата на колежа на комитета на началниците на щабове в гр. Норфолк, където бяха определени ***основните принципи на „стратегическите комуникации"***: *квалифицирано ръководство, правдоподобие, достъпност, диалог, мащабност, съгласуваност, целенасоченост, оперативност, последователност, приемственост и непрекъснатост.* За уточняване на концепцията за стратегическата комуникация се планира на всеки две години тези принципи да се коригират.

Принцип на квалифицираното ръководство. Ръководителите са длъжни ясно и точно да представят задачите на стратегическата комуникация за постигане на поставените цели във всички области на своята дейност, включително материално-техническото осигуряване и разузнаването.

Принцип на правдоподобието. Действията, тяхното възприемане и обяснение трябва да бъдат правилно интерпретирани и отчетливо координирани, а също така да предизвикват доверие у целевата аудитория.

Принцип на достъпността. Необходимо е задълбочено разбиране на културата, идентичността, начина на живот, историята и обществения строй на целевата аудитория. Аудиторията възприема действията в съответствие със собствената си ценностна скала. Без разбиране на манталитета на целевата аудитория е невъзможно постигането на даден резултат. Осъзнаването на влиянието на субективните фактори (културното, лингвистичното, историческото, религиозното, природното и други) е важно за ефективното въздействие върху целевата аудитория. При това изграждането на отношения и взаимодействие с различните организации, с местното население, с научните кръгове, с търговските и не търговските организации спомага за най-доброто разбиране на целевата аудитория.

Принцип на диалога. Многостранният обмен на мнения спомага за взаимното разбирането и установяването на отношения на доверие.

Принцип на мащабността. Стратегическите комуникации нямат временни или пространствени граници.

Принцип на съгласуваности на действията. Стратегическите комуникации означават съгласувани, интегрирани на всички нива в единна система действия, т.е. те са процес, извършващ се по единен замисъл и план на всички нива на йерархията, както по „вертикалата" – от тактическото до стратегическото ниво, така и по „хоризонталата" – в пределите на едно ниво. Ръководителите координират и съгласуват своите действия, възможности и средства в зоните на отговорност, влияние и интереси с цел постигане на очаквания резултат. Всяка структура или организация е част от системата на комуникациите.

Принцип на целенасочеността. Стратегическите комуникации трябва да бъдат насочени към получаване на конкретно зададен (желан) резултат. Това не е само „още едно средство в арсенала на ръководителя", а ръководство за действие на всички структури, съгласувано по задачи за постигане на поставените цели. Процесът на комуникация, съдържанието, целите и практическите стъпки зависят от политиката, стратегическите възгледи, подходите към планирането на операциите и приетите управленски решения.

Принцип на оперативността . Необходим е правилен избор на аудитория, информация, време и място за провеждане на акциите. Стратегическите комуникации трябва да са фокусирани върху дългосрочни резултати. Оперативното реагиране на изменящите се условия и кризисните ситуации могат да дадат стратегически ефект. Стратегическите комуникации трябва да достигат до целевата аудитория посредством специални съобщения, важни именно за дадената аудитория. Стратегическите комуникации водят към необходимостта от широко обсъждане на проблема за синхронизация на идеите, действията и информацията за постигане на глобалните стратегически цели. При това влиянието върху процеса на вземане на решения от противника е ключов момент и често пъти е ограничен от временните рамки за информационно въздействие с цел постигане на желания ефект.

Принцип на непрекъснатостта. Стратегическата комуникация е непрекъснат процес, за успешното осъществяване на който е необходимо наличие на постоянна обратна връзка между планиране и действия, от една страна, и анализ с оценка на резултатите от тези действия – от друга страна. В идеалния случай този процес трябва да преминава по-бързо, отколкото при противника.

Процесът на реализация на Стратегическата комуникация се състои от следните етапи:

– уточняване на политическите цели;

– разпознаване на целевата аудитория;

– определяне на желания поведенчески ефект на обекта на въздействие;

– провеждане на анализ на аудиторията (какви са нейните представи, позиции, поведение и как е необходимо да се променят);

– определяне на идеологическите цели и ориентация;

– формулиране на основите цели за подготвените съобщения и планираните акции;

– съгласуване на информационното въздействие, организираните акции и политическите действия;

– синхронизация на действията на носителите на информация по време на рамката;

– планиране на първостепенните и неотложните мероприятия и контрамерките;

– оценка на резултатите и коригиране на плановете.

В качеството на носители на информация, съгласно концепцията на стратегическата комуникация, роля могат да играят *информационните и физическите домейни*.

Към <u>информационните домейни</u> се отнасят радиото, наземната, кабелната и спътниковата телевизия, печатът, Интернет, поточното видео, мобилните телефони, обществените организации и слуховете.

<u>Физически домейни</u> са войсковите учения, демонстрацията на сила, визитите, конференциите, различните работни семинари, научни и военни обмени на опит, асоциацията на випускниците, организацията и провеждането на възстановителни работи, търговията и хуманитарната помощ, благодарение на които военнополитическото ръководство на САЩ се опитва да предизвика симпатия към своята страна и нейните ВС или страх пред тяхната мощ.

Арсеналът от средства на стратегическата комуникация е разнообразен. Към тях преди всичко се отнасят средствата за масова информация (СМИ), а също така свръзките и телекомуникациите, инфраструктурата на безжичната връзка, социологическите изследвания, културологичните и лингвистичните средства, избирателните технологии и методики за преброяване на гласовете на избирателите, масовите тренинги и образователните програми.

Съгласно решението на американския конгрес, научноизследователски работи по използване на теорията на стратегическата комуникация се организират и провеждат в министерството на отбраната на САЩ, в бойните командвания, в управлението на заместника на МО по разузнаването, в обединения щаб и Държавния департамент. Непосредствено в МО за организацията на

изследванията отговаря заместника на министъра по придобиване, технологии и логистика (Undersecretary for Acquisition, Technology and Logistics - AT&L). Във военното ведомство активно се провеждат и научноизследователски работи по развитието на средствата за моделиране и оценка на социалните компютърни мрежи, мониторинга на СМИ, моделирането на динамиката на развитие на различни системи и създаване на единна среда на „стратегическите комуникации", както вътре в министерството на отбраната, така и между различните ведомства.

През всяка финансова година се заделят средства за мероприятия, свързани с изследването и създаването на нови технологии по формиране на „зона на доверие" за „стратегическите комуникации". Разработки се осъществяват също така и в сферата на контрол и анализ на компютърните мрежи, машинния превод, иновационния анализ и избирателните технологии.

Отделът за технологии за бързо реагиране (Rapid Reaction Technology Office - RRTO) при управлението на НИОКР и техниките и отделът за осигуряване на нетрадиционни бойни действия (Irregular Warfare Support - IWS) при апарата на помощник министъра на отбраната по специоперациите и конфликтите с ниска интензивност и взаимосвързаните възможности (Special Operations Low-Intensity Conflict and Interdependent Capabilities - SO/LIC-IC) се занимават с изследвания в областта на използване на възможностите на теорията на стратегическите комуникации в общодържавен мащаб. Тези структури са наложили тясно взаимодействие със съответните апарати на Държавния секретар по въпросите на публичната дипломация и връзките с обществеността, с националния контра терористичен център, с агентството на САЩ по международното развитие, с министерствата на вътрешната сигурност и правосъдието, както и с неправителствените организации.

Научно-техническите средства, използвани за интересите на формиране на „зона на доверие" за „стратегическите комуникации", по класификацията на МО на САЩ се *подразделят на пет групи:*

Първата група – ***средства за анализ на информацията***, осигуряваща и предоставяща достъп до обекти на инфраструктурата. Те анализират целия спектър информационни ресурси, започвайки от обичайните новини и завършвайки с професионална информация за пазара.

С помощта на дадените средства се провежда семантичен анализ на съобщенията, насочен към откриване в различните мрежови СМИ на страна или регион на тематична информация, характеризираща позицията по въпросите, засягащи сигурността или създаващи заплаха за националните интереси на САЩ. С цел разкриване на идеологиите, формите и начините за действие на екстремистите, а също така и за установяване на техните лидери се планира да се осъществява постоянен (денонощен) контрол на интернет-дневниците (блоговете), интернет-сайтовете, сайтовете за обмен на файлове от типа на *YouTube* или *Twitter*, да се определят идентификационните данни на ползвателите, да публикуват свои съобщения на тези сайтове и да се води контрапропаганда в информационните мрежи.

Освен това, се предполага развиване на предаванията в КВ- и УКВ- диапазоните чрез спътници-ретранслатори, разположени на геостационарни орбити, които осигуряват възможност за приемане на сигнала чрез обикновени радиоприемници на територията на враждебните за САЩ страни.

Втората група – ***обществени средства за масови комуникации*** – това са информационни бази от данни, непосредствено СМИ, виртуалните сдружения.

САЩ планират създаването на интегрирани социални мрежи на платформата Web 2.0 мултимедия в страните със слабо развита телекомуникационна инфраструктура, които използват клетъчна връзка за изход в Интернет. Това е най-актуално за държавите, намиращи се в определената зона на отговорност на централното, европейското и африканското командване на ВС на САЩ.

В системата за анализ и контрол на социалните мрежи се планира да се обърне особено внимание преди всичко на разкриване на социалните връзки на ръководството и другите ключови фигури на различните страни и изучаване на техния психологически портрет. Техническите възможности позволяват да се осигури мрежова идентификация на всеки един ползвател по неговите мрежови връзки (контакти).

Третата група – „***средства на диалога***", които са предназначени за анализ на радикалните и контра радикалните послания и идеи.

При това се извършва анализ в мащаб, близък до реалността, времето и подреждането по степента на важност на съобщенията в СМИ. Програмното осигуряване позволява ежедневно да се проверяват множество вестници във всяка европейска страна, да се подбират съобщения по ключовите думи, да се класират позитивните и негативните изказвания, засягащи интересите на САЩ.

Четвъртата група – ***средства за моделиране и прогноза***, които използват игровото и алтернативното, многовариантно моделиране за целите на прогнозиране на развитието на обстановката на основата на получените данни, както и прогнозиране на възможните реакции на целевата аудитория при целенасоченото информационно въздействие.

Петата група – ***средства за тренировка на взаимодействието***, използвани за отработване на въпросите на взаимодействие както вътре в правителствените структури, така и междуправителствените учреждения и неправителствените организации.

Днес нито МО на САЩ, нито Държавния департамент имат единна база, където се събира аналитична информация, получена в резултат на дейността на агентства в рамките на концепцията за „стратегическите комуникации". За изграждане на единна банка данни ще са необходими около 2-3 млн. долара. Дадената банка ще стане основа за създаване на единна автоматизирана система за ситуационен анализ и предупреждаване, струваща около 9-10 млн. долара. По мнението на експертите на министерството на отбраната на страната, въвеждането в експлоатация на дадената система ще позволи съществено да се съкрати времето за вземане на решения и да се постигне значително информационно превъзходство.

За ефективното функциониране на изброените средства са необходими помощ, екипировка, осигуряване с технически средства, обучение и стимулиране на СМИ, предназначени за осигуряване на „свободно" осветляване на събитията по дадена тематика.

С привличането на горе назованите средства се извършва търсене на начини за разпределяне на локалните ресурси с достъп през Интернет (книги, филми, списания и т.н., съдържащи елементи на въздействие върху целевата аудитория), достъпни за изтегляне от всеки ползвател.

Предполага се, при помощта на специално подбрани публикации, разкази, митове, символични асоциации, компютърни игри да се изгради в мрежата, и преди всичко у мюсюлманското население, ново, изгодно за американското ръководство възприемане на публичната дипломация на САЩ.

При това е важно да се вземе под внимание нивото на развитие на страната, културата, избирателната система, във връзка с което се набелязва да бъдат създадени средства и бази от данни, адаптирани към лингвистичните, социалните и културните особености на целевата аудитория. Освен това, планира се провеждане на изследвания в областта на културологичните различия, особеностите на мисловния процес и процеса на вземане на решения от целевата аудитория.

Също така ще бъдат проведени мероприятия по организацията на физиологичната защита на персонала за стратегическите комуникации в случай на нарастване на социалното напрежение, стихийни бедствия или използване на оръжие за масово поразяване.

По такъв начин концепцията за стратегическите комуникации е една от основополагащите в системата на информационното противоборство на САЩ.

Мероприятията по информационно въздействие върху военнополитическото ръководство и общественото мнение на различните страни, върху световната общност като цяло се провеждат не само като съставна част на комплекса мероприятия по подготовката за операции (бойни действия), а вече стават тяхно основно съдържание.

Развиването на концепцията за стратегическите комуникации е продължение на стратегията за непреки действия, заключаваща се във въздействието върху отделните, не главни елементи на системата, промяната на състоянието на които в резултат на това довежда до преход на системата в нужното състояние.

Изводи:

1) Стратегическите комуникации представляват оркестриране и синхронизиране на действия, образи и думи с цел постигане на желания ефект. Лидерите са двигателната сила на стратегическите комуникации, те трябва да поставят комуникациите в основата на всяко действие. Успешната стратегическа комуникация означава интегрирани действия и послания и ясно лидерско поведение.

2) Не е трудно да се забележи, че във външнополитическата сфера „стратегическата комуникация" представлява синхронизация на въздействието чрез „слово и дело" върху приятелите и съюзниците и разнообразен спектър на използване на комуникациите в рамките на информационното противоборство. Но отделянето на едното от другото на практика става крайно сложно по следните причини:

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

– в съвременния свят, отбелязват специалистите, границите между войната и мира, военните и гражданските системи и пространства, както и между информирането и влиянието или манипулирането все повече са размити. Тези изменения закономерно поставят въпроса за новите способи за защита на обществото. Разпространението и влиянието върху човешкото съзнание на бойното поле е имало място и по-рано. Но професионалното водене на бой в съзнанието и подсъзнанието на хората, с използване на сложни методи на комуникационно въздействие на глобално ниво с масово потапяне на все по-голяма част от човечеството във виртуалния свят на Интернет, социалните мрежи позволяват, да се развиват нови видове информационно въздействие и информационно оръжие.

3) Средствата за масова информация и комуникации, откритите информационни ресурси, глобалната информационна мрежа на Интернет активно се използват от министерството на отбраната и Държавния департамент на САЩ не само за мониторинг на заплахите за националната сигурност на страната, за проучване на общественото мнение, позицията на държавите по отношение на САЩ, но и с цел манипулиране на общественото мнение, дезинформация и въвеждане в заблуда на военнополитическото ръководство на другите страни, принуждаването му към вземане на изгодни за Вашингтон и неговите съюзници решения.

4) Ефикасността на стратегическите комуникации ще е от ключова значимост през XXI век и САЩ и техните съюзници ще потвърждават своето разбиране за стратегическата роля на комуникациите. Битката за спечелването на умове и сърца ще продължава да бъде актуална. Стратегическите комуникации разполагат с потенциала да бъдат ефикасен инструмент за повлияване, интегрирайки се в процесите на планиране и реализиране на политики, операции и дейности, а бъдещето ще открои кои ще са точните методи и подходи. Стратегическите комуникации на САЩ и техните съюзници продължават своето развитие в зоната между традициите и новаторството.

References:

1. П. Колесов, Ведение Соединёнными Штатами информационных войн. Концепция "Стратегических коммуникаций", Зарубежное военное обозрение №6 2010 г.

2. Сашо Воденичарски, Артефакти на стратегическите комуникации от древен Египет, Годишник на ВА "Г. Раковски", Факултет „Национална сигурност и отбрана", кн 3 от 2013 г., стр. 190.

3. Руси Маринов, Интерактивни стратегически комуникации, НБУ 2012 г.

4. Joint Senior Public Affairs Course, Public Affairs Leadership Department, Defense Information School, Fort Meade, USA.

5. Joint Publication 3-61, Glossary, USA Armed Forces

6. Валери Иванов, Елица Николова, Гражданско-военното сътрудничество в контекста на стратегическите комуникации, Военен журнал, кн. 3-4, 2012 г.

7. Пашенцев Е. Н., Стратегическая коммуникация США: „Имперское перенапряжение сил", 2012 год.

МЕЖДУНАРОДНА НАУЧНА КОНФЕРЕНЦИЯ 2018

СБОРНИК ДОКЛАДИ

Издание първо. Тираж 25

Предпечатна подготовка във Факултет “Артилерия, ПВО и КИС” - Шумен