

ВОЕННА АКАДЕМИЯ „ГЕОРГИ СТОЙКОВ РАКОВСКИ“

ГОДИШНА НАУЧНА КОНФЕРЕНЦИЯ

110 ГОДИНИ ТРАДИЦИЯ, КАЧЕСТВО, ПРЕСТИЖ

Част II

12 – 13 април 2022 г.

София

RAKOVSKI NATIONAL DEFENCE COLLEGE

ANNUAL SCIENTIFIC CONFERENCE

110 YEARS OF TRADITION, QUALITY, PRESTIGE

Part II

12 – 13 April 2022

Sofia

ОРГАНИЗАЦИОНЕН КОМИТЕТ

Председател

полковник доц. д-р Димитър Ташков

Членове

полковник проф. д-р Георги Димов

полковник проф. д-р Емил Енев

проф. д.н. Митко Стойков

полковник доц. д-р Петко Димов

подполковник Веселка Методиева

Технически секретари

подполковник гл. ас. д-р Петрана Кокудева

подполковник гл. ас. д-р Калин Ранчев

подполковник гл. ас. д-р Илиан Сотиров

майор ас. Кристина Крумова

майор Любомир Райков

д-р Анелия Христова

старши преподавател Диана Боримечкова

ас. д-р Атанаска Попова

ас. Мария Неновска

ORGANISING COMMITTEE

Chairman

Colonel Assoc. Prof. Dimitar Tashkov, PhD

Members

Colonel Prof. Georgi Dimov, PhD

Colonel Prof. Emil Enev, PhD

Prof. Mitko Stoykov, DSc

Colonel Assoc. Prof. Petko Dimov, PhD

Lieutenant Colonel Veselka Metodieva

Technical secretaries

Lieutenant Colonel Assist. Prof. Petrana Kokudeva, PhD

Lieutenant Colonel Assist. Prof. Kalin Ranchev, PhD

Lieutenant Colonel Assist. Prof. Ilian Sotirov, PhD

Major Assist. Prof. Kristina Krumova

Major Lyubomir Raykov

Anelia Hristova, PhD

Senior Lecturer Diana Borimechkova

Assist. Prof. Atanaska Popova, PhD

Assist. Prof. Maria Nenovska

РЕДАКЦИОННА КОЛЕГИЯ

Председател

полковник проф. д.н. Георги Карастоянов

Заместник-председател

полковник проф. д-р Камен Калчев

Членове

полковник проф. д-р Мирослав Ст. Димитров

полковник доц. д-р Галин Иванов

доц. д-р Румен Николов

доц. д-р Ирина Миндова-Дочева

доц. д-р Валентина Георгиева

EDITORIAL BOARD

Chairman

Colonel Prof. Georgi Karastoyanov, DSc

Vice Chairman

Colonel Prof. Kamen Kalchev, PhD

Members

Colonel Prof. Miroslav St. Dimitrov, PhD

Colonel Assoc. Professor Galin Ivanov, PhD

Assoc. Prof. Rumen Nikolov, PhD

Assoc. Prof. Irina Mindova-Docheva, PhD

Assoc. Prof. Valentina Georgieva, PhD

110 години традиция, качество, престиж

Сборник доклади от Годишна научна конференция – Част II

12 – 13 април 2022 г., София

110 Years of Tradition, Quality, Prestige

Proceedings of the Annual Scientific Conference – Part II

12 – 13 April 2022, Sofia

© Военна академия „Георги Стойков Раковски“, издател, 2022

ISBN (online): 978-619-7478-94-5

ISBN (print): 978-619-7478-97-6

Съдържание

ПАНЕЛ

НОВИТЕ ВОЙНИ И РАЗВИТИЕТО НА ВОЕННОТО ИЗКУСТВО – ТЕОРИИ, ТЕНДЕНЦИИ

MANDATORY REQUIREMENTS REGARDING LAND TACTICAL FORCES' CONFIGURATION	11
Major Superior Instructor Claudiu Valer Nistorescu, PhD Candidate Colonel Prof. Niculai-Tudorel Lehaci, PhD	
URBAN WARFARE AND ITS IMPLICATIONS FOR LAND FORCES	20
Major Superior Instructor Claudiu Valer Nistorescu, PhD Candidate Colonel Prof. Niculai-Tudorel Lehaci, PhD	
TERMINATION OF THE SECOND KARABAKH WAR: CONSEQUENCES FOR THE PARTIES	26
Khayal Iskandarov Ibrahim, PhD in philology Assoc. Prof. Sadi Sadiyev Saleh	
COUNTERING OPERATIONAL LEVEL DECEPTION.....	28
Major Superior Instructor George-Ion Toroi, PhD Candidate	
MILITARY DECEPTION IN CONTEMPORARY OPERATING ENVIRONMENT	39
Major Superior Instructor George-Ion Toroi, PhD Candidate	
SECURITY OF REMOTE ELECTRONIC IDENTIFICATION: THE CASE OF POLAND	48
Remigiusz Lewandowski, PhD	
АНАЛИЗ НА ОБУЧЕНИЕТО НА ПОТРЕБИТЕЛИ НА „ИНФОРМАЦИОННА СИСТЕМА ЗА УПРАВЛЕНИЕ НА ФИНАНСОВИ И МАТЕРИАЛНИ РЕСУРСИ“	64
подполковник д-р Светозар Ботев д-р Валя Симеонова	
НОВИ СПОСОБНОСТИ В КОДИФИКАЦИОННИЯ ИНСТРУМЕНТ НА ИНФОРМАЦИОННА СИСТЕМА „ЛОГИСТИКА НА БЪЛГАРСКАТА АРМИЯ“	71
подполковник д-р Светозар Ботев д-р Валя Симеонова	
РАЗВИТИЕ НА ИНФОРМАЦИОННА СИСТЕМА „ЛОГИСТИКА НА БЪЛГАРСКАТА АРМИЯ“ ДО 2021 Г.	76
подполковник д-р Светозар Ботев д-р Валя Симеонова	
ПРЕДПОСТАВКИ ЗА ТРАНСФОРМАЦИИТЕ НА ВОЕННА АКАДЕМИЯ „Г. С. РАКОВСКИ“ В ПЕРИОДА 1944 – 2001 – РЕТРОСПЕКЦИЯ С ПОГЛЕД КЪМ БЪДЕЩЕТО	81
полковник проф. д-р Емил Енев	
ОБМЕН НА РАЗУЗНАВАТЕЛНА ИНФОРМАЦИЯ В БОРБАТА СРЕЩУ ТЕРОРИЗМА.....	90
доц. д-р Мирослав Мирчев	
ИЗПОЛЗВАНЕ НА ТЕХНИКИТЕ НА ВОЕННАТА ЗАБЛУДА В УКРАИНСКИЯ КОНФЛИКТ	98
полковник доц. д-р Калин Градев майор гл. ас. д-р Кръстю Кръстев	

ОПЕРАТИВНИ СПОСОБНОСТИ, НЕОБХОДИМИ НА СИСТЕМАТА ЗА КОМАНДВАНЕ И УПРАВЛЕНИЕ ЗА СПРАВЯНЕ С ПРЕДИЗВИКАТЕЛСТВОТА, ПРОИЗХОЖДАЩИ ОТ БЪДЕЩАТА ОПЕРАТИВНА СРЕДА	108
майор Кръстьо Парасков	
РУСКИТЕ ХИПЕРЗВУКОВИ ОРЪЖИЯ	115
доц. д-р Пламен Богданов	
ФАКТОРИ, ВЛИЯЕЩИ НА ИЗПОЛЗВАНЕТО НА РАЗУЗНАВАТЕЛНИ ФОРМИРОВАНИЯ В ОПЕРАЦИИ ПРИ БЕДСТВИЯ И АВАРИИ	124
подполковник Добромир Дамаков, докторант	
ОРГАНИЗИРАНЕ И ПРОВЕЖДАНЕ НА ЕВАКУАЦИЯ НА БЕДСТВАЩО НАСЕЛЕНИЕ	133
полковник доц. д-р Георги Георгиев	
ДОКТРИНАЛНИ АСПЕКТИ НА ОСИГУРЯВАНЕТО И ПОДДРЪЖКАТА	141
доц. д-р Светослав Велев	
РАЗУЗНАВАТЕЛЕН АНАЛИЗ НА ТРАНСФОРМАЦИЯТА НА СТРУКТУРАТА И ФУНКЦИИТЕ НА ПОСТМОДЕРНТЕ ТЕРОРИСТИЧНИ ОРГАНИЗАЦИИ.....	150
доц. д-р инж. Добрин Анастасов	
НАПРАВЛЕНИЯ ЗА ПОВИШАВАНЕ УСТОЙЧИВОСТТА НА ПЪТНАТА МРЕЖА ВЪВ ВОЕНЕН КОНФЛИКТ	156
подполковник д-р Данаил Петев	
УСТОЙЧИВОСТ И НЕПРЕКЪСВАЕМОСТ НА РАБОТАТА НА ВЕДОМСТВА И ОРГАНИЗАЦИИ ПРИ БЕДСТВИЯ	161
гл. ас. д-р Даниела Балева	
БЕДСТВИЯ – МИГРАЦИЯ И БЕЖАНЦИ	167
гл. ас. д-р Даниела Балева	
КОМУНИКАЦИЯ ПРИ БЕДСТВИЯ	172
гл. ас. д-р Даниела Дуганова	
АДАПТИВНОСТ НА РАЗУЗНАВАТЕЛНИЯ ЦИКЪЛ	179
доц. д-р Елислав Иванов	
ЧОВЕШКИЯТ ФАКТОР В АВИАЦИЯТА – ОТ ПЪРВИЯ ПОЛЕТ ДО ДНЕС	185
д-р Маргарита Куманова	
ОТБРАНИТЕЛНОТО ПЛАНИРАНЕ ЗА ПОДДЪРЖАНЕ И РАЗВИТИЕ СПОСОБНОСТИТЕ НА ВЪОРЪЖЕНИТЕ СИЛИ НА РЕПУБЛИКА БЪЛГАРИЯ.....	190
д-р Ганчо Душков	
ИЗПОЛЗВАНЕ НА ВЪОРЪЖЕНИТЕ СИЛИ В КОНТЕКСТА НА КОЛЕКТИВНАТА ОТБРАНА НА СТРАНАТА	196
майор Лъчезар Русев	
ИЗПОЛЗВАНЕ НА ГЛАДКОЦЕВНО ОГНЕСТРЕЛНО ОРЪЖИЕ ОТ ПОЛИЦЕЙСКИТЕ СЛУЖИТЕЛИ ПРИ ПРОВЕЖДАНЕ НА ВИСОКОРИСКОВИ ОПЕРАЦИИ – СПЕЦИФИКИ И ТАКТИЧЕСКО ПРИЛОЖЕНИЕ.....	203
Марин Григоров, докторант	
ВЪЗНИКВАНЕ И РАЗВИТИЕ НА МОРСКИЯ „СПЕЦНАЗ“ НА РУСИЯ	211
капитан III ранг Георги Калинов	

ФАКТОРИ, ВОДЕЩИ ДО ТРАНСФОРМАЦИЯ НА ОПЕРАЦИИТЕ В ОТГОВОР НА КРИЗИ	216
гл. ас. д-р инж. Данко Фаразов	
ОПЕРАТИВНА СЪВМЕСТИМОСТ – СЪЩНОСТ И ПРЕДИЗВИКАТЕЛСТВА ЗА ПОСТИГАНЕ ПРЕД СИСТЕМАТА ЗА КОМАНДВАНЕ И УПРАВЛЕНИЕ	223
майор Кръстьо Парасков	
ВЪЗМОЖНОСТИ ЗА ПРЕДСТАВЯНЕ НА ВОЕННИЯ КОРАБ КАТО СЛОЖНА СИСТЕМА ОТ ЙЕРАРХИЧЕН ТИП	229
старши инструктор Красимир Ангелов	
ПОУКИТЕ ОТ ОПЕРАЦИИТЕ И УЧЕНИЯТА КАТО НЕОБХОДИМИ ЗНАНИЯ ЗА ПОВИШАВАНЕ НА ОТБРАНИТЕЛНИТЕ СПОСОБНОСТИ	235
подполковник д-р Пламен Петков	
СЪВРЕМЕННИТЕ ТЕХНОЛОГИИ ЗА РАЗУЗНАВАНЕ НА РУСИЯ И ТЯХНОТО ИЗПОЛЗВАНЕ В УКРАИНСКИЯ КОНФЛИКТ	243
майор гл. ас. д-р Кръстю Кръстев	
АНАЛИЗ НА СЪЩЕСТВУВАЩА СИСТЕМА ЗА УПРАВЛЕНИЕ НА ИНФОРМАЦИЯТА В ЩАБА НА СУХОПЪТНИ ВОЙСКИ	253
майор ас. Мартин Христов	
КОМПЛЕКС ВЪЗДУШНА ОБСТАНОВКА ПЕРСПЕКТИВИ ЗА РАЗВИТИЕ	261
полковник проф. д-р Петър Христов	

ПАНЕЛ

ТРАНСФОРМАЦИЯ, ПРЕВЪОРЪЖАВАНЕ, СПОСОБНОСТИ

ОБРАЗЪТ НА ТЕРОРИЗМА ПРЕЗ ХХІ ВЕК	271
доц. д-р Мирослав Мирчев	
СПЕЦИАЛНИ СПОСОБИ ВЪВ ВЪОРЪЖЕНИТЕ СИЛИ НА САЩ ЗА СЪБИРАНЕ НА РАЗУЗНАВАТЕЛНА ИНФОРМАЦИЯ	277
д-р Антон Михайлов	
ТРАКИЙСКИЯТ ПОХОД НА СЦИПИОНИТЕ ПРЕЗ 190 Г. ПРЕДИ ХРИСТА.....	282
д-р Йордан Илиев	
НОВОТО ЛИЦЕ НА РИСКА В ЕПОХАТА НА ДИГИТАЛНАТА ТРАНСФОРМАЦИЯ.....	290
Валентин Мончев, докторант	

Contents

PANEL

THE NEW WARS AND THE DEVELOPMENT OF THE ART OF WAR: THEORIES AND TRENDS

MANDATORY REQUIREMENTS REGARDING LAND TACTICAL FORCES' CONFIGURATION	11
Major Superior Instructor Claudiu Valer Nistorescu, PhD Candidate Colonel Prof. Niculai-Tudorel Lehaci, PhD	
URBAN WARFARE AND ITS IMPLICATIONS FOR LAND FORCES	20
Major Superior Instructor Claudiu Valer Nistorescu, PhD Candidate Colonel Prof. Niculai-Tudorel Lehaci, PhD	
TERMINATION OF THE SECOND KARABAKH WAR: CONSEQUENCES FOR THE PARTIES	26
Khayal Iskandarov Ibrahim, PhD in philology Assoc. Prof. Sadi Sadiyev Saleh	
COUNTERING OPERATIONAL LEVEL DECEPTION.....	28
Major Superior Instructor George-Ion Toroi, PhD Candidate	
MILITARY DECEPTION IN CONTEMPORARY OPERATING ENVIRONMENT	39
Major Superior Instructor George-Ion Toroi, PhD Candidate	
SECURITY OF REMOTE ELECTRONIC IDENTIFICATION: THE CASE OF POLAND.....	48
Remigiusz Lewandowski, PhD	
ANALYSIS OF THE TRAINING OF USERS OF THE "INFORMATION SYSTEM FOR FINANCIAL AND MATERIAL RESOURCES MANAGEMENT"	64
Lieutenant colonel Svetozar Botev, PhD Valya Simeonova, PhD	
NEW CAPABILITIES IN THE CODIFICATION TOOL OF THE "LOGISTICS OF THE BULGARIAN ARMY" INFORMATION SYSTEM	71
Lieutenant colonel Svetozar Botev, PhD Valya Simeonova, PhD	
DEVELOPMENT OF THE "LOGISTICS OF THE BULGARIAN ARMY" INFORMATION SYSTEM BY 2021	76
Lieutenant colonel Svetozar Botev, PhD Valya Simeonova, PhD	
PREREQUISITES FOR TRANSFORMATIONS OF THE MILITARY ACADEMY "G. S. RAKOVSKI" IN THE PERIOD 1944 – 2001 – RETROSPECTION WITH A LOOK AT THE FUTURE.....	81
Colonel Prof. Emil Enev, PhD	
THE EXCHANGE OF INTELLIGENCE INFORMATION IN THE FIGHT AGAINST TERRORISM.....	90
Assoc. Prof. Miroslav Mirchev, PhD	
USE OF MILITARY DECEPTION TECHNIQUES IN THE UKRAINIAN CONFLICT	98
Colonel Assoc. Prof. Kalin Gradev, PhD Major Krastyu Krastev, PhD	

OPERATIONAL CAPABILITIES REQUIRED BY THE COMMAND AND CONTROL SYSTEM TO DEAL WITH THE CHALLENGES ORIGINATING FROM THE FUTURE OPERATIONAL ENVIRONMENT	108
Major Krastyo Paraskov	
RUSSIAN HYPERSONIC WEAPONS	115
Assoc. Prof. Plamen Bogdanov, PhD	
FACTORS AFFECTING THE USE OF INTELLIGENCE FORMATIONS IN DISASTER AND ACCIDENT OPERATIONS	124
Lieutenant colonel Dobromir Damakov, PhD	
ORGANIZATION AND CONDUCT OF THE EVACUATION OF DISASTER STRICKEN POPULATION	133
Colonel Assoc. Prof. Georgi Georgiev, PhD	
DOCTRINAL ASPECTS OF COMBAT SUPPORT	141
Assoc. Prof. Svetoslav Velev, PhD	
INTELLIGENCE ANALYSIS OF THE TRANSFORMATION IN THE STRUCTURE AND FUNCTIONS OF POSTMODERN TERRORIST ORGANIZATIONS	150
Assoc. Prof. Dobrin Anastasov, PhD	
DIRECTIONS FOR INCREASING SUSTAINABILITY OF ROAD NETWORK IN MILITARY CONFLICT	156
Lieutenant colonel Danail Petev, PhD	
SUSTAINABILITY AND CONTINUITY OF THE WORK PROCESS OF DEPARTMENTS AND ORGANIZATIONS IN CASE OF DISASTERS	161
Assist. Prof. Daniela Baleva, PhD	
DISASTERS – MIGRANTS AND REFUGEES	167
Assist. Prof. Daniela Baleva, PhD	
DISASTERS COMMUNICATION	172
Assist. Prof. Daniela Duganova, PhD	
ADAPTABILITY OF THE INTELLIGENCE CYCLE	179
Assoc. Prof. Elislav Ivanov, PhD	
HUMAN FACTORS IN AVIATION – SINCE THE FIRST FLY TILL TODAY	185
Margarita Kumanova, PhD	
DEFENSE PLANNING TO MAINTAIN AND DEVELOP THE ABILITY OF THE BULGARIAN ARMED FORCES	190
Gancho Dushkov, PhD	
USE OF THE ARMED FORCES WITHIN THE CONTEXT OF THE COUNTRY’S COLLECTIVE DEFENSE	196
Major Rusekov Lachezar	
USE OF SMOOTHBORE FIREARMS BY POLICE OFFICERS IN CONDUCTING HIGH-RISK OPERATIONS – SPECIFICS AND TACTICAL APPLICATION	203
Marin Grigorov, PhD Student	
ORIGINE AND EVOLUTION OF RUSSIAN NAVAL “SPECNAZ”	211
Lieutenant-commander Georgi Kalinov	
FACTORS LEADING TO TRANSFORMATION OF CRISIS RESPONSE OPERATIONS	216
Assist. Prof. Danko Farazov, PhD	
INTEROPERABILITY – NATURE AND CHALLENGES TO ACHIEVE BY THE COMMAND AND CONTROL SYSTEM	223
Major Krastyo Paraskov	

OPPORTUNITIES FOR REPRESENTING THE NAVAL SHIP AS A COMPLEX SYSTEM OF HIERARCHY TYPE	229
Senior Instructor Krasimir Angelov	
LESSONS LEARNED FROM OPERATIONS AND TRAININGS AS A NECESSARY KNOWLEDGE FOR IMPROVEMENT OF DEFENSE CAPABILITIES.....	235
Lieutenant colonel Plamen Petkov, PhD	
MODERN RUSSIAN INTELLIGENCE TECHNOLOGIES AND THEIR USE IN THE UKRAINIAN CONFLICT	243
Major Krastyu Krastev, PhD	
ANALYSIS OF AN EXISTING INFORMATION MANAGEMENT SYSTEM AT THE LAND FORCES HEADQUARTERS.....	253
Major Martin Hristov, Assistant Professor	
AIR SPACE SITUATION COMPLEX	261
Colonel Prof. Petar Hristov, PhD	

PANEL

TRANSFORMATION, REARMAMENT, CAPABILITIES

THE IMAGE OF TERRORISM IN THE XXI CENTURY	271
Assoc. Prof. Miroslav Mirchev, PhD	
SPECIAL METHODS IN THE US ARMED FORCES FOR COLLECTING INTELLIGENCE	277
Anton Mihaylov, PhD	
THE THRACIAN MARCH OF THE SCIPIOS IN 190 BEFORE CHRIST	282
Jordan Iliev, PhD	
THE NEW FACE OF THE RISK IN THE DIGITAL TRANSFORMATION AGE.....	290
Valentin Monchev, MSc, PMP, PhD Candidate	

Панел

**НОВИТЕ ВОЙНИ И РАЗВИТИЕТО
НА ВОЕННОТО ИЗКУСТВО –
ТЕОРИИ, ТЕНДЕНЦИИ**

Panel

**THE NEW WARS
AND THE DEVELOPMENT
OF THE ART OF WAR –
THEORIES AND TRENDS**

MANDATORY REQUIREMENTS REGARDING LAND TACTICAL FORCES' CONFIGURATION

Major Superior Instructor Claudiu Valer Nistorescu, PhD Candidate

"Carol I" National Defence University

Bucharest, Romania

E-mail: nistorescu.claudiu@unap.ro

Colonel Prof. Nicolai-Tudorel Lehaci, PhD

"Carol I" National Defence University

Bucharest, Romania

E-mail: lehacitudor@yahoo.com

Abstract: Today's operational environment is continuously changing. New challenges and requirements have emerged due to the unpredictable threats' character to the states' security. In this context, national defense, augmented by the tenets of collective defense imposes a sustainable response in order to defeat those threats. Land power, by its unique ability to projects effects on the land environment and to influence population and other actors' behavior, will remain the essential element for the military instrument of state's power. Therefore, the adaptation and reconfiguration of the land tactical units become mandatory to accomplished land forces' overall mission. Initiatives in building new capabilities and consolidating the existing ones reveal the importance of their modernization process. Additionally, the development of the doctrines, tactics, techniques and procedures support tactical units' operations on the battlefield, by providing commanders and their subordinates an efficient "how to fight". Consequently, mental adjusting is required in order to meet the fast-paced changing in the operational environment and ensure the necessary "will to fight" for the soldiers. Taking in consideration these facts, it is obvious that land forces tactical units must evolve and the analysis' main purpose is to emphasize a few mandatory directions that should be followed in order to achieve this ultimate goal.

Keywords: *land forces; tactical units; modern battlefield requirements; military capabilities*

Introduction

International security environment generate the need to adapt military structures and forces, including the tactical ones. The evolution of contemporary operational environment is intrinsically determining nations to adapt their military capabilities, in order to counter asymmetric and irregular threats. In this hybrid threat-based climate, a continuously transformation of tactical forces from a multi-domain operations perspective, seems to be the solution. Land forces need to swiftly evolve to be able to cope with new challenging situations. Their evolution is vital for the successful outcomes of multinational joint forces needed for an efficient collective defense.

Therefore, enhancing land forces strengths and capabilities is an imperative issue, still not enough, taking in consideration the complexity of the contemporary military operations. Corroborating with a global tendency in reducing military budgets and decreasing soldiers' number, these objectives become difficult to achieve. However, NATO through its *Smart Defence Concept*¹ encourages allies to develop strong and reliable common capabilities, including tactical forces. This kind of forces have to be "credible, networked, aware, agile, and resilient"², on the same time, in order to project desired effects in respect of effectiveness and efficiency. For completing these tasks, multiple actions must be done, including innovation and transformation, adapting concepts and procedures, and training.

Gaining effectiveness and efficiency in land operations is not simple and no matter what kind of operations land tactical forces are conducting, this aspect should be their primary goal. Therefore, several activities are mandatory in order to generate the appropriate premises for their success. These activities presuppose realizing a right balance between physical and human aspect of the force, obtaining the ability to use the force where and when it is necessary and also achieving the right level of force³. High-technologies integration, enhanced and surgical lethality, multi-domain capabilities, maneuverability, survivability and adaptability are just a few features that describe the needs of land tactical units for conducting future operations.

Having these aspects in mind, the main purpose of the present analysis is to emphasize the need to reconsider the modality in which land tactical units must be configured. By identifying the mandatory requirements, that have to be done in their future's projection, I have tried to give solid fundamentals for the research.

Reliable references given by allied publication, but also doctrines developed by some state members, were the primary source for the outlined findings. Moreover, the analysis is strongly supported by recent history battles examples which provide reliable and relevant information about the requirements of the land tactical units. The research does not refer to a specific state, nor does it take in consideration military balance power for a designated region. However, the global tendencies in developing the land forces, especially at the tactical level, were mandatory benchmarks for it. Therefore, several questions are designated to focus and direct the overall research, and consequently the study is closely connected with the need to answer them. These questions are:

- Which are the references that generate the need to reconfigure land tactical forces?
- Which are the new requirements for land tactical forces in order to effectively respond to the actual operational environment's challenges?
- What capabilities have to be developed for land tactical forces with the purpose to strengthen their fighting power?

Before starting to outline and analyze the requirements that modern tactical land forces must have, I think a short clarification about the concept could be helpful. Land tactical forces are those forces which are employed at the tactical level and are designated to accomplish *tactical activities*⁴ in order to project, through their combat power, desired effects on the battlefield, with the purpose to sustain operational objectives. The description (it is not a definition) is not exhaustive, but I believe it comprises the essence regarding land tactical forces. However, the study will emphasize others aspect of their features.

*Allied Land Tactics*⁵, the compass publication for NATO countries in developing their land tactical forces, describes these types of forces. The "core" of tactical forces is formed by heavy, medium and light forces, but also includes several special capabilities as airmobile, air assault and airborne forces, reconnaissance, mountain and amphibious forces. Their full description, in terms of mobility, firepower and protection, including suitable tactical task, employment recommendations, but also limitations are useful guidelines for tactical units' configurations. Therefore, the present research is guided by the need to find solutions with respect to these principal characteristics of the tactical land forces.

I. References regarding the necessity of land tactical forces reconfiguration

● Historical references

Throughout history, the connection between military art, military science and the forces' transformation was a permanent landmark for the military organization. Armed conflicts' development is closely related with the humanity evolution. Even if the nature of warfare described in terms of chaos, danger and fear, uncertainty and psychological pressure is always the same, the character of warfare is different. The later is permanently influenced by policies, strategies and tactics, or the number of actors involved. But, the major reason in changing character of warfare is technology. The humanity's breakthroughs became the power engine for the military transformation and many times the efforts in research activities had a military purpose.

Regarding modern war typology, military specialists have identified four generations⁶, their characteristics being a direct result of the weapons systems features.

The 1st generation war was a confrontation of "columns and lines formation" and began with the start of 17th Century and last near to the second half of the 19th Century. Land forces' design was in accordance with the tactics used. Machinegun was the reason for what this type of war became obsolete.

Due to an extraordinary industrial revolution, a new era of warfare was developed starting with the beginning of 20th century. Artillery systems were able to deliver a massive fire quantity in support of infantry units. During 1st World War an algorithmically conduct of war was developed where the artillery was the masterpiece. Huge armies were trapped in the trenches and maneuvers were most of the time ineffective. J.F.C. Fuller emphasized, in one of his analysis, the reality of the 2nd modern warfare generation saying that "artillery conquers and infantry occupies." Instead of that, new weapons, platforms and equipments were designed. Airplanes and tanks were used in battle for the first time and chemical weapons appeared to be a terrifying means. The consequent adjustments of land forces were made. Camouflage BDUs and helmets became mandatory, lines and column formations were no longer efficient. There was also an increase of the importance in using terrain features.

But, 3rd generation warfare represents today the fundamental change in the operational art. What we call now *blitzkrieg* was possible due to the mechanized forces' development. Deep operation doctrine was possible due to enhanced capability to penetrate enemy lines and striking rearward having an appropriate support. German Army ground forces exploit the maneuverability of its armored corps supported by Stuka airplanes. As a result the French Army

collapsed in two weeks. The transformations made at tactical level were significant. Combined arms formations were developed for the first time and forms of maneuver in offensive actions were the key to defeat the enemy. Radios were integrated to the mechanized and motorized platforms. New operational concept appeared as strategic bombardment or close-air-support. But the major change that 3rd generation warfare brought to the military organization was a new way of thinking. German *Auftragstaktik*⁸ allowed and empowered field commanders to exercise "disciplined initiative" and "assume calculated risk"⁹ in order to exploit tactical opportunities and strike enemy's vulnerabilities.

Since then speed, surprise and shock actions became more important than portion of fire delivered. Very quickly, after 2nd World War armies need to evolve and to adapt to the new requirements. After Vietnam conflict, US Army through its Training and Doctrine Command/TRADOC had to reconsider the requirements in conducting ground warfare, intrinsically the configuration of land tactical forces. General Donn A. Stary forged starting with 1977 a new doctrine for land operations that was designed to counter a possible Warsaw Pact offensive. *AirLand Doctrine* was put in practice by US Army Field Manual 100-5 in 1982. The army corps perspective was resurrected and then the operational level was defined. Also, new operational concept were introduced: extended battlefield including deep, close and rear battles, technological superiority, joint operations, battlefield air interdiction/BAI etc.⁹ As a consequence, tactical formations were redesigned in order to exploit the advantages of superior technologies and way of thinking. Combat support units were assigned to the brigade and division level. The corps had its own intelligence and long-range capabilities and also the ability to command large formations. The corps had also its own aviation resource and the possibility to conduct both CAS in the close battle area and BAI in the deep battle area. The doctrine was successfully tested ten years later during Desert Storm Operation (1990-1991)¹⁰.

The 4th generation of modern warfare keeps the imperatives of the previous generation, but adds the information era perspective. In this era, the speed and accuracy could make irrelevant conventional capability. The same is true for the irregular and asymmetrical activities where classical military responses are no longer effective. Taking in consideration these realities we wonder if the land tactical forces still have a future? Michael E. O'Hanlon, in his book, *The Future of Land Warfare*, gives us an answer. He reveals that ¾ from total military personnel from the world's regular army come from their land components¹¹.

As a conclusion I wish to emphasize the fact that the permanent transformation of the military forces, including tactical ones is necessary. Only by adapting capabilities, formations, training, doctrines and leadership could a performing force be obtained.

● Operational environment transformation

The transformation of the operational environment is a certainty and therefore the military organization needs to swiftly adapt in order to respond the challenges. As I said before, land forces are unique through their ability to produce effects on the population. Unfortunately, modern warfare characteristics demonstrated that tactical land units are not always properly prepared. Counterinsurgency operations from the last twenty years in Iraq and Afghanistan highlight their vulnerabilities, at least in the conflict's beginning. Armored capabilities were inefficient on the streets of Bagdad or Basra, as well as the dismounted patrols. Consequently, tactics, techniques and procedures, as well as training and equipping were enhanced. One of the greatest objectives was to change soldiers' mentality and way of thinking. Commanders needed to shift from a conventional threat to an undefined one, due to the fact that there were no any frontlines and the battles were ambiguous as same as the enemy. Gradually, commanders centered to a "zero casualties strategy" well-sustained by the technological supremacy. Anyway, lessons learned from recent armed conflicts showed that to "win people's minds and hearts" is more difficult than it seemed to be.

The major challenge for contemporary tactical land forces is to swiftly shift from combat to support operation and vice-versa. Theoretically, they have this ability, but many times commanders are not able to give an optimal solution due to a predefined mindset. The "zero casualties' strategy", that I have spoken before, is not useful in classical combat. The 2006 Lebanon War demonstrated a series of vulnerabilities of the ground forces of the Israeli Army. Even if Israeli armored capabilities were technologically superior with respect to their opponents, they suffered disproportioned losses. The conflict's aftermath analysis shows that the Israeli Tactical Units were not adequately prepared for a conventional confrontation¹². The conflict started in 2014 in Ukraine has dramatically changed the "game's rules". Hybrid threats emphasized the need to counter both the irregular activities of a potential adversary and the possibility to conduct combat operations against its conventional forces. NATO members, especially Eastern border ones realize that their military capabilities must be transformed in order to cope with new threats including enemy's conventional forces. The need to reconsider land capabilities is generated by the possibility to have a large-scale conflict with a peer/or near-peer adversary. Unfortunately, today's reality

shown by the recent armed conflict in Ukraine, demonstrated that international community's concerns about a possible large-scale ground combat operations are definitely founded.

Operational environment is also shaped by the weapon systems' development. Their oriented high lethality as well as the range's increasing and enhancement of their survivability is the principal direction where the improvements were made. At the same time recent offensive in the cyber and space domain of different competitor states generate the need to adapt tactical land forces to the multi-domain requirements.

Restricted terrain-orientated operations including urban terrain, jungles or mountainous areas, still remain a challenge for future operation. Conducting military operations, in these demanding environments, implies flexible and versatile forces with an appropriate balance between mobility, fire support, logistical support and soldiers' motivation. The need to realize sufficient combat power to sustain simultaneously multiple battles could be a priority in this kind of terrain. Therefore, a rapid force's disaggregation and aggregation is another essential requirement.

● **High technologies influences**

Today's high technologies global proliferation corroborated with a facile access to related products is challenging "the technological advance of the Alliance"¹³. Therefore, NATO tactical forces' transformation must be related with the latest technology in order to keep the military edge. Unfortunately, there is a significant technological advance between Member States. Consequently, there are strong efforts to mitigate the effects and to realize an appropriate level of interoperability.

At the tactical level, technologies could have a significant impact on the forces' development. UAV/UAS are integrated to the platoon level and soldiers could benefit from the information provided by multiple sensors. Command and control system is upgraded by 5G technologies. Artificial intelligence and robotics are integrated to the tactical units and there are a few projects of developing radio commanded platforms. Hypersonic capabilities could augment the conventional ones. US Army TRADOC identify "potential game changers"¹⁴ for 2035, including Multi-domain swarms, advanced ATGM & MANPADS, Camouflage, Cover, Concealment, Denial, & Deception (C3D2), long-range artillery and missiles, Computing/Cyber¹⁵.

Moreover, the research in advanced materials gives the opportunity to enhance future soldier systems. High technologies allow the development of future smart bases and logistics, mixed reality and everything computer and intrinsically tactical forces should adapt and evolve in order to meet the new requirements.

● **Time and space requirements**

There was a permanent battle for time and space in combat operations, but today's need to obtain dominance in respect of time dimension rather than space seems to be stronger than ever. Timely decision-making generate timely actions and a subsequent advantage for the one who manages to outrun the opponent in his decision cycle. Spatial dimension is also reconsidered. Standoff and anti-access/area denial capabilities are instruments designated to serve political objectives rather than occupying terrain. Also, it is true that there is a real competition in terms of fire range and precision. Precision guided munitions/PGM is available to produce desired effects at every level of the operation.

● **Economic issues**

The analysis of the economic issue related with the tactical land forces' development is not one of our main objectives. However, it should be outlined that the overall budgets for defence are in a continuously decreasing state, due to the constant strain to the national budgets¹⁶. Therefore, the military research and development sectors will be directly affected in a negative manner. As a consequence, defence systems will rely in an increasing way on the commercial products. At the same time, there are some actors that are raising their military budgets in order to strength their capabilities. For example, indicators show that China is in this situation and right now it has the second largest military budget in the world¹⁷.

II. Requirements for land tactical forces

In comparison with Cold War era where there was a single-focused threats' mentality, contemporary security environment poses complex and multiple challenges regarding national security. The past forces' requirements were very different and took in consideration the need to deter a single type of threat. On the contrary, today's forces should be effectively tailored to be able to respond both to asymmetric and unconventional threats and conventional ones.

The need for transformation and adapting is pressing with the purpose to obtain those tailored and flexible forces. Therefore, military forces shift from a threat-based-planning to a capabilities-threat-planning in order to fulfill the imperatives of contemporary operational environment. Moreover, there is an emphasis on the effects'

importance instead of kinetic results¹⁸. Massing of forces is not longer a mandatory prerequisite for success in military operations and, many times, concentration of “massive and impressive” force does not generate an appropriate “utility of force”, as general Sir Rupert Smith highlighted in his book the *Utility of Force*¹⁹.

In order to meet the contemporary requirements for NATO forces, *Framework for Future Alliance Operations* initiates and describes four major directions where transformation and innovation are needed. These future abilities for NATO forces include the following domains: prepare, project, engage and sustain²⁰.

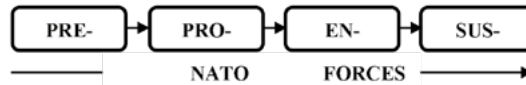


Fig. 1. Directions in land tactical forces transformation

Preparing the force is strictly related to the accomplishment of DOTMLPFI²¹ requirements. Tactical land forces are related with the national level of ambition. To establish the appropriate level of force is the primary step that should to be followed. The level of force depends on:

- country's territorial dimensions;
- international political engagements, including military alliances;
- population number with respect to the active people able to serve and to be enlisted;
- regional security context and the existence of, frozen or open conflicts;
- internal and latent sources of conflicts (ethnic, religious);
- type of relief.

A proper education of the military personnel is an essential condition that ought to be achieved in order to obtain an efficient and responsive force. The education process includes the individual component as much as collective component. Realistic and highly-demanding training and exercises, in accordance with the demands of contemporary military operations, is the only way to obtain a well-prepared force. For land tactical units the training process is sensitive because it supposes the involvement of human component in different operating environments: urban terrain, mountainous areas, jungles and swamps, arctic areas etc. To make things more difficult, civilian considerations pose a series of restraints to land operations. The leadership education is important as well. Only by developing true leaders, could the premises for prevailing on the battlefield be established. Also it is true, that forces should constantly integrate lesson learned from recent conflicts and consequently adjust doctrines with the purpose to fight well the next war, not the last one.

Realizing an optimal mix of forces, between armored, fire support capabilities, reconnaissance and combat engineer should be a permanent objective for developing tactical capabilities. To accomplish this essential objective a few directions should be followed. The need for enhanced maneuverability generates an inherent reduction of the mass and armored platforms' dimensions. This fact causes a reduction of the platforms' firepower. Therefore measures to increase both lethality of the weapon systems and platforms' abilities to survive on the battlefield have to be taken in order to compensate this restraint. Conversely, artillery systems need to achieve the same level of mobility like the supported unit and should be integrated with mobile platforms able to follow the maneuver elements.

Another requirement for tactical forces is improving their capabilities to survive on the battlefield. To achieve this goal a series of measures have to be taken in consideration: reducing the unit's footprint in all spectrums, increasing the speed and abilities to change the position, enhancing optical camouflage, integrating active measures of protection and acquiring intelligence about the enemy intentions and actions. Counter enemy's EW and cyber threats should be also taken in consideration.

Building modern antitank capabilities based on antitank guided missiles systems/ATGM is another requirement to obtain robust land forces. 5th generation ATGMs *fire-and-forget* type integrate high technologies in order to extend fire range, precision and lethality. Multiple guiding systems in different spectrums, multi-purpose warhead, non-line of sight capabilities and enhanced survivability based on a stand-off capability are the main features that this kind of weapon systems have.

Combat engineer as well as reconnaissance forces should adequately build in accordance with the supported units' destination. Therefore, their training and equipping have to integrate with the maneuver unit where they belong, in order to effectively support their mission.

There is no doubt that protection measures play a vital role for land tactical forces. Air defence systems should allow a stratified layered protection for tactical units, including HQs, combat disposal, assembly areas or dislocation routes. Modern technologies as CRAM SHORAD-VSHORAD and MANPADs should be integrated to the tactical units according to their mission and destination.

Appropriate air capabilities should be allocated to the tactical level both for close air support/CAS, battle air interdiction/BAI and air transportation of troops and equipments, including logistics. Division and corps maneuvers will be considerably enhanced by air capabilities allowing those tactical units to set up air mobile and air assault forces.

All these requirements for land tactical forces should integrate high technologies and innovations. Forces must be flexible and mobile, and able to conduct expeditionary operations. The maneuver elements should be adequately combined with combat support elements and, also well-sustained by an efficient logistical system. The result should be a well-dimensioned force able to penetrate enemy's tactical combat disposal, fix its maneuver elements and neutralize combat support elements, in order to strike the main force and exploit a potential success.

Today's armed conflict is seldom characterized by the existence of non-contiguous areas of operation with no defined frontlines, where the enemy is many times ambiguous. In restricted terrain tactical units at brigade level and above could not maneuver properly using their full combat power. Many times, a tactical unit could be simultaneously engaged in multiple battles or skirmishes. Consequently, it could be difficult to deliver proper combat support for each subordinate unit. Therefore, tactical units, at brigade level and above, have to develop the ability to swiftly disaggregate and aggregate their forces in order to form an appropriate mix of combined maneuver force. Logistical issues should be a permanent concern of field commanders in order to maximize their chance to success.

The requirements highlighted in this study are mandatory in order to obtain an efficient tactical force. Moreover, to ensure the effectiveness of the implementation of those objectives, an appropriate philosophy of command is needed. Mission command, the NATO assumed philosophy of command, empowers subordinate commanders to take initiative in order to fulfill their mission. The commander's intent and trust-based climate along the chain of command is the key for the implementation of mission command²². This type of command is inherent for the manoeuvrist approach to operation, which is the principal approach to operation integrated by NATO forces. Manoeuvrist approach to operation stresses the need for affecting enemy's *understanding, cohesion and will to fight*, rather than physical destruction, and mission command facilitates the fulfillment of these objectives²³.

As a final thought, I wish to emphasize the importance of considering the importance of the soldier as the centerpiece of the transformation process. His abilities to act, adapt and influence should be considered the principal milestones in land tactical forces' configuration.

III. New capabilities needed for land tactical forces' configuration

Referring to the military capabilities that land tactical forces need to realize, we must take in consideration the already existent ones. Maybe, it would be much appropriate to consider simultaneously the need to strengthen the present capabilities and building the new ones, in order to adequately respond to the present challenges. However, with the purpose to respond to the 3rd research questions, we will try to highlight the main directions in which land capabilities should be developed or enhanced.

The concept of *military capability* is defined by NATO as "the ability to create an effect through employment of an integrated set of aspects categorized as doctrine, organization, training, materiel, leadership development, personnel, facilities, and interoperability."²⁴ The same publication describes another few terms related with the capability concept: capability area, capability, capability package, capability requirement and capability target²⁵. By analyzing these concepts, we can conclude that the capabilities development is a complex process which implies various activities. First of all, a proper evaluation of the present capabilities has to be made. Secondly, a desired end state should be established regarding the capability that should be achieved and also the capability's integration in an area of capability. The identification and allocation of the necessary resources have the same importance as well as the identification and fulfillment of the specific requirements.

Military experts identify different acceptances of this concept, but in relation with the purpose of our research, we want to emphasise two aspects: the military capability as a tactical entity/unit and the military capability as a weapon system. In both variants, the capability keep the ability to produce a desired effect on the battlefield and need a proper DOTMLPFI integration.

When we speak about the military capability as a tactical unit, we have to consider this issue using the "building blocks" principle, theorized by American researcher, Paul K. Davis in a RAND Corporation research

study²⁶. Consequently, each tactical unit contributes as a building block to realizing a new superior capability. Three to five infantry battalions build the spin for an infantry brigade capability which is enhanced by appropriate artillery, air defence, reconnaissance, engineer, signal and CBRN defence capabilities. And the same is valid for division and corps, the latter one being the highest tactical formation.

The key for obtaining a new and superior capability is to realize a superior combat power rather than just putting together and summing the constituent units' combat power. Therefore, combat support elements of the higher echelon need to be qualitatively superior to those existent at the subordinate units' level. The higher echelon needs to preserve the ability to shape the battle for its subordinate units. A corps as a warfighting formation has to provide intelligence support for the division, long range artillery with the purpose to reduce enemy's combat power, aviation support, multiple layers of air defence, EW, etc.

Also it is true that a qualitative equipping of the tactical unit produces a higher level of combat power. Modern warfare generates the need for maneuverability, speed and mobility. Therefore, maneuver brigades should gain these abilities. New modern armored platforms are needed for a proper equipping, according with the units' main destination. Heavy infantry brigades should realize an optimal combination between tanks and heavy IFV. Armored capabilities' ability to survive should be increased by integrating modern Active Protection Systems/APS. These systems are designed to defeat antitank threats and are able to counter multiple types of antitank projectiles and missiles. The most-known efficient APSs are Israeli's Trophy and Iron Fist systems that have proven in combat the ability to enhance platform's survivability²⁷. At the same time by integrating ATGMs at the armored platform (heavy, medium and even light platforms), tactical units enhance their antitank capability and gain the premises to fight more efficient against enemy's armored units. Moreover, it could be an opportunity to reduce the pressure on the designated antitank armored at the battalion and brigade level. Modern portable ATGM's demonstrated their significant value in recent combat in Kiev and Kharkov, in Ukraine.

Reconnaissance and combat engineer formations need to enhance their mobility, speed, fire power and protection by using the same type of vehicles adapted to their specific. At the heavy and medium infantry brigades, reconnaissance units should be built as a robust armored force able to conduct theater-entry operation, combat reconnaissance and cover and guard task.

The artillery means have to keep the same rate of mobility with the units where they belong. In conclusion, armored brigades and heavy and medium infantry brigades should be augmented with wheeled or tracked self-propelled artillery systems. These systems, in order to obtain an effective fire, should be integrated with a modern Battlefield Management Systems/BMS and precision guided munitions/PMG, Excalibur type. Norwegian wheeled self-propelled artillery systems developed Multiple Round Simultaneous Impact/ MRSI special function that allows the system to provide a similar effect on the target as Multiple Launcher Rocket Systems/MLRS²⁸. However, light infantry brigades should be equipped with light artillery systems in order to allow them a swift deployment, especially by air. The same is true for specialized units that conduct operations in restricted terrain. For example the appropriate artillery means for mountain units remain light mortars, this weapon system being very useful in dense urban terrain too. Anyway there is an increasing need to enhance precision and therefore a sensor-to-shooter capability is mandatory in these types of terrain. Low-level units' tactical drones give an essential intelligence asset for an efficient target acquisition.

As we said before, protection is vital for tactical units survival on the battlefield. Air defence systems have to be multilayered and adapted both to the unit's destination and the features of the terrain. A mountain brigade or a light infantry brigade operating in restricted terrain (mountainous and urban terrain) should develop an air defense system based on MANPAD. When these units are integrated in the higher echelon's operation they benefit from its protection's umbrella. The main idea is that the tactical units have to ensure the specific layers to cover the threats where strategic and operational assets usually do not engage. For example SHORAD and VSHORAD systems as well as CRAM and MANPAD could easily engage targets as low-flight jets and helicopters, drones and swarm air threats, different types of projectiles.

Due to an increasing number of threats in the electromagnetic spectrum, new EW and SIGINT assets should be taken in consideration to strengthen the brigade and division formation. The need for conducting air operation justifies the reason to build air capabilities starting with division level. Airmobile or air assault forces allow tactical units to conduct swiftly offensive and deep operations, or to counter enemy's operations in the own rear area. Moreover, resupplies and medical evacuation for independent or isolate units could be significantly augmented by air capabilities.

In the end, we are trying to issue a few directions regarding the organization of tactical forces. Undoubtedly, the equipping with new weapon systems of the tactical units will generate changes in their organization. Moreover the present fundaments of land operation encourage military decision-makers to transform tactical units' organization.

Having these references in mind, we consider the tactical units' organization in three main constituent subordinate units, to be obsolete. We motivate this fact by emphasizing the importance of exploiting tactical opportunities and responding simultaneously to multiple threats. Moreover, there is a risk of tactical rigidity and predictable action as a result of respecting the three-unit formation's rule. Therefore, in our opinion a four main components organization of the tactical units could be more advantageous. The combat power is directly influenced as well as the maneuver capability. A four main units/subunits formation also allows the commander to build a stronger reserve.

However, according with the situation and the mission received the commander should establish the "the best forces or best combination of forces to achieve the assigned mission"²⁹. He or she has to consider both the strengths and the vulnerabilities of the force, and consequently acts to enhance the first ones and mitigate the latter one. Only by accomplishing this essential requirement, could the premises for tactical success be achieved.

Conclusions

Building the forces we need, for the coming years, is not a simple task. Military capabilities should be designed with the purpose to cover the requirements for all levels of military operation, no matter which the campaign's theme is. Constant development and experimentation activities must be realized in order to keep the military edge.

US Army throughout its *Army Modernization Strategy-2019* is stressing the importance of developing land capabilities including: long-range precision weapon systems and munitions, new generation combat vehicles, positioning/navigation/timing, air and missile defense, increase soldier's lethality, synthetic training environment, efficient networks³⁰. *The Operational Environment and the Changing Character of Warfare* issued by US Army TRADOC in the same year, speaking about "potential game changers to 2035"³¹ is adding swarm-type threats, sophisticated ATGMs and MANPADs, robotics, Camouflage, Cover, Concealment, Denial, & Deception/C3D2 and cyber as the domain where innovation is necessary. This goal comes both from the need to keep technological dominance, as a prerequisite for victory and the necessity to counter enemy's action.

Maybe, these objectives are too ambitious for small country's armies. However, NATO members have to realize that permanent innovation and adaptations of their forces, including tactical ones, is mandatory. Technological advance for NATO as an Alliance has to become a technological advance for each state, in respect with their potential enemies. Small member states benefit than the collective defense prerogatives, but they are part of this arrangement and have also to contribute to it. Land tactical forces have to keep up with the fast-paced changes in order to effectively respond to contemporary challenges. This kind of forces must be able to handle both combat operations, humanitarian aids and search and rescue operations. Therefore, proper equipping and doctrinal adjustments are essential to successfully face future threats. Only by realizing these objectives, the proverbial "an army is always preparing to fight well the last war" could become irrelevant.

REFERENCES

1. https://www.nato.int/cps/en/natohq/topics_84268.htm accessed 03.01.2022
2. North Atlantic Treaty Organization. *Framework for Future Alliance Operations*. SACEUR&SACT, 2018, p. 5.
3. Army Doctrine Publication, ADP 1, Land Operations, Ministry of Defence, Land Warfare Development Centre, Great Britain, p.1-5.
4. Tactical activities refers to those activities conducted by tactical force throughout the entire campaign theme including offensive, defensive, stability and enabling activities. Source: *North Atlantic Treaty Organization, Allied Tactical Publication, NATO Standard, ATP-3.2.1, Allied Land Tactics, Edition B, Version 1*, NATO Standardization Office (NSO), 2018, p. 1-9.
5. North Atlantic Treaty Organization. *Allied Tactical Publication, NATO Standard, ATP-3.2.1, Allied Land Tactics, Edition B, Version 1*, NATO Standardization Office (NSO), 2018.
6. Robert Leonhard. *The Principles of War for the Information Era*. NY, SUA: Ballantine Books, 1998, p.9.
7. Auftragstaktik is today's mission command philosophy of command and it was developed by Field Marshal Moltke the Elder, Prussian Army Chief of Staff between 1857 and 1888.
8. Headquarters, Department of the Army. *Army Doctrine Publication, ADP 6.0. Mission Command*, SUA, 2019, p. 1-7.

9. John L. Romjue. *From Active Defense to AirLand Battle: The Development of Army Doctrine, 1973-1982*. Historical Office, United States Army Training and Doctrine Command. Fort Monroe, Virginia, 1984, p. 51. accessed on <https://www.tradoc.army.mil/wp-content/uploads/2020/10/From-Active-Defense-to-AirLand-Battle.pdf> at 07.01.2022.
10. Major Robert J. Paquin. *Desert Storm: Doctrinal Airland Battle Success or "The American Way of War"?*. Accessed on <https://apps.dtic.mil/sti/pdfs/ADA370380.pdf> at 08.01.2022.
11. Michael E. O'Hanlon. *The Future of Land Warfare*. Washington, D.C, SUA: Brookings Institution Press, 2015, p. 3.
12. *English Summary of the Winograd Commission Report*. Accessed on <https://www.nytimes.com/2008/01/30/world/middleeast/31winograd-web.html> at 07.01.2022.
13. North Atlantic Treaty Organization. *Framework for Future Alliance Operations*. SACEUR&SACT, 2018, p. B-1.
14. *The Changing Character of Warfare: The Urban Operational Environment*, TRADOC Pamphlet 525-92-1, Headquarters, U.S. Army, Training and Doctrine Command. Fort Eustis, Virginia, SUA, 2020, p. 13
15. Ibidem.
16. North Atlantic Treaty Organization. *Strategic Foresight Analysis*, NATO Report, SACEUR&SACT, 2017, p. 8, 37.
17. Ibidem, p. 24.
18. Paul K. Davis. *Military Transformation? Which Transformation, and What Lies ahead?* Accessed on https://www.rand.org/content/dam/rand/pubs/reprints/2010/RAND_RP1413.pdf at 10.02.2022.
19. Rupert Smith. *The Utility of Force*. United Kingdom: Penguin Books, Penguin Random House, 2019, p. 5.
20. North Atlantic Treaty Organization. *Framework for Future Alliance Operations*. SACEUR&SACT, 2018, p. 26.
21. DOTMLPFI-Doctrine. *Organization, Training, Material, Leadership, Personnel, Facilities, Interoperability*.
22. North Atlantic Treaty Organization. *Allied Tactical Publication*, NATO Standard, ATP-3.2.2., Command and Control of Allied Land Forces, Edition B Version 1, NATO Standardization Office (NSO), 2016, p. 1-7.
23. North Atlantic Treaty Organization. *Allied Joint Publication*, NATO Standard, AJP-3.2, *Allied Joint Doctrine for Land Operations*, Edition A Version 1. NATO Standardization Office (NSO), 2016, p. 2-7.
24. North Atlantic Treaty Organization. *AAP-06*, NATO Glossary of Terms and Definitions (English and French). NATO Standardization Office (NSO), 2019, p. 23.
25. Ibidem.
26. Paul K. Davis. *Analytic Architecture for Capabilities-Based Planning. Mission-System Analysis and Transformation*, vol. MR-1513-OSD, RAND National Defense Research Institute, 2002, p.52.
27. Trophy is the most used APS in the world and it is available in HV (Heavy Vehicle) variant for heavy armored including tanks and in MV (medium Vehicle) for medium platforms as IFV or APC; the system is used by Israeli's Merkava tanks and also have successfully integrated on German Leopard 2 platforms, English Challenger platforms and various type of IFV and APC. Source: <https://www.rafael.co.il/worlds/land/trophy-aps/> accessed on 13.01.2022.
28. <https://www.army-technology.com/projects/archerhowitzer/>, <https://www.baesystems.com/en/product/archer> accessed on 15.01.2022.
29. North Atlantic Treaty Organization. *Allied Tactical Publication*, NATO Standard, ATP-3.2.1, *Allied Land Tactics*. Edition B, Version 1, NATO Standardization Office (NSO), 2018, p. 3-3.
30. *Army Modernization Strategy*. Headquarters, U.S. Army, SUA, 2019, p. 7.
31. *The Operational Environment and the Changing Character of Warfare*. TRADOC Pamphlet 525-92, Headquarters, U.S. Army, Training and Doctrine Command, Fort Eustis, Virginia, SUA, 2019, p. 13.

URBAN WARFARE AND ITS IMPLICATIONS FOR LAND FORCES

Major Superior Instructor Claudiu Valer Nistorescu, PhD Candidate

"Carol I" National Defence University
Bucharest, Romania

E-mail: nistorescu.claudiu@unap.ro

Colonel Prof. Nicolai-Tudorel Lehaci, PhD

"Carol I" National Defence University
Bucharest, Romania

E-mail: lehacitudor@yahoo.com

Abstract: There is no doubt that contemporary operational environment, through its requirements, emphasizes the importance of the military operations in dense urban terrain. Taking in considerations the trends with respect of future conflicts and corroborating them with the increasing rate of urbanization, paying attention to this type of operation seems to be logical. Moreover, recent conflicts in build-up areas reveal the sensitive character of these operations. Their ambiguity, mental and physical demands, as well as special tactics, techniques and weapon systems involved, force military planners to adopt a different approach to operation. Having in mind these premises, we have tried to highlight the urban warfare's implications for land forces. Without the intention to be exhaustive, we have strived to emphasize a few considerations in respect of forces' organization, training and equipping, and also doctrinal adjustments.

Keywords: *urban warfare; land forces; military capabilities; urban tactics*

Introduction and research methodology

Military forces encounter many challenges today. The need to adapt their doctrines, organization and equipping comes from the constant changing of the operating environment. Urban areas have always been a challenging and demanding terrain with respect to conducting military operations, both for commanders and soldiers. The nature of urban warfare is the same throughout the century. The same feeling of fear, anxiety and frustration was felt by the soldiers of Russian 62nd Infantry Division led by General Cuiikov in Stalingrad, as the American soldiers trapped in an endless counterinsurgency conflict on the streets of Sadr City.

Recent conflicts demonstrated that the military operations in urban terrain cover the whole spectrum of conflict: large scale combat operations (Grozny, Bagdad Mosul), counterinsurgency (Kandahar, Kabul, Mogadishu), counterterrorism (New York, Paris, London or Mumbai). Moreover, when natural disasters take place, the military instrument is directly involved with the purpose of mitigating the effects and to provide humanitarian assistance¹. Taking in consideration these aspects of the contemporary reality and the predictions of the future's warfare, it seems to be necessary to analyze this type of warfare.

The present study tries to realize a concise image about the features of the modern urban warfare with respect to the land forces' development. The research's limitations are strictly related with the multiple aspects of the urban warfare and, therefore, it was difficult to cover all of them. However, we have tried to emphasize the principal ones that generate consequences to military urban operations. Also, a pertinent analysis of those identified implications, including doctrine adjustments, force organization, training and equipping was issued. The results are especially generated by a profound evaluation of the present requirements for the urban operations, corroborated with the analysis of predictions about future armed conflicts. The influences of high technologies for the military operations were also taken in consideration.

Urban operations' fundamentals

Military experts emphasize the fact that "urban combat is messy and destructive and seen as something to be avoided"². However, military forces have to be able to conduct operations in this particular environment. With the purpose to respond to the question *Why are military operations in urban terrain necessary?*, we will try to emphasize a few critical points.

Most of the time, during low-intensity-conflicts the enemy has tried to exploit the advantages of the urban terrain. This type of conflict is characterized by irregular and unconventional actions, conducted by a force which

is normally considered weaker. Therefore, the necessity to conduct operations in urban terrain is a result and a consequence of the reasoning to annihilate or neutralize existing enemy threats, or to protect local population. In this case, the enemy is usually the one who dictates where the battle takes place with the purpose to compensate his quantitative and qualitative disadvantages.

When we refer to large-scale combat operations in a high intensity conflict situation, the approach is different. Even if the enemy's unconventional and irregular forces retain their possibility to hybridize the urban warfare, there are factors which significantly influence the reason for conducting military operations in this type of terrain. These factors include: political, tactical or economic advantage, potential threat to operation. Consequently, the urban area becomes a military objective that has to be seized and controlled for a period of time.

This particular land operating environment is a result of three components that generate what is called "the urban triad"³. Those components have significant impacts on the urban operations' development and consist in: *physical terrain, population and infrastructure*. The particularities embedded to urban operations by the character of these components impose mandatory activities when this kind of operation is conducted: understand the environment, shape the battlefield, engage the opponent, consolidate the gains and realize the transition to local/governmental authorities/USECT.⁴

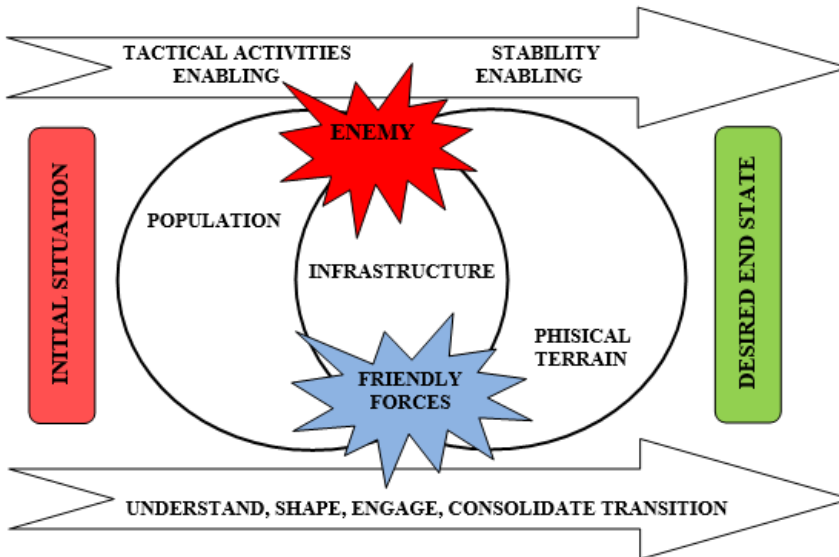


Fig. 1. Urban triad and its implications for the urban operations spectrum

Starting from this point it should be outlined that military planners and field commanders should have in mind the following ideas when military operations in urban terrain are conducted:

- the necessity to understand the operating environment in order to assess the current situation as a mandatory premise for the establishment of a desired end state;
- identifying the factors that are opposing to the desired end state;
- determining the centers of gravity/CoGs and decisive points;
- the importance of shaping the battlefield in support of the decisive operation and subsequent success of operation;
- finding proper solution to effectively mass forces' combat power to engage those COGs, either throughout a direct or an indirect approach;
- the need to maintain the initiative and consolidate gains;
- most likely population is part of the urban terrain;
- the importance of an effective transition of the responsibilities to the governmental authorities.

Moreover, all levels commanders need to realize that "we have to destroy the city in order to save it" is no longer feasible. Maybe it has never been. The population could be the most critical factor that interacts with military

operations. Local population could play a force multiplier role, or on contraire, could dramatically diminish the forces' combat power. Therefore, collateral damage should be taken in consideration, including infrastructures, facilities and services. Unfortunately, too many times "cities kill armies and armies kill cities"⁵. A detailed study about the Russian experience in Chechnya, Israel's intervention in Lebanon (1982) and British experience in North Ireland outlines the fact that urban conflicts are "*neither of short-duration nor low cost*"⁶. In conclusion, military planners and commanders should attentively determine the level of force needed and the proportion of its application, in order to achieve an appropriate utility of force.

Implications for land forces' operations

Doctrinal implications. Tactics and techniques in urban terrain.

If an urban area becomes a military objective, commanders supported by their staff have to plan, prepare and execute a military operation in order to fulfill their assigned mission. The operation's planning process is not different in comparison with other environments processes. However, due to the terrain features, there are some specific doctrinal requirements. Today's modern armies have developed doctrines and field manuals with the purpose to support the conduct of military operations in this type of terrain. Based on the USECT concept (understand, shape, engage, consolidation, transition) doctrinal regulations tries to offer a "how to fight" for land forces.

The general framework for urban operation includes a coherent approach, no matter where the doctrinal guidance comes. In offensive operations, forces assigned to seize an urban objective should initially advance to the objective. The city's isolation is the next inherent and logical step and after that an initial force should be tasked to gain a foothold in the built-up area. Once the foothold is gained, subsequent actions have to be taken in order to destroy or neutralize the enemy's main forces and to clear the city. If the military end state is achieved the transition process is normally started.

Mirroring the offensive action of the opponent, a conventional force which is tasked with defensive activities in an urban area, will strive to deny or to reduce the enemy's advantages. Therefore, the advancing of the offensive force will be probably hampered and counterattacks will be mounted in order to deny seizing that foothold. The defender most likely will exploit the terrain advantages and will transform each building in a "fortress." The battle inflicts heavy losses both on the attacker and the defender, no matter who the winner is in the end. Counterinsurgency operations in urban area combine both offensive and defensive activities with a great emphasis on the stability operations. Commanders and soldiers should be mentally trained to shift from combat to peace operations and vice-versa.

"So what really is different about operations in urban terrain?"⁷ The answer for this question could be found by analyzing the variables that gives specificity to the urban operations. These are: the dimensions of the urban terrain, the density of the build-up area and the order of the effects produced by the terrain to the military operations. They impose a different approach to operation, and doctrinal adjustments are necessary.

In order to mitigate the limitations of the urban terrain or to obtain a relative advantage, commanders should take in consideration some issues. First of all, there is a necessity to obtain a simultaneous relative superiority in multiple locations. The urban battle is usually divided in many small battles, and an effective combat support is difficult to be ensured from a central position, in the classical manner. Therefore, combat support elements have to be divided allowing maneuver subordinate units to receive a proper combat support where and when is needed. As a consequence tactical units should have the ability to realize a rapid disaggregation and/or aggregation of the force.

The reality shows that military organizations many times, throughout the history, were "preparing to fight the last war rather than the next"⁸. This idea, even if it is an apocryphal one, stresses the need to continually adapt both doctrines and tactics in order to obtain success in military operations, including in urban areas. But, it is not very simple to achieve these goals due to the organization's resistance to change that comes from human nature. Adjusting the "how to fight" depends of the commanders' ability to understand the situation and predict future implications for the military operations. Their willingness to act and assume risks gives the organization an opportunity to outrun their enemies. Russian Army in Chechnya,, after the 1st Battle of Grozny in 1996 "made a comeback, but only after a change in command and the new leadership's willingness to shift tactics"⁹.

Tactics and techniques are "products" of the *higher level doctrines* which give them guidance with respect to complying with principles and operations' fundamentals. Although, tactics, techniques and procedures still have a descriptive character, their predictive prerogative is pregnant. The training prior operation, as well the execution, is based on the knowledge offered through different tactical publications different domains.

Considering urban tactics and techniques we just want to outlines a few issues that we have considered relevant for the present. First of all, they are decisively influenced by the terrain characteristics. "*The nature of cities tends to channel combat operations along narrow lanes of activity*"¹⁰. This fact hampers maneuver abilities, obstructs line of sight and reduces dramatically fire support possibilities as well as mutual support between units.

The "binomial" formation formed by armored and dismounted infantry still remains a reference. In urban large scale combat operations tactics have to include the benefits offered by heavy forces, but only with a proper support of infantry and aerial surveillance. Armored vehicles are vulnerable to enemies' top attacks, as well as base-ground attack with antitank guided missiles/ATGMs. The enemy will most likely organize ambushes along narrow streets and will try to block armored maneuvers.

Helicopters' support could be an advantage but, at the same time, it represents a major vulnerability for own forces due to their lack of protection against enemies' short range weapons, including MANPAD, ATGMs, heavy machineguns and even small arms fires. However, when a standoff capability is achieved it could be a significant asset for land forces.

Effective fire support is difficult to achieve with respect to collateral damages, especially to local population. Buildings significantly fracture the terrain and reduce the possibilities of the artillery means. Mortars are the most suitable fire support asset and the tactics and techniques require an attentive analysis of the terrain in order to determine deployment requirements, fire positions, and protective measures. However, light mortars need to be dispatched with infantry platoons in order to provide additional and effective fire support. Precision guided munitions are very useful when are provided and could bring tactical, operational or even strategic effects with a significant reduction of collateral damage.

UAV/UAS will definitely be a permanent mean in future confrontation. Both parts will try to use these instruments to gain an advantage either by obtaining information or by striking the enemy's forces. Commanders should take in consideration that insurgent forces have the possibility to use cheap commercial drones with the purpose to attack in an unconventional manner.

The last problem that we want to bring into attention, regarding doctrinal implications, is the importance of the junior leaders' initiative. Even if high technologies allow today a detailed control of the operations, due to the restrictive and many times chaotic character of the urban warfare, disciple initiative is mandatory. When determining the effects wanted on enemy's forces, field commanders should visualize the actions needed to obtain those effects. By identifying risks and critical points, a commander must accept the necessity to allow subordinates commander to manifest their initiative.

Doctrines, tactics, techniques and procedures for urban warfare ought to give the land forces the fundamentals to conduct successful operations. Moreover, contemporary land forces should enhance their capabilities to counter enemy's guerilla tactics and terrorist tactics (or a combination of them), both in combat and counterinsurgency operations. The ability to counter guerilla actions and tactics implies a permanent adaptation of own tactics. As it was declared in the plan to secure Baghdad in 2008, the success in counterinsurgency depends on the action taken by friendly forces to clear the city, control the operation and retain the initiative in order to facilitate government further control¹¹.

• Organizational and training implications

Resources' limitation does not allow developing distinct forces only with the purpose to operate in urban terrain. There are two general solutions to compensate these shortages. First of all, forces' training for this type of operation should ensure knowledge and skills to operate in this environment according with the unit's mission and destination. Secondly, depending by on operation's type, threats and objectives, units' grouping and regrouping are well-suitable to realize the needed level of force. The risk of the utilization of non-organic forces could be mitigated by training together for this type of missions. But, at the same time, there is a significant enhancement of the unit combat power and also of its versatility.

Task grouping method or "ad-hoc" force configuration during operation is not new under the sun, but today's operational environment stresses the necessity of it. The key to obtain a balanced force in urban terrain is gaining the ability to rapid forces' disaggregation and aggregation. Achieving this goal gives the opportunity to realize superiority when and where it is needed. However, including additional combat engineer assets with EOD capabilities to the maneuver battalions could be taken in consideration. MANPAD sections assigned to the company level could be an issue worth to be considered. Due to an increasing necessity of intelligence in urban terrain, we also consider the constitution of company's level ISR cells as a mandatory requirement.

Training for urban combat is neither short time, nor easier than other types of training. On the contrary, the training could be time and resources-consuming. Undoubtedly, training in proper conditions influences the outcomes of the future battles. Therefore, urban ranges with different facilities including OPFOR, replicators or role players are mandatory. The range should mirror the all dimensions of the urban terrain and the regular training should exceed the estimated time when a unit could be engage in combat. Virtual reality ranges, simulators and augmented reality could also play an important role for the land forces training.

In a recent study about military urban operations, NATO emphasis the need “to determine the most effective agile organization and force composition”¹². The same publication reveals that “NATO training exercises should replicate the intellectual, physical, psychological and emotional challenges posed by urban operations”¹³.

• Equipping implications

Equipping tactical land forces for urban combat is not a simple task. Due to the physical demands and the necessity to move fast, it should be taken in consideration to reduce the equipment overall mass. Therefore, ballistic protection equipment, communication systems and other essential equipment have to be made using light innovative materials.

Dismounted units should maintain their flexibility and ability to swiftly move in dense urban terrain, but at the same time, they need sufficient fire power. Short range antitank guided missiles/ATGMs are useful as well as MANPADS. These weapon systems must be allocated to the lowest tactical level (platoon and squad size subunits). By integrating the “fire and forget” capability, units gain an enormous advantage against counter battery fires.

Active protection systems/APS enhance armored survivability by neutralizing antitank projectiles even from short range. The best well-known systems are Israeli Trophy and Iron Fist that are already integrated on tanks and infantry fighting vehicles from many modern armies¹⁴.

Breaching assets are indispensable when fighting in buildings as well as thermobaric munitions when enemy is located in tunnels and underground areas. As we said before, precision guided munitions are necessary to obtain an enhanced effect and, also to avoid collateral damage. Loitering munitions could be extremely useful in urban combat and plays a double role, both for surveillance and striking the enemy forces in an unexpected way and in covered positions.

Short range tactical UAV/UAS dispatched to the platoon level is another issue that needs attention. In this way, tactical low level commanders' achieve an inestimable ISR asset. Navigation and timing assets, as GPS and BFT, are mandatory for modern force, both dismounted and mounted on vehicles. The same is true regarding night vision devices and jamming assets.

Conclusions

The results regarding the urban warfare implications to the land forces operations are neither exhaustive, nor simple to put into the light. Sir Rupert Smith, a former British general, described the importance of achieving a proper balance between offensive and defensive capabilities and abilities, too. In his latest reviewed edition of *The Utility of Force*, he outlined that “the essence of all tactics and movement, and the basic tactical dilemma is to find the correct balance between how much effort to apply striking the opponent to achieve the objective and how much to countering his blows”¹⁵. In our opinion, urban terrain, due the population interference, considerably gives a much deeper character to this dilemma.

As a final thought, we wish to stress again the idea that urban warfare imposes a special attention for military organizations, both for leaders and planners. Most likely, the urban conflicts will be prolonged for a long period of time, even after enemy's conventional forces defeat. If the transition is not effective, the seeds for insurgency, terrorism and humanitarian disasters are on a fertile soil. These could have long terms consequences for the land forces engaged in urban operations.

In conclusion, commander should continuously strive to train their units in order to become able to conduct operations in urban area. Urban warfare demands flexibility, adaptability as well as physical and mental efforts. Formations and tactics should be adapted to the operating environment's requirements. High technologies and new weapon systems give a great advantage but, in the mean time, urban restrictions could render ineffective these assets. Therefore, soldiers and junior commanders should be able to take initiative, improvise and adapt in order to ensure survivability of their force simultaneous with mission accomplishment. Maybe, one of the major challenge for young officer is to make a swiftly change from combat operations activities to stability and vice-versa. They need to understand the importance of local population and its role for the final outcome. History has demonstrated for too many times that only by gaining their support is a military victory in urban terrain truly a victory.

REFERENCES

1. *The Changing Character of Warfare: The Urban Operational Environment*. TRADOC Pamphlet 525-92-1, Headquarters, U.S. Army, Training and Doctrine Command, Fort Eustis, Virginia, SUA, 2020, p. III.
2. *Reimagining the Character of Urban Operations for the U.S. Army*. RAND Corporation Report 1602, RAND Corporation, Santa Monica, California, 2017, p. XIII.

3. Headquarters, Department of the Army Headquarters, United States Marine Corps. *Urban operations*, ATP 3-06 MCTP 12-10B, U.S.A., 2017, p. 1-3.
4. North Atlantic Treaty Organization. *Allied Tactical Publication*, NATO Standard, ATP-99, *Urban Tactics*. Edition A Version 1, NATO Standardization Office (NSO), 2017, p. 1-5.
5. *Large-Scale Combat Operations – The Division Fight*. US Army Command and General Staff College Press Book Published by the Army University Press, 2019, p. 295
6. *Urban Warfare Study: City Case Studies Compilation*, Marine Corps Intelligence Activity. ATTN: MCIA 04, Quantico, Virginia, USA, 1999, p. 7 and 22.
7. *Large-Scale Combat Operations – The Division Fight*. US Army Command and General Staff College Press Book Published by the Army University Press, 2019, p. 283.
8. UK Ministry of Defence. *Development. Concepts and Doctrine Center, Army Doctrine Publication, Army Doctrine Primer*, Great Britain, 2011, p. 2-4.
9. Reimagining the Character of Urban Operations for the U.S. Army. *RAND Corporation Report 1602*, RAND Corporation, Santa Monica, California, 2017, p. 31.
10. *Urban Warfare Study: City Case Studies Compilation*. Marine Corps Intelligence Activity, ATTN: MCIA 04, Quantico, Virginia, USA, 1999, p. 13.
11. David E., Johnson, M., Wade Markel, Brian Shannon. *The 2008 Battle of Sadr City: Reimagining Urban Combat*. RAND Corporation, Arroyo Center, 2013, p. XII.
12. North Atlantic Treaty Organization. *Framework for Future Alliance Operations*. SACEUR&SACT, 2018, p. D-3.
13. Ibidem.
14. <https://www.rafael.co.il/worlds/land/trophy-aps/> accessed on 29.01.2022.
15. Rupert Smith. *The Utility of Force*. United Kingdom: Penguin Books, Penguin Random House, 2019, p. 14.

TERMINATION OF THE SECOND KARABAKH WAR: CONSEQUENCES FOR THE PARTIES

Khayal Iskandarov Ibrahim, PhD in philology

War College of the Armed Forces
Republic of Azerbaijan

Assoc. prof. Sadi Sadiyev Saleh

International Military Cooperation Department
Ministry of Defence
Republic of Azerbaijan

Abstract: The opinions on the consequences of the Second Karabakh War have been presented in the paper. The factors leading to the victory of Azerbaijan and defeat of Armenia are indicated. The authors have construed the thoughts of various analysts and experts and associated the results of Second Karabakh War with their findings.

Keywords: *The Second Karabakh War; conflict; gain; victory; defeat; concession*

The Armenia–Azerbaijan conflict had entered the history of the twentieth century as one of the most tragic conflicts, the consequences of which have seriously affected the fate of millions of people. Until the peace agreement of 10th November, 2020, the conflict had been accentuated as one of the most protracted conflicts because of Armenia's unconstructive policy. For twenty-seven years, Yerevan had eschewed negotiations and international community simply observed and OSCE Minsk Group co-chairs made formal statements. For the last 5-6 years the conflict over Karabakh had been at the focus of attention with sporadic shootings. August 2014, April 2016, July 2020 were more conspicuous months with regard to the confrontation between the parties (Piriyev et al., 2020). That was the reality of the Karabakh conflict. Everything was evident, Armenia had occupied Azerbaijan's territory and Baku had tolerated for thirty years with an expectation of peaceful settlement of the conflict. Azerbaijan had always expressed a will for peaceful settlement of the conflict. It should be particularly mentioned that, Armenia had other territorial claims in Azerbaijan in order to extend its so-called "security belt". There were intelligence reports that Armenia had been planning an offensive operation against Azerbaijan with the purpose of seizing other lands. Armenian policy of transferring YPG/PKK terrorists who received training in Iraq and Syria to Karabakh region is a proof of our argument. Pashinyan's government had been preparing for war, while the world community expected them to prepare their nation for peace. Finally, on September 27, Armenian armed forces initiated offensive operations along the entire frontline. However, Azerbaijan Armed Forces launched counterattacks, which ushered in a new security environment in the region. Azerbaijan's resolute counter-offensive operations against Armenia reverberated around the globe. Thus, Azerbaijan Armed Forces smashed the first echelon of Armenian Army and broke down the so-called "impregnable defense line". Armenian government did not expect it, therefore, Azerbaijan's successful combat operations shattered their reputation among Armenian community.

For each of the parties, the war can have one of the following four consequences: – defeat; – concession; – gain; – victory (Slantchev, 2004). Azerbaijan achieved the highest of these consequences – victory. Because the determination of the Supreme Commander-in-Chief, the capabilities of our Armed Forces, the unity of our people allowed us to achieve this result. Thus, on November 10, 2020, the President of the Republic of Azerbaijan, the Prime Minister of the Republic of Armenia and the President of the Russian Federation signed a joint statement on the termination of the war. With this statement, the victory of Azerbaijan and the capitulation of Armenia were unequivocally declared. If before the war, Armenia had an opportunity to gain from the conflict, in the first stage of the Second Karabakh War (when Azerbaijan Army launched counter-offensive operations and broke the enemy's line of defense) it was apparent that, Erevan was completely deprived of the last two consequences. From the first days of the war, Azerbaijan began to lay down conditions. It should be noted that official sources show that, the loss of personnel of the Armenian army is around 2500-3000 people. However, it is a fact that the Armenian leadership hides the number of casualties from the people, refuses to take hundreds of corpses left on the battlefield, and presents the dead soldiers as missing or fugitives. As early as mid-October, Turkish and Russian media reported

that the Armenian army had lost about 8,000 men, and in early November about 13,000 (Piriyev et al., 2020). L.F. Richardson notes that if a party with a smaller population loses 0.05-5% of the total population, then its defeat is inevitable (Stein, 1980). According to this hypothesis, Armenia with about 2.5 million population lost more than 0.05% of its population in early November, which was one of the main reasons for the defeat (Piriyev et al., 2020). Armenia, which suffered a large loss of personnel and military equipment, could have prevented the subsequent loss by accepting the terms of the Azerbaijani side at that time. However, the incompetent political leadership of Armenia could not assess the situation realistically. Thus, Armenia was faced with the worst consequences of the war (concession and defeat).

The war can be prolonged if there is a balance between the opportunities and capabilities of the parties. However, it is a reality that, even having considered the illegally stored arsenal of Armenia, there was a significant difference between the armed forces of the parties in favor of Azerbaijan in terms of strength, power and capabilities. The number of enemy's destroyed weapons and vehicles shows that, not only the resources available in the Armenian army were depleted, at the same time the equipment provided by their supporters were wrecked. This made only two of the consequences of the war possible for the Armenian leadership: compromise and defeat. In early November, having called the people for fighting, Pashinyan stated that no concessions were possible. In fact, Armenia's "resistance" and the mobilization of the remaining personnel were intended to save the government. Pashinyan and his team wanted to create the image that, "they did their best" to absolve themselves of responsibility for the historic defeat. However, this approach was more dangerous than accepting the terms of Azerbaijan. Having considered the real situation on the battlefield, the difference between the available resources, the determination of the Azerbaijani soldiers to win and the despondency of the Armenian army, Armenia's "resistance" would not have lasted long. The political and military leadership of Armenia knew this very well. Ordinary armenians were unaware of all this and believed in the leadership's narration about the war. Therefore, mostly the grassroots were taken aback when the Armenian government signed the capitulation agreement. Undoubtedly, the Armenian leadership saved itself from complete defeat by accepting the conditions of Azerbaijan and making concessions. As Pashinyan himself admitted: "*If the war had not stopped, 20,000 to 30,000 Armenian soldiers would have perished on the battlefield*" (Piriyev et al., 2020). As a rule, defeat is accompanied by regime change in the defeated country. Therefore, Pashinyan's team temporarily prolonged the life of the government by withdrawing the rest of army in accordance with the timetable set in the agreement. What is important is that against the background of Azerbaijan's resources, the difference between the dates of the realization of these two consequences of the war for Armenia would not be more than a few days.

REFERENCES

1. Klingberg, F.L. The historical alternation of moods in American foreign policy. *World Politics*. No 4, (1952), p. 239-273.
2. Slantchev, B.L. How Initiators End Their Wars: The Duration of Warfare and the Terms of Peace. *American Journal of Political Science*. Vol. 48, No. 4 (October 2004), p. 813-829.
3. Stein, A.A., Russett, B.M. Evaluating War: Outcomes and Consequences. *Ted Robert Gurr eds. Handbook of Political Conflict: Theory and Research*. New York: The Free Press, 1980, p. 399-422.
4. Piriyev, H., Tahirov, R., İskenderov, X. Mühəribənin bitmə müddəti və sülh şərtləri (ikinci Qarabağ müharibəsinin nümunəsində)". *Hərbi bilik*, No. 4 (2020), p. 5-13.

COUNTERING OPERATIONAL LEVEL DECEPTION

Major Superior Instructor George-Ion Toroi, PhD Candidate

“Carol I” National Defence University

Bucharest, Romania

E-mail: george_toroi@yahoo.com

Abstract: Military deception has long been recognized as an effective tool for confusing and confounding the enemy. But what if the enemy is using deception to mislead and manipulate your operations? In that case, military counter-deception represents a vital tool for developing an accurate picture of the enemy's operational intentions, but also for preventing damages on your mission accomplishment. However, countering deception operations is no easy task for most of the modern militaries and requires a lot of experience and self-awareness. It implies more than just detecting the enemy deception. It also involves the process of how one uses this information.

“Russia views deception (Maskirovka) to be a vital precursor to success”¹. Combining this with the benefits one might encounter out of employing deception, should constitute reason enough for western countries to develop effective counter-deceptive measures and procedures.

Military counter-deception methods provide a way for analysts to understand how the opponent intends to deceive, and can help the military to minimise the negative effects of its deception, but also to develop suitable responses to the threats before they interfere with the friendly objectives accomplishment.

Keywords: *deception; counter-deception; information; analysis; influence; target*

“All warfare is based on deception”

Sun Tzu

Introduction

*Commanders and staff must consider the enemy's use of deception.*²

History abounds with examples of deception operations. Regardless of the period, misleading was an essential component of the design of operations. It is a proven fact that employing such actions might bring operational advantages, otherwise unreachable. “All warfare is based on deception” represents one of the most famous and relevant truism with respect to warfare. That being said, preparing for war must encounter activities to counter the enemy's deception. Although this is a logical deduction to what Sun Tzu stated, history has demonstrated that many armies were caught unprepared when they dealt with adversary's deception operations. Even today, studies in counter-deception are far less developed than the ones for deception operations. Although, most of the international actors are aware of the high possibility of being deceived in a potential conflict, their doctrines with respect to this domain are rudimentary. For example, the US dedicated only two pages out of ninety-two for counter-deception, in their military deception doctrine³.

Furthermore, the features of the contemporary operational environment are huge enablers for deception operations. Only if we think about how the information environment has evolved, this fact becomes obvious. Nowadays, discerning right from wrong, truth from lies or information from misinformation or disinformation can be an almost impossible job one can make. Moreover, the huge quantities of data that needs processing can also constitute a premise to poor understanding of some situation. Furthermore, the evolution of communication technology has profoundly transformed our society. Nowadays, everybody and everything is interconnected and interdependent. All of this represents realities that malicious actors can use in order to manipulate perceptions on a large scale.

Despite its importance, military deception is an under-explored topic. This article will address the basics of military deception, with a particular focus on detecting it. I will begin with a definition of military deception and its various forms, followed by a discussion of the various ways in which it is enacted.

Given the advantages of using deception and the ease with which aspects of today's operating environment make it possible, one must be prepared to identify and defeat the adversary's use of such a tactic. However, “countering deception is a tough business”⁴. Considering this entire context, the main objective of my article is to identify possible solutions to overcome and counter the opponent's use of deception tactics at the operational level of war. To this end, the primary research question this article wants to analyse is:

How to counter enemy operational level deception in today's context?

In this respect, I divided the topic into three main sections:

First and foremost, I believe that a thorough examination of the principles of deception, including theory and process, is essential. One cannot counter something unless he has a comprehensive understanding of what it is and how it works. For this reason, I will do an examination of the methods, tactics, means and techniques deception operations employ in order to succeed. The intended outcome of this will serve as the foundation for the counter-deception section of this paper.

Next, I will move to the counter-deception, establishing the need and benefits of doing this, but also the steps that have to be followed in order to properly execute it. The whole process of counter-deception will be developed upon the results extracted from the previous section with respect to the deception "modus operandi" in our contemporary operating environment. This is of critical significance to the overall objective of this paper as it will provide a focal point for improving the counter-deception process.

Finally, I will turn my attention to the principals that, if followed, will exponentially boost the probabilities to notice and counter the opponent's use of deceptive techniques.

Fundamentals of deception

Deception is an art. It is about using a variety of methods to trick others into believing things that are not true. It is about getting your opponent to make mistakes that will portray as opportunities for the deceiver. Deception is an age-old military tactic and can be considered as a vital tool of warfare.

„Denial and deception operations provide force-multiplying advantages by enabling operational access and joint forcible entry operations under A2/AD conditions and contributing to the cognitive demise of an adversary as part of the psychological warfare effort. In addition, counter-denial and deception operations are critical to future conflicts, as demonstrated by our adversaries' skilled use of deception in Syria, Iraq, and the Crimean Peninsula"⁵.

The first step towards countering adversaries' deception is to have a comprehensive understanding of how these operations are planned and conducted and why do they represent a viable option employed by commanders in conflicts.

"Military deception is actions executed to deliberately mislead adversary military, paramilitary, or violent extremist organization decision makers, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission"⁶.

There are several key elements with regards to the definition that shows what deception is and worth highlighting:

- *"How to do it"*. As can be seen, deceit entails tricking the opponent into believing a false story. This can be accomplished by adopting a number of specific methods and techniques that have been proven, in prior confrontations, to increase the odds of deception.

- *"Against whom"*. Deception operations have a specific target. All the misleading efforts are directed towards this target, trying to convince him of the deceptive image, persuading him to take some actions that will actually benefit the deceiver in the end. The target is identified as being the opponent's decision-making body, the one with the proper authority to put into practice the desired reaction.

- *"To what end"*. Deception operations should always be employed in support of the mission. That's why a thorough analysis must be done in order to identify if deception is feasible and can support through its possible effects the overall concept of operations towards achieving the desired end-state conditions. The opponent's reaction (action or inaction), based on his perception, is what constitutes the prerequisite for mission accomplishment with respect to the deception operations.

Uncertainty is a key facilitator for deception operations because it affects the target's capacity to form its perception of the operational situation. In this respect, depending on the desired outcome and adversary's pre-existing beliefs, deception may be employed either to reduce or enhance the target's level of ambiguity regarding a certain situation, both of which implying misleading. These two methods of deception⁷ are:

- **A-Type** – ambiguity producing deceptions;
- **M-Type** – misleading deceptions.

Increasing the target's level of ambiguity can be accomplished by presenting him with multiple reasonable possibilities from which he can choose, all of which are in reality harmful to him. When using this strategy, there are two possible outcomes: either gaining time to undertake other military actions by slowing the enemy's decision-

making process, or increasing the likelihood that the target will choose one of the deceiver's false alternatives, in which case he will fall into a trap. "This type of deception is typically successful with an indecisive decision maker who is known to avoid risk"⁸.

On the other hand, decreasing the target's level of ambiguity is suitable when the adversary already considers one of the options to represent his best answer to a particular problem. However, at a closer examination, this alternative will do the deceiver a benefit if the opponent will pursue it. In this case, the deceiver should use deception to convey information that increases the opponent's confidence in his decision. "Planners often have success using these deceptions with strong-minded decision makers who are willing to accept a higher level of risk"⁹.

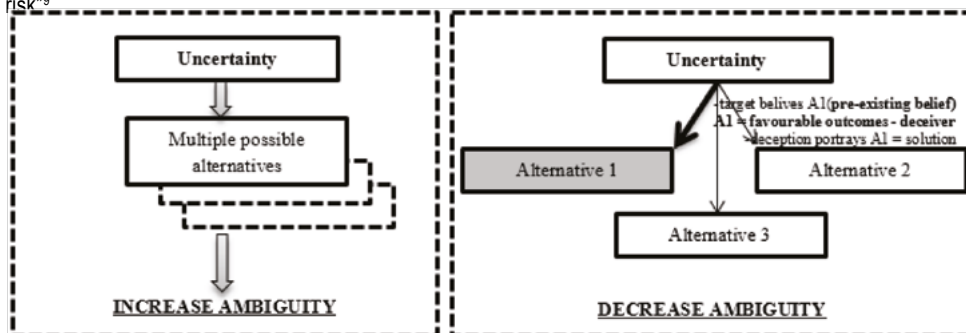


Fig. 1. Deception and uncertainty

Deception does not equal lying. The deceitful message isn't entirely false. Deception must incorporate both true and false information. It needs to be so as, in order to succeed, it should not come as a surprise for the opponent. The entire deceptive picture should make sense for him. Otherwise, the deceptive story would become easily detectable and may be used in order to double trick the initial deceiver. One of the principles of deception says that the fewer the lies within a deceptive story the greater the chances for its success.

Moreover, deception implies both revealing and concealing information from the adversary in order to draw the desired deceptive picture. To this end, deception uses active measures also known as simulation and cover or dissimulation methods. For each of these two methods there are several specific types of deception that might be employed.

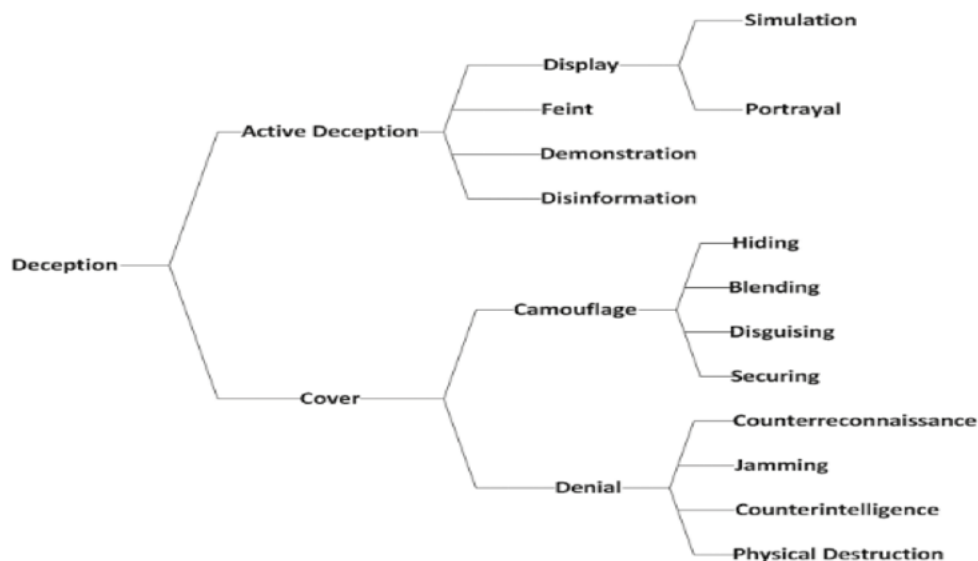


Fig. 2. Taxonomy of deception¹⁰

Successful deception operations imply a very complex process. Deception should have a clear objective towards which all the deceptive efforts should be directed. Furthermore, based on what the deceiver wants to achieve by employing deception, the target's desired perception should be defined. This is what the opponent should believe in order to take the anticipated actions. Perception is how someone interprets what he sees. The enemy creates this image based on the observables the deceiver is portraying for him. One other important element in the deception process that the deceiver needs to analyse and employ is represented by the channels used to convey the deceptive message to the target. The greater the number of channels through which the message is delivered, the greater the likelihood of success. However, there should be a synchronization among the information sent through all of the channels otherwise the opponent will become suspicious and the chances for success will decrease substantially.

At a minimum, deception process should incorporate the following:

- A clear objective.
- A story that should be conveyed to the target in order for him to form the desired perception. The story is delivered to the opponent by employing some deceptive actions supported by the proper techniques, means and methods.
- The target's decision and reaction.

Multiple approaches are frequently used in successful deception. The fuller the deception story, the more information the victim needs to filter through, and the more likely he will do so in accordance with the deceiver's wishes. The only limit to the deception strategies that can be used is the deceiver's creativity.

A compelling story is at the core of an effective deceit. Successful deception strategists have a creative imagination that is both vivid and disciplined. Creating a deception story needs more than just the skill to weave a complex and detailed scenario. It also necessitates a thorough understanding of the opponent decision maker's ideas, prejudices, and biases. For example, it is simpler to reinforce a deception target's pre-existing belief than it is to modify it, according to "Magruder's Principle", one of the core maxims of deception.

The deception actions that provide this story must fit with the enemy's expected broad sequence of events. They must appear rational and cannot seem to be contradictory. In this respect, an analysis about how the opponent expects things to unfold is paramount. This analysis should also point out the adversary's weaknesses and vulnerabilities that can be used when planning deception operations.

Deception is used at all levels of warfare, being often interwoven and interdependent. However, the focus of this paper is on operational deception and how it might be overcome.

Warfare has changed considerably over the centuries. In the past, battles were typically decided by which army had the biggest or strongest soldiers. Nowadays, however, the operational level of warfare has become increasingly important. In today's complex conflicts, operational commanders are charged with the complex task of developing and executing the strategies and plans that will achieve strategic goals. They must evaluate and adapt to a rapidly evolving situation, and are ultimately responsible for the success or failure of operations. The operational level of warfare refers to the processes and activities involved in shaping the current military environment in order to achieve one's strategic goals.

Operational level deception tries to influence the opponent's military leaders' capacity to execute operations at the operational level of war. Theatre level surprise is the main benefit operational level deception might ensure. Considering the importance of "jointness" within today's military operations, but also the great impact that deception might have with respect to the outcome of the military confrontation, I think the study of operational level counter-deception should be of outmost importance for every military organisation. In this respect, this paper studies the operational level counter-deception process and principles that needs integration within the overall concept of operations.

Operational level counter-deception process

In the heat of battle, it's difficult to sort out truth from fiction. This is where military counter-deception comes into play. Its methods should be integral to any military operations.

"Counter-deception includes the intelligence activities to identify denial and deception operations as well as the operational activities undertaken to negate, neutralize, diminish the effects of, or gain advantage from foreign denial and deception operations"¹¹. Counter-deception is a staff responsibility intended to discover and counter the enemy deception aimed at eroding friendly troops' will, awareness, or the use of force. Countering enemy deception is a mix job between intelligence and operations branches as it involves both detection and counteraction.

The development of measures to counter the enemy deception is a must as they contribute to the protection of C2's own systems against the misleading actions of the opponent. Considering that „deception must be an integral part of all operations”¹² and that “OPSEC and deception planning are required against all adversaries”¹³ counter-deception should also be taken into account when constructing the overall concept of operations. “It is thus imperative that the staff remain alert to the possibility of potential adversarial deception and understand adversarial tactics, techniques and procedures and the wider political and cultural context in which their approach to deception sits”¹⁴.

Countering the opponent deception operations should start by concealing those essential information the adversary needs in order to portray a successful deception. OPSEC goes hand in hand with deception. Deception and OPSEC are complementary activities, and their complementary planning increases the chances of creating the opponent's desired perception with respect to the deceiver's capabilities, actions and intentions by portraying only carefully selected information. “Security is a prerequisite for any successful deception”¹⁵.

However, employment of OPSEC measures might represent an important factor in countering the opponent's deception as well. Concealing information regarding the own C2 structure, decision-making process, intelligence collection vulnerabilities, to name but a few, will either prevent the enemy from using deception operations or enhance the probability to detect a not so well prepared opponent's deception.

Therefore, OPSEC measures should mitigate the enemy employment of deception considering he will not have access to the necessary information in order to create a sound and feasible plan in this respect. However, should the adversary decides to move forward with deception, he will have a huge disadvantage, not knowing essential information regarding the target, the channels, the filters or other essential deception elements. A poor prepared deception plan might portray operational opportunities that need to be exploited by the target.

Counter-deception entails more than just recognising the adversary use of deception. It is a process that involves three steps¹⁶:

- *detecting the opponent's deception;*
- *confirming the opponent's deception;*
- *countering / exploiting the opponent's deception.*



Fig. 3. Counter-deception process

Operational level deception detection

“The *detection of deception* against friendly forces is a J2 responsibility”¹⁷. Friendly intelligence capabilities are essential in identifying the adversary's attempts to deceive. There are two components of the intelligence function that are heavily involved in the process of detecting the adversary's deception efforts: the intelligence collection assets and the analysis staff. By foreseeing and recognizing the deceptive manoeuvres of adversaries, commanders can take appropriate actions to prevent or mitigate harm. Deception detection is the first and most important step of the counter-deception process. It facilitates the possibility to minimize the enemy deception impact, but can also support, if feasible, the development of plans to surprise the adversary and gain the upper hand in the confrontation.

However, in order to set the stage for counter-deception, skilled deception personnel must first get a thorough understanding of the enemy's deception philosophy, procedures, capabilities, and restrictions. It's also crucial to know how he has employed deception in previous battles. Additionally, a comprehensive understanding of how deception works is also critical to detecting the opponent's deceptive activities, but also to set the stage for a productive counter-deception operation. The ability to detect and understand military deception is an important part of any military operation, regardless of whether it's a conventional battle you're fighting or an unconventional crisis you need to navigate. Deception techniques are designed to confuse, mislead, and sometimes trick enemy forces in order to gain a decisive edge. It's usually difficult, if not impossible, for enemy soldiers to know when they're being deceived. The first and best way to protect your forces from being deceived is to be aware of deception methods so you can avoid being fooled.

The intelligence community is often the first to identify enemy deceptive indicators and plays the largest role in confirming or debunking a deception. Considering that military counter-deception efforts are an integral

part of any military operations, commanders must ensure that the intelligence structures have the resources and authorities they need to identify deception early on and confirm or support denying it quickly without any delay.

However, the target's intelligence structures are of utmost importance for the deceiver as well. From deception operations perspective, they are considered filters that collect the deceptive data, process it and deliver the outcome information to the target for its decision. The intelligence staff role in the deception process is to collect all the deceptive observable and to create an overall image of the situation which is then disseminated to the target. Based on this, the target gets the desired perception that will determine him to make anticipated decisions that will put into motion a desired reaction, from which the deceiver will benefit.

From a counter-deception perspective, detection of the enemy's deceit take place from the time when the sensors detect the portrayed actions to the interpretation of the overall operational picture. For this reason, in order to make sure that the desired information reaches the target, the deceiver must do a thorough analysis of all this filters when planning the deception. In this respect, he must understand the entire intelligence process, considering both personnel and procedures. This understanding is crucial for the deceit success. The more this information is hidden from the adversary, the more chances for the counter-deception to succeed. That's why OPSEC plays again a huge role in detecting the opponent's deceptive messages, by setting the scene in this regard.

However, considering the analysis the opponent does on the target's intelligence process in order to display specific information with higher chances of success, detecting deception is no easy job. If the deception operation is well planned, prepared and resourced, it becomes extremely hard to be identified. Barton Whaley one of the most famous researchers of the military deception domain has concluded in one of his study: "Indeed, this is a general finding of my study—that is, the deceiver is almost always successful regardless of the sophistication of his victim in the same art"¹⁸.

Furthermore, efficient deception will bring increased risks to the accuracy of data evaluation. For this reason, the opponent's intention to use deception must always be considered when processing information.

Intelligence cycle processing phase is when deception should be detected. Identifying the adversary's deceit is not necessarily about collecting lots of information, although this is a plus, but about the quality of the analysis made regarding those information. When it comes to detecting trickery, observing isn't enough. A proper identification of these actions requires a profound understanding of the operational situation. Understanding is a consequence of a thorough analysis and interpretation of collected data.

In this respect, the intelligence analysts should always be sceptical with respect to the information they have to process and should not jump easily to conclusions. If time permits, multiple sources confirmation of the analysis conclusions should be made. Double checking the information against credible information and sources might reveal possible incongruities which should raise some questions for the analyst. This constitutes one of the first steps towards detecting and countering the opponent's deception operations. Often, the best way to detect military deception is to look for inconsistencies between different sources of information.

Although the analysis and interpretation process is the basis for detecting deception, intelligence collection also plays an essential role in this respect. The ability to identify and observe information besides the one intended by the deceiver can enhance the possibility for the analysts to detect the deceptive intention of the adversary. This can be made by identifying some incongruities within the information collected from several sources. As deception is heavily reliant on imagination and creativity, counter-deception should make use of the same qualities. Analysts must always see the information collected from different perspectives, analysing several hypothesis and alternatives with respect to this data.

„Achieving the goal of counter-deception requires, above all, sound knowledge"¹⁹. However, analysts must be aware of their biases and prejudices, as well as judgement errors that might interfere in their process of evaluating, analysing and interpreting information.

Military intelligence analysis has evolved significantly over the past century, with the development of complex technologies and techniques to support the collection, collation, and analysis of data. Many of this can also support the deception detection efforts, which are the process of identifying attempts by an opposing force to deceive or mislead the analyst through the use of false information, misleading actions, and other deceptive tactics.

Opponent's operational level deception confirmation

The second step towards countering the enemy's deceptive efforts is confirming the opponent's deception. Based on the results from step one, if intelligence uncovers or indicates possible enemy deceit, the staff must

thoroughly investigate the situation and guarantee that the information, as well as its anticipated impact on the friendly operations, is presented to the commander, as counter-deception is a command-led and driven activity.

Confirming the enemy deceit requires tremendous efforts to determine its entire deception plan. Actually, this is much easier said than done. Deception operations are very well planned and executed, and can be done with a relatively small number of people. Confirming that an operation is false requires a much larger amount of personnel. This makes it very hard to catch the enemy in a lie. However, this step is essential for the development of response options, which will take place next. The more accurate our information is regarding the enemy deceit, the more chances for a successful exploitation of the situation will arise.

The whole confirmation process starts, if not done already, with an examination of the vulnerabilities that the deceiver could have exploited. This analysis requires a deeper understanding of all the information environment dimensions: physical, informational and cognitive. The analysis should identify vulnerabilities prone to deception techniques within all the target's systems.

Having identified their vulnerabilities, the deception target's staff should then do an analysis of the deceiver plan. In this respect every little detail is significant. In order to be productive, this examination should be conducted from the deceiver perspective. Some of the study's conclusions should focus on the following:

- discover if proper conditions exist in order for the enemy to employ deception;
- understand the motives behind the enemy deception operation;
- identify the enemy deception aim and goals;
- what is the desired perception that the deceiver wants to create for its target;
- what is the deception story;
- how does the deceiver want to implement it? What specific events and actions does he want to portray in this regard? What means, tactics and methods are best suited for him to employ;
- what are the appropriate channels and conduits he will use in order to deliver the desired message;
- identify possible measures of effectiveness the deceiver wants to accomplish in order for its deception to succeed;
- what forces, when and where will he be using in order to assess the implementing of the deceptive observables?

After developing a thorough understanding regarding the enemy deception, the outputs of this sub-step should be used to focus friendly intelligence collection efforts to confirm or deny the existence and scope of the actual enemy deception plan and related execution. The information the sensors collect will be then analysed by the same people that made the previous assumptions regarding the opponent's deception plan. It is of outmost importance that the necessary OPSEC measures are taken so that only selected friendly personnel are aware of the collection purposes and proper masking techniques are employed. The outcome of the intelligence collection should support the improvement of the assumptions previously made and should conduct to the actual confirmation of the deceiver's plan.

Opponent's operational level deception countering / exploitation

Knowing about an enemy's deception plan allows a commander to take the necessary steps to prevent it or exploit the opportunity. "The response to the detection of deception against friendly forces is a command-led J3/5 responsibility"²⁰.

Confirmation of the enemy's deception is crucial for the friendly plan adjustment and can represent, in most cases, an advantage that needs exploitation. Knowledge of the enemy deception plan must become a critical EEFI for the friendly commander for the counter-deception to succeed.

"The commander will seek to ensure their own EEFI remain protected and may task additional joint intelligence and collection capabilities to reveal the true dispositions and intentions of adversarial forces. The commander will then require a series of actions and managed information releases, planned to cause adversaries to continue expending time, effort and resources to reinforce a deception plan that they believe is working"²¹.

Having confirmed that the enemy is employing deceptive operations and having identified the specifics of his deception plan, the selected staff can now move to countering or exploiting the opponent's plan. In order to identify the best suited option, two distinct steps need to be followed. First, a thorough analysis related to the effects the enemy deception is creating on the friendly current and future operations and second, development of specific options to respond to the threat the opponent's deception is posing for the friendly forces and mission.

The commander may pick from numerous alternatives to respond to the adversary's deception scheme, depending on the risks involved. He has the option of ignoring, exposing, exploiting, or defeating the opponent's deception.

If the enemy deception does not affect significantly or at all friendly operations, commanders may choose to disregard it. In this scenario, waste of enemy resources and energy will result. However, a close monitoring of the adversary's deceptive events should take place in order to minimise the impact of further unanticipated developments in the deceiver's plan that may hinder friendly forces ability to fulfil the mission.

The second option the deception target can employ is to publicly expose the deceiver plan. Gaining neutral actors support or decrease the deceiver's influence in the area, thus weakening his position, might be some of the outcomes resulted from implementing this option.

Exploiting the enemy deception is by far the most challenging option a commander needs to analyse. However demanding this might be, it is also the option that might get you closer to defeating your opponent. Exploiting requires double-tricking the deceiver, thus making him becoming the deceived. In order to succeed, one needs to maintain the impression of being deceived, but also to conduct simultaneous operations to enhance the ability to exploit a future opportunity. It requires developing a deception plan that has some limitations with respect to continuing to do what the initial deceiver expects friendly forces to act. However, knowledge of enemy deception plan constitutes an advantage when trying to develop your own counter-deception plan. In this situation, the **M-Type**, misleading deceptions may represent the most suitable option to be employed. In this respect, maintaining the opponent's positive perception regarding its deception is essential for the counter-deception process.

Commanders may choose to defeat the deceiver's actions by destroying its capabilities and resources that enable him the possibility to deceive. However, a detailed analysis of the consequences that may result from the deceiver's deceptive capabilities destruction should be undertaken. Furthermore, outcomes of this analysis should identify second and third order effects and risks for the friendly forces and mission.

Choosing one of the above options should be the consequence of an analysis regarding risks associated versus benefits gained by adopting any it. This analysis must always be done with respect to the friendly force objectives and mission accomplishment.

Counter-deception principles

„A holistic analytical approach to a fully effective counter-deception capability requires a prepared mind and a prepared organization. Achievable? Yes, but not easily”²². In order to support the counter-deception efforts commanders must always be aware of some principles that can help them protect their forces from being deceived. There are four well-known counter-deception principles²³: know yourself, know your channels, know your enemy and know the situation.

All of the above principles will support a deeper situational awareness with respect to adversary deception operations and how it may be avoided or countered so that in the end one can accomplish its objectives without falling into a trap. Sun Tzu has stated more than 2000 years ago that: “If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle”²⁴. This aphorism has proven to be valid throughout the years and may very well be suited also for today's military conflicts.

Successful detection of deception is found to be “largely or entirely intellectual rather than technological in nature”²⁵. That emphasises the importance of human analysis done in order to detect and exploit the enemy deception. Although technology may be of some help, in the end the human mind is the one that identifies enemy deceptive activities, but also decides how to react in order to make use of this situation to achieve the desired end state.

Know yourself

Knowing yourself is essential in counter-deception operations. Out of the three steps of the counter-deception process, knowing yourself can support mostly the first two, detecting and confirming of the opponent's deception. When doing this analysis of your own force it is imperative that you identify as much vulnerabilities as possible that the adversary may use as basis for his deceptive intent. Vulnerabilities represent weakening spots within your structure that the adversary may be inclined to use in his deceptive operations. It is also crucial that you do this analysis with a high degree of correctness regardless of how painful might that be. Personal ego should be left outside when doing such an analysis. The more accurate the analysis done the more protective measures can be taken in order not to be surprised by the opponent's deception.

Analysing yourself requires examination of both personnel and procedures. Personnel examination requires understanding the biases, prejudices and limitations of the mind of all those involved in collecting, analysing and taking decisions throughout the whole deceptive process. The human mind is a complex organ, capable of grandeur and wonder. But it is also a curious thing, prone to mistakes and blind spots. When we are faced with a complex problem, our first instinct is to come up with a simple answer, even if that answer is far from the truth. This is an unfortunate tendency, but it is also a natural one. When analysing the procedures involved in the collection, analysis and interpretation, as well as in taking decisions, one should examine timings, methods employed, vulnerabilities, but also techniques and doctrines used in support.

A thorough understanding of what deception is and how it works is essential when starting to do this analysis. This prerequisite is vital because the self-inquiry that the force is doing should be treated from the deception point of view, trying to identify vulnerabilities that can be exploited through misleading operations by the opponent. The overall idea of the analysis is to identify if you are prone to be deceived and how.

Every aspect regarding deceptive information collection, analysis and interpretation, dissemination, decision making process should be examined. Every filter that influences the deceptive message towards the target should be analysed. At a minimum, the following issues need a thorough analysis when trying to know yourself from the deceit point of view:

- How many sensors to collect the information the force has? Are they experienced? Are they well trained?
- What are the limitations of the technical sensors?
- How do you collect the deceptive message? Are there any limitations with respect to the whole electromagnetic spectrum?
- Who is processing the data collected? What personal, cultural or organisational biases can be identified that are relevant for the processing phase?
- How do you evaluate the collected data?
- How do you analyse and interpret the data collected? What techniques and procedures do you use in this regard?
- How long is this process going to last?
- What are your own decision-making process limitations?
- How long will it take for the commander to take a decision?
- What are the enemy deception target preconceptions, prejudices and biases? What is his leading style, his military experience and character?
- Are there any limitations with respect to the force situational awareness?

Know your channels

This principle can either be understood separately or as a sub-principle of the previous one. Either way an analysis regarding the deceptive channel the enemy might employ needs to take place. This analysis should reveal information about how the data is collected, how long is the channel available to receive the message, how trustworthy is that source for you, or how the sensors might denature the true meaning of the message. These are only some of the information one needs to examine when doing such an analysis in order to maximise your chances to detect the enemy deception efforts.

Analysing your channels might give you a flavour of which one is prone to be used by the enemy in his deceptive efforts. Considering one of the deception maxims that states the more channels used to send a deceptive message, the more credible it become for the target, own channel analysis is a must in the counter-deception efforts of the force.

Know your enemy

Knowing your enemy allows you to better anticipate how he will employ deceptive methods to gain the desired advantage. The analysis made on the opponent should focus on revealing his deceptive doctrine, lessons from its previous employment of deception, what assumptions does he employ in order to plan the deceit, its level of knowledge with respect to friendly forces, disposition and intentions, his situational awareness, his desired end-state, objectives and intentions, as well as means and motives to employ deception. For this analysis to be as relevant as possible it is crucial to examine these facts from the adversary's perspective. "Being able to put yourself into the mind of the adversary may be the counter-deception analyst's main, perhaps only, effective weapon"²⁶.

However, one should be aware that lack of history with regards to employing deception doesn't necessarily mean the adversary won't make use of such methods. Usually, honest people are the ones with the greatest chances of success.

Know the situation

Knowing the situation requires continuous monitoring of the conflict development in order to identify new observables that might contradict the information previously collected, which should lead to some incongruities when analysing the bigger operational picture. Environmental assessment is a must when trying to identify enemy deceptive activities, as any minor change in the operating environment might have an impact on the probability of deception operations employment by the opponent. Changes within his command structures or the materialization of some favourable conditions for employing deception are some of the most common developments that have a huge influence regarding deceit.

Conclusions

Military counter-deception is the art of detecting deception and providing the most suitable response in order to obtain an advantageous outcome of this situation. It is a complex field that requires a variety of skills and backgrounds, including a strong understanding of military doctrine and tactics, a firm grasp of the art of warfare, as well as huge experience in this domain. It is imperative that counter-deception methods are an integral part of military operations, with the goal of providing commanders with the best information possible to help them make the best decisions possible in a given situation. Armed with a deep understanding of enemy intentions, military commanders can take action to ensure the security of their forces and, consequently, the success of their operations.

The purpose of counter-deception is to identify a deceptive strategy and adjust the analysis accordingly to avoid being manipulated by the deceptive actions, but also to develop strategies that exploit the situation by double-tricking the adversary, thus converting him from deceiver to the one that is deceived. However, this is not as simple as might sound. It requires very well trained personnel in collecting and analysing the information, but also organisations that understand their limitations and vulnerabilities, as well as commanders that know their biases and prejudices and willingness to deal with them. Applying the counter-deception principles highlighted in this paper might amplify the chances to detect the enemy deception operations, thus enhancing the chances for mission accomplishment. Furthermore, deceit detection might reveal some opportunities that can support effectiveness in reaching the set objectives for the military operations.

In conclusion, considering the constant employment of deception throughout the history, but also the features of contemporary operating environment which enhance the effects of military deception operations, I consider that appropriate counter-deceptive measures must be implemented within all concepts of operations, regardless of the mission type the military should accomplish.

REFERENCES

1. Army Field Manual – *Warfighting Tactics. Part 1: The Fundamentals*. UK Ministry of Defence, 2018, p. 3A-4.
2. Ibidem, p. 3A-2.
3. FM 3-13.4, *Army Support to Military Deception*. US Department of the Army, 2019, p. A-1.
4. Michael Bennett, Edward Waltz. *Counterdeception Principles and Applications for National Security*. London: Artech House, 2007, p. x (Introduction).
5. <https://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-82/Article/793229/twenty-first-century-information-warfare-and-the-third-offset-strategy/> accessed on 24.02.2022.
6. FM 3-13.4, *Army Support to Military Deception*. US Department of the Army, 2019, p. 1-1.
7. Donald C. Daniel (collective). *Multidisciplinary Perspectives On Military Deception*. US Department of the Navy, United States Naval Postgraduate School, Monterey, California, 1980, p. 8.
8. FM 3-13.4, *Army Support to Military Deception*. US Department of the Army, 2019, p. 1-7.
9. Ibidem.
10. James D. Monroe. *Deception: Theory and Practice*. US Naval Postgraduate School, Monterey, California, 2012, p.44.
11. Michael Bennett, Edward Waltz. *Counterdeception Principles and Applications for National Security*. London: Artech House, 2007, p. 7.
12. Army Field Manual – *Warfighting Tactics Part 1: The Fundamentals*. UK Ministry of Defence, 2018, p. 3A-5.
13. AJP 3.10.2, *Allied Joint Doctrine for operations security and deception, edition A, version 2*, NATO Standardization Office, 2020, p. 1.
14. Ibidem, p. 9.
15. Michael Bennett, Edward Waltz. *Counterdeception Principles and Applications for National Security*. London: Artech House, 2007, p. 34

16. FM 3-13.4, *Army Support to Military Deception*. US Department of the Army, 2019, p. A-1.
17. AJP 3.10.2, *Allied Joint Doctrine for operations security and deception, edition A, version 2*, NATO Standardization Office, 2020, p. 5.
18. Whaley, B. *Stratagem: Deception and Surprise in War*. Center for International Studies. Massachusetts Institute of Technology, 1969, p. 76.
19. Michael Bennett, Edward Waltz. *Counterdeception Principles and Applications for National Security*. London: Artech House, 2007, p. X (Introduction).
20. AJP 3.10.2, *Allied Joint Doctrine for operations security and deception, edition A, version 2*. NATO Standardization Office, 2020, p. 5.
21. Ibidem, p. 9.
22. Michael Bennett, Edward Waltz. *Counterdeception Principles and Applications for National Security*. London: Artech House, 2007, p. xi (Introduction).
23. Robert M. Clark, William L. Mitchell. *Deception Counterdeception and Counterintelligence*. London: SAGE Publications, 2019, p.282.
24. Sun Tzu. *The Art of War*. India, New Delhi: Rupa Publications, 2016, p. 14.
25. Michael Bennett, Edward Waltz. *Counterdeception Principles and Applications for National Security*. London Artech House, 2007, p. xi (Introduction).
26. Ibidem, p. 178.

MILITARY DECEPTION IN CONTEMPORARY OPERATING ENVIRONMENT

Major Superior Instructor George-Ion Toroi, PhD Candidate

“Carol I” National Defence University

Bucharest, Romania

E-mail: george_toroi@yahoo.com

Abstract: The application of military deception operations in combat is a long-standing tradition. The fog of war is a time-honoured tactic, and it is one that is still used by modern militaries. Uncertainty is a prerequisite for deception success. Military deception is the practice of deceiving enemy forces about the location, size, dispositions, or intentions of friendly forces with the intent of misleading the enemy as to the most effective course of action. The intended objective is to create operational opportunities for the deceiver that will transcend in advantages in support of efficient mission accomplishment.

However, as technology has become a larger part of warfare, so too has the complexity of modern battlefields increased. The speed of modern communication, the range and accuracy of modern weaponry, and the power of modern computing have combined to create modern battlefields that are faster, more volatile, and more interconnected than ever before. As a result, military deception has become a more critical part of modern warfare than ever before with enhanced effects over the adversary. Today, deception can take many forms, from subtle disinformation to overt propaganda, with the primary goal of keeping the enemy off balance and out of the truth.

Comprehensive understanding of how deception works in today's operating environment can bring two related benefits for every modern military: it can offer effective options to be employed in achieving the desired end-state of the battle, but can also support developing protective measures against enemy deceptive measures.

Keywords: *deception; influence; target; perception; decision; uncertainty*

*“In wartime, truth is so precious that it should
always be attended by a bodyguard of lies”.*

Winston Churchill

Introduction

“All warfare is based on deception” wrote Sun Tzu more than 2000 years ago. This aphorism has proved its validity throughout the years. The abundance of examples in all military history sustains this idea. One might even argue that deception is a constant feature of warfare, being part of its nature, amongst others such as chaos, human endeavour, uncertainty, etc.

But with the accelerated rate of technological evolution that we witness today, there are many that say deception is overrated. The expansion of the intelligence collection capabilities and their performances makes it almost impossible to hide military activities so one might think it is harder to create surprise, thus deceive.

This article examines previous statements and tries to identify solutions for how deception might still work in this complex environment. But, no matter the level of complexity with respect to technological evolution, the advantages gained by employing deception make it still an attractive method to achieve military objectives even though, apparently, it became harder to do it these days.

The primary research question that this scientific article wants to analyse is:

Is deception still an option in today's conflicts, considering the contemporary operating environment features?

To this end, I approach the subject in several sections:

First, I believe it's a must to have a deeper comprehension on the fundamentals of deception. Without theory there is no proper practice. In this respect, I will do an analysis of various definitions of deception and how different actors address it and then I will focus the attention on identifying the “why” of deception and what advantages one might gain as a consequence of employing such actions. Furthermore, I will provide a description of the types, methods and means of deception. The outcome of the examination should be a consolidated understanding on different concepts specific to military deception.

Then, having a solid foundation of the theory of deception, I will analyse how deception actually works. To this end, I will explore the process of deception and how it corresponds with the overall concept of operations. I will highlight the essential aspects that need to be addressed when planning, conducting and assessing deception operations. The outcome of this analysis will consist of a grasp of how deception process should look like in order to maximize its chances of success.

Finally, I will turn my attention towards the characteristics of today's operating environment and how these influence the usage of deception. The outcome of this analysis should reveal certain patterns on if and how deception works within this environment.

Theory of deception

Deception operations can be an important effect multiplier on the battlefield. However, the high risks associated with these operations require a thorough understanding and a solid theoretical foundation of the concept. When considering deception in support of the mission accomplishment, the necessity of clearly understanding these operations comes from several reasons:

- Deception operations are very complex and require tremendous effort to implement and monitor. In order to be effective, one needs to comprehend the principles, the specific methods, the means and techniques that drive these operations.
- Deception operations are intelligence driven operations. They rely on the information provided by the intelligence staff with respect to the adversary's preconceptions and biases, decision making process and vulnerabilities or channels to convey the deceptive message to the target, to name but a few. Hence, there are some risks associated to deception that come from the intelligence interpretation regarding the adversary.
- Furthermore, the benefits that might be achieved from employing deception make it a very tempting option on the battlefield.
- Understanding deception might mitigate negative consequences that can result from its failure.
- The diversity of enemy reactions to the deceptive message requires a high level of flexibility for the deception operations. Failure to comply with this might result in some risks associated with mission accomplishment.
- Last, but not least, employing deception implies weighting costs over benefits. Without a solid knowledge about deception operations, one might make use of it in inappropriate conditions that can get to mission failure.

"Manoeuvring the mind" of the opponent into doing or not doing some specific actions that are detrimental to his interests can be considered to be the essence of deception operations. The consequences of those actions create operational effects that are perceived as advantages and opportunities for the deceiver. The entrancing thing about deception is that it makes the adversary act without him even know or suspect of the unfavourable consequences his decisions create for his forces on the battlefield. To be able to do this requires a comprehensive understanding of the theory of deception and how and why it works. First of all I will do an analysis on the **definitions** of this concept in order to identify common themes that can be interpreted as the backbone of military deception operations.

"Military deception is actions executed to deliberately mislead adversary military, paramilitary, or violent extremist organization decision makers, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission" ¹.

"Deception is defined as: deliberate measures to mislead targeted decision-makers into behaving in a manner advantageous to the commander's objectives" ².

There are some common themes with respect to both of these definitions:

- the **aim** of deception is to mislead the adversary thus making him misinterpret the operational environment and situation;
- deception operations have a clearly define **target**: the adversary's decision making body;
- deception must lead to certain changes in the operational environment that can portray some **advantages** for the deceiver;
- successful deception requires a certain **behaviour** of the target that can lead to the desired operational changes;

Benefits of deception

Having a solid understanding of what deception is, I will next do an analysis of why should it be employed in warfare. Throughout the years deception has been an integral part of countless operations. History is full of

examples when commanders have used deception and seen it as a need in order to achieve victory. Nowadays, many of the military doctrines still see it as a must when it comes to planning and conducting military operations.

„Deception must be an integral part of all operations“³.

“OPSEC and deception planning are required against all adversaries“⁴.

But what is it about deception that makes it such an attractive tool to use in conflicts? To fully grasp the meaning of this concept one needs to further comprehend the **benefits** that deception brings to the table for the deceiver.

There are four big areas that deception can support as part of the concept of operations⁵: surprise, security, freedom of action and economy of effort.

The primary benefit of deception is that it can be used to create *surprise* on the battlefield, thus achieving an operational advantage over the adversary. Surprise is a principle of war for most of the international actors. It is proven that it can be a great effect multiplier on the battlefield. The main tool one can employ in order to create surprise is deception. The employment of such operations can support masking real intentions and also essential elements of the troops' disposal and objectives, consequently creating ambiguity, confusion and degraded situational awareness for the adversary.

Deception can maximize the surprise effect over the opponent by using hidden forces in moments and locations that do not correspond to the opponent's situational awareness, thus creating a shock effect on him that can be exploited by the deceiver. Creating a false perception to the opponent regarding the fighting power of the deceiver might also enhance the surprise effect at a certain moment.

Security refers to preserving combat effectiveness and it is essential for achieving the military objectives. To this end, deception can play an important role. There are several ways one can employ in this regard:

- distract the enemy's attention from the main effort;
- use decoys in order to make the enemy consume its resources;
- mask manoeuvring forces;
- mislead the enemy regarding the location of command and control systems, force disposition and composition, critical vulnerabilities and capabilities;
- portray several plausible options to the enemy in order to confuse him and make him delay its decisions, thus gaining time for preparations or other activities that might enhance security;

Deception might be an option to create *freedom of action* for the deceiver. Channelling the enemy's attention towards insignificant operational areas will enhance freedom of action where it is actually needed. On the battlefield, it is imperative that you can manoeuvre unimpeded as this might give you opportunity to fulfil some of your objectives in shorter times and with minimum casualties. It becomes obvious, then, the benefit that deception can bring for the force.

Deception operations might support *economy of effort* as well. If employed correctly, deception can save time and resources to accomplish objectives. Depending on the situation, it can also save lives in the process of creating the conditions desired.

Furthermore, deception can support the mission accomplishment by creating effects on the adversary. To this end, it may be employed to:

- degrade the adversary's fighting power;
- make him lose the initiative;
- make him waste resources on unimportant targets;
- expose his real disposition and intentions;
- make him become vulnerable;
- divert his ISR and fires effort;
- overwhelm its ISR systems with information thus make him lose tempo or even initiative.

It is obvious that the multitude of benefits one can obtain by employing deception make it an essential element that commanders need to take into account when planning military operations. Nevertheless, when incorporating such actions within the overall concept of operations, the staff should do an accurate **analysis on the risks** these operations pose to the force and its mission **over the benefits** that might be gained. So, no matter how tempting the latter might look, commanders should always identify proper conditions to employ deception⁶ so that the inherent risks are minimized.

The ultimate risk deception operations pose to the force is that, if not successful, the adversary might detect it in time to counter its intended effects, even use it to do a counter-deception operation. In this case, the deceiver might become, in the end, the deceived.

That's why deception must always be regarded as a high-risk activity. There are some circumstances that pose even a greater risk to the overall mission:

- if there are no adequate conditions to make use of deception (for example, the adversary has a good history when it comes to identifying deceptions);
- when information regarding the enemy is partial and inconclusive and it's almost impossible to precisely predict targets reactions to the deceiver's false information;
- the lack of information with regards to the adversary's C2, decision-making and intelligence process will also enhance the risks associated to deception operations.

Methods, types and means of deception

Uncertainty is a crucial component of deception and a huge enabler for these types of operations. It affects both the deceiver and its target.

On one hand, although the initiator plans what to achieve and how to best use deception in this regard, there is still a great level of variability when it comes to anticipate the outcome of its actions, mainly due to the numerous factors that might interfere with the deceptive information that was sent. To minimize the risk of deception being discovered and thus the deceiver being subjective to counter-deception actions, it is imperative that certain measures be taken by the initiator in order to manage that risk.

On the other hand, the target may very well be exposed to deception in an uncertain and chaotic situation. A decreased level of situational awareness of the adversary makes it the perfect "playground" for deception operations.

Although uncertainty plays an important role for both parties involved in deception, I consider that the most affected is the target as it is the one not knowing what is happening and thus being subjective to become deceived.

There are two critical ways to employ deception in an uncertain situation and both of them are related with the target's level of understanding with respect to the operational situation. This understanding is the foundation for the situational awareness. But the problem with understanding is that it relies on how one perceives a circumstance, which makes situational awareness dependent on the perception one might have with regards to that situation. One might even inquire that the situational awareness is actually an illusion or an interpretation in a specific moment in time regarding how things are unfolding.

Deception involves misleading the adversary by manipulating its perception of the operating environment. For this reason, deception takes advantage of the state of uncertainty specific to armed conflict and may influence the status of the adversary's situational awareness.

Nevertheless, individuals participating in deception operations, particularly potential targets make judgments and take decisions in uncertain circumstances, when they don't have all the information available for that situation. In these conditions, uncertainty causes a target to be unsure of what his potential opponent will do, creating the perfect environment for deception operations. Therefore, it becomes obvious that war-specific uncertainty can create the preconditions for the success of deception operations. As for the parties involved in the conflict, uncertainty means not having all or the correct details regarding the operational situation and this is what deception can exploit.

There are two options that can be employed when it comes to uncertainty in order to be able to deceive your adversary. On one hand, when deemed appropriate, deception can be used to increase the opponent's confusion by portraying several plausible options for him. The increased uncertainty might generate a longer time for him to react, thus creating opportunities for the deceiver to gain initiative. On the other hand, deception might be employed to decrease the adversary's confusion in connection with a certain situation. One can make use of this option when the enemy actions are, in fact, detrimental to his interests. In this situation, the deception goal is to reduce the ambiguity and encourage the adversary to continue on this wrong path.

Donald C. Daniel and Katherine L. Herbig, along with a group of other researchers, were the first to propose these two types of deception concepts⁷. They referred to it as:

- **A-Type** – ambiguity producing deceptions;
- **M-Type** – misleading deceptions.

The fact that this taxonomy is used by the US in its most recent tactical and operational (joint) level deception doctrines makes it still valid and accurate in today's operating environment^{8,9}.

In order to increase or decrease the adversary's level of ambiguity regarding a certain context, the deceiver needs to be able to present a particular picture to the target. For this, deception requires sending specific information

to the target through selected channels in order for him to reconstruct the image desired by the deceiver. Deception is not only portraying false information to the opponent. It is about sending a message. This can be done by both revealing and concealing information. This message should be a mixture of false and true information in order for the deception to succeed. There is no formula to the percentage of true and false information in order to be able to deceive. It is rather a question of who the target is and what the overall context is. Nevertheless, there is a wide acceptance, in the deception literature, of a principle that states: the less false the message is, the higher the chances for success.

The objective of deception is to make the adversary react in a way that supports the deceiver. Its reaction comes as a consequence of the perception he has made for a specific situation. This perception is the image that the deceiver wants to create to his opponent in order for him to behave in the manner intended.

As stated earlier, in order to create the desired perception of the target, deception sends messages. These actions can be accomplished by both revealing and concealing some information. For this reason, deception applies the two methods: simulation and dissimulation¹⁰. For each of these two methods, there are several types of deception.

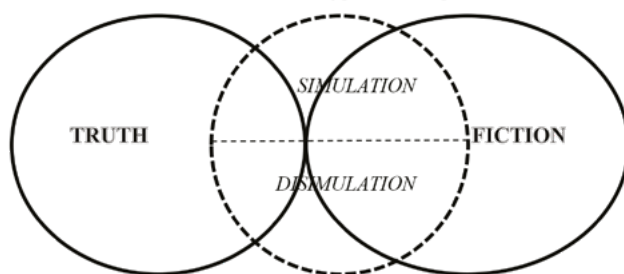


Fig. 1. Deception methods¹¹

Table 1

Types of deception¹²

DECEPTION	SIMULATION (active measures)	Display
		Feint
		Demonstration
		Disinformation
	DISSIMULATION (cover)	Camouflage
		Denial

Depending on the situation, deception may include actions specific to one or more of the types listed above. No matter which one is employed. It requires specific means to put it into practice: physical, technical and administrative means¹³.

Deception process

There are some military theorists that consider deception the supreme art of war, supporting Sun Tzu's theory that „the supreme art of war is to subdue your enemy without fight”. To be able to make your opponent take willingly actions that are not in its interest, but rather in yours, requires higher level of understanding and intelligence. Effective deception equals superiority in the cognitive domain. It is based on intelligence rather than strength, and it is heavily reliant on creativity and imagination.

“Deception is a key tenet of the manoeuvrist approach¹⁴. It is perceived as an indirect approach towards exploiting the adversary's vulnerabilities, especially the cognitive ones.

T.E. Lawrence stated that “with 2000 years of examples behind us, we have no excuse, when fighting, for not fighting well¹⁵. But that is not necessarily true when it comes to deception, because history proved that, no matter the technological development one actor had, there was another that innovated solutions to avoid those limitations coming up with ideas to deceive its adversary. Deception requires imagination. One can argue that the limits of deception are dependent on the limits of the deceiver's imagination.

But how does it actually work?

First of all, as stated before, deception is not about making the adversary believe something, but rather making him act (behave) in a certain manner. His behaviour is a consequence of how he perceives the operational situation. Creating the desired perception for the target is of utmost importance for the deception success.

Deception is a very complex process, but at a minimum it requires the following steps: the aim and the goals of deception, the desired perception of the target, the observables, the channels, filters, the target's decision and his reaction.

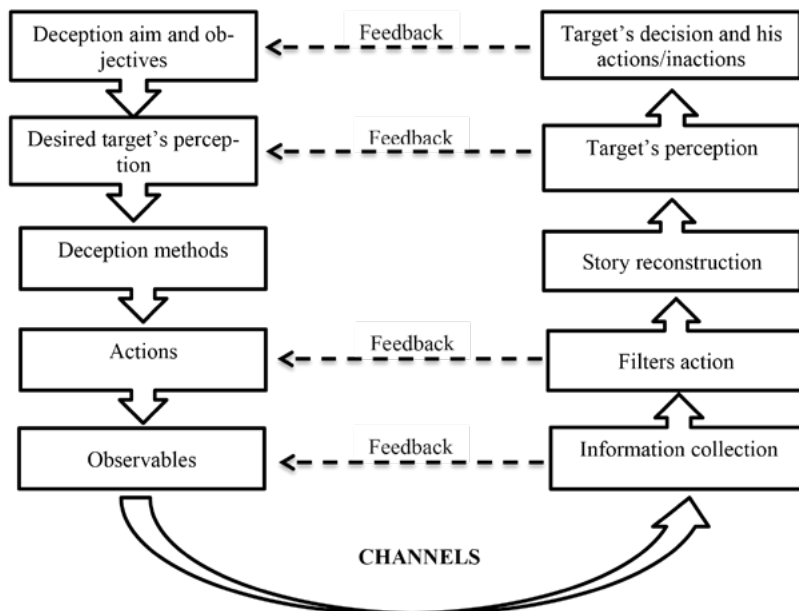


Fig. 2. Deception process

The above figure represents a simplified process of deception that should be followed in order to create the desired operational effects. The entire process should start only if the commander decides that deception can be an effective tool in support of its mission. If so, he first states the aim of the deception and the goals he intends to obtain by employing stratagems. Their role is to focus all the deceptive efforts towards it and maintain a clear understanding within the HQs with respect to why deception is used for.

After establishing the overall purpose of the deception, the staff needs to define the desired perception of the target. This is a crucial step as it constitutes the basis upon which the target will react in the manner intended by the deceiver.

The subjective observation of an objective reality is referred to as perception. As a basic component of the cognitive dimension, perception serves as a filter through which the target views the operating environment. However, this filter is influenced by societal, religious or cultural factors. Influencing the target's vision of the environment will cause him to interpret threats, challenges or even his own weaknesses in a new way, thus influencing his preparations and reactions to the situation.

In order to enhance the chances to create the desired perception, the staff should do a thorough analysis on the target. This analysis entails looking into at least the following information about the target:

- examination of deception channels and how the target evaluates them;
- adversary's information cycle and weaknesses that can be exploited through deception;
- its procedures for decision making;
- the target's predispositions, biases, and prejudices;
- the target's leadership style, experience, demeanour and personality;
- its grasp of the operating environment, particularly his knowledge of our forces (capabilities, disposition, and intentions).

After the perception required is defined, the deceiver should do an analysis on what information the force must send and how in order for the target to form that perception. This process involves selecting the most suitable actions and the appropriate channels, but also employing the right methods and means for it. After the actions were portrayed, the enemy's collection systems gather the data, analyse and interpret it and present the overall picture to the target for his decision. Ideally, the picture presented to the target should correspond with the perception intended by the deceiver for the target to form.

In other words, deception requires decomposing the image that the target should perceive into small pieces that the adversary collects and reconstructs. From this point of view, deception is similar to a puzzle. The deceiver should make sure that the opponent gets all the small pieces and has the ability to remake the puzzle in the form intended by the deceiver.

However, the deception process does not end with the target's behaviour change. The end game of deception is for the adversary to make a certain decision and react in a predicted manner so that an operational advantage arises for the deceiver.

As it can be seen, the process is very complex and depends on many variables that might interfere with the intended deception. This requires a high flexibility with respect to the deception plan in order for the deceiver to adapt to changing situations that might arise and still be able to deceive the adversary.

Deception operations in contemporary operating environment

There were times, not long ago, when deception was considered obsolete. The 2014 annexation of Crimea took everybody by surprise and made western countries realize that deception still represents an efficient way to gain operational advantages. In this respect, many NATO countries and NATO itself started a revitalisation of this "lost art", the development of recent doctrines dedicate to military deception operations being a good indicator in this regard. Nevertheless, there are some military specialists that argue the efficiency of deception operations considering the fast evolution of our society. The assumption is that, nowadays, it became almost impossible to hide military actions or forces considering the technological evolution of the intelligence collection systems.

So, is deception still a viable option considering the operating environment of today's conflicts?

First of all, in order to find answers to the above question, I will highlight the main features of the contemporary operating environment and then do an interdisciplinary analysis considering the theoretical concepts presented before.

The operating environment is „a composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander“¹⁶. As a consequence, the operating environment can be considered a framework that involves all those interrelated variables that can have a direct and immediate influence on military actions. Understanding it requires an in-depth analysis on various factor that can affect military operations such as the actors involved and their strategies and interests, the physical and non-physical domains, but also resources, means and capabilities employed. Apprehension of the operating environment's features is a must for every military force as it represents the basis for modelling and equipping the force in accordance with the necessity, but also for training certain types of operations that might be required in case of a conflict.

Most of the international actors do regular analysis of the operating environment in order to adapt their systems^{17, 18, 19}. All of these studies identify several key aspects of today's operating environment:

- the accelerated urbanization of the society, which will determine the urban environment to become the main battleground for future conflicts;
- the growing importance of the information environment, which will stress the need to have timely, accurate and precise information;
- the society's dependence on information systems which led to a growing significance of the cyber domain in armed conflicts;
- the space domain has become a provider of capabilities essential in contemporary warfare;
- the rapid evolution of technological developments;
- the hybridity and multidimensionality of the confrontation.

“The *urban environment* presents the most complex physical terrain that exists”²⁰. It is a common understanding that urban warfare is a very complex one. “The U.S. Army faces numerous challenges in our current and near-term future operational environments. None will be more difficult than conducting operations in the world's urban areas”²¹. There are several aspects specific to the urban environment that influences deception operations:

- Population can be used both as target and as channel of deception. Deceiving the local population might create some operational situation that the adversary needs to deal with. In order to solve it, the opponent might need to redistribute his resources, thus creating the opportunity for the deceiver to obtain freedom of action in some specific areas. In the same time deceiving the population might be used in order to gain some time for other actions.

- The multitude of channels to convey information in support of deception (media, social-media, internet, locals etc.).

- Surprise is a combat multiplier and can substantially reduce the cost of urban warfare²². Considering that deception is the primary tool to create surprise on the battlefield, one can inquire that deception is a viable option when it comes to urban warfare.

An essential component of the operating environment is the *information domain*. Its essence is the information. Nowadays it's very facile to send a lot of information wherever you want, in a matter of seconds. The main features of today's information environment such as high volume and transmission speed of information, increased accessibility to the information or the protection of the sender's anonymity represents perfect tools for deception operations. Considering these features, filtering objective information and maintaining an unaltered reality has become almost impossible. Disinformation is the most suited type of deception that one can employ with regards to how the contemporary information environment looks like.

The growing dependence of the military force on the cyber systems has brought many advantages, but it also represents a huge liability. "All security systems can be compromised"²³. Cyber deception is a reality. Using the *cyber domain* as a channel to portray deceptive information to the adversary has grown in importance considering the force dependence on this type of capabilities, as mentioned before. A relevant example of using cyberspace for deception operations is the "honeypot". This is a cyber-decoy that is used to make the adversary perform cyber actions against it. As a consequence, the deceiver is being able to depict some of the opponent's procedures and even create vulnerabilities within its systems. The purpose of misleading actions in cyberspace can be dual. Either placing false information in the opponent's operating systems to confuse him and delay his actions, or camouflaging and protecting sensitive information about his own strength, information that can be used to surprise the opponent at the decisive moment of the fight.

Space has become, nowadays, a huge enabler for military operations. One can even suggest it is an integral element of all military activities, both in peacetime and during conflicts. Military C2, ISR, communication or navigation systems are all dependent on space capabilities. It is almost impossible to imagine a fight without being able to use these systems. However, "satellites can be jammed, hacked or weaponized. Anti-satellite weapons could cripple communications and other services our societies rely on, such as air travel, weather forecast or banking"²⁴. Space can support deception operations as well. Denial may be an example of deception type that can be employed in order to degrade the effectiveness of the adversary's satellites capabilities, thus affecting its ISR systems and facilitating freedom of movement for the deceiver's forces in a specific moment of the battle in order to surprise the opponent. Furthermore, the satellites may be used to convey deceptive information becoming one of the channels used for deception.

„The role—and therefore the importance—of deception is significantly expanding as *technology* introduces new avenues to deceive and globalization expands the opportunities for deception and potential adverse impacts"²⁵. Today's technology has primarily facilitated the expansion of a variety of deception means and methods, but at the same time has amplified the effects and consequences of such actions, which can take place on a much larger scale than in the past. Therefore, the importance of understanding misleading in the context of technological developments, which offer more and more innovative possibilities for implementing such actions, is essential in order to be able to detect and counter the deception.

There are some specialists that consider deception a non-viable nowadays, considering the technological developments of the information collection sensors. They believe that it is almost impossible to hide military activities due to the expansion of sensors and their performances. But deception is not about hiding things; it's about hiding real intentions and portraying false ones. So it's not about being able to see the activities, but rather to be capable to analyse and interpret it correctly.

An easy way to influence perceptions today is social-media. The explosive growth of these applications has revolutionized the way we interact with each other. However, the emergence and use of this online environment has also created new opportunities for deception. Due to the magnitude of the effects resulting social media has become one of the most practised deception channels.

There are many other examples that can be used either as channels or as methods and means for deception related to the emergent technologies. Some examples might be the Artificial Intelligence, Big Data, virtual reality, robotics, drones and many more.

Considering the analysis presented here, I consider that the contemporary environment, characterised by the acronym VUCA (volatile, uncertain, complex and ambiguous), is an enabler for deception operations across all domains. However, "deception plan must be coherent across all domains, the EMS, and the information environment to effectively counter the enemy's multi-domain reconnaissance"²⁶.

Conclusions

In a world characterized by unrestricted access to information, ambiguity, uncertainty, technological developments, the possibilities, intricacies and importance of deception operations has exponentially grown. They have become a constant in today's military operations. Although they are very complex, these actions can bring about lots of benefits for every commander on the battlefield.

As a conclusion, the answer to the primary research question of this scientific paper is affirmative. Indeed, deception is a viable option in today's conflicts, considering the contemporary operating environment features. However, one should understand the theoretical aspects with respect to military deception and how it works in order to maximize its efficiency and minimize the inherent risks to the mission.

REFERENCES

1. FM 3-13.4, *Army Support to Military Deception*. US Department of the Army, 2019, p. 1-1.
2. AJP 3.10.2, *Allied Joint Doctrine for operations security and deception, edition A, version 2*. NATO Standardization Office, 2020, p. 4.
3. *Army Field Manual – Warfighting Tactics Part: The Fundamentals*. UK Ministry of Defence, 2018, p. 3A-5.
4. AJP 3.10.2, *Allied Joint Doctrine for operations security and deception, edition A, version 2*. NATO Standardization Office, 2020, p. 1.
5. *Army Field Manual – Warfighting Tactics Part 1: The Fundamentals*. UK Ministry of Defence, 2018, p. 3A-2.
6. AJP 3.10.2, *Allied Joint Doctrine for operations security and deception, edition A, version 2*. NATO Standardization Office, 2020, p. 25.
7. Donald C. Daniel (collective). *Multidisciplinary Perspectives On Military Deception*. US Department of the Navy, United States Naval Postgraduate School, Monterey, California, 1980, p. 8.
8. FM 3-13.4, *Army Support to Military Deception*. US Department of the Army, 2019, p. 1-6.
9. JP 3-13.4, *Military Deception*. US Joint Chiefs of Staff, 2017, p. 1-8.
10. *Army Field Manual – Warfighting Tactics Part 1: The Fundamentals*. UK Ministry of Defence, 2018, p. 3A-6.
11. James D. Monroe. *Deception: Theory and Practice*. US Naval Postgraduate School, Monterey, California, 2012, p.43.
12. Ibidem, p. 44.
13. FM 3-13.4, *Army Support to Military Deception*. US Department of the Army, 2019, p. 1-11.
14. *Army Field Manual – Warfighting Tactics Part: The Fundamentals*. UK Ministry of Defence, 2018, p. 3A-2.
15. *Army Doctrine Publication – Operations*. UK Ministry of Defence, 2010, p.1-2.
16. AAP-06, *NATO Glossary of terms and definitions (English and French)*, ed. 2019. NATO Standardization Office (NSO), 2019, p. 93.
17. *Strategic Foresight Analysis*. NATO Allied Command Transformation, Norfolk, 2017.
18. *Global Strategic Trends – The future starts today, 6th edition*. UK Ministry of Defence, 2018.
19. *Global Strategic Trends 2040 – A more contested world*. US National Intelligence Council, 2021.
20. ATP-99, *Urban Tactics, Edition A, Version 1*. NATO Standardization Office, 2017, p.2-1.
21. TRADOC Pamphlet 525-92-1, *The changing character of warfare: The urban operational environment*. U.S. Army Training and Doctrine Command, 2020, Forward.
22. MCRP 12-10B.1 – *Military Operations on Urbanized Terrain (MOUT)*. US Marine Corps, 2018, p.1-13.
23. <https://www.fifthdomain.com/dod/army/2018/08/29/the-army-is-testing-deceptive-cyber-technology-despite-past-struggles/> accessed on 21.02.2022.
24. https://www.nato.int/cps/en/natohq/opinions_171022.htm accessed on 22.02.2022.
25. Michael Bennett, Edward Waltz. *Counterdeception Principles and Applications for National Security*. London: Artech House, 2007, p. 2.
26. TRADOC Pamphlet 525-3-1, *The US Army in multi-domain operations 2028*. U.S. Army Training and Doctrine Command, 2018, p. 37.

SECURITY OF REMOTE ELECTRONIC IDENTIFICATION: THE CASE OF POLAND

Remigiusz Lewandowski, PhD
War Studies University
Poland

Abstract: The paper is based on an analysis of technological solutions used in Poland in the field of remote identification. These solutions were analyzed taking into account various criteria, including adequacy to individual stages of the identification process and various types of functionalities and features such as a range of stored data, a range of applications, requirements to service providers, channels of application as well as readiness to eIDAS2.

The paper leads to the conclusion that Poland has very developed and widely used solutions in the field of remote identification. Most of them are universal, i.e. they can be applied to all stages of the identification process. Moreover, it is also important that the discussed tools are applicable both in the public and commercial channel. Among all the analyzed solutions, the following provide the greatest social utility in terms of security and public availability: banking identity and video verification based on the electronic layer of the ID card.

Keywords: *remote identification; identity; security; eIDAS*

Preface

In the modern world, a significant part of our social and economic activities takes place in cyberspace. The lockdown caused by the COVID-19 pandemic significantly strengthened and dynamized this phenomenon. Legal transactions and confidential conversations take place in cyberspace, and many of them have very serious financial and legal consequences. A good example of the migration of legal activities to cyberspace is the particularly popular online banking, where all banking activities can be performed on-line by the customer. Another spectacular example is e-voting, which in some countries (e.g. Estonia) is an equal form of voting in general elections next.

There is no doubt that the indicated trend will develop, and in cyberspace both natural and legal persons will carry out more and more activities. However, with the development of technology, the question of the security arises. To what extent are these solutions protected against manipulation? In this area, the biggest challenge is gaining certainty as to the identity of persons who perform selected activities in cyberspace. This is especially important in the context of the legal and financial consequences of activities carried out in cyberspace. For example, when opening a bank account, a bank should be absolutely sure about the identity of its client. Certainty must also be maintained in the process of its handling, i.e. a bank executing an on-line transfer order should also be sure that the credit transfer was ordered by an authorized person. Is such absolute certainty guaranteed by the currently used instruments in the field of electronic identification? The answer to this question, based on the analysis of the legal and factual situation in Poland, is provided in this article. This issue is not trivial as identity security, and in particular identity verification, is a challenge even in on-site conditions¹.

Due to the social and economic benefits resulting from the transfer of activity to the sphere of cyberspace, electronic identification is subject to quite dynamic development. This development affects both the private and public sectors. It should be admitted, however, that the banking sector played an extremely important role in popularizing electronic identification practically all over the world. Seeing economic benefits in online banking, banks developed an electronic identification system that ensures the security of remote transactions. At the same time, this development and the growing importance of the Know Your Customer (KYC) principle was stimulated by legal requirements related to anti-money laundering (AML). It is questionable to what extent this system responds to contemporary security challenges and to what extent it uses existing technologies.

Literature review

The issue of modern identification systems in cyberspace (i.e. those used remotely) in the context of their security and reliability is not very widely discussed in the literature. This state of affairs results from the

¹ In typical conditions in branch banking, employees usually do not have sufficient competence to verify identity based on the image of the face (to compare the face on the ID document with the customer's face). Hence, frauds involving the use of stolen identity documents remain a current problem.

characteristics of the identity proofing process. This is because this process is based on the registration stage, which for many years has been predominantly using the traditional approach of physical contact between the person undergoing identification and the verifying person. Moreover, the last stage of the identification process, i.e. authentication, is also based, in a significant part of the cases, on classic means of identification, such as login and passwords. Only recently has the expansion of alternative methods been visible on a larger scale at all stages of identity proofing.

A significant part of research devoted to identity security in cyberspace touches upon issues related to technology. ETSI technical report [2021] covering, *inter alia*, the review of technologies and legal requirements in selected European countries in the field of identity proofing for purposes related to trust services indicates that authentication in a remote mode can take place using two basic methods: face biometrics (with the presence of a person verifying compliance on-line or automatically) and the transfer of identity attributes from other trusted sources (such as an electronic identification system or a qualified electronic signature). The authors of the report conclude that the remote process of face-to-face identification is problematic, because equivalence to physical presence is not well-defined as no requirements are posed neither for the quality of (physical) identity documents nor for the competence or procedures to be carried out by the person performing the check.

Goode [2019] points out that biometric systems play a key role here in enabling digital identity verification services, but a significant challenge of this technology is liveness and spoof detection (commonly called presentation attack detection, PAD).

International organizations, such as the World Bank, actively participate in the promotion of solutions based on digital identity and support countries in the process of their implementation [World Bank, 2018]. The UN promotes the use of biometric registration of refugees [UNHCR, 2018]. Currently, selected countries have implemented or plan to implement digital identity solutions based on biometrics and blockchain. Among the EU countries, the following states have notified their electronic identification schemes to the European Commission: Czech Republic, Estonia, Italy, Netherlands, Denmark, Spain, Latvia, Germany, Slovakia, Croatia, Belgium, Luxembourg, Lithuania, Portugal². Nevertheless, the process of building digital identity systems cannot be considered complete. This process is ongoing and includes both those countries that have notified their schemes and those that have not yet done so (e.g. Poland). Moreover, the methods and tools used in identity proofing are constantly evolving. The legal framework in this regard, in particular Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (hereinafter: eIDAS), leave the Member States considerable freedom in the choice of identification means and authentication mechanisms. That is why research in this area relating to methods in use in individual countries is so important in order to be able to find optimal solutions.

In addition to technological issues, the subject of research is also the identity management model itself. On the basis of practical problems of the user with a multitude of logins and passwords as well as threats from hackers, postulates regarding self-sovereign digital identity are increasingly being put forward. Allen [2016] defined self-sovereign identity as „the next step beyond user-centric identity [where] the user must be central to the administration of identity”. This approach is significantly different from traditional identity management in which – as Wagner et al. [2018] state “a user’s identity is defined from the perspective of the provider for a specific purpose and is therefore only valid within the domain of that specific provider within that purview”. As indicated by Toth and Anderson-Priddy [2019], self-sovereign digital identity can give citizens explicit sovereignty over their digital identities, enhance privacy for citizens and reduce reliance on passwords. This new paradigm of digital identity management is based on the assumption that it is the citizen himself who manages his attributes, selecting in a given identification process those that are adequate to this process. Certification and the attributes are carried out by a trusted party. The implementation of self-sovereign digital identity, however, is associated only with a fragment of the entire identity proofing process, and in particular with the stage of authentication. Therefore, the selection of means for the registration stage remains an open issue even in this model.

Methods

The paper is based on an analysis of technological solutions used in Poland in the field of remote identification. These solutions were analyzed taking into account various criteria, including adequacy to individual

² <https://ec.europa.eu/digital-building-blocks/wikis/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eIDAS+schemes+under+eIDAS>

stages of the identification process and various types of functionalities and features such as a range of stored data, a range of applications, requirements to service providers, channels of application as well as readiness to eIDAS2.

The article uses the available literature on the subject and legal acts regulating electronic identification.

The term of “identity”

The security and comfort of living in modern societies depend on the level of technological development. One of the most important aspects of security is identity security. It refers to providing certainty, i.e. unambiguous knowledge about the identity of a person. The English term “identity” comes from the Latin word “idem”, which means identity and continuity. The Merriam-Webster's Dictionary indicates four essential meanings of the term identity. In the first sense, it is:

- a) *the distinguishing character or personality of an individual, or*
- b) *the relation established by psychological identification.*

In the second sense, the dictionary defines identity as *the condition of being the same with something described or asserted*. The third meaning of the term in question is:

- a) *sameness of essential or generic character in different instances, or*
- b) *sameness in all that constitutes the objective reality of a thing.*

Finally, in the fourth sense, the Merriam-Webster's Dictionary indicates that identity is *an equation that is satisfied for all values of the symbols*. The Dictionary of the Polish language, in turn, gives the word identity with five meanings. In the first sense, the term means *sameness*. Thus, it is an understanding analogous to the second and third definitions of the term identity, included in the Merriam-Webster's Dictionary. The second meaning, according to the Dictionary of the Polish language, is *self-awareness in relation to an individual*. This meaning corresponds to the first English definition of the term identity. The third meaning of the term identity in Polish is: *facts, features and personal data that allow the identification of a person*, which is close to the first English definition included in point a). The fourth Polish meaning in relation to the community is: *awareness of common features and a sense of unity*, which corresponds to the first English definition included in point b). Finally, the fifth meaning of the term in question is a mathematical and logical definition consistent with its English understanding of identity contained in the fourth definition in Merriam-Webster's Dictionary.

In connection with the subject of this work, the definition of the term identity is particularly important as: facts, features and personal data allowing the identification of a person. Although it is a dictionary definition, and not a specialist one and based on in-depth research in the field of sociology, legal sciences or security sciences, it is quite broad and directionally correct, because it leads to the conclusion that identity is related to the need to identify a given person, i.e. to verify that the person is who he or she claims to be or who we believe he or she is.

The meaning of the term identity quoted above from the Dictionary of the Polish language is related to the facts, features and personal data used to verify and identify identity. Biometric features fall under the broader category of personal data and are one of the cornerstones of identification or identity verification. They are part of a wider catalog of personal data which includes „any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”³. Thus, the catalog of personal data specified by law is open and the main premise in this case is whether a given information enables the direct or indirect identification of a specific person. Such understanding of personal data is in principle consistent with the dictionary understanding of identity as: facts, features and personal data allowing the identification of a person. However, this is a too narrow understanding and does not include the specific attribute of identity, i.e. the human being, of everything that constitutes him as one person, unique in the physical and mental dimension. As Sakson-Obada [2008] points out, the physical dimension is important for identity, because the body of each person is unique and contains a unique set of possibilities that no other human being has.

The sociological literature on the subject indicates that identity, including the identity of a single person, is a dynamic phenomenon and changes in the processes of social interactions, although at the same time identity

³ Article 4, Regulation (EU) 2016/679 Of The European Parliament and of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation); O.J. L 119.

remains, especially that relating to social groups, a factor ensuring durability, stabilization and continuity. It can be assumed that the dynamics of human identity refers not only to the cultural and worldview dimensions, but also to the biological dimension related, for example, to the aging process. Man undergoes changes in time. Is human identity, then, changeable and impermanent? If so, then "the same" – it would seem – human being in the long run will not be „the same“ person, but someone completely different. After all, his or her „specific factors determining the physical, physiological, genetic (...) identity“ may change. Even such seemingly permanent biometric features of a person, such as his fingerprint or even DNA, may intentionally or unintentionally change.

The literature does not currently provide a sufficiently satisfactory definition of the term identity in relation to an individual. Sociologists associate the concept of identity with the process of giving people a social existence. Gorazdowski [2017] combines human identity with the acquisition of knowledge and skills throughout life, from birth to death, the expansion of his intellectual resources and the development of coping strategies in various life situations. Moreover, he indicates the basic function of identity as identifying a person or group on the basis of selected features. In turn, Jankowska [2016] practically limits identity to personal data contained in identity documents. Sowirka [2013] presents a similar narrow understanding of identity, referring it to personal data contained in identity documents. Cygan [2015] defines similarly to the Dictionary of the Polish language, i.e. as „facts, features, personal data to identify a person, but also self-awareness.“

Therefore, it is justified to propose an author's definition of identity as the entirety of person's physical, physiological, genetic and psychological features as well as attributes in the form of a name, surname and other individually assigned attributes, which together constitute a person's individuality and uniqueness. According to the above definition, it is not one or several factors that determine a person's identity, but their overall presence. As indicated in the previous examples, a person's physical, physiological, and genetic characteristics can change. Also, his/her psychological features may change, including even – as a result of the disease – his/her personal conviction about his/her own identity. However, these changes do not result in a new identity, as they never take place *en block*. The natural aging process and disease do not modify all the individual characteristics of a given person. Even deliberate manipulation of these features, including medical intervention, is not possible for all these features „constituting the individuality and uniqueness“ of a given person. It may be relatively easy to try to change attributes such as name and surname or an individual personal number to authenticate oneself in ICT systems. These are the most common examples of the so-called identity theft through the use of someone else's personal data by an unauthorized person and use of someone else's selected individual attributes. However, such acts only create the appearance of a new or someone else's identity. A criminal who takes someone else's name and surname does not obtain the identity of the rightful owner of this personal data, because he/she is not able to take over the entirety of the discussed features „constituting the individuality and uniqueness“ of another human being. Therefore, Girdwoyń [2004] rightly points out that „assigning any feature (or a set of features) of an identified object of uniqueness does not seem possible, because its rarity, which is the basic premise of individuality, is at best related to only the class of all examined objects of a given type. and it does not have to have a universal value“. Therefore, it should be emphasized once again that the certainty as to a person's identity cannot be based solely on one or several of his features or attributes. Absolute certainty can only be provided by the totality of these features and identifiers, although in practice, for pragmatic reasons, a certainty based on probability is used (if a given phenomenon is quantifiable) or simple subjective judgment.

Identification proofing process

Pursuant to Article 2 point of eIDAS electronic identification means the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person. For the purposes of this paper, only the identification of a natural person will be considered. The main challenge when using electronic identification is the identification proofing process. It can be broken up into 7 common stages:

- 1) Registration;
- 2) Validation;
- 3) Verification;
- 4) Vetting/Risk Assessment;
- 5) Issuance;
- 6) Authentication,
- 7) Authorization.

Registration is the stage that initiates electronic identification. It includes the provision of a proof of identity by a natural person. The most common type of proof is an ID card or passport containing key data enabling identification: name, surname, date and place of birth as well as a photo of the face. This data is located in the graphic layer of the identity document and also – in the case of many countries – in the digital layer. In addition, other data (e.g. fingerprints) are also stored in the digital layer.

The next step is validation, in which the identity verifier confirms the authenticity, validity and completeness of the information provided by the person about his/her identity. An example of a typical and important activity at this stage is, for example, checking the authenticity and validity of an identity document. In the case of an expired document or a document for which there are reasonable suspicions that it has been forged, no further steps in the identification process can be carried out.

In the third stage, i.e. verification, it is verified whether the presented data identifying a specific person belongs to this person who is currently under the identification process. The traditionally used method at this stage is to compare the image of a person's face (in real conditions) with the image stored or printed in an identity document. This comparison may be carried out on the basis of the subjective perception of the person performing the verification or using automatic identity verification methods (using artificial intelligence). Apart from the face image, other human biometric features (e.g. fingerprints) can also be used. However, the necessary condition is the presence of exemplary biometric features in the presented identity documents or in other data sources (e.g. public registers) directly related to a given identity document and the person to whom this identity document relates. Identity verification on the basis of data other than the facial image is generally carried out automatically (with use of specialized IT systems).

An important element of identification proofing is the analysis of the risk associated with the person undergoing identification. The scope of the analysis is directly related to the purpose for which the identification is carried out. For example, in the case of identification for the purpose of opening a bank account and/or obtaining a bank loan, it is important to check the identity document in the appropriate databases of classified documents (stolen, lost or canceled).

Successful implementation of the above steps leads to the issuance of an electronic identification means, i.e. material and/or immaterial unit containing person identification data and which is used for authentication for an online service. A typical means of electronic identification is an individual login to a given ICT system (e.g. online banking system) with a password individually set by the customer. A relatively new (material) means of electronic identification are electronic ID cards (equipped with an electronic layer, i.e. microprocessors), used to authenticate the holder in ICT systems in order to provide online services.

After issuing the electronic identification means, it is possible to log into the online system using an individual login and assigned password, i.e. authentication with each online access to a given ICT system. In other words, authentication – when using means of electronic identification – is an electronic process that enables the origin and integrity of the user's verified data to be confirmed electronically. Pursuant to Article 97 of Directive 2366 of the European Parliament and of the EU Council on payment services in the internal market (hereinafter: PSD2), Member States shall ensure that a payment service provider applies strong customer authentication where the payer:

- 1) accesses its payment account online;
- 2) initiates an electronic payment transaction;
- 3) carries out any action through a remote channel which may imply a risk of payment fraud or other abuses.

With regard to the initiation of electronic payment transactions, Member States shall ensure that, for electronic remote payment transactions, payment service providers apply strong customer authentication that includes elements which dynamically link the transaction to a specific amount and a specific payee.

Strong customer authentication should be understood as authentication using at least two elements (independent in the sense that violating one of them does not weaken the credibility of the others) belonging to the following categories:

- 1) knowledge (something that only the user knows),
- 2) possession (something that only the user possesses),
- 3) inherence (something the user is).

Such authentication should be designed in a way that protects the confidentiality of the authentication data. At the same time, it should be noted that the requirement of (strong) authentication within the meaning of PSD2 covers not only access to the online system, but also the authorization of specific transactions (initiation of an

electronic payment transaction and activities via the remote channel, which may be associated with the risk of payment fraud or other abuses).

Expressing consent to the performance of a specific activity in the online ICT system, i.e. authorization, may be carried out using various tools, including those specific to authentication. It is possible to use more than one solution simultaneously. The typical solutions used at the authorization stage include:

- 1) SMS one-time password,
- 2) One-time password on the code card (TAN),
- 3) Code in the ICT system application (of a given service that requires identification),
- 4) Biometric solutions (e.g. facial image),
- 5) Token,
- 6) Qualified electronic signature.

Solutions used in electronic identification

Efficient and effective implementation of the electronic identification requires support by specialized IT tools. These tools, based on various technological approaches, focus primarily on handling selected or all stages of electronic identification. They are mainly used in sectors where confirmation of identity and certain identity attributes (e.g. age) is required by law, and is also important from the point of view of the safety and interests of the user and the online service provider. As a consequence, in Poland, the sectors where electronic identification is the most technologically developed and widespread include (in relation to online services):

- 1) The financial sector, especially banking,
- 2) The gambling sector,
- 3) Utilities sector,
- 4) Public service sector,
- 5) Sector of retail sale of alcoholic beverages.

An interesting case is the Polish online alcohol sales sector. The Act of October 26, 1982 on upbringing in sobriety and counteracting alcoholism does not allow the sale of alcohol to minors and intoxicated persons. At the same time, the sale of alcoholic beverages is possible only on the basis of the granted permit and in the place specified in the application for granting the permit. These laws formally restrict the online sale of alcohol, although in practice such sales do exist. The requirement to verify the age of the buyer is achieved by checking the ID card by the courier (in the case of mail order sale) or the seller (in the case of collection at the point of sale) or by attaching the scan of the ID card by the buyer in the purchase process. Therefore, it is an evident example of a failure to adapt the law to the contemporary technological and commercial realities, and the consequence of this state of affairs is the practice by traders that do not guarantee the sale of alcohol to adults and sober people.

Analysis of the electronic identification processes used in practice in Poland indicates a number of different technological solutions, the scope of which, however – with regard to individual elements of the identification process – differs, as shown in Table 1.

Table 1 shows the scope of application of various technological solutions at individual stages of the identification process. As the table shows, only a few of the analyzed solutions can be applied to all stages of the identification process. These are: automatic and operator-assisted video verification based on digital or graphic layer of identification document, solutions based on banking identity, AIS, a verification credit transfer, qualified electronic signature, Personal and Trusted Profiles as well as mCitizen. These universal solutions differ not only in terms of technology, but also in terms of functionality. The functional differences between them are presented in Table 2.

Video verification based on an ID card

Video verification on the basis of the graphic layer of the identity card is a process consisting in collecting data identifying a natural person from his/her identity document and comparing, through „live” video transmission, his/her image with the image in the identity card. The compliance of the image on the document with the image of the person undergoing identification is tested with the use of artificial intelligence algorithms. The liveness of a person is also tested (through the requirements of performing certain physical activities, e.g. moving the head). Data constituting the person's identity are taken from the graphic layer by reading them from the camera during video transmission. The authenticity of the document is checked by the requirement to present to the camera certain optical security features of the ID card. In practice, the document number is automatically checked in the

databases of restricted documents. The video verification can be fully automatic or it can be assisted by an operator who instructs the person on particular activities.

Video verification on the basis of the electronic layer of the ID card is a process similar to the one presented above. The main difference is the source of data constituting the attributes of the identity. They (including a photo of the face) are downloaded directly from the ICAO application stored in the ID card microprocessor. These are data that simultaneously appear on the graphic layer of the ID card. However, according to ICAO requirements, the data stored in the electronic layer does not contain national diacritics. This means that the data in the graphic layer may differ from the data in the electronic layer. The data is read using NFC transmission, e.g. using a smartphone. The condition for reading data from the ICAO application is to provide or scan the Machine-Readable Zone, i.e. alphanumeric string printed on the ID card. The authenticity of the document is verified on the basis of the electronic certificate of the issuer of the identity card read from the card chip (Country Signing Certification Authority and Country Verifying Certification Authority). Check of optical security features of the document is not required.

Solutions based on banking identity

This solution consists in using the identification process (not necessarily electronic) carried out in the bank much earlier – when initially establishing business relations with a given person and the bank. The provisions of Polish banking law require a very reliable and precise process of identifying a person who wants to become a bank customer. Only a properly identified person can obtain from a bank an electronic means of identification enabling the use of electronic banking. The idea of using a banking identity is that with the help of an electronic identification means (e.g. an individual login with a password) issued by a given bank, the bank's customer (and also the holder of the aforementioned electronic identification means) can confirm his/her identity in another service provided by another subject. This solution is popular in Poland and offered by a company owned by the Polish banking sector. It does not require the user to perform additional identification activities apart from entering the login and password to the bank's transaction system (registration stage). His/her data (identity attributes) have already been registered and validated beforehand, and the identity has been verified by the bank. Therefore, this solution is based on an electronic identification means already issued by the bank, i.e. an individual login (and assigned password), with the possibility of using this means for identification for purposes other than logging into his/her own bank and making financial transactions. So banking identity "opens the door" to other online services, providing the service provider necessary identification attributes (e.g. name, date of birth etc.) of the customer. Therefore, the only verification activity in the process is the verification of the login and password compatibility by the bank that issued this electronic identification means. At the same time, it is presumed that at the stage of establishing the customer's original relationship with the bank and issuing the customer with an electronic identification means, the customer identification process was properly carried out and the electronic identification means issued once by the bank may be the basis for another entity to issue a different measure. As a consequence, the bank – with the consent of the client – transfers personal data along with confirmation of identity to a new entity (online service provider), which requires identification of the indicated person.

Account Information Service

PSD2 has opened up new opportunities for the use of customer data held by banks. The directive created the foundations for a new market, the so-called open banking market, created by various types of services that can be provided on the basis of three pillars of PSD2:

- 1) access to information about the customer's account (AIS, Account Information Service),
- 2) payment initiation (PIS, Payment Initiation Service),
- 3) confirmation of the availability of funds on the account (CAF, Confirmation of the Availability of Funds).

Pursuant to PSD2, the performance of the above activities – relating to a given bank – is possible not only directly by the customer of that bank, but also – on behalf of the customer – by an authorized third party (TPP, Third Party Provider). One of the main objectives of PSD2 was to create formal and legal conditions conducive to the emergence of new models of cooperation between the banking sector and fintechs, and to use the technological potential of fintechs for the quick and efficient implementation of innovative solutions on the payments market. However, a prerequisite for achieving these goals was to provide fintechs with access to data held by banks. The fundamental problem was the issue of banks' willingness to open up to new entities (TPP) and to ensure appropriate data exchange interfaces. The solution to this problem was based on Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive 2015/2366 of the European Parliament and of the Council

Tabela 1

Technological solutions used in different stages of electronic identification in Poland

Stage of identification process / Technological solution	Registration	Validation	Verification	Vetting / Risk Assessment	Issuance	Authentication	Authorization
Automatic video verification based on the graphic layer of the ID card	Yes	Yes	Yes	Possible to be implemented by the service provider*	Yes	Yes	Yes
Operator-assisted video verification based on the graphic layer of the ID card	Yes	Yes	Yes	Possible to be implemented by the service provider*	Yes	Yes	Yes
Automatic video verification based on the digital layer of the ID card	Yes	Yes	Yes	Possible to be implemented by the service provider*	Yes	Yes	Yes
Operator-assisted video verification based on the digital layer of the ID card	Yes	Yes	Yes	Possible to be implemented by the service provider*	Yes	Yes	Yes
Solutions based on banking identity	Yes	Yes	Yes	Possible to be implemented by the service provider*	Yes	Possible but rare	Possible but rare
Solutions based on AIS	Yes	Yes	Yes	Possible to be implemented by the service provider*	Yes	No	No
Solutions based on a verification credit transfer	Yes	Yes	Yes	Possible to be implemented by the service provider*	Possible but not used in practice	Possible but not used in practice	Possible but not used in practice
Qualified electronic signature	Yes	Yes	Yes	Possible to be implemented by the service provider*	Possible	Yes	Yes

Stage of identification process / Technological solution	Registration	Validation	Verification	Vetting / Risk Assessment	Issuance	Authentication	Authorization
Personal Profile of the electronic identification card	Yes	Yes	Yes	Possible to be implemented by the service provider*	Yes – Personal Profile is a means of electronic identification	Yes	Yes
Trusted Profile	Yes	Yes	Yes	Possible to be implemented by the service provider*	Yes – Trusted Profile is a means of electronic identification	Yes	Yes
mCitizen (mObywatel)	Yes	Yes	Yes	Possible to be implemented by the service provider*	Possible but not used in practice	Possible but rare	Possible but rare
SMS/OTM	No	No	No	No	No	Yes	Yes
App passwords	No	No	No	No	No	Yes	Yes
TAN card	No	No	No	No	No	Yes	Yes
Token	No	No	No	No	No	Yes	Yes
Video verification based on a pattern in a data storage	No	No	No	No	No	Yes	Yes
Fingerprint verification based on a pattern in a data storage	No	No	No	No	No	Yes	Yes

* Service provider – an entity providing services that require the implementation of the identification process.

Source: own analysis.

Table 2

Functionalities of selected identification solutions

Solution / Functionalities	Scope of stored data	Range of applications	Other functionalities	Requirements for service providers	Main channel of applications	Potential volume of end-users	eIDAS2 readiness
Automatic and operator-assisted video verification based on a digital layer of an identification document	Personal data available on supported documents along with a photo	On-site, online, mobile	Integration with the database of lost and stolen documents, recognition of false documents, age verification, recognizing fake photos and videos.	High	Commercial	About 6 M holders of electronic identification documents equipped with digital layer	Yes, an independent audit necessary
Automatic and operator-assisted video verification based on a graphic layer of an identification document	Personal data available on supported documents along with a photo	On-site, online, mobile	Integration with the database of lost and stolen documents, recognition of false documents, age verification, recognizing fake photos and videos	Low	Commercial	About 29 M holders of electronic identification documents	Yes, an independent audit necessary
Banking identity	Personal data: first name, middle name, surname, personal number, date of birth, place of birth, country of birth, citizenship, type of identity document, series and number of an identity document, date of issuance of an identity document, expiry date of an identity document, confirmed telephone number, legal age, family name	Online, mobile	Login to an existing account, transaction authorization via SMS or a push notification, creating a Trusted Profile	High	Commercial and public	About 16 M users (total potential: about 22 M)	Higher level of assurance required

Solution / Functionalities	Scope of stored data	Range of applications	Other functionalities	Requirements for service providers	Main channel of applications	Potential volume of end-users	eIDAS2 readiness
AIS	Personal data: name, surname, address Financial data: account number, receipts / expenses, transaction type	Online, mobile	Customer scoring	Low	Commercial	About 22 M bank accounts users	No
Verification credit transfer	Personal data: name, surname, address	Online, mobile	-	Low	Commercial	About 22 M bank accounts users	No
Qualified electronic signature	Personal data	Online, mobile	-	High	Commercial and public	Less than 1 M of holders	Yes, an independent audit necessary
Personal Profile	First name, middle name, surname, date of birth, a unique identifier built by the sending Member State in accordance with technical specifications for cross-border identification as persistent as possible Additionally possible: gender, maiden name, place of birth, current address	On-site, online, mobile	Advanced electronic signature, creating a Trusted Profile	Medium	Commercial and public	About 3 M holders of electronic identification documents equipped with activated digital layer	Yes
Trusted Profile	Personal data and personal number	Online, mobile	-	Low	Public	About 11 M of active users + potential of 22 M of digital identity users	Yes, higher level of assurance required if based on banking identity
mCitizen	Personal data and personal number	On-site, online, mobile	Integration with the database of lost and stolen documents,	Low	Commercial and public	Potential of all Trusted Profile users (11 M)	Yes, higher level of assurance required if based on banking identity

Source: own compilation

with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication (hereinafter: RTS). The document defines the requirements for the use of strong customer authentication and the principles of communication between providers maintaining payment accounts (e.g. banks) with entities providing access to the account (TPP). According to RTS, each payment service provider maintaining online payment accounts (e.g. a bank) should offer at least one access interface enabling secure communication with the TPP.

In the case of identification, the AIS service is of particular importance. It consists in the provision by an entity authorized to provide this service, at the user's request and with the user's consent, of consolidated information regarding the user's payment account or accounts available online, kept by one or more other payment service providers (banks). The service therefore allows access to specific data identifying the person, i.e. name and address. Thanks to the banks making their API available, it is possible for the TPP (and the client – after logging in to the banking system) to download his/her data and – on this basis – to determine their compliance with the declared data.

The scope of the data made available is therefore significantly smaller than in the case of the banking identity solutions discussed above. The AIS service is treated as a payment service, the provision of which, without providing other payment services, requires an entry in the relevant register of the Polish Financial Supervision Authority.

In practice, the use of the AIS service is quite difficult, because despite the obligation imposed on banks to offer an access interface for communication with TPP, there is no uniform standard in this respect and no unambiguous catalog of data that is provided by banks under AIS has been developed so far. This increases the costs of using this service, because it requires TPP to adapt individually to the API of individual banks. Moreover, it happens that some banks do not provide such data as the name and surname of the account holder under the AIS. Hence, this hinders the functioning of this identification service.

Verification credit transfer

Bank credit transfer verification is a fairly popular form of remote identity verification. This solution takes advantage of the fact that the data required for the execution of a bank credit transfer includes, inter alia, name and surname or name of the transfer sender, i.e. the person who has the bank account that is debited in connection with the transfer order. A verification transfer is therefore a regular bank credit transfer, usually for a small amount (e.g. PLN 1 or PLN 0.001), given by the person under identification to the entity verifying the identity. The concept of a verification transfer is therefore based on the comparison of the name indicated in the identification process with the name appearing on the transfer order (the name of the transfer sender). Verification transfers are quite popular especially in case of short-term loans, and especially Buy Now Pay Later (BNPL) services. This form of identity verification is based primarily on the trust that accompanies banks and the procedures for opening bank accounts. At the same time, it benefits from the presumption that the person holding his bank account was properly verified at the time the account was opened and that he did not transfer credentials to his account to third parties. The weakness of the verification transfer is the limited scope of the data of the person subject to identification. This weakness was also highlighted by the Polish Financial Supervision Authority, pointing out that „these data will only be used to assist in the verification of the client's identity”⁴.

Qualified electronic signature

Electronic signature means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign. Qualified electronic signature means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic sign. The strength of a qualified signature is the legal guarantee, which treats a qualified certificate in the same way as a handwritten signature. On the other hand, an unqualified certificate is usually used to encrypt information, sign files, authenticate the server or log into the system. Moreover, the qualified certificate is issued only by authorized Certification Centers. As for the non-qualified certificate, it can also be issued by non-certified entities. A qualified signature therefore provides high certainty as to the identity of the person using it.

⁴ https://www.knf.gov.pl/knf/pl/komponenty/img/Stanowisko_UKNF_dot_identyfikacji_klienta_i_weryfikacji_jego_tozsamosci_w_bankach_oraz_oddzialach_instytucji_kredytowych_w_oparciu_o_metode_wideoweryfikacji_66066.pdf

The advanced electronic signature mechanism is based on public key cryptography, which is an issue that is so extensive and specialized, and at the same time separate from the subject of this paper, that it was decided to present only the basic characteristics, leaving the reader the opportunity to broaden his/her knowledge in other literature sources. The electronic signing process using PKI starts with generating the so-called hash, i.e. a unique document hash function using a cryptographic algorithm⁵. The generated hash is individual for each document, and each change made in the document requires – if one wants to place an advanced electronic signature under it – generating a new hash. The hash is encrypted using a password-protected private key of the signer. The encrypted hash as an electronic signature is attached to the document and thus the electronically signed document is ready for distribution. Additionally, the sender's public key is attached to the document. This creates a key pair: private key and public key. By design, the private key is secret only known to the owner, while the public key may be known to the public.

In the phase of signature verification the document is separated from the electronic signature again. The same hash algorithm is run on the document, generating a specific hash function (decrypted hash). At the same time, the encrypted hash received from the sender is decrypted using the sender's public key, which results in a hash function. However, the use of a public key involves the problem of verification by the person who received the public key from the sender, whether it is a public key at all, whether the key was used in accordance with the intention of its owner and who is its owner. This problem is solved by a certification mechanism that allows you to certify the fact that a specific public key is associated with its owner. Thus, the certificate is an electronic document containing the public key and specific features that personalize the owner of the key. The concept of certification is therefore associated with the existence of the so-called a trusted third party (trust service provider), i.e. the issuer of the certificate. The personal certificate includes:

- 1) first name,
- 2) surname,
- 3) citizenship,
- 4) the common name appearing in the certificate (it may contain only the name and surname of the subscriber),
- 5) applicant's identification attribute – at least one of the following:
 - a) personal number,
 - b) passport (series and number),
 - c) ID card (series and number),
 - d) tax identification number.

In the final stage of signature verification, both obtained values (hashes, i.e. hash functions) are compared with each other. If they match, the document is considered unmodified (preserving document integrity) and the sender has been verified. On the other hand, the lack of compliance implies two possibilities: the modification of the document or the lack of positive verification of the sender.

A qualified electronic signature is a tool that ensures strong identity verification. Nevertheless, it is not a common solution, as it is currently used mainly by entrepreneurs, and its scope of application mainly covers activities resulting from legal provisions (e.g. signing financial statements). Hence its social usefulness is limited.

Personal Profile

Pursuant to Article 2 clause 1 point 10 of the Act of 6 August 2010 on ID Cards, a Personal Profile is a means of electronic identification containing data confirmed by a certificate of identification and authentication. The ID cards currently issued in Poland contains a digital layer. The digital layer includes, among others: an identification and authentication certificate with data enabling electronic identification and authentication. The ID cards meet the requirements for a qualified electronic signature creation device and enables its holder to:

- 1) authenticate in online services using a Personal Profile,
- 2) use a personal signature;
- 3) confirm presence at a specific time and place.

The use of an ID card with a digital layer for authentication in online services, applying with it a personal signature or confirmation of presence, requires the user to have a card reader and appropriate software. The process of signing a document or logging in to online services is presented in Fig. 1.

⁵ E.g. RSA, i.e. Rivesta-Shamira-Adleman algorithm.

The use of the electronic ID card and the Personal Profile contained therein as a means of electronic identification requires additional equipment of the user with an ID card reader and software. The ID card chip, in which the digital layer is placed, is an RFID microprocessor, enabling contactless communication between the ID card and the reader. For this reason, in order to read data from the electronic layer, it is enough to just put the document to the reader (e.g. a smartphone). The user then enters the Card Access Number (CAN) which is printed in the form of a barcode on the reverse of the ID card. It is required in order to establish (via a card reader) the connection between the digital layer of the ID card and the ICT device or system. After entering the 6-digit CAN number, its compliance is verified in order to establish an encrypted connection between the reader and the ID card (PACE; Password Authenticated Connection Establishment).

The solution based on the Personal Profile is offered by one of the State Treasury companies in the form of an application installed on smartphones. Due to the relatively low number of issued electronic ID cards, this is not a solution commonly used in Poland at present.

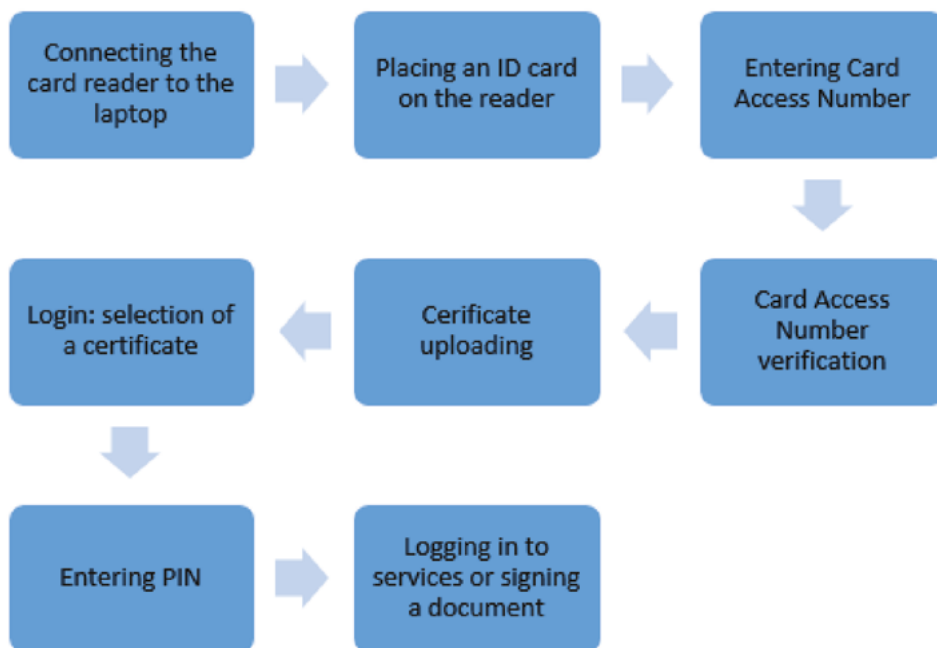


Fig. 1. The process of signing a document or logging in to online services with use of Personal Profile

Source: own compilation.

Trusted Profile

Pursuant to Article 3 point 14 of the Act of February 17, 2005 on the computerization of the activities of entities performing public tasks, a Trusted Profile is a means of electronic identification containing a set of data identifying and describing a natural person. The Trusted Profile confirms the person's identity in his/her contacts with the public administration. It is issued at the request of a citizen after initial check whether the person applying for the Profile is who he/she claims to be. There are four possibilities to verify the applicant's identity during this initial check:

- 1) through physical identity verification based on the presented ID card or passport or other document allowing for unequivocal confirmation of the identity of the person,
- 2) with the use of a qualified electronic signature, provided that the signature contains at least the name and surname and the personal number,
- 3) with the use of an electronic identification means used for authentication in the IT system of a domestic bank, provided that this means confirms the following data: name and surname as well as personal number,

4) with use of a Personal Profile.

Physical verification takes the classic form of identity checking on the basis of certain public documents. With regard to the Trusted Profile, it can be carried out by the consul, the head of the tax office, the voivode, the Social Insurance Institution and the National Health Fund, domestic banks or post operators (the so-called confirmation points).

Establishing a Trusted Profile with the use of a qualified electronic signature does not seem to be rational, because in fact it means creating one electronic identifier (with functionality limited to contacts with public administration) by using another electronic means of identification (with a wide functionality).

Two other ways of verifying a Trusted Profile application are already discussed solutions based on banking identity and a Personal Profile.

mObywatel (mCitizen)

mObywatel is a mobile government app that constitutes a digital wallet, in which certain data coming from public documents (such as identification card or driving license) can be stored. A special feature of the mObywatel solution is the possibility of remote identity verification by transferring personal data (photo, name) to any person/institution/company in the form of a QR code. Data in mObywatel come directly from Public Registers, in particular from the Register of Personal IDs. mObywatel is a peculiar precursor of the European digital identity wallet, referred to in the Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity (eIDAS2)⁶. mObywatel does not contain a number of functionalities assigned to the designed European digital identity wallet, however conceptually it is similar to it. mObywatel has been designed mainly for the purpose of the citizen's contact with public administration, but its regulations do not exclude the possibility of using it, and especially the functionality of remote identity verification, in relations between the citizen and the business sector.

One-time password in SMS

Telephone numbers issued by Polish GSM operators are assigned to individual persons. This also applies to prepaid SIM cards. As a consequence, the telephone number is a specific attribute of identity that is unequivocally, though not permanently, related to a given person. Due to the widespread use of mobile phones and the above-mentioned individual relationship with a person, the use of one-time passwords in SMS as a method of authentication and authorization has become popular. The risk of abuse related to the use of a mobile phone, e.g. taking it over by an unauthorized person, makes it not a secure method. Therefore it is limited only to authentication and authorization. It is commonly used in banking, also as one element of Strong Customer Authentication (possession – a mobile phone with a specific number).

App passwords

The wide availability of online services, and at the same time the significant popularity of mobile phones, have made mobile apps more important, which on the one hand provide convenient and free access to services, and on the other hand – an additional instrument for authorization and authentication. Thus, app passwords have become an instrument of authorization and authentication alternative to the one-time SMS passwords. They are considered safer than SMS passwords as they are not disclosed (unlike SMS passwords displayed on the smartphone screen).

TAN card

Transaction authorization number (TAN) cards were one of the first authentication and authorization instruments, popular in particular in banking. In a time when mobile phones were a luxury and SMS prices were high, TAN cards were the natural solution. TAN card can be a plain, printed sheet of paper or a form similar to a credit card. Often, subsequent numbers are covered with an imprint or foil, which is removed before use, revealing the hidden password – this makes it easier to determine the number of unused codes, and at the same time protects the codes against unauthorized reading.

⁶ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0281>

Token

A security token is a peripheral device used to gain access to an electronically restricted resource. The idea of a token is usually based on the code it generates, i.e. a one-time password. Therefore it is a more sophisticated, digitalized form of a TAN card. The token is used in addition to or in place of a password. Some tokens may store cryptographic keys or passwords. Some designs incorporate tamper resistant packaging, while others may include small keypads to allow entry of a PIN or a simple button to start a generating routine with some display capability to show a generated key number.

Tokens are still present as instruments used in the identification process (authorization and logging), especially in the area of banking, but the scope of their use is much narrower than before.

Video verification based on a pattern in the data carrier or service provider's registers

Video verification can be based on the face image taken live in the identification process, but compared to the pattern recorded in a data storage other than the identification document (and its chip). In this case, the biometric data is rarely stored centrally within the service provider's biometric database, but rather stored locally, i.e. on a device owned by the user (e.g. on a smartphone). This method is limited to authentication and authorization only, and the remaining (prior) steps in the identification process must be accomplished using other methods.

Fingerprint verification against a pattern in the data bearer or service provider's registers

This method is analogous to the video verification based on a pattern in a data storage. Due to the sensitivity of the biometric data, which is the fingerprint, the verification is in practice limited to the situation in which the fingerprint pattern is stored locally (e.g. on a smartphone owned by the user). As in the previous case, this method is limited to the authentication and authorization steps.

Conclusions

Poland has very developed and widely used solutions in the field of remote identification. Most of them are universal, i.e. they can be applied to all stages of the identification process. Moreover, it is also important that the discussed tools are applicable both in the public and commercial channel. Among all the analyzed solutions, the following deserve special attention: banking identity and video verification based on the electronic layer of the ID card.

Banking identity is a mass solution based on the processes carried out by banks when opening bank accounts. This solution is extremely convenient for the user, as it does not require any activities other than the standard logging into the banking system. At the same time, it is a safe solution, because banks, on the basis of applicable law and their own interest, pay great attention to identity verification when establishing initial relationships with the client. Due to these features, the banking identity was used as a method of confirming the identity for the purpose of obtaining another means of electronic identification, i.e. a Trusted Profile.

Video verification based on the electronic layer of the ID card is also a very safe solution, as it eliminates the subjective verification of identity based on the image of the face and the subjective verification of the authenticity of identity documents. These activities are performed automatically. The face comparison is made by IT systems based on artificial intelligence and ensuring very low error rates. The authenticity of the document is verified on the basis of electronic certificates, which have not yet been falsified by criminals. The only problem that remains is currently a relatively low number of identity cards with an electronic layer. However, it will grow over time.

Banking identity and video verification based on the electronic layer of the ID card provide therefore the greatest social utility in terms of security and potential availability (potential volume of end-users).

АНАЛИЗ НА ОБУЧЕНИЕТО НА ПОТРЕБИТЕЛИ НА „ИНФОРМАЦИОННА СИСТЕМА ЗА УПРАВЛЕНИЕ НА ФИНАНСОВИ И МАТЕРИАЛНИ РЕСУРСИ“

подполковник д-р Светозар Ботев

Командване за логистична поддръжка, s.botev@armf.bg

д-р Валя Симеонова

Командване за логистична поддръжка, valiasimeonova_sweet@abv.bg

Резюме: В доклада са представени същността и значението на провежданото обучение за работа с Информационна система за управление на финансови и материални ресурси и необходимостта от провежданите курсове. Управленските информационни системи са неразделна част от всяка една бизнес организация в наши дни. Информационната система за управление на финансови и материални ресурси представлява система за мониторинг, управление и контрол на логистични и финансови процеси извършвани в Българската армия.

Ключови думи: *информационна система; мониторинг; обучение; управление и контрол*

ANALYSIS OF THE TRAINING OF USERS OF THE “INFORMATION SYSTEM FOR FINANCIAL AND MATERIAL RESOURCES MANAGEMENT”

Lieutenant Colonel Svetozar Botev, PhD

Logistic Support Command

Sofia, Bulgaria

E-mail: s.botev@armf.bg

Valya Simeonova, PhD

Logistic Support Command

Sofia, Bulgaria

E-mail: valiasimeonova_sweet@abv.bg

Abstract: The report presents the nature and importance of the Information System for Management of Financial and Material Resources and the need for the courses. Management information systems are an integral part of any business organization today. Information system for management of financial and material resources is a system for monitoring, management and control of logistical and financial processes carried out in the Bulgarian Army.

Keywords: *information system; monitoring; training; management and control*

Въведение

Онова, което характеризира съвременното общество и определя неговия облик, е главоломното навлизане на високите технологии и информационни системи във всички сфери на човешката дейност. Управленските информационни системи са неразделна част от всяка една бизнес организация в наши дни. Състоят се от хардуер и софтуер, към които неразделна част са и необходимите бизнес процеси, нужни за ефективното управление на потока от данни и информация. Информационните системи предоставят на ръководителите данни за вземането на решения. За функциониране на системите е необходимо създаването на екип за поддръжка – на софтуер, база данни, хардуер и оптимизиране на процесите. В центъра на всяка една система е базата данни и инструментите нужни за отчитане, събиране и коригиране на информацията.

Инструментите позволяват на потребителите да търсят, извличат, експортират намиращата се в базата данни информация. Чрез информационната система се контролират ежедневните дейности на подчинените в йерархичната верига. Целта на информационните системи е да подобрят комуникацията

и връзките между служителите, да предоставят необходимата информация, да намалят разходите на организациите и съкратят ръчния труд. Управлението чрез системите не само позволява генерирането на подробни отчети за изпълнение на дейностите в организацията, но служи и като инструмент за управлението на подчинените чрез поставяне на конкретни задачи.

Информационната система за управление на финансови и материални ресурси (ИСУФМР) е ERP система от последно поколение. ERP системите се считат за най-високия клас програмно осигуряване. ERP (Enterprise Resource Planning) системата е компютърно интегрирана, многомерна и многофункционална система, изградена на база клиент-сървър технология, основана на бизнес модела за планиране, контрол и глобална оптимизация на цялостната логистична верига на процесите през целия жизнен цикъл на материалните средства и съпътстващите ги финансови операции.

ИСУФМР представлява система за мониторинг, управление и контрол на логистични и финансови процеси извършвани в Българската армия. Тя има за цел да подобри ефективността на управлението на логистичното осигуряване на Българската армия, като свърже в единна работна среда логистичните органи от всички управленски нива. Системата осигурява в реално време актуална информация за наличните материални и финансови ресурси и предоставя средства за управление и контрол на протичащите логистични процеси. [2]

Функционалният обхват на информационната система включва единни стандартни процедури и работни процеси от следните области:

- планиране;
- снабдяване и доставки;
- складиране и съхранение;
- употреба и използване;
- управление на материалните средства;
- техническо обслужване;
- ремонт;
- индивидуално вещеве осигуряване;
- управление на финанси и счетоводство.

Информационната система осигурява:

- гарантиране на коректност и свързаност на логистичната и финансова информация;
- оптимизиране на документооборота в логистичните и финансови процеси в Българската армия;
- унифициране на логистичните и финансови процедури;
- оптимизиране и повишен текущ контрол върху оперативната дейност;
- оптимизиране на информационните потоци в Българската армия;
- значително намаляване на документооборота и времето за обмен на информация;
- повишаване на ефективността на управление на материалния и финансовия поток;
- намаляване времето за организиране и изпълнение на доставки;
- подобряване на отчетно-аналитичните функции.

Обучението на потребителите на ИСУФМР се провежда в офиса на информационната система в административната сграда в гр. София бул. „Тотлебен“ № 34 или на място във военните формирования. Курсовете в отдела се провеждат на групи по десет обучаеми, а във военните формирования – в зависимост от броя на развърнатите работни места, по предварително утвърден график от началника на отбраната. Обучението се извършва по специализирани програми изготвени от Командване за логистична поддръжка (КЛП) в съответствие с функционалните задължения на крайните потребители. На успешно преминалите курса на обучение се издава сертификат за работа със системата подписан от командира на КЛП.

Методология на изследването. Изследването е базирано на проведено обучение и попълване на анкетни карти на хартиен носител от преминалите обучение потребители. Резултатите са важни както за обучаемите – какво са научили по-бързо и доколко им е полезно, така и за екипа, провеждащ обучението – какви недостатъци има в учебния план.

Целевите групи на анкетираните са съставени от военнослужещи и цивилни служители – мъже и жени на различна възраст, различно образование, заемащи различни длъжности. Анкетното проучване е проведено непосредствено след приключване на обучението през месец септември 2021 г.

Анкетата е един често използван метод за социологическо проучване. Според различни източници тя създава по-голямо чувство за независимост у респондента, поради дистанцията на анкетатора при по-

пълване на анкетната карта, обстановката предразполага към по-голяма откровеност. Анкетата е много гъвкав инструмент, защото въпросите могат да се зададат по различни начини. Въпросите биват: открити – има възможност за отговор със свои думи, закрити – включени са възможни варианти за отговор и респондентът избира един от тях и полузакрити – наред със структурираните отговори се дава възможност и за други отговори и допълнения.

Първата група анкетираните е съставена от офицери от Военновъздушните и Военноморските сили. Общо попълнените анкетни карти по образца от Приложение 1 са 10 броя. Втората група анкетираните е съставена от офицери, сержанти и цивилни служители от Военновъздушни сили, Военноморски сили и Сухопътни войски. Общо попълнените анкетни карти по образца от Приложение 1 са 15 броя.

Целта на зададените въпроси в анкетата е да се получи информация относно ефективността на провежданото обучение и насоки за подобряването му в бъдеще.

Съдържание на анкетата:

Първите четири въпроса изясняват дали обучението и учебните пособия отговарят на очакванията на обучаемите и дали отделеното време обхваща процесите, свързани със задълженията на обучаемите.

От пети, шести и седми въпрос се разбира дали обучаемите се чувстват готови да работят с информационната система, могат ли самостоятелно да се справят с поставените им задачи и дали с получените знания биха могли да оказват помощ на други потребители.

От осми въпрос става ясно дали има несъответствия между логистичните процеси и реализирането им в системата.

Последният, девети въпрос дава възможност на обучаемите да посочат какви препоръки имат към екипа, който провежда обучението и какво биха променили, ако имаха тази възможност.

Анализ на получените резултати. Основната цел на изследването е да се установи доколко е ефективно проведеното обучение, има ли недостатъци и какви предложения има за подобряването му. Тъй като е проведено обучение на две групи, ще бъде направен сравнителен анализ между тях.

Анализ на анкетираните от първата група. На първите три въпроса дали проведеното обучение и учебните пособия са отговорили на техните очаквания, времето отделено за обучение било ли е достатъчно, всички от първата група от десет обучаеми отговарят положително.

Четвърти въпрос е дали обучението обхваща процесите, свързани с непосредствените задължения на служителите – 80% от тях отговарят положително, обучението обхваща процеси от техните задължения, а останалите 20% отговарят, че длъжността им не изисква такова обучение.

Пети, шести и седми въпрос са свързани с готовността на служителите за работа с информационната система – чувстват ли се готови да работят с информационната система, ще могат ли самостоятелно да работят и считат ли, че с получените знания ще могат да оказват помощ на другите потребители – 90% от анкетираните отговарят с „Да“, а останалите 10% отговарят с „Не“.

Следващият, осми въпрос е дали има несъответствия между логистичните процеси и реализирането им в системата – 90% от потребителите отговарят отрицателно, а 10% отговарят положително.

Последният въпрос е дали потребителите биха променили нещо в обучението и какви препоръки биха дали. 40% от анкетираните отговарят, че нямат препоръки, тъй като не са достатъчно компетентни, но биха искали да се увеличи времето за практическа работа, 10% не посочват никакъв отговор. Останалите 50% споделят, че екипът, провеждащ обучението, е отзивчив и компетентен и надграждат знанията им, но биха искали електронните каталози да са достъпни за повечето потребители.

Анализ на анкетираните от втората група. На първия въпрос дали обучението отговаря на очакванията им и на втория – учебните пособия подпомагат ли обучението по време на курса, всички посочват положителен отговор.

От третия въпрос се разбира отделеното време за обучение дали е било достатъчно за служителите. Повече от половината служители – 60%, дават отговор „Да“, а останалите 40% дават отговор „Не“, като поясняват защо. Операциите, които трябва да се усвояват са много, а отделеното време за обучение не е достатъчно, въпросите по ръководството също са много. За запознаване с информационната система в общи линии и с начина на работа с нея времето е достатъчно, но не и за научаване на всички въпроси, също и за затвърждаване на наученото досега.

От четвърти въпрос става ясно дали обучението обхваща въпроси свързани с непосредствените задължения на обучаемите. По-голяма част, 80% от присъстващите, отговарят положително. Останалите

20% обучаеми посочват отрицателен отговор, като поясняват, че не работят с информационната система. Тук възниква въпросът защо присъстват на курс тези хора?

От следващия пети въпрос разбираме дали служителите се чувстват готови да работят с информационната система. 60% от присъстващите отговарят, че са готови да работят, но останалите 40% служители смятат, че не са готови да работят и посочват причините – необходимо е повече време както за обучение, така и за практика. Нужна е допълнителна работа за разглеждане на всички въпроси по счетоводна обработка на документи в системата.

Шести въпрос дава информация могат ли самостоятелно да работят с информационната система. 70% от анкетираните отговарят с „Да“. Това означава, че продължителността на курса е достатъчна, научили са се да работят с информационната система. 30% отговарят с „Не“ – настояват за повече часове практика, също така и повече време за изясняване на процесите.

С получените знания от проведеното обучение служителите дали ще могат да оказват помощ на другите потребители разбираме от седми въпрос. 60% отговарят положително, смятат че са получили знанията да помагат и на други потребители. 10% проявяват несигурност и отговарят и с „Да“, и с „Не“. 30% отговарят отрицателно. Смятат, че нямат достатъчно знания да оказват помощ, биха могли да помогнат за определени процеси. В някаква степен биха могли да запознаят служителите с информационната система.

Осми въпрос е дали има несъответствия между логистичните процеси и реализирането им в информационната система. Всички анкетирани са на едно мнение, отговарят с „Не“.

Последният, девети въпрос, отправен към служителите е какво биха променили в обучението и биха ли посочили препоръки. 60% не са посочили никакъв отговор. Това може да означава, че са доволни от така проведен курс. 20% препоръчват удължаване на периода за обучение, 10% не биха променили нищо. 10% от присъствалите на обучението отговарят, че на този курс трябва да присъстват лица, на които ще им е полезно това обучение, които ще работят с информационната система.

Тук може да допълним, че командирите на военните формирования определят кои хора ще присъстват на курсовете, така че тази препоръка е необходимо да я отнесат към командирите на съответните военни формирования.

От получените резултати може да се обобщи следното:

Според двете групи проведеното обучение и използваните учебни пособия са отговорили на очакванията им. Отделеното време за обучение, отново според двете групи, не е достатъчно, въпросите и операциите по ръководството са много. Почти всички от обучаемите споделят, че длъжността им не изисква притежаването на знания и умения за работа с информационната система.

Служителите и от двете групи посочват, че не са готови да работят с информационната система на 100%, но в същото време отбелязват, че биха могли да оказват помощ на други потребители. Тук се забелязва несъответствие между отговори и знания.

Основните препоръки, които посочват служителите са:

- по-голям период за обучение;
- създаване на електронни каталози;
- да присъстват хора, на които ще им е полезно това обучение.

Проблемни въпроси:

– провеждане на обучение на потребители без функционалните им задължения да са свързани с работа в ИСЛБА;

– намаляване способностите на специалистите за въвеждане на планираните по графика военни формирования в системата;

– обучение на логистично разнородни специалисти дълго време преди реално да работят с ИСЛБА;

– неувереност на потребителите за работа с ИСЛБА;

– неподходящи справки свързани със срочните отчетни донесения;

– необходимост от допълнително време за опресняване на знанията на специалистите при реално зареждане на данни;

– въпреки изцяло практико-приложното обучение, обучаемите искат удължаване срока на обучение;

– текучество на персонала.

Положителни страни:

- натрупване на способности за работа с ИСЛБА на логистично разнороден персонал;
- запознаване с възможностите на ИСЛБА за унифицирана работа на логистично разнороден персонал;
- възможност за обобщаване на множество данни към щабове от различните нива на управление.

В заключение може да се каже, че информационната система подобрява комуникацията и взаимодействието между служителите, предоставя необходимата информация, намалява разходите на организациите и съкращава ръчния труд. Обучението се извършва по специализирани програми, изготвени от КЛП в съответствие с функционалните задължения на крайните потребители. На успешно преминалите курса на обучение се издава сертификат за работа със системата подписан от командира на КЛП.

Приложение 1

ВЪПРОСНИК

Анализ на обучението на потребители
на „Информационна система Логистика на Българската армия“

звание, име презиме, фамилия,

военно формирование

1. Отговори ли проведеното обучение на очакванията Ви?

а. Да

б. Не

ако не защо:.....
.....
.....
.....

2. Учебните пособия, които използвахте достатъчни ли са и подпомогнаха ли Ви?

а. Да

б. Не

ако не защо:.....
.....
.....
.....

3. Времето отделено за обучение, достатъчно ли беше за изучаване на предвидените в учебната програма въпроси?

а. Да

б. Не

ако не защо:.....
.....
.....
.....

4. Обучението обхваща ли процесите, свързани с непосредствените Ви задължения?

а. Да

б. Не

ако не защо:.....

.....

.....

.....

5. Чувствате ли се готови да работите с информационната система?

а. Да

б. Не

ако не защо:.....

.....

.....

.....

6. Можете ли самостоятелно да се справите при работата с информационната система?

а. Да

б. Не

ако не защо:.....

.....

.....

.....

.....

7. Считате ли, че с получените знания ще можете да оказвате помощ на други потребители?

а. Да

б. Не

ако не защо:.....

.....

.....

.....

8. Има ли несъответствия между логистичните процеси и реализирането им в системата?

а. Да

б. Не

ако да, кои процеси и какво е несъответствието:

.....

.....

.....

.....

.....

9. Какво бихте променили в обучението ако Вие го ръководехте и какви са препоръките Ви към екипа, провеждащ обучението?

.....

.....

.....

.....

/звание, подпис, име и фамилия/

ЛИТЕРАТУРА

1. НП на въоръжените сили на Република България. Доктрина за Логистиката в Българската армия. Министерство на отбраната, 2013.
2. Михайлов, Ж. Логистичната ИС на БА – проект без алтернатива. https://cio.bg/digitalizacia/2014/07/23/3440488_logistichnata_is_na_ba_proekt_bez_alternativa/

REFERENCES

1. NP na vaorazhenite sili na Republika Bulgaria. Doktrina za Logistikata v Balgarskata armia. Ministerstvo na otbranata, 2013.
2. Mihaylov, Zh. Logistichnata IS na BA – projekt bez alternativa. https://cio.bg/digitalizacia/2014/07/23/3440488_logistichnata_is_na_ba_proekt_bez_alternativa/

НОВИ СПОСОБНОСТИ В КОДИФИКАЦИОННИЯ ИНСТРУМЕНТ НА ИНФОРМАЦИОННА СИСТЕМА „ЛОГИСТИКА НА БЪЛГАРСКАТА АРМИЯ“

подполковник д-р Светозар Ботев

Командване за логистична поддръжка, *s.botev@armf.bg*

д-р Валя Симеонова

Командване за логистична поддръжка, *valiasimeonova_sweet@abv.bg*

Резюме: Основен елемент в системите за управление е кодификационният инструмент. Информационна система „Логистика на Българската армия“ разработва специфичен кодификационен инструмент, съчетаващ логистична и финансова информация с разнообразни възможности за търсене на номенклатури.

Ключови думи: кодификационен инструмент; възможности; логистична система; различно търсене

NEW CAPABILITIES IN THE CODIFICATION TOOL OF THE “LOGISTICS OF THE BULGARIAN ARMY” INFORMATION SYSTEM

Lieutenant Colonel Svetozar Botev, PhD

Logistic Support Command

Sofia, Bulgaria

E-mail: *s.botev@armf.bg*

Valya Simeonova, PhD

Logistic Support Command

Sofia, Bulgaria

E-mail: *valiasimeonova_sweet@abv.bg*

Abstract: The codification tool is a key element in management systems. The Information System “Logistics of the Bulgarian Army” develops a specific codification tool combining logistics and financial information with various capabilities for searching items.

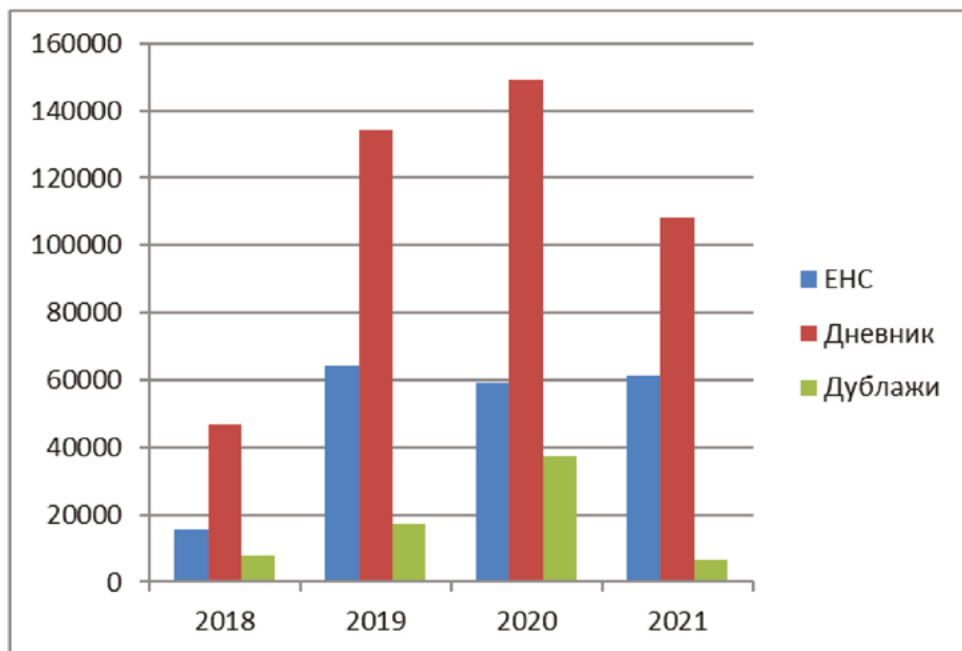
Keywords: *codification tool; capabilities; logistic system; search engine*

Информационната система за управление на финансовите и материални ресурси (ИСУФМР) е съвкупност от взаимосвързани модули попълвани от специалистите във всички военни формирования и анализирани от управлението в Министерството на отбраната (МО). Системата може да повиши нивото на ефективност в управлението и създаването на оперативна съвместимост на Министерството на отбраната и НАТО в многонационална среда и по всички деклариран мисии на Българската армия. В този смисъл ИСУФМР е проект без алтернатива за всеобхватно повишаване на оперативната съвместимост и ефективността при управление на логистичните и финансовите информационни потоци в Българската армия и МО.

В основата на ИСУФМР е собственият кодификационен инструмент, наречен Единен номенклатурен списък (ЕНС). В развитието на ИСУФМР е имало желание за използване на NATO stock number NSN, но поради липсата на финансови данни в него частично се използва в този етап на развитие. След спирането на присвояване на Единен материален код (ЕМК) с министерска заповед ОХ-1082/2001 не се използва в настоящия инструмент. За съставянето на ЕНС се използват стандарти БДС ISO ГОСТ и каталози на използваните изделия в МО.

Най-точната информация за работата на специалистите по въвеждане на ИСУФМР в реална експлоатация може да се черпи от въведените номенклатури в ЕНС. От фигура 1 се виждат въведените

номенклатури в ЕНС. Въведен брой номенклатури в ЕНС към 12.2016 г. – 242 291, 09.2021 г. – 457 975 или въведени за периода – 215 684. Начало 2018 г. – 261 125. Начало 2019 г. – 281 735, Начало 2020 г. – 346 450 и начало 2021 г. – 407 466, начало 2022 г. – 466 506. Номенклатури с NSN – 12.2016 г. – 2, 12.2021 г. – 7163 или въведени за периода – 6330. Добавени номенклатури за 2021 г. – 61 163, 2020 г. – 59 271, 2019 г. – 64 311 и 2018 г. – 15 514.



Фиг. 1. Заведени номенклатури в ЕНС през годините

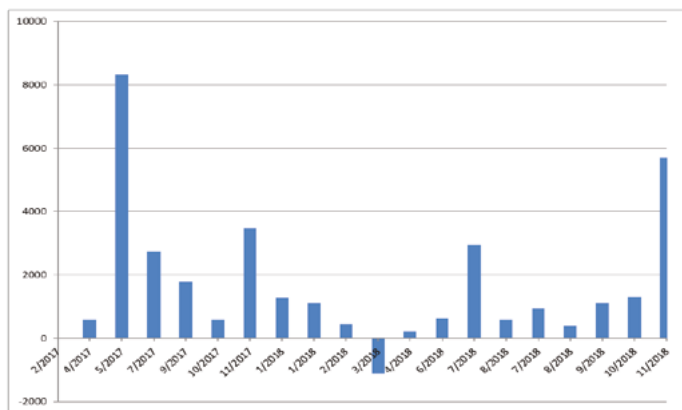
Фигура 1 показва явен ръст през 2019 г. Какви са причинно-следствените връзки и как се е случило това е описано в този доклад. Приложените данни във Фигура 1 сравняват наличните в ЕНС номенклатури, получените заявки за нови номенклатури, фигуриращи в дневника и дуближите на заявки в него. Данните показват почти дойно количество на заявените спрямо създадените номенклатури в ЕНС, което може да се обясни с подаването на заявки извън приоритизирания за периода. Дублирането на заявки в дневника основно е поради неправилно попълнени данни от потребителите, подготвящи заявките за нови номенклатури. Тези факти не изчерпват и други негативни влияния. Получените заявки за 2021 г. са 108 330 номенклатури, като има заявки които са обработвани по 4 пъти поради необходимост от детайлизираща информация. Всички обработвани по 4 пъти заявки са 6565 номенклатури. През 2021 г. въведените в търсачката номенклатури са 58 588. Очевидно е, че ако всички заявки са обработени, 55% от номенклатурите в подаваните заявки за нови номенклатури се намират в търсачката. Тук обаче остава въпросът дали този процент е обективен, има ли заявки, на които поради една или друга причина се дават номера от ЕНС, за да вървят напред формиранията с много записи.

Интересен е факта например е, че през 2020 г. от подадени 148 937 номенклатури в дневника са върнати 1073 заявки с 114 161 записа, а за 2021 г. – 629 заявки или 38 358 записа. В отчета за второто тримесечие в дневника са 626 заявки с 26 371 записа, като 21 794 са добавени в ЕНС, а общата бройка е 446 307. Не е ясно от този дневник воден в електронен вид колко от подаваните заявки за нови номенклатури са реално за нови номенклатури, имат ли дуближи или са минали по други пътища за добавяне в ЕНС. Воденият дневник дава само статистическа информация но не и реални данни за въведените в търсачката номенклатури.

Изложените в този обзор данни са детайлни и изчерпателни и отразяват реалната фактология в хода по реално въвеждане в експлоатация на системата. Авторите описват кога и как е направено при-

равняването на 3 пилотни формирования с по около 50 000 записа. Статистическите данни от водения електронен дневник показват военни формирования с 66 000 записа с подадени номенклатури през 2018 г., 19 с 3 заявки, през 2019 г. – 12 980, през 2020 – 17 с 3 заявки, 2021 – 644 с 29 заявки. Очевидно е, че са подадени приблизително 13 000 хиляди от 66 000 записа, което е 20%. През 2021 показват, че включените за въвеждане 3 пилотни формирования с по около 50 000 записа всяко са подали едва 10%. Тези факти явно показват, че или формированията се намират по-голямата си част от наличностите в ЕНС или поради подчинеността си на разнородни специалисти във видовете въоръжени сили, са пропуснати подадените от тези военни формирования заявки за нови номенклатури и се налага специалисти от звеното за въвеждане на информацията да приравнява техните наличности. Данните от електронния дневник са показателни за различните подходи за подготовката на информация за зареждане на всяко едно формирование.

Предложената статистическа информация може да породи и редица други взаимносвързани въпроси за ефективността на търсачката, ефективността на персонала при работата с търсачката, познания на персонала за съхраняваните имущества и способности за работа с наличните каталози за изделията и др. Авторите работеха целенасочено за подобряване на търсачката в името на потребителя. Постигнатите резултати са видни на фигура 2 и фигура 3.



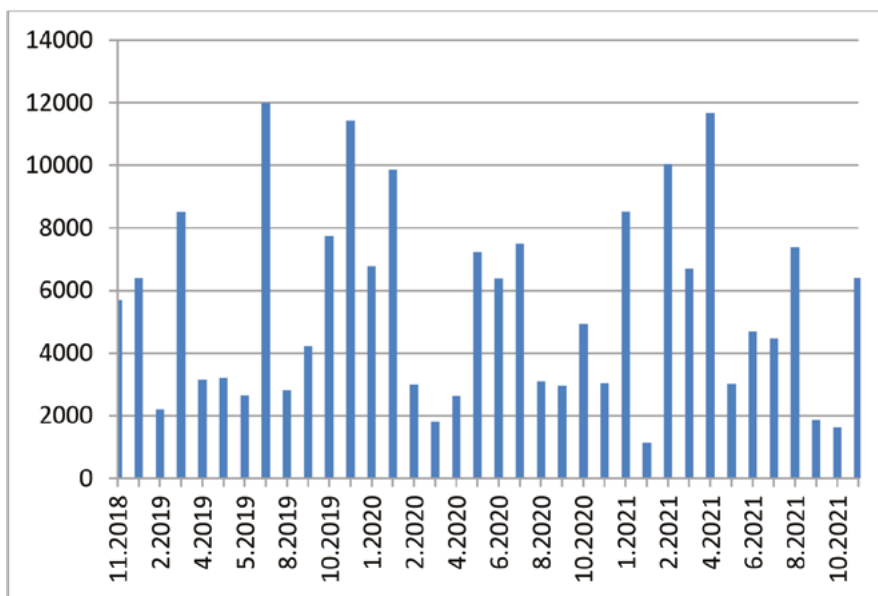
Фиг. 2. Заведени номенклатури в ЕНС през месеците на 2017 и 2018 година

Фигура 2 показва, че през 2017 и 2018 г. средномесечно се качват около 1800 номенклатури. Отрицателното количество през март 2018 година е поради некоректно заведена информация, спрени са повече от качените номенклатури. Открояващите се данни от фигура 2 са постигнати от авторите с използване на алгоритми (изкуствен интелект) за подобряване в работата по приравняването. Въпреки негативните квалификации срещу авторите от методическото ръководство на проекта постигнатите резултати са три пъти по-добри от тези на всички потребители до момента. Максимално подадените и добавените номенклатури са съответно над 8 хиляди и около 6 хиляди. Това е пет-шест пъти повече от статистическата средномесечна норма.

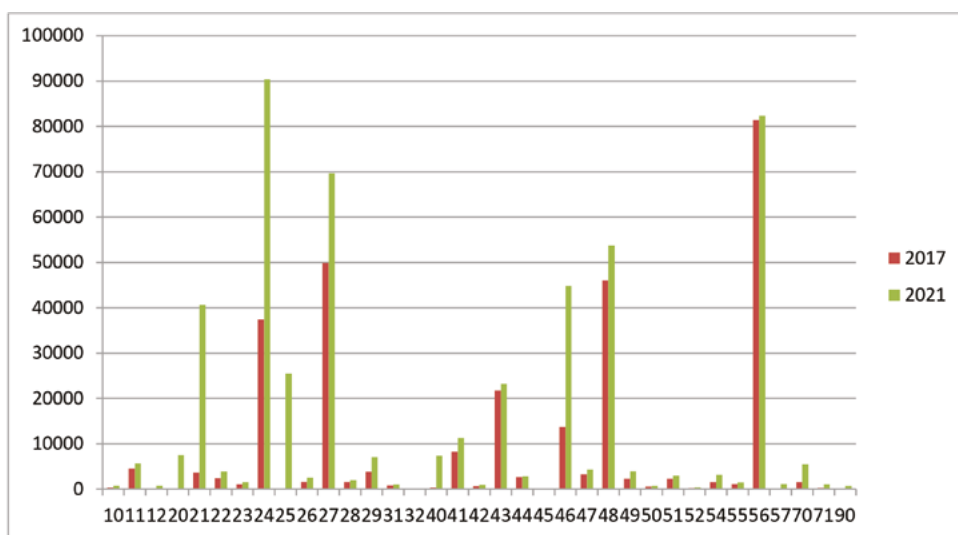
Фигура 3 показва, че през 2018 – 2021 г. средномесечно се качват около 3000 номенклатури. Пиковите стойности сочат, че кодификационният инструмент ЕНС притежава способности за добавяне месечно на до 12 хиляди записа без технически проблеми. Тези отчетени стойности не са измислени, а са реални и надхвърлят близо десетки пъти нормите при работата без предложените от автора доработки на търсещия кодификационен инструмент на системата. За подобряване работата с ЕНС по приравняването на номенклатури от потребителите авторите са описали техническите процедури с примери в инструкцията му.

Кодификационният инструмент на системата претърпя огромно развитие в способностите си и даваната информация от 2017 г. до сега. След първите шест военни формирования търсачката придоби нови способности за автоматизирано търсене по номер и име на материалните средства. Предложените и реализирани алгоритми реално се ползват и в момента от всички потребители на ЕНС. Авторите анализираха практически негативните критични точки възникнали при процеса приравняване към ЕНС от потребителите с цел автоматизиране. Ако това се бе случило по-рано и бе обяснено детайлно на по-

требителите, резултатите щяха да са по-рано на лице. Фактите показват, че специалистите от военните формирования с 66 000 записа след подобряването на търсачката от администратора по предложен алгоритъм от авторите, неприравнените номенклатури буквално за месец се стопиха наполовина само с автоматизирана обработка. Оттам дойде и другата нова функционалност, с която може да се връщат еднозначните отговори на търсачката в експортирания файл за приравняване. Все малки доработки за постигане на желанния краен резултат. Практиката показва, че за един ден един от авторите може да върне около 500 записа с обичайното копиране от търсачката и пускане във файла за приравняване. С тази малка доработка с формула за броени минути данните си намират еднозначно местата. Така се пести време на потребителя за ежедневните му дейности.



Фиг. 3. Заведени номенклатури в ЕНС през месеците на 2017 и 2018 година



Фиг. 4. Добавени номенклатури по групи от ЕНС

Друг разрез на данните показва добавените номенклатури и в кои групи са те. Фигура 4 показва че 21, 24, 25, 27, 46 са групите с най-много добавени номенклатури. В ЕНС са добавени нови групи за ВМС. Може да се даде лош пример за ефективност на наличните в 56-а група „Метал“, която има над 80 хиляди. Добавените номенклатури за периода 2018 – 2021 г. са 800, а реално се използват 1200 от тях.

Посочените данни във фигури 1, 2, 3 и 4 ясно показват, че в ЕНС се е натрупал потенциал и са създадени възможности за приравняване на повечето налични в Българската армия и МО номенклатури. Създадените доработки с участието на авторите вече допринасят за настоящите способности за реализиране на цифровизацията на финансовите и материални ресурси използвани в Министерството на отбраната.

Проблемни въпроси:

- слаба информираност на потребителите;
- бавно приравняване на наличните във в.ф. и ЕНС;
- липса на автоматизация за процеса по приравняване;
- ръчна промяна в съществуващите програми за финансово-материален отчет по места;
- осигурена е свързаност с КИС ЩИТ на Българската армия, с малка част от военните формирования, като забавя обновяването на ползваните нови версии ЕНС;
- приравняване на наличните ресурси от служители на ИСУФМР без да виждат какво точно приравняват;
- различни подходи при прехвърлянето на информацията между системите;
- директно оказаната помощ от авторите и до днес частично или изобщо не е разбрана от потребителите по места.

Положителни страни:

- концентриране на финансово материалната информация на едно място;
- придобиване на нови способности от ЕНС с цел автоматизирано приравняване на номенклатури.

ЛИТЕРАТУРА

1. НП на въоръжените сили на Република България. *Доктрина за Логистиката в Българската армия*. Министерство на отбраната, 2013.

REFERENCES

1. NP na vaorazhenite sili na Republika Bulgaria. *Doktrina za Logistikata v Bulgarskata armia*. Ministerstvo na otbranata, 2013.

РАЗВИТИЕ НА ИНФОРМАЦИОННА СИСТЕМА „ЛОГИСТИКА НА БЪЛГАРСКАТА АРМИЯ“ ДО 2021 Г.

подполковник д-р Светозар Ботев

Командване за логистична поддръжка, *s.botev@armf.bg*

д-р Валя Симеонова

Командване за логистична поддръжка, *valiasimeonova_sweet@abv.bg*

Резюме: Въведени данни в Информационна система Логистика на Българската армия за периода 2014 – 2021 година включително.

Ключови думи: въведени артикули; счетоводна система; логистична система; Българска армия

DEVELOPMENT OF THE “LOGISTICS OF THE BULGARIAN ARMY” INFORMATION SYSTEM BY 2021

Lieutenant Colonel Svetozar Botev, PhD

Logistic Support Command

Sofia, Bulgaria

E-mail: *s.botev@armf.bg*

Valya Simeonova, PhD

Logistic Support Command

Sofia, Bulgaria

E-mail: *valiasimeonova_sweet@abv.bg*

Abstract: Described are records, imported in the Bulgarian army fully integrated interoperability logistics system BILS, in the period 2014-2021.

Keywords: *imported items; account system; logistics system; Bulgarian army*

Информационната система за управление на финансовите и материалните ресурси (ИСУФМР) съществува в Доктрината за логистика на Българската армия, която е в приоритетите за развитие на всички управленски нива в Министерството на отбраната (МО) и Българската армия и е ориентирана изцяло към потребителите от логистичната система от всички нива. ИСУФМР е съвкупност от взаимосвързани модули, потъпвани от специалистите във всички военни формирования и анализирани от управлението в МО. Системата може да повиши нивото на ефективност в управлението и създаването на оперативна съвместимост на Българската армия, МО и НАТО в многонационална среда по всички декларирани мисии на Българската армия. В този смисъл ИСУФМР е проект без алтернатива за всеобхватно повишаване на оперативната съвместимост и ефективността при управление на логистичните и финансовите информационни потоци в Българската армия и МО².

Информираността в реално време по отношение на логистичните ресурси е от съществено значение за съпоставяне на „реалната логистична картина“ с планирането на ефективно логистично осигуряване и необходимия за неговото осъществяване личен състав. Опростените механизми за докладване, заявяване и отчет осигуряват точно и ефективно разпространение на информацията до всички, които се нуждаят от нея¹. Съвременното логистично управление на запасите позволява ефективно да се използват посочените системи за организиране на доставките, като ги свързва в едно цяло с интегрираната информационна система в общата логистика на Българската армия¹.

Проектът БПЛС стартира през 2003 г. и преминава през различни фази на технологично развитие до 2013 г. Със заповед на Началника на отбраната 134/30.06.2014 г. е въведена в реална експлоатация.

Служителите, работещи по реалното внедряване на ИСЛБА, се преподчиняват от стратегическо ниво – дирекция „Логистика“, към оперативното ниво през 12.2016 г. в СКС, а понастоящем от 09.2021 г. – в

Командване на логистичната поддръжка (КЛП). Ретроспекцията показва, че в първите 13 години информационната система, управляваща ресурсите в Българската армия, е разработвана от избрани специалисти в различни области, работещи с откъсване от ежедневните им задължения под ръководството със заповеди и разпореждания на дирекция „Логистика“. Работата по внедряване в реална експлоатация и свързаните с нея проблемни въпроси продължава и в момента.

Промените настъпили през 2006 година налагат промени с въведеното двустранно счетоводно записване в държавния сектор. Исторически двустранното счетоводно записване през 2006 г. се случи за три месеца, в които бяха осигурени финансови средства за компютърни конфигурации, инсталиране на софтуер и въвеждане на наличностите по военните формирования. Всичко това се случи за кратко време, а сега минават години, но данните не могат да се въведат в обща информационна система. Въпросът е основателен, но не трябва да се разглежда сяко, а да се видят натрупаните проблемни въпроси и свързаните изисквания от различни правни норми. Основен проблем, влияещ и до ден днешен, е липсата на специфичен кодификационен инструмент за въвеждане на данни без да са уеднаквени, както в оперативните отчети по видове имущества. Въведените данни в използваните счетоводни програми са фокусирани досега повече върху счетоводната част на данните, а не толкова върху логистичните детайли. Накратко казано – данните в използваните счетоводни софтуери са въведени такива, каквито ги е имало, без да бъдат кодифицирани. Така децентрализираните финансово складови модули не са свързани помежду си с единна база данни и нямат автоматизираната възможност за обобщаване на водените оперативни отчети. Поставените високи цели по два дни на 26-те пилотни военни формирования по въвеждането в реална експлоатация по писмо изготвено от дирекция „Логистика“, утвърдено от Началника на отбраната през 2014 г., така и не се реализираха на практика и до днес.

Вторият период на развитие на ИСУФМР от 12.2016 г. до 09.2021 г. е свързан с разногласия и разнопосочни мнения за хода на въвеждане в реална експлоатация, даден през 2014 г. За изминалите пет години (2017 – 2021) в реална експлоатация на ИСУФМР под управлението на Съвместно командване на силите (СКС) въвеждането вървеше със забавяне съгласно утвърдените от дирекция „Логистика“ графици. Натрупаните проблеми при разработването на системата се отразяват върху въвеждането на реални данни. Загубените години за убеждаване на оперативното и стратегическото ниво за необходимостта на точно такава система в ежедневната работа на тези звена и до момента не се е променила. Събирането на еднакви данни, така нареченото „служебно начало“, на едно място ще облекчи оперативния отчет, който специалистите по видовете имущества водят ежемесечно. Липсата на разработени справки по оперативния отчет на имущества в ИСУФМР и до днес не може да промени мнението на работещите специалисти на оперативното и стратегическо ниво към системата.

Статистически от личния опит на авторите може да се каже, че първите шест въведени от изброени военни формирования до 2019 г. включително се случиха в неясна среда както за специалистите от военните формирования, така и за хората, които въвеждахме данните. Забавянията от подаването на данните до зареждането им за първите шест изброени военни формирования беше до две години. Тези огромни забавяния могат да се обобщят, че са от обективен и субективен характер. Преди всичко неяснотата в подадените файлове за зареждане и тъкностите за достигане до желания краен резултат никой никъде не беше описал. Добри примери или фаворити сред наваксващите изоставането са в.ф. 24480 Ловеч, които за около пет месеца успяха с автоматизирани подходи да разнесат данните за две години. Всичко това се случи защото имаше специалист на точното място в точното време с необходимото и достатъчно взаимодействие.

Обучението на всички заети с въвеждане в експлоатация вървеше в движение с проби и грешки, защото никой не е тествал системата с реални данни, за да отчете проблемите, да подобри работата и в името на желаните добри крайни резултати. Натрупаният опит с първите шест формирования се използва по възможно най-добрия начин за въвеждането на следващите в.ф. – видно от фигура 2. Специалистите, водещи обучения за подготовка на данните по графика, бяха ангажирани само с тази дейност без реалната подготовка за нея. Авторите участваха в процеса по подготовката и въвеждането в реална експлоатация за първите шест въведени формирования, описани в настоящия доклад (фигура 1).

Файловете за зареждане. В началото на 2017 година никой не виждаше смисъл да има „добра производствена практика“ и въведените данни във файлове „Наличности КА“ и „Наличности ДА“ да кореспондират както с инвентаризационните описи, генерирани от ползваните счетоводни продукти, така и с техните номера с цел по-лесна работа с новия за потребителите софтуер. Това е предпоставка за намаляване на възможността за допускане на субективни грешки при разнасяне на стопанските операции в системата. В началото 2018 г. за файловете все още нямаше ясна визия кое, как и в каква форма да бъде попълвано. Реалните подобрения настъпиха след анализ на всичко случило се преди това, по предложе-

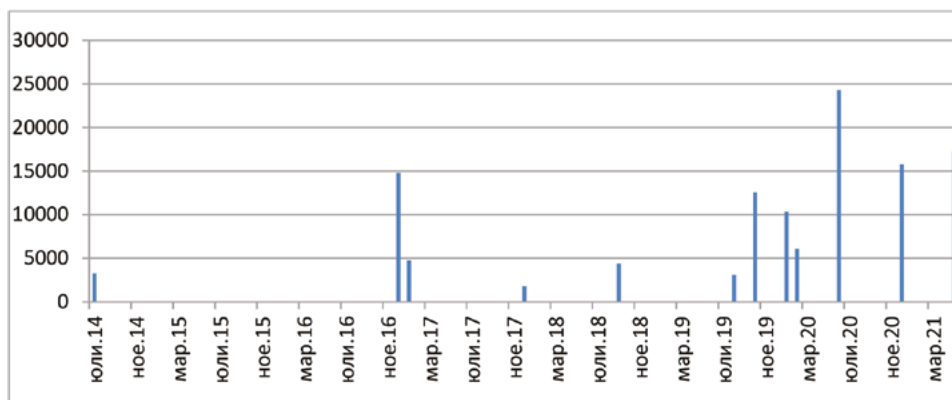
ние на авторите се добавиха синтезирани указания за постигане на желания краен резултат. Добавиха се указания за работа с файла, формализираха се полетата и за да може коректно да се въвеждат данните от ЕНС и логистичните характеристики водени в оперативните отчети. През 2021 г. файловете за зареждане на наличности вече получиха и вграден ЕНС. Стигна се до там празен файл „Наличности КА и ДА“ да е с размер от 25 мегабайта и при 100 склада общото им количество надхвърля 2,5 гигабайта. Специално внимание се отдели на „Наличности ДА“ за 46 група, поради изискването на закона за счетоводството.

След условно наречения „успех“, се поляризира сектор на двете крайности: едната – въвеждане на всяка цена без логистични данни, и втората – желание за максимално попълване на логистична информация. Това доведе до настоящите резултати. Специалистите от щабвете не използват данните, които са въведени в системата. Справка за активността на потребителите, които са специалисти по видовете имущества от в.ф. 48960 показва, че не влизат в системата, за да черпят информация от нея. Тук също може да има разклонение на различни полюси, като единият е „няма информация за нас“, а другият е „няма справки от срочните отчетни донесения“ и др. Бавното реализиране на формите генерирани ежедневни документи по приходно-разходните стопански записвания в ИСУФМР обезверяват потребителите от тактическите нива, с което намаляват и увереността, че е възможна автоматизирана обработка. Добавянето на МОЛ без модификация в модул „Склад“ доведе до връщане в изходно положение на разработените ежедневни приходно-разходни документи.

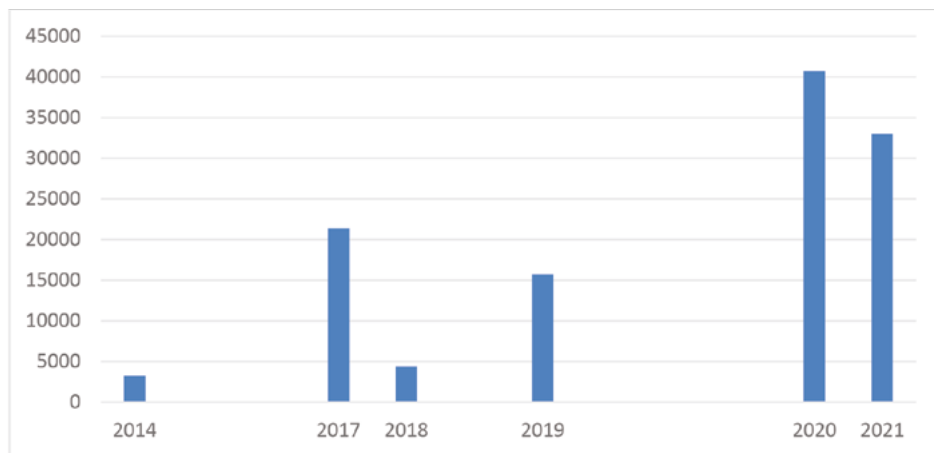
Практиката до момента показва, че няма проведена пълна инвентаризация и до сега в системата при положение, че в.ф. 24510 София работи от 05.2014 г. Това са само факти и всеки ги интерпретира по възможно най-добрия начин без естествено да иска мнението на потребителите реално работещи със системата. Необходимо е да бъде споменато, че въвеждането на събраната информация от първите шест военни формирования беше в неясна среда и заложените финансови данни от използвания софтуер трудно се постигаха. При всяко зареждане се търсеше равнение на някоя натрупана стотинка в повече или по-малко. Дали поради незнание или невнимание в началото прости на хартия изисквания се реализираха бавно и с много усилия на администратора и подготвили данните. С течение на времето и след поредица тестове добрите резултати не закъсняха. Техническата нередност при въвеждане на данните за счетоводно изравняване на сумите по сметки бе констатирана от автора и отстранена от администратора. Следващите въведени военни формирования за периода 2020 г. и 2021 г. от специалистите водели обучения във военни формирования ползваха наготово натрупания опит от авторите (виж фигура 1 и 2). Практиката отново доказва необходимост от съчетаване на специалисти с логистична, счетоводна и кибер насоченост за постигане на желания краен резултат.

В момента ИСУФМР има въведени дванадесет военни формирования, работещи само с нея без друг софтуер. ИСУФМР има потенциал да предостави ефективно решение за осъществяване на принципа на „Служебното начало“, състоящ се в еднократно събиране и многократно използване на информацията в цялата йерархия на Българската армия и МО. На този етап от развитието на ИСУФМР „Служебното начало“ е залегнало за въведените военни формирования и частично при автоматизираното обобщаване на данни.

Постигнати резултати за пет години за периода 2017 до 2021 година.

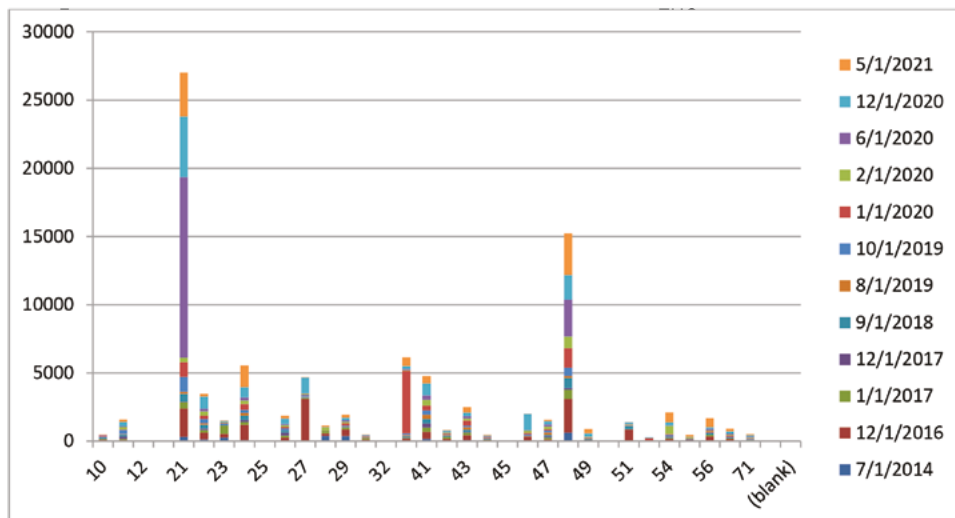


Фиг. 1. Въведен брой записи във ИСПБА съгласно датата за зареждане



Фиг. 2. Въведен брой записи във ИСЛБА

Фигура 1 и 2 показват, че за периода от 2014 г. до 2017 г. е имало застой във въвеждането на данни в ИСЛБА. За периода от 2017 г. до 2019 г. средно въвежданите на година записи във ИСЛБА са около 15 000. Поставената добра основа и изясняване на подробностите по въвеждане от авторите през периода от 2017 г. до 2019 г. се използва от други специалисти за постигане на резултатите в периода от 2020 г. до 2021 г., със средно 35 000 на година. Може да се обобщи, че в началото на 2022 година записите в ИСЛБА са около 120 000, които са 57 000 номенклатури.



Фиг. 3. Заредени номенклатури в БПЛС по групи от ЕНС

Интересно впечатление прави, че резервните части от група 21 от налични в ЕНС около 40 000 общо са въведени 25 хиляди. 24 група от 90 000 общо в ЕНС се използват около 6000. 27 група с около 70 000 общо в ЕНС се използват около 4500. 43 група от 22 000 общо в ЕНС се използват 2500. 46 група от 45 000 общо се използват около 2000. 48 група в ЕНС 53 000 общо се използват 15 000. 56 група в ЕНС 80 000 общо се използват 1200. От наличните в ЕНС 466 506 номенклатури към януари 2022 година се използват около 57 000 номенклатури, което е около 9% от общия брой номенклатури.

Посочените данни във фигура 1, 2 и 3 ясно показват, че в ЕНС се е натрупал потенциал и са създадени възможности за приравняване на повечето налични в Българската армия и МО номенклатури. Създадените доработки с участието на авторите вече допринасят за настоящите способности за реализиране на цифровизацията на финансовите и материалните ресурси, използвани в МО.

Проблемни въпроси:

- неясна среда. Какво точно, къде точно, каква точно информация да се въведе в ИСУФМР;
- липса на съответно популяризиране на предлаганите услуги от ИСУФМР и произтичащата от това слаба информираност на служителите, използващи въведената логистична и финансова информация;
- липса на йерархичен оперативен отчет по различни класове материални средства в ИСУФМР;
- слаба заинтересованост на всички нива на управление от данните, въведени в йерархичната структура на ИСУФМР.

Положителни страни:

- ползване и предоставяне на електронни услуги на потребителите в системата;
- концентриране на финансово материалната информация на едно място;
- възможност за обобщаване на огромен обем от информация. Разработване на модификации, обслужващи най-тежките звена, периодично обобщаващи движението както на финансови, така и на материални ресурси;
- възможност за автоматизирано търсене на наличните номенклатури „Приравняване“;
- възможност за автоматично изваждане на данни от ЕНС;
- анализиране и управление на логистичните и финансовите потоци;
- управление чрез съчетаване на специалисти с логистична, счетоводна и кибер насоченост за постигане на желания краен резултат;
- различни подходи при прехвърлянето на информацията между системите за постигане на желания краен резултат.

Насоки за развитие:

- използване на принципа за „Служебното начало“;
- изграждане на комуникационни канали към всички потребители;
- въвеждане на повече логистични данни свързани с оперативния отчет;
- автоматизиран оперативен отчет от всички управленски нива.

ЛИТЕРАТУРА

1. Димитров, М. и др. *Военна логистика. Основи на военната логистика, първа част*. София: Военна академия „Г. С. Раковски“, 2017.
2. НП на въоръжените сили на Република България. *Доктрина за Логистиката в Българската армия*. Министерство на отбраната, 2013.

REFERENCES

1. Dimitrov, M. et al. *Voenna logistika. Osnovi na voennata logistika, parva chast*. Sofia: Voenna akademiya „G. S. Rakovski“, 2017.
2. NP na vaorazhenite sili na Republika Bulgaria. *Doktrina za Logistikata v Balgarskata armia*. Ministerstvo na otbranata, 2013.

ПРЕДПОСТАВКИ ЗА ТРАНСФОРМАЦИИТЕ НА ВОЕННА АКАДЕМИЯ „Г. С. РАКОВСКИ“ В ПЕРИОДА 1944 – 2001 – РЕТРОСПЕКЦИЯ С ПОГЛЕД КЪМ БЪДЕЩЕТО

полковник проф. д-р Емил Енев
Военна академия „Г. С. Раковски“, e.enev@rndc.bg

Резюме: В следвоенното развитие на българската армия условно се очертават три основни периода, които са обвързани с три основни световни събития – края на Втората световна война, Блоковото противопоставяне и създаването на двата военно-политически съюза (Варшавския договор и НАТО) и третият – края на Студената война, 1990 година. Тази периодизация съпада с периодите на развитие на Българската народна армия и Българската армия, като неин приемник след 1991 година. Съвсем естествено е развитието на структурите на Военната академия и нейните образователни способности да са изцяло свързани с развитието на въоръжените сили на страната.

Дали това е единствената причина и какво бъдеще ни очаква?

Ключови думи: образование; обществено развитие; строителство на въоръжените сили; свързаност

PREREQUISITES FOR TRANSFORMATIONS OF THE MILITARY ACADEMY “G. S. RAKOVSKI” IN THE PERIOD 1944 – 2001 – RETROSPECTION WITH A LOOK AT THE FUTURE

Colonel Prof. Emil Enev, PhD
Rakovski National Defence College
Sofia, Bulgaria
E-mail: e.enev@rndc.bg

Abstract: In the period of post-war development of the Bulgarian army, there are three key periods that are outlined. They are tied to three large-scale world events – the end of World War II, the opposition of NATO and the Organization of Warsaw pact, such as military-political alliances, and the third – the end of the Cold War 1990. This periodization determines the periods of development of the Bulgarian National Army and the Bulgarian Army as its successor since 1991. It is quite natural for the development of the Structures of the Military Academy and its educational abilities to be fully related to the development of the country's armed forces. Is this the only reason why we expect us?

Keywords: education; public development; construction of armed forces; connectivity

Политически предпоставки

Годината е 1931. Успоредно с изучаваната до момента в Преподавателския курс генералшабна специалност започва усвояването на нова специалност с еднаква продължителност на обучение – три години. В Академията се оформят два самостоятелни отдела – Генералшабен от 1931 г. и Интендантски от 1935 г., и във всеки от тях се води съответното обучение на висше тактическо и оперативно ниво. Съгласно Държавен вестник, брой 224 от 24.IX, Закон за висшето образование от 1948 г. отделът е основно звено, което може да бъде приравнено на сегашен департамент. До 1944 г. в тях завършват обучението си 521 офицери¹.

В следвоенното развитие на Българската армия условно се очертават три основни периода, които са обвързани с три основни световни събития – края на Втората световна война, блоковото противопоставяне и създаването на двата военнополитически съюза (Варшавският договор и НАТО) и третият – края на Студената война през 1990 година. Тази периодизация съпада с периодите на развитие на Българската народна армия и Българската армия, като неин приемник след 1991 година. Съвсем естествено е разви-

¹ Петров Тодор и други. Военна академия „Г. С. Раковски“. ISBN 978-619-7478-20-4, стр. 12.

тието на структурите на Военна академия и техните образователни способности да са изцяло зависими от развитието на въоръжените сили на страната.

През първия следвоенен период – 1945 – 1955 г. във Военна академия „Г. С. Раковски“ се извършват редица структурни и организационни промени. Приетият през 1951 г. Правилник на академията напълно отговаря на повишените изисквания и задачите, които МНО поставя пред нея. Учебният процес и цялостният ред в академията значително се изменят и в тях широко навлизат съветските методи на обучение и възпитание. Научно-изследователската работа е поставена на планова основа. По този начин новите задачи, стоящи пред БНА и пред академията, както и огромната работа, която се извършва, довеждат до нейното по-нататъшно развитие. Полагат се основите и се развива структурата на основния и заочния факултет. Създава се новата структура и се прецизира постепенно предметът на дейност на катедрите, които в последствие заедно факултетите ще се слепят в единна структура.

Първият период от историята на основните структури в Академията, предшественици на факултет „Командно-щабен“ от края на Втората световна война до 1955 г., когато България става член на Варшавския договор, се характеризира с приваждането на армията в съответствие с изискванията на Парижкия мирен договор. В рамките на този период се очертават два етапа. Първи – 1945 – 1948, когато армията се превръща в инструмент на отечественофронтовската власт. Втори 1949 – 1955, когато се усвоява опитът от Втората световна война и се възприема съветския модел на военното строителство, военната наука и изкуство. Ето неговите по-характерни особености, които се отразяват непосредствено на тенденциите в развитието на военното образование и основните звена на Военна академия „Г. С. Раковски“.

Настъпилите драматични промени в Европа след Втората Световна война не подминават и България. На 10 февруари 1947 г. в Париж е подписан договор за мир между България и Съюзените и Сдружени сили. Договорът де факто за първи път в нашата военна история обособява четири вида въоръжени сили.

В годините на Студената война се осъществяват значителни организационни и структурни промени, които се изразяват главно в създаване на нови управленски и обучаващи звена, промени в сроковете на обучението, увеличаване на личния състав и други. Събитията започват да добиват реални измерения от пролетта на 1949 година, когато войските не само формално са преименувани в Сухопътни войски, Военновъздушни сили, зенитна артилерия, Военноморски флот. Нараства необходимостта от кадри във връзка с превъоръжаването на армията с нова съветска материална част и техника. Това е едно от условията, които налагат приспособяването на структурата на Академията към реструктурирането на войската. Източноевропейските армии стават „народни армии“, което освен идеологически има конкретен политически смисъл.

До 1954 съветизацията на източноевропейските армии е завършена. Още в първите месеци на съветската окупация висшето армейско командване е подменено с комунистически кадри и е извършена чистка в офицерския корпус, а до средата на 50-те офицерският състав е изцяло заменен с кадри, отговарящи на критерия за политическа лоялност и подходящ класов произход. Прочистването на образователната система от старите буржоазни и фашистки елементи не може да подмине и военното образование. Това може да стане единствено посредством въвеждане на нови нормативно-правни документи, които налагат създаване на нови структури и подмяната на неблагонадеждния за новата власт академичен състав. И това се случва, посредством постепенната промяна в законовата рамка.

Нормативни причини

Технологията на промяна на структурата и функциите на органите за ръководство, командване и управление на войската е много ярко изразена с промяната на нормативната база. Това явление в последствие рефлектира и върху структурата и задачите, които трябва да изпълнява Военна академия „Г. С. Раковски“ и нейните академични звена. Процесът стартира незабавно след края на Втората световна война. Това става паралелно с промените по политически причини. На 5 юли 1947 г. в бр. 153 на Държавен вестник е обнародван първият общообхватен закон посветен на висшето образование. За първи път се приема подобен закон, който изцяло и детайлно да урежда висшето образование в България. Откриване на нови ВУЗ, факултети, отдели, специалности, катедри става задължително със закон. Със закона се урежда статута на висшите училища, те са държавни. Структурата на ВУЗ се обуславя от факултети, отдели, специалности. На 24 септември 1948 г. в Държавен вестник е обнародван 2-рият закон за висшето образование, година след първия. В него се дава изключителна власт на председателя на КНИК върху висшите училища. Именно председателят на комитета утвърждава чрез правилници устройството на ви-

сите учебни заведения. Пак той утвърждава избраните от общите събрания на ВУЗ ректори и заместник-ректори. Мандатът на ръководствата вече е тригодишен.

С оглед на спогодбите и задълженията на Парижкия договор от 1947 г. през 1949 г. се приема нова нормативна база, свързана с функционирането на въоръжените сили.

В този период подготовката на командни и щабли специалисти за съединенията и обединенията до 1951 г. се осъществява основно във Военната академия. Независимо от материалните лишения започва бързо нарастване на промените на образователната система. Целта е тя да се превърне по подобие на съветската. Към момента на посочените законови промени обучението във Военна академия се извършва в два отдела. Двамата отдела, в които се обучават слушатели, Оперативен и Снабдителен (преименувани от Генерал-щабен и Интендантски) съществуват до 27.09.1950 г. Те са съчетавали функциите на академични и административни звена. Управлението на академичните структури е смесено.

През лятото на 1948 г. с доклад до Министерски съвет Карло Луканов (От септември 1945 г. Карло Луканов е член на комисията по управлението в ЦК на БРП (к.)). От 1945 до 1946 г. е директор на Българското радио в София. След това е подпредседател на Държавната планова комисия (1947 – 1949) и същевременно от януари 1948 г. е подпредседател на Комитета за наука, изкуство и култура. През 1949 г. става председател на КНИК, а от 5 декември 1949 до 28 февруари 1952 г. е и на Държавната планова комисия. Бил е заместник-председател на Министерския съвет през периода 1952 – 1954 г.) предлага да се въведе заочна форма на обучение, която да влезе в сила още през учебната 1949 – 1950 г. Заочното обучение се налага от факта, че след 9 септември 1944 г. във висшите училища се приемат голям брой студенти. Голяма част от тях са от бедни семейства и се налага самите те да работят, за да могат да се издържат. Това обстоятелство води до тяхното нередовно участие в учебния процес. Така вече всички, които не могат да учат висше образование редовно, ще бъдат прехвърлени в заочната форма на обучение.²

Този документ идва тъкмо навреме и за ръководството на войската, където кадровите проблеми с комплектуване на войската с офицерски състав се задълбочават.

Реакцията на ръководствата на Министерството на отбраната и на Военната академия „Г. С. Раковски“ не закъсняват. Те са точно в основната насока на действие, предложена от Карло Луканов. С нея от 01.01.1949 г. към Военната академия „Г. С. Раковски“, се формира „Заочен факултет“ със следните задачи: да подготвя офицери с висока военна квалификация за дейна и отговорна служба в щабовете (оперативни и тилови) на съединения, частите и родовете войски, както и за попълване на Генералния щаб (ГЩ) и Тила на войската с щабни работници (началници на секции и отделения). През зимния период факултетът следва да получава от учебното отделение на Академията необходимите за обучение на слушателите учебни документи (записки, списъци, тактически задачи) и да ги изпраща на слушателите за самоподготовката им. През летния семестър под ръководството на началника на първи курс следва да се провежда теоретическата и практическата подготовка и изпитите на слушателите.

Действията – документи и факти

Реакциите на ръководствата на Министерството на отбраната и на Военната академия „Г. С. Раковски“ следват политическите събития. Със заповед 687 от 23.11.1948 г. министърът на народната отбрана обявява инструкция за организацията и дейността на Заочния факултет.

Това е първата стъпка към реструктурирането на Академията в съответствие с новоразработената нормативна база, свързана с висшето образование и отбраната на страната.

Паралелно с катедрите, през месец март 1949 година, Заочният факултет официално е формиран със заповед 16 от март 1949 г.³ на началника на Военна академия ген. м-р Кръстев. На 16.06.1950 г. в своя заповед № 300 министърът на народната отбрана определя реда и изискванията за приемане на слушателите първи курс на Военната академия „Г. С. Раковски“⁴. В края на месец август 1950 г. под входящ № 1896 в Академията е получено служебно писмо № 3321 от 28 август 1950 г. на Организационно-мобилизационния отдел на Министерството на народната отбрана (МНО) за прилагане на новия щат на Академията за 1950 г. Съгласно него се създава нова щатно-длъжностна организация на Военна академия „Г. С. Раковски“.

² Доклад от Карло Луканов, ЦДА, Ф. 143, о. 2, а. е. 6, л. 36, 37, 38.

³ ЦВА, Ф 1517, О – I, Д 26, стр. 40.

⁴ Библиотека на Военна академия „Г. С. Раковски“, МЗ, П 943, стр. 220-222.

Така организационно приключва подготовката за закриването на Оперативен и Интендантски отдел и формирането на новите структури, факултети, отговарящи на изискванията на обнародвания на 24 септември 1948 г. в Държавен вестник⁵ Закон за висшето образование. Настъпил е моментът за централизиране на администрирането, ръководството и управлението на новосъздадените факултети.

Ефектите

На 27 септември 1950 г. е издадена Заповед № 201 на началника на Академията генерал-майор Асен Кръстев за подчинеността, дисциплината и вътрешния ред. Тя е разработена в изпълнение на служебно писмо № 3321 от 28 август 1950 г. Това е заповедта, с която началникът на Основния факултет става заместник-началник по строевата част на Академията, а в негово подчинение преминава и заочния факултет.

В началото на своето съществуване във Военна академия звеното „факултет“ е предназначено основно за ръководене и администриране на слушателския състав. За разлика от факултетите на другите, цивилни учебни заведения, академичните факултети не включват в състава си катедри като академични звена. Наред с укрепването на материалната база тече и смяна на кадровия офицерски състав – за решаване на проблема с кадрите на 17.03.1950 г. е прието постановление на ЦК на БКП за състоянието, обучението и възпитанието на Народната войска. С него към съществуващите три военни училища се създават още осем, а освен Военна академия „Г. С. Раковски“ от 1951 г. се разкриват и военно-техническата и военно-политическата академия. Основание за това е и Постановление П – 73 от 25.01.1951 г. на Министерския съвет. Срокът на обучението в академията се намалява от три на две години с цел по-бързо попълване на офицерския състав и покриване на некомплектите в оперативнотактическите звена.

В отговор на тези нарастващи потребности на 01 юли 1951 г. едновременно с Военна академия „Г. С. Раковски“ започват да функционират още две академии – Военнополитическа и Военнотехническа. Следва период на пренасочване, 1951 – 1954, през който съставът на катедрите от Военна академия „Г. С. Раковски“ основно преминава към Военно-техническа академия. Ето как в годините и времето се развиват тези процеси.

1951 г. – Висша военна академия „Г. С. Раковски“.

На 23.05.1951 г. със заповед на началника на Военна академия № 149⁶ академичният състав се преназначават и се извършва промяна на длъжностите по щата.

1951 г. – Военнотехническа академия.

На 12 декември 1951 година, към Авиационния факултет на Военнотехническата Академия (ВТА) с вътрешна заповед се създават катедри под името „Тактика на ВВС и шурманска подготовка“, катедра „Бронетанкова и автомобилна техника“, катедра „Инженерно-артилерийска“, катедра „Тил“.

През 1951 г. при формирането на Военнотехническата академия катедра „Тил“ се включва в състава на новосъздадената академия. Към Военна академия „Г. С. Раковски“ остава само група от четирима преподаватели по тилово осигуряване на войските от Българската армия.

1952 г. – Висша военна академия „Г. С. Раковски“.

През 1952 година се формират нови катедри, с което структурата на академията се обогатява и утвърждава. Този извод е направен в заповед № 67/27.02.1952 г. по повод на извършена проверка от МНО на 28 и 29 януари същата година. За учебната 1952 година се обособяват катедрите „Щабна служба“, „История на военното изкуство и войните“, „Чужди езици“.

1952 г. – Военнотехническа академия.

През 1952 година към артилерийския факултет на Военнотехническата академия е включено и първото класно отделение със зенитен профил за подготовка на командно-щабни офицери за нуждите на щабове на ПВО и зенитните части. За обучението му са назначени преподаватели в състава на катедра „Земна артилерия“. Класни отделения със зенитен профил постъпват всяка година, като започва обучение на офицери в академичен курс.

1953 г. – Висша военна академия „Г. С. Раковски“.

Развитието на научната работа е направлението, което бележи тази година за военнообразователната система. През 1953 г. са определени условията за следване и обучение на адюнктите.

⁵ Държавен вестник, брой 224 от 24.IX 1948.

⁶ ЦВА, Ф 1517, О – I, Д 669, стр. 53-59.

1953 г. – Военнотехническа академия.

Основните събитие извън рутинната дейност тук са свързани с катедра „Тил“. През 1953 г. към катедра „Тил“ се открива редовна аспирантура с две щатни места за редовни адюнкти (аспиранти, докторанти).

1954 година – Висша военна академия „Г. С. Раковски“.

Със заповед № ОК-06/01.02.1954 г. на началника на Висшата военна академия „Г. С. Раковски“ се обявява випускът на слушателите завършили основния и задочния факултети на Висшата военна академия „Г. С. Раковски“ през 1954 г., както следва: А. Основен факултет. Б. Задочен факултет.

През 1954 година с Протокол № 13/18.05.1954 г. на заседанието на президиума при МНО са взети решения при следния

Дневен ред:

1. Разглеждане въпроса за срока на обучението и реорганизацията на ВУЗ.

Накрая министъра на народната отбрана даде следните указания:

1. Всички военни училища и военни академии да имат три годишен срок на обучение, с изключение на Народното военно пехотно училище „Васил Левски“ и Интендантското училище, а Военноморското училище да има четиригодишен срок на обучение.

8. Висшата военна академия „Г. С. Раковски“ да се преименува на Военна академия „Г. С. Раковски“.⁷

В резултат на тези решения следва Заповед № 00168/19.07.1954 г. на министъра на народната отбрана⁸

Съдържание: Увеличаване на срока на подготовката и реорганизация на военните училища и военните академии в Българската народна армия.

1. Начиная от началото на учебната 1954/1955 г. военните училища и академии да преминат на нормален срок на обучение, както следва:

– Народното военноморско училище „Н. Й. Вапцаров“ и задочните факултети при академиите – **4 години**, а всички останали училища и академии в БНА – **на срок от 3 години**.

2. Поради това, че във ВВА „Г. С. Раковски“ се приемат офицери без завършено висше военно образование и се преминава общовойскова програма, която не е разчетена на втора степен на висше военно образование, за напред тя да се именува **Общовойскова военна академия „Г. С. Раковски“**.

В края на 1955 година Военнополитическата академия прекратява своето съществуване и се влива в състава на Военна академия „Г. С. Раковски“.

През втория период на своето следвоенно развитие – 14.05.1955 до 1991 г. Българската армия е част от Обединените въоръжени сили на Варшавския договор. Този период включва в себе си три етапа от развитието на Българската армия (1955 – 1960; 1961 – 1985; 1985 – 1991)

Първият етап, 1955 – 1960, се характеризира с това, че Българската армия се изгражда на основата на разбирането на факта, че ядреното оръжие е много по-мощно от конвенционалните средства за огнево въздействие.

Това развитие не спира и в периода 1956 – 1960 г. През 1956 г. се разформира факултет „Тилов“ на Военно-техническата академия. През 1957 г. катедра „Инженерно-експлоатационна“ се прехвърля към новосъздадения факултет „Бронетанкова и автотракторна техника“ на Военно-техническата академия. Постепенно процесите на превъоръжаване приключват. За времето на своето функциониране, 1951 – 1958 г., Военнотехническата академия изпълнява мисията си за подготовка на военно-инженерни кадри. От есента на 1958 година Военна академия „Г. С. Раковски“ става единен и единствен център за подготовката на квалифицирани командни, инженерно-технически и политически офицерски кадри. Военно-техническата академия е разформирована и се влива във Военната академия. Започват процесите на реструктуриране на катедри и преподавателски състав, които да дават необходимите знания и умения на командния и инженерния състав от тактическите, оперативно-тактическите и оперативните звена на командната верига на Българската народна армия.

Със заповед №00544/1.07.1958 година на началника на ГЩ на Българската армия е обявено разформироване на Военно-техническата академия и сливането ѝ с Военна академия „Г. С. Раковски“.

Сливането на двете академии, реструктурирането на катедрите и съвместяването на способ-

⁷ ЦВА, Ф 1517, О – I, Д 669, стр. 62.

⁸ ЦВА, Ф 1517, О – I, Д 754, стр. 221-225.

ности не преминава безпрепятствено. На 07.04.1959 г. началникът на Военната академия (ген. лейт. Славчо Трънски) прави доклад до Началника на ГЩ за насоките на висшето военно образование и дисциплините, които следва да се изучават в Академията⁹. В доклада се посочва, че бързото развитие на науката и появата на нови по-усъвършенствани оръжия и техника налагат не само изменения в организацията на войските и способите за воюване, но и във военното обучение и възпитание. Измененията се отнасят преди всичко до изучаването на нови дисциплини, тясно свързани с новите оръжия и техника, и промяна на тематиката на някои от досега изучаваните с цел повишаване на техническата култура на офицера и да се засили специалната му подготовка. Като основни недостатъци се посочват:

- Липса на координация и приемственост в обучението и възпитанието във военните училища и Военната академия. Тоест съществува повторение на тематиката на по-рано изучения материал във военните училища.

- В програмите на Военната академия не се предвижда изучаването на някои нови дисциплини като висша математика, атомна физика, радиохимия, механика, електроника, радиотехника, ракетна техника и др. Едновременно с това се предлага да отпаднат дисциплини като топография, стрелково оръжие, законознание, физическа подготовка и др.

- Ниско ниво на преподаването по някои дисциплини.

- Начин на приемането на слушателите – приемат се офицери без средно образование, без завършено ВВУ. Кандидатстват малък брой състезатели за едно място. Предложено е да се осигурят да кандидатстват за едно място не по-малко от трима кандидати.

- Претовареността на учебните планове и програми, многото предмети, големият обем от материал, стремежът да се даде от всичко по малко. Като основна задача на Академията е да даде на офицерите широки теоретически познания и метод за решаването на най-различни въпроси, задачи и проблеми, а не да им даде практика. Практиката ще я добият във войските.

- Структурата на учебната година не е напълно издържана поради необходимостта завършилите да постъпват в частите към 1 ноември.

За преподавателския състав се въвеждат следните длъжности, звания и степени:

- асистиенти – които да ръководят упражненията и занятията;

- преподаватели – изнасят лекциите;

- заместник-началник на катедра, началник на катедра и началник на факултет (доцент или професор) – изнасят основни лекции.

Премахват се зачетите и се въвеждат изпити за всички дисциплини.

Дава се предложение за съставяне на единно ръководство (правилник) за целия учебен процес на висшето военно образование. Определят се и дисциплините за изучаване и профилирането им.

На 13 януари 1961 год. Началникът на Военна академия генерал-лейтенант Трънски, със свой доклад до Началника на Генералния щаб – МНО, прави няколко предложения, относно реорганизацията на факултетите в Академията¹⁰. Това води до промени, при които катедрите влизат в състава на факултети и в подчинение на началниците на факултети. След тази структурна реформа академията и факултетите „Команден“ и „Инженерен“ преминават към следващото си качествено ниво.

Усъвършенстването

Вторият етап е в периода 1961 – 1985 г., когато господства схващането, че ядреното оръжие е главното средство за воюване. През този период военно-образователната система продължава да се усъвършенства. Съставът на факултетите на академията продължава да се сменя. Това се извършва на базата на оценките, анализите и потребностите на БНА, Генералния щаб и ръководството на Военна академия „Г. С. Раковски“.

През месец май 1961 г. началникът на Генералния щаб на БНА изготвя доклад до министъра на народната отбрана относно организационната структура, състав и задачите на ВУЗ от сухопътните войски¹¹. Докладът като цяло съдържа основно информация, отнасяща се към реорганизиране на военните училища. По отношение на Военна академия се предлага следното:

⁹ ЦВА, Ф 3 О – I, Д 122, стр. 1-29.

¹⁰ ЦВА, Ф 25 О – VIII-а, Д 177, стр. 18-21.

¹¹ ЦВА, Ф 25 О – VIII-а, Д 177, стр. 345-347.

– Военната академия „Г. С. Раковски“ да се реорганизира от пет факултета (общовойскови, политически, артилерийски, автобронетанков и въздушен) и четири общоакадемични катедри (общообразователна, езици, общотехническа и радиорелейна) в три факултета (команден, политически и инженерен) и две общоакадемични катедри (общообразователна и езици);

– във военната академия „Г. С. Раковски“ да не се приемат слушатели за инженерните профили.

През месец юни на 1961 г. Началникът на Генералния щаб на БНА генерал-лейтенант Врачев изготвя друг доклад (вероятно отново до министъра на народната отбрана), който конкретно засяга реорганизирането на Военна академия „Г. С. Раковски“¹². В доклада се засягат два основни въпроса: единият е свързан с реструктурирането на Академията, като изтъкнатите съображения са като тези посочени в доклада на началника на Академията от миналата година. Предлага се Военната академия „Г. С. Раковски“ да се реорганизира от пет факултета (общовойскови, политически, артилерийски, автобронетанков и въздушен) и четири общоакадемични катедри (общообразователна, езици, общотехническа и радиоелектроника) в три факултета (команден, политически и инженерен) и две общоакадемични катедри (общообразователна и езици).

Вторият въпрос засяга броя на слушателите, като се предлага той да бъде намален. Като мотив за това се посочва проведената през 1960/61 год. реорганизация на БНА, която води до съкращаване на 13 полка и отделни батальони (дивизиони).

През месец април 1962 г. началникът на Генералния щаб, генерал-майор Семерджиев, изготвя доклад до министъра на народната отбрана, относно изменения в организацията на ВУЗ и подготовката на офицерски кадри. Този доклад засяга основно реорганизацията в дейността на военните училища.¹³

През 1961 година от Президиума на МНО е взето решение да се съкрати инженерния факултет в Академия „Г. С. Раковски“, да престане да съществува от 1962 г. и по този начин Академия „Г. С. Раковски“ да остане с два факултета – оперативно-тактически и политически. За техническата подготовка на слушателите от двата факултета да се оставят минимално необходимата учебно-материална база и преподавателски състав, а излишните да се прехвърлят в училищата.

На 30 април 1963 г. е издадена заповед на Министъра на народната отбрана на НРБ генерал-полковник Джуров под номер 0131 относно реорганизацията на висшите военни училища и Военна академия „Г. С. Раковски“¹⁴.

През втория период на развитие на военнообразователната система, 1955 – 1964 г., се реализира окрупняването ѝ посредством поэтапно обединяване на военните училища и на академиите и отново се увеличава срокът на обучение. Структурата на Военна академия „Г. С. Раковски“ остава непроменена, с два факултета – оперативно-тактически и политически.

За голямо наше съжаление, достоверните исторически източници и оригиналните писмени документи, с които успяхме да се сдобием приключват на времевия рубеж 1976 – 1977.

Третият период 1986 – 1991, който се характеризира с промените в армиите на страните, членки от Варшавския договор, отговарящи на постановките на Единната отбранителна доктрина на Варшавския договор, паритет в ядрените потенциали на двата противопоставящи се военнополитически блока и премахване на тактическото и оперативно-тактическото ядрено оръжие.

Какво се случва след промените през 1989 г. по-голямата част от нас помнят. Защо се е случило, какви са основните политически и нормативни причини е въпрос на други изследвания. Характерен белег на промените е тяхната насоченост към съкращения на финансовите разходи. Те са породени от множество причини, като най-често се изтъква финансовата и ресурсната необезпеченост на въоръжените сили. Друга характеристика на този период е промяната в законите и нормативната база, която се характеризира със стихийност и липса на хармония. Хармония не само в нормативната база, но и в структурата за командване и управление на въоръжените сили на република България и тази на НАТО. Липсата на воля за създаване на сходен подход с този на Алианса за разлика от годините на първия и втория период разгледани в този доклад.

Резултатите от това могат да се видят в последните оценки за способностите ни, особено на фона на хибридните заплахи и събитията, развили се след 24.02.2022 г. Нека си припомним техните осем им-

¹² ЦВА, Ф 25 О – VIII-а, Д 177, стр. 343-344.

¹³ ЦВА, Ф 25 О – VIII-а, АЕ 210, стр. 68-77.

¹⁴ ЦВА, дело 1-II, Министерски заповеди. Оригинални министерски заповеди, стр. 103-109.

ператива и се замислим, особено за човешките ресурси, тяхната подготовка, доктрините, концепциите и инфраструктурата. Като че ли нищо не се е променило кой знае колко от доклада на генерал-лейтенант Славчо Трънски до началника на ГЩ от 07.04.1959 г. за насоките на висшето военно образование и дисциплините, които следва да се изучават в Академията.

Дали това е така? Дано не се налага да разбираме!

ЛИТЕРАТУРА

Библиотека на Военна академия „Г. С. Раковски“, МЗ, П 943, стр. 220-222

Библиотека на Военна академия „Г. С. Раковски“, МЗ, П 943, стр. 223-228

1. *Висши учебни заведения*, ЦДА, Ф. 143, о. 2, а. е. 27, л. 120.

2. *Военна академия „Георги Стойков Раковски, исторически очерк*. София: Военно издателство, 1990, стр.55, 56, 62.

3. *Доклад от Карло Луканов*, ЦДА, Ф. 143, о. 2, а. е. 6, л. 36, 37, 38.

4. *Държавен вестник*. брой 224 от 24.IX 1948.

5. *Закон за висшето образование*. *Държавен вестник*. бр.224 от 24 Септември 1948.

6. Иван Янев. *Висшето образование в България, 1944–1948*. [онлайн] <https://chitanka.info/text/14756-vissheto-obrazovanie-v-bulgarija-1944194>, посетен на 15.06.2020.

7. Кепов, Б. *Закон за висшето образование: Укази, наредби, правилници и др. във връзка с приложението му*. София, 1953, стр. 62.

8. Петров, Тодор и други. *Военна академия „Г. С. Раковски“*. София: Военна академия „Г. С. Раковски“, 2019, стр. 12. ISBN 978-619-7478-20-4

9. Парижки мирен договор ЧАСТ III. ВОЕННИ, ВОЕННО-МОРСКИ И ВОЕННО-ВЪЗДУШНИ КЛАУЗИ, ОТДЕЛ I. Член 9.

10. *Правилник за Висшата атестационна комисия при КНИК по присъждане на учени степени извания*. ЦДА, ф. 143, о. 1, а. е. 159, л. 54.

11. *Аспирантура при висшите учебни заведения и научно-изследователските институти*. Централен Държавен Архив, Фонд 143, опис 2, архивна единица 27.

12. Ранчев, К. *Стратегическо ръководство на Българската армия в условията на блоково противопоставяне (1955 – 1991 г.)*. [дисертационен труд].

13. ЦВА, Ф 1517, О – I, Д 26, стр. 24.

14. ЦВА, Ф 1517, О – I, Д 257, стр.26.

15. ЦВА, Ф 1517, О – I, Д 26, стр. 40.

16. ЦВА, Ф 1517, О – I, Д – 26 стр. 374.

17. ЦВА, Ф 1517, О – I, Д 26, стр. 477.

18. ЦВА, Ф 1517, О – I, Д – 29 стр. 233.

19. ЦВА, Ф 1517, О – I, Д 30, стр. 242, 243.

20. ЦВА, Ф 1517, О – I, Д 669, стр. 53-59.

21. ЦВА, Ф 1517, О – I, Д 55, стр. 27-29.

22. ЦВА, Ф 1517, О – I, Д 55, стр. 31-33.

23. ЦВА, Ф 1517, О – I, Д 754, стр. 221-225.

24. ЦВА, Ф 3 О – I, Д 122, стр. 1-29.

25. ЦВА, Ф 25 О – VIII-а, Д 177, стр. 18-21.

26. ЦВА, Ф 25 О – VIII-а, Д 177, стр. 345-347.

27. ЦВА, Ф 25 О – VIII-а, Д 177, стр. 343-344.

28. ЦВА, Ф 25 О – VIII-а, АЕ 210, стр. 68-77.

29. ЦВА, дело 1-II, Министерски заповеди. Оригинални министерски заповеди, стр.103-109.

30. ЦВА, Ф 25 О – VIII-а, Д 177, стр. 345-347.

31. ЦВА, Архив ГЩ, Ф 1, Д 37, Т I, стр. 147-153.

32. ЦВА, Кабинет на министъра на отбраната, Дело 10 –Т II, стр. 117-122.

33. ЦВА, Кабинет на министъра на отбраната, Дело 10 –Т II, стр. 174-192.

REFERENCES

Biблиотека na Voenna akademiya „G. S. Rakovski“, MZ, P 943, str. 220-222

Biблиотека na Voenna akademiya „G. S. Rakovski“, MZ, P 943, str. 223-228

1. *Visshi uchebni zavedeniya*, CSA, F. 143, o. 2, a. e. 27, l. 120.

2. *Voenna akademiya „Georgi Stoykov Rakovski, istoricheski ocherk*. Sofia: Voенno izdatelstvo, 1990, str.55, 56, 62.

3. *Doklad ot Karlo Lukanov*, CSA, F. 143, o. 2, a. e. 6, l. 36, 37, 38.

4. *Darzhaven vestnik*, No 224, 24.IX 1948.

5. *Zakon za vissheto obrazovanie*. *Darzhaven vestnik*. No 224, 24 Sept. 1948.

6. Ivan Yanev. *Visheto obrazovanie v Bulgaria, 1944–1948*. [online] <https://chitanka.info/text/14756-vissheto-obrazovanie-v-bulgarija-1944194>, poseten na 15.06.2020.

7. Kepov, B. *Zakon za visheto obrazovanie: Ukazi, naredbi, pravilnitsi i dr. vav vrazka s prilozhenieto mu*. Sofia, 1953, str. 62.

8. Petrov, Todor i drugi. *Voenna akademiya „G. S. Rakovski“*. Sofia: Voenna akademiya „G. S. Rakovski“, 2019, str. 12. ISBN 978-619-7478-20-4
9. Parizhki miren dogovor CHAST III. *VOENNI, VOENNO-MORSKI I VOENNO-VAZDUSHNI KLAUZI*, OTDEL I. Chlen 9.
10. *Pravilnik za Vishata atestatsionna komisiya pri KNIK po prisazhdane na ucheni stepeni izvaniya*. CSA, f. 143, o. 1, a. e. 159, l. 54.
11. Aspirantura pri visshite uchebni zavedeniya i nauchno-izsledovatelските instituti, Tsentralen Darzhaven Arhiv, Fond 143, opis 2, arhivna edinita 27.
12. Ranchev, K. *Strategicheskoto rakovodstvo na Balgarskata armia v usloviyata na blokovo protivopostavyane (1955 – 1991 g.)*. [disertatsionen trud].
13. CMA, F 1517, O – I, D 26, str. 24.
14. CMA, F 1517, O – I, D 257, str. 26.
15. CMA, F 1517, O – I, D 26, str. 40.
16. CMA, F 1517, O – I, D – 26 str. 374.
17. CMA, F 1517, O – I, D 26, str. 477.
18. CMA, F 1517, O – I, D – 29 str. 233.
19. CMA, F 1517, O – I, D 30, str. 242, 243.
20. CMA, F 1517, O – I, D 669, str. 53-59.
21. CMA, F 1517, O – I, D 55, str. 27-29.
22. CMA, F 1517, O – I, D 55, str. 31-33.
23. CMA, F 1517, O – I, D 754, str. 221-225.
24. CMA, F 3 O – I, D 122, str. 1-29.
25. CMA, F 25 O – VIII-a, D 177, str. 18-21.
26. CMA, F 25 O – VIII-a, D 177, str. 345-347.
27. CMA, F 25 O – VIII-a, D 177, str. 343-344.
28. CMA, F 25 O – VIII-a, AE 210, str. 68-77.
29. CMA, delo 1-II, Ministerski zapovedi. Originalni ministerski zapovedi, str. 103-109.
30. CMA, F 25 O – VIII-a, D 177, str. 345-347.
31. CMA, Arhiv GSHT, F 1, D 37, T I, str. 147-153.
32. CMA, Kabinet na ministara na otbranata, Delo 10 –T II, str. 117-122.
33. CMA, Kabinet na ministara na otbranata, Delo 10 –T II, str. 174-192.

ОБМЕН НА РАЗУЗНАВАТЕЛНА ИНФОРМАЦИЯ В БОРБАТА СРЕЩУ ТЕРОРИЗМА

доц. д-р Мирослав Мирчев

Военна академия „Г. С. Раковски“, *mirchevm1958@gmail.com*

Резюме: Докладът разглежда въпроси свързани с едно от най-важните направления в борбата срещу тероризма – обмен на разузнавателна информация между правоохранителните и специалните служби. Анализирани са натрупаният световен опит на САЩ, Руската федерация, ООН и ЕС за координиране на усилията за противодействие на терористичната заплаха. Отделено е място на ролята и задачите на разузнавателните и контраразузнавателните структури на САЩ и на Руската федерация за участието им в контртерористични операции както на територията на техните страни, така и зад граница.

Ключови думи: *тероризъм; Съвет за информационен обмен; Експертен комитет на Съвета на Европа за борба с тероризма; спецтероризъм; Федерална служба за сигурност; Главно разузнавателно управление на ГЩ на ВС; ГРУ; Регионална антитерористична структура; Шанхайска организация за сигурност*

THE EXCHANGE OF INTELLIGENCE INFORMATION IN THE FIGHT AGAINST TERRORISM

Assoc. Prof. Miroslav Mirchev, PhD

Rakovski National Defence College

Sofia, Bulgaria

E-mail: *mirchevm1958@gmail.com*

Abstract: The report has examined one of the most important areas in the fight against terrorism, related to the exchange of intelligence information between the law enforcement agencies and the special services. The accumulated world experience by the USA, the Russian Federation, the UN and the EU in coordinating of their efforts to counteract the terrorist threat has been analyzed. The role and tasks of the intelligence and counterintelligence structures of the USA and the Russian Federation in counter-terrorist operations, both on the territory of their countries and abroad, have been given a place in that material.

Keywords: *terrorism; Information Sharing Council; Committee of Experts on Terrorism; CODEXTER; spectrorism; Federal Security Service; FSB; Main Intelligence Directorate of the General Staff of the Army Forces; GRU; Anti-Terrorist Centre; Regional Anti-Terrorist Structure; Shanghai Security Organization*

Един от глобалните проблеми в борбата срещу тероризма е свързан със своевременния обмен на достоверна разузнавателна информация между държавите, в които е засечена терористична активност, подготвят се терористи или с такива, в които предстои да бъде извършен атентат. Нуждата от подобно сътрудничество в тази област възниква веднага след атентатите от 11.09.2001 год. в САЩ, когато се оказва, че нито една специална служба в света не е готова да създаде система за глобален обмен на подобна „чувствителна информация“.

Първите опити, които дават реални резултати са свързани със създаването на системата „Ешелон“, което е опит от страна на САЩ за формиране на общ международен координационен механизъм за обмен на информация по въпросите на тероризма с някои от своите най-верни съюзници по т.нар. „англо-саксонска ос“ – Великобритания и Австралия. През м. юни 2004 год. трите държави създават Глобална антитерористична мрежа, чиято основна задача е насочена към ограничаване дейността на „Ал Кайда“ и подкрепящите я други терористични групировки. Тази мрежа включва първоначално американския Национален контртерористичен център (National Counterterrorism Center), британският Общ център за терористични анализи (Joint Terrorism Analysis Centre), създаден през м. юни 2003 год.) и австралийският Национален център за оценка на заплахата (National Threat Assessment Centre), създаден през м. октомври 2003 год.). Към нея до края на 2004 год. се присъединяват още канадският Интегриран център за

оценка на заплахата (Integral Threat Assessment Centre) и новозеландската Обединена група за оценка на заплахата (Combined Threat Assessment Group). В резултат на общо съгласие и одобрение на териториите на тези пет държави са създадени центрове за радиоразузнаване, прераснали в глобалната антитерористична мрежа ECHELON.¹

Отделно от това ЦРУ изгражда мрежа от обединени разузнавателни центрове под името „Контртерористични разузнаватели центрове“ (Counterterrorist Intelligence Centers) в държави, намиращи се в Европа, Близкия изток и Азия. Появяват се публикации за наличието на такъв център в Париж – „База Алианс“ (Alliance Base), създаден между ЦРУ и френската Генерална дирекция за външна безопасност (DGSE). Задачата на тази структура е проследяването в световен мащаб за придвижването на лица заподозрени в терористична дейност, както и разработката на операции по тяхното залавяне или ликвидиране.

Въпросът за подобряване на системата за обмен на информация, касаеща тероризма в САЩ, е поставен с цялата си тежест през 2004 год., когато президентът Буш-младши подписва Указ № 13356, регламентиращ този процес между специалните служби на федерално и местно ниво. Година по-късно отговорностите за изпълнение и ръководство на създадената програма за обмяна на данни се възлагат на Управлението на директора на Националното разузнаване (Office of the Director of National Intelligence, ODNI).

В края а 2005 год. е създаден *Съвет за информационен обмен* (Information Sharing Council, ISC), чиято задача е да формулира политиката и принципите, на базата на които ще се извършва обменът на информация между държавните и частните структури, имаща отношение към борбата с тероризма. Определени са и трите приоритетни области за сътрудничество между структурите – политическа, икономическа и бизнес. През м. октомври същата година Съветът за информационен обмен (СИО) започна контакти със Службата за електронно обслужване (Electronic Directory Service) и Института за отбранителни изследвания (Institute for Defense Analyses) за търсенето на най-рационалните решения за създаването на програма, позволяваща ефективния обмен на информация. В рамките на СИО са създадени три работни групи: първата е за получаване на достъп до информация и нейната обработка, втората е за управление и сътрудничество на Съвета с други структури, а третата за сигурност на информацията. Основната цел, която се поставя с тяхното изграждане е да бъде подобрена ефективността при събирането на информация, определени приоритетните направления, избегнато дублиране, да бъдат предложени варианти за най-оптимални решения, а анализираната информация да достига по-бързо до крайните потребители. За това са създадени два пилотни проекта. Единият е за събиране и обработка на несекретни данни от ФБР, а другият, с една от лабораториите на Министерството на енергетиката, за анализ и даването на експертни оценки за реални заплахы от терористични атаки. При първия проект структурите на ФБР обработват всички получени по електронен път писма и сигнали, анализират ги и ги съхраняват в съответната база данни. По този начин се осигурява по-бърз достъп до цялата налична информация свързана с терористичните заплахы и тяхното правилно идентифициране. Във втория случай Министерството на енергетиката спонсорира проект, който извършва техническа и аналитична експертиза на данните, имащи отношение към потенциални заплахы, свързани с т.нар. „ядрен тероризъм“.

По този начин СИО се превръща в национална система за съхранение и информационен обмен по въпросите на тероризма. Тази комбинация от политика, процедури и технологии, свързващи ги ресурси (хора, системи, база данни и информационни масиви), федерални, държавни, местни структури и такива от частния сектор, практически облекчава обмена на информация, достъпа до нея и сътрудничеството на структурите от системите за разузнаване и контрразузнаване, ангажирани с борбата срещу тероризма.

В работната схема на СИО, като единен подход, са включени всички структури, имащи отношение към предотвратяването на терористични атаки на щатско и местно ниво. На тях са поставени задачи за добиването на информация, свързана с тероризма, оценка на риска, разпределение на финансовите ресурси, изготвянето на планове за ответни действия, за защита и възстановяване на важни обекти от критичната инфраструктура.²

Настоящата архитектура на структурите на САЩ, имащи ангажименти и отговорности в целия комплекс от мероприятия по борба с тероризма е следната:

1. Съвет за национална сигурност (National Security Council).
2. Заместник-съветник по въпросите на националната безопасност, отговарящ за борбата с тероризма (Deputy National Security Advisor for Combating Terrorism).
3. Комитет по антитероризъм и национална готовност (Principals Committee on Counter-terrorism and National Preparedness).

4. Национален координатор по въпросите на безопасността, защита на инфраструктурата и контра-тероризма (National Coordinator for Security, Infrastructure Protection and Counter-terrorism).

5. Съвет за вътрешна сигурност (Homeland Security Council);

6. Национален контратерористичен център (National Counterterrorism Centre);

7. Център за наблюдение на терористичната активност (Terrorist Screening Centre);

8. Министерство за вътрешна сигурност (Department of Homeland Security);

9. ЦРУ – Антитерористичен център (Counterterrorism Centre);

10. ФБР – Управление за борба с тероризма (Counterterrorism Division).

В състава на американските въоръжени сили структурите за борба с тероризма са: Обединена междуведомствена координационна група за борба с тероризма (Joint Interagency Coordination Groups) и Централното командване (CENTCOM, Joint Interagency Task Force).³

Обменът на информация между посочените структури се извършва на базата на постановление на Конгреса, който с акт № 1016 от 2004 год. разпорежда *„извършване на реформа в разузнавателната общност с цел предотвратяване на заплахата от тероризъм“*. През м. август същата година с указ на президента № 13356 е заповядано цялата информация, касаеща тероризма, да бъде включена в информационния обмен между федералните служби както на федерално, така и на местно ниво. За това е създадена нова структура – **отдел** и изработена съответната система за информационен обмен, за която пряко отговаря ODNI.

В рамките на ООН за обмен на информация свързана със заплахите от тероризъм е изграден *„Сектор за превенция от тероризма към Управлението на ООН за борба с наркотиците и престъпността“* (Terrorism Prevention Branch of the UN Office on Drugs and Crime, TPB UNODC). Неговата дейност е свързана основно с изработването на нормативната база за подпомагане на страните, членки на ООН, в работата им по ратифицирането на близо 13 международни конвенции и протокола, третиращи борбата срещу тероризма. Това включва организирането на международни конференции, работни семинари, разработване на модели за обмен на информация за по-ефективно противодействие на заплахата от тероризъм. През 2004 год. с Резолюция № 1535 в рамките на Сектора е създаден *„Контратерористичен комитет“*.

Щабквартирата на Сектора се намира във Виена. Щатът му е от 30 сътрудника, а неговото финансиране се осигурява от бюджета на ООН, одобрен от Общото събрание, както и от доброволните вноски на страните, членки на ООН. Годишният му размер е около 900 000 щ.д.

Системата на ЕС за борба и обмен на информация срещу тероризма включва: *Координатор на ЕС за борбата срещу тероризма, Специална комисия за борба с проявите на международния тероризъм към Съвета на Европа, Експертен комитет на Съвета на Европа за борба с тероризма и Европол*.

През 2001 год. по време на заседание на министрите на правосъдието и на вътрешните работи на страните членки Великобритания поставя въпроса за разширяване пълномощията на Европол в борбата срещу тероризма. На дневен ред е поставен въпросът за улесняване на процедурите по екстрадирането на лица, заподозрени в терористична дейност, затягането на контрола върху банкови операции, предоставяне на неограничен достъп до архивите на Интернет провайдъри и на телефонни компании. Три месеца по-късно започва работата по формирането на общ европейски подход за борба с международния тероризъм. Постигнато е политическо решение за въвеждането на единна европейска заповед за арестуване на заподозрени терористи и пресичане на канали за финансиране на терористична дейност.

През 2004 год. Австрия излиза с инициатива за създаването на специализирана европейска служба за борба с тероризма. По време на направените обсъждания по този въпрос няма единно мнение, но надделяват вижданията на Великобритания, Германия, Франция, Испания и Италия за това да отговаря новосъздадена структура – *Координатор на ЕС за борбата срещу тероризма*. В неговите функции влизат координиране на контратерористичната дейност на територията на страните, членки на ЕС, в това число и по въпросите на разузнаването, сигурността и контрола над финансовите потоци, свързани със съмнения за терористична дейност.⁴ През м. октомври 2004 год. Съветът на Европа създава *Специална комисия за борба с проявите на международния тероризма* на територията на страните членки.

Експертният комитет на Съвета на Европа за борба с тероризма (Committee of Experts on Terrorism, CODEXTER) е координиращ междуправителствен орган. Неговите основни задачи са свързани с: борбата срещу тероризма; радикализация, водеща до тероризъм и получаване на знания за терори-

зма, включително чрез Интернет; разработването на специални техники за разследване на терористичната дейност; даване на оценка за възможни пропуски в законовата рамка, предвидена от международните правни инструменти на Съвета на Европа в областта на предотвратяването и потискането на тероризма, включително по отношение на Международното хуманитарно право и за връзки между тероризма и организирана престъпност.

Служителите от Експертния комитет на Съвета на Европа за борба с тероризма (ЕКСЕБТ) предлагат за одобрение нормативни документи за защита на свидетели и лица, сътрудничащи с правосъдитните органи срещу терористични организации, изготвят профили на държави, свързани с техните законодателни и институционални инициативи за борба с тероризма, наблюдение за изпълнение на подписаните и ратифицираните от правителствата на ЕС закони и инициативи за насърчаване на ефективното прилагане на инструментите на Съвета на Европа, свързани с борбата срещу тероризма, обмена на информация за най-добрите практики за борба с тероризма при пълно зачитане на правата на човека и върховенството на закона, както и създаването на базата данни по дела на Европейския съд за правата на човека, касаещи борбата с тероризма.

ЕКСЕБТ работи в тясно сътрудничество с международни органи, като Изпълнителната дирекция на Комитета за борба с тероризма на ООН (CTED), Сектор за превенция от тероризма към Управлението на ООН за борба с наркотиците и престъпността (TPB UNODC), Организацията за сигурност и сътрудничество в Европа (ОССЕ), Европейския Съюз и Глобалния форум за борба с тероризма. През 2018 год. ЕКСЕБТ е реорганизиран в *Комитет за борба с тероризма на Съвета на Европа* (CDCT).⁵

Основното схващане в позициите на европейските държави в борбата срещу тероризма е, че той е заплаха за сигурността, ценностите на демокрацията, правата и свободите на европейските граждани. ЕС определя борбата с него като основен приоритет както за своите страни-членки, така за международните си партньори.

След поредицата от терористични атаки от 2015 год. ЕС прие различни нови инициативи, свързани с: подобряване на обмена на информация; засилване на проверките по външните граници на ЕС; ограничаване и предотвратяване на онлайн радикализацията; подобряване на контрола върху огнестрелните оръжия; цифровизиране на съдебното сътрудничество; инкриминиране на деяния, свързани с тероризъм; ограничаване финансирането на тероризма; актуализиране на наличната база данни за пътници, използващи въздушен транспорт и засилване на сътрудничеството с държави извън ЕС.

През м. ноември 2020 год. след терористичните нападения, извършени във Франция, Германия и Австрия, министрите на външните работи от ЕС се споразумяха да засилят още повече съвместните си усилия за борба с тероризма и да усъвършенстват системата за обмен на информация между правоприлагащите, съдебните и разузнавателните органи на страните членки за проследяването на чуждестранни терористи и борбата с организираната престъпност. Тази нова оперативна система ще започне да функционира след 2023 год. и ще осигури единен интерфейс за търсене и биометрично съпоставяне с цел улесняване установяването на самоличността.

За да осигури ефективен отговор на всички посочени предизвикателства, през януари 2016 год. в рамките на Европол е създаден *Европейски център за борба с тероризма* (European Counter Terrorism Centre, ECTC). Той е оперативна структура за експертиза, която осигурява все по-нарастващите потребности на ЕС в усилията в борбата му срещу тероризма. Дейността на Центъра е съсредоточена върху осигуряването на оперативна поддръжка по искане от държава, членка на ЕС, за извършване на: разследвания; неутрализиране дейността на чуждестранните бойци; споделяне на разузнавателни данни и опит в сферата на финансирането на тероризма (чрез Програмата за проследяване на финансирането на тероризма и звеното за финансово разузнаване); ограничаване на онлайн терористична пропаганда и екстремизъм (чрез звеното за насочване на интернет към ЕС); пресичане на нелегален трафик на оръжие и координиране на международно сътрудничество между органите за борба с тероризма.

През последните години ЕС засили и мандата на други агенции на ЕС в областта на правосъдието и вътрешните работи (Евроюст, Frontex, CEPOL и eu-LISA), за да подкрепи усилията за борба с тероризма на страните членки. Освен че полага усилия за повишаване на оперативната съвместимост, ЕС работи и за подобряване на съществуващите бази данни. Например през 2018 год. Съветът прие правила за укрепване на *Шенгенската информационна система* (ШИС), с които въведе нови видове сигнали за случаи свързани с терористични дейности.⁶

За ефективна борбата срещу тероризма както на територията на Руската федерация, така и зад граница, през 2006 год. е създаден *Национален комитет за борба с тероризма* (НКБТ). Той е координационен орган на изпълнителната власт на федерално и местно ниво и отговаря за изготвянето на съответните планове и предложения за защитата от терористична заплаха до законодателната и изпълнителната власт. Негов председател е директорът на Федералната служба за сигурност (ФСС). Основните ангажменти на НКБТ са свързани с:

- подготовка на предложения до президента на Руската федерация относно формирането на държавната политика и подобряване на законодателството в областта на борбата с тероризма;
- координиране на всички антитерористични дейности на федералните органи на изпълнителната власт и комисиите в регионите на Руската федерация, както и организиране на взаимодействието на тези структури с местните органи за самоуправление, обществени организации и сдружения;
- определяне на мерки за премахване на причините и условията, допринасящи за появата на тероризма, като се осигурява защита на обекти от потенциални посегателства;
- участие в борбата срещу тероризма и подготовка на международни договори на Руската федерация в тази област;
- гарантиране на социална защита за лица, които вече са ангажирани в борбата срещу тероризма и социално подпомагане на жертвите от терористични актове;
- решаване на други задачи предвидени от законодателството на Руската федерация.

Понастоящем страната използва следните **методи** за борба с тероризма:

1. Превенция, която е свързана с предотвратяване на терористични атаки чрез идентифициране и елиминиране на условия и причини, допринасящи за извършването на терористични атаки.
2. Разкриване, потискане и разследване на всеки акт на тероризъм.
3. Свеждане до минимум и елиминиране на последиците от всякаква проява на тероризъм.

В началото на м. март 2006 год. е приет Закон за противодействие на тероризма, който е подписан от Владимир Путин на 06.03.2006 год. Съгласно този нормативен акт правителството получава правото да прилага изискванията за антитерористичната защита на обекти и територии, за да гарантира сигурността на всички физически и юридически лица.⁷

За борба с тероризма Руската федерация е създадала и поддържа комплекс от оперативно-бойни, специални, военни и други мерки, военната техника, оръжия и специалните средства, които се използват за предотвратяване на терористичен акт, неутрализиране на терористи, осигуряване на безопасността на населението, институциите и организациите, както и за минимизиране на последствията от терористичните актове. Съгласно Закона за противодействие на тероризма структурите, които пряко са ангажирани с целия спектър от задачи, свързани с терористичната заплаха в Руската федерация са:

– *Федералната служба за сигурност* (ФСС), която осъществява противодействие на тероризма посредством предупреждение, разследване и пресичане на престъпления, имащи терористичен характер, в това число и такива, преследващи политически цели, в съответствие със съществуващото законодателство;

– *Министерство на вътрешните работи* (МВР), което води борба с тероризма посредством предупреждение, разследване и пресичане на заплахи с терористичен характер, преследващи корупционни цели;

– *Службата за външно разузнаване* (СВР) добива информация по въпросите, свързани с премахване на заплахата от тероризъм и предприемане на мерки за активно противодействие срещу терористичната заплаха (в съответствие с указ на президента „За мерките по противодействие на тероризма“ от 15.02.2006 год.) извън територията на Руската федерация;

– *Федералната служба за охрана* (ФСО), която осигурява безопасността на важни държавни и инфраструктурни обекти от терористични атаки;

– *Министерство на отбраната* (МО) има отговорности за защитата на всички оръжия за масово унищожаване, ракетно и друг вид въоръжение, боеприпаси и взривни материали, територията, въздушното и морското пространство и участие в контратерористични операции, включително и зад граница.

За подобряване на цялостната дейност по обмена на информация и координацията, свързана с противодействие на терористичната заплаха, на 20.06.2000 год. страните, участници в Общността на независимите държави (ОНД), вземат решение за създаване на *Антитерористичен център*. Той започва

да функционира на 01.12.2000 год. след като Съветът на държавните ръководители от ОНД утвърждава неговия статут, личен състав, финансово и логистично осигуряване, както и правилник за действие. Първоначално Антитерористичният център е изцяло под контрола на руските специални служби, а щаб-квартирата му се намира в Москва. Съгласно едно от приложенията на Правилника за дейността на Антитерористичния център ръководител на тази структура трябва да бъде заместник-началника на службата за сигурност, на чиято територия се намира Центъра, за срок от 6 години. През 2001 год. е открит негов филиал в Бишкек, Киргизстан.

Финансово Антитерористичният център зависи изцяло от Москва, която внася близо 50% от необходимите за неговата дейност средства, а останалите се разпределят равномерно между другите страни членки. До 2005 год. дейността на Центъра е бойкотирана от узбекските представители. Същата година е създадена и общата база данни за събиране и анализ на цялата информация, постъпваща по въпросите на тероризма.

Постепенно обаче основният акцент в дейността на Антитерористичния център се измества и той започва да изпълнява задачи свързани със запазването на толерираните от Руската федерация режими от т.нар. „цветни революции“. На 12.05.2005 год. директорът на ФСБ Николай Патрушев внася документ, в който предоставя информация за подготвян заговор за сваляне на беларуския президент Александър Лукашенко. На следващия ден е метежът в източния узбекистански град Андижан, при който загиват 187 души. След като ФСС предлага помощ на своите узбекистански колеги за разследване на размириците за сваляне на президента Шавкат Мирзиюев, правителството на страната взема решение за присъединяване към Антитерористичния център.⁸

От тогава досега отстраняването на опасностите от възникване на „цветни резолюции“, целящи свалянето на някои потомствени режими в страните, членки на ОНД, заема основно място в оперативната дейност на Центъра. Постепенно тази тема започва да доминира в заседанията на Антитерористичния център и обмяната на информация между представителите на различните разузнавателни и контраразузнавателни служби на участващите държави.

Центърът се ръководи от представител на службата за сигурност на съответната държава (като правило нейния първи заместник), където временно се намира щаб-квартирата му, за срок от три години с възможност за удължаване на мандата с още три. Дейността на ръководителя на Антитерористичния център се подпомага от трима заместника, които са представители от Съветите на министрите на съответните министерства на вътрешните работи, отбраната и граничните войски на страните, членки на ОНД. Организационната структура на Центъра включва следните отдели:

- „Координационно-оперативен отдел“, който се занимава с организиране на взаимодействието на компетентните държавни структури, имащи отношение към борбата срещу тероризма и проявите на екстремизъм. Изпълнява задачи по подготовката и провеждането на съвместни антитерористични мероприятия и операции. Към тях се отнасят тези, свързани с издирването на лица, извършили престъпления, определени от съответното законодателство на държавите, участници в ОНД, като „терористични“, както и на лицата, които ги укриват. Отделът отговаря за организирането и провеждането на подготовката на специалисти за антитерористичните подразделения на съответната държава, което се извършва от инструктори на Центъра със специално предназначение на ФСС на Русия. Организира и провежда командно-щабни и оперативно-тактически учения на специалните части, ангажирани в борбата срещу тероризма. Неговите сътрудници водят и методическа дейност, свързана с подготовката и провеждането на научнопрактически конференции, семинари и други мероприятия, свързани с обмяната на опит. Издава и учебни пособия като „Методическо ръководство за освобождаване на заложници“, „Справка за международните терористични организации в Централна Азия+ и др.;

- „Отдел за ситуационен анализ, мониторинг на заплахата и подготовка на проекти за решения“, в чиито функции влизат изработването на предложения до Съвета на държавните ръководители на страните от ОНД и други заинтересовани органи, имащи ангажименти в борбата с международния тероризъм. Отделът събира и анализира, постъпващата информация относно динамиката и тенденциите в проявите на международния тероризъм и екстремизъм не само в рамките на ОНД, но и в световен мащаб. Въз основа на събраната информация отделът създава база от данни, включваща информация за терористичните организации – структура, ръководство, членска маса, лица, оказваща подкрепа на терористите, и др. При поискване тази информация се предоставя на заинтересованите министерства и ведомства на страните от ОНД;

- „Отделение на Антитерористичния център за Централно-азиатския регион“, с щаб-квартира в Бишкек, Киргизстан. Отговаря за координиране дейността на Центъра в Казахстан, Узбекистан, Таджикистан и Киргизстан;

- „Научно-консултативен съвет“, занимава се основно с изследването и обработката на материали, имащи оперативна стойност, но добивани от открити източници на информация. Ежемесечно изготвя аналитични справки за състоянието, тенденциите и измененията в развитието на обстановката за сигурност, настъпили вследствие на терористичната активност. Първото съвместно учение на Антитерористичния център е проведено в края на 2001 год. в Ошката област на Киргизстан, когато са отработени въпроси по пресичане нелегалното преминаване на бойци от Ислямското движение на Узбекистан (ИДУ) през териториите на Таджикистан и Киргизстан и включването им в операциите на афганистанското Движение „Талибан“. Основният акцент е поставен върху координиране и управление на действията на контратерористичните подразделения на участващите страни, членки на ОНД.

Второто учение е проведено на територията на три държави, като първо е разгърнат щаб в Киргизстан, който е подготвил методическите цели на учението, след което се пристъпва към практическата му част, проведена на територията на Казахстан. Отработваните въпроси са били свързани с освобождаването на заложници, задържани в сграда, след това на заложници, намиращи се в болница и автобус. Третият етап от учението е на територията на Таджикистан, където основен акцент е бил поставен върху освобождаването на заложници на полигон. То е проведено с бойни стрелби при поддръжката на авиация. През лятото на 2003 год. подобно учение се организира единствено между контратерористичните подразделения на Русия, Казахстан и Украйна. Представителите на силовите ведомства на останалите държави от ОНД са поканени само като наблюдатели.⁹

Русия развива активно дейност по въпросите на борбата с тероризма и по линия на Шанхайската организация за сигурност (ШОС). Тя е създадена като регионална международна организация за укрепването на доверието във военната област и взаимно съкращаване на военните сили в граничните райони през 1996 год. от държавните глави на Русия, Китай, Казахстан, Таджикистан и Киргизстан, известна първоначално като „Шанхайската петорка“. След включването през 2001 год. и на Узбекистан организацията е преименувана на ШОС. В края на 2021 год. в организацията членуват осем държави – Русия, Китай, Индия, Казахстан, Киргизия, Пакистан, Таджикистан и Узбекистан. Със статут на наблюдатели се ползват Афганистан, Беларус, Иран и Монголия. Партньори на ШОС са Азербайджан, Армения, Камбоджа, Непал, Турция и Шри-Ланка.¹⁰

Структурата на ШОС, която е ангажирана с въпросите на тероризма, е *Регионалната антитерористична структура на Шанхайската организация за сигурност* (РАТСШОС). Тя започва да функционира през 2004 год. като първоначално нейната щабквартира се намира в Бишкек, но след това е преместена в Ташкент, Узбекистан. В нея работят 7 специалисти от Русия и Китай, 6 от Казахстан, 5 от Узбекистан, 3 от Киргизстан и 2 от Таджикистан. Бюджетът на тази антитерористична структура е близо 2 млн. щ.д. и се образува от вноските на държавите на квотен принцип – по 24% за Русия и Китай, 21% за Казахстан, 15% за Узбекистан, 10% за Киргизстан и 6% за Таджикистан.

Като база за създаването на РАТСШОС служи подписаната между държавите, създали ШОС, Конвенция за борба с тероризма, сепаратизма и екстремизма. Първоначално РАТСШОС носи името „Бишкекската група“ на ръководителите на правозащитните и специалните служби, като целта е да се положи началото на диалог за обсъждане на актуални проблеми на сигурността в региона и да се координират съвместните им действия. На 07.06.2002 год. на своята среща в Санкт Петербург държавните глави на страните от ШОС подписват Съглашение за създаването на РАТСШОС. През м. юни 2004 год. в Ташкент по време на подписването на Съглашението за сътрудничество в борбата с незаконния трафик на наркотици, психотропни вещества и техните производни официално е открита щабквартирата на РАТСШОС. За неин пръв ръководител е назначен заместник-председателя на Службата за национална сигурност на Узбекистан В. Т. Касимов. През 2007 год. е създадена базата данни, в която се събира и анализира информация за терористични организации и е утвърден единен подход при изготвянето на списък с лицата, обвинени в международна терористична дейност и връзки с терористични, сепаратистки и екстремистки организации. Постъпващите данни се класифицират като секретни и несекретни, а достъп да тях имат единствено представителите на страните от ШОС. Работните езици са руски и китайски.

За осигуряване на оперативност при обмяната на данни е организирана защитена система за връзка между държавите, участници в РАТСШОС. Същата година започва и съвместното обучение на

специалисти и инструктори от антитерористичните формирования на тази структура, които да участват в общи учения.²

Държавното и военното ръководство на Руската федерация отчитат, че трансграничните форми на тероризъм са едни от най-опасните престъпления във вътрешен план и в международните отношения. Направен е изводът, че терористичното посегателство върху използването на оръжия за масово унищожение (ядрени и химически) е сериозна заплаха за съществуването не само на страната, но и за цялото човечество. Затова през последните години Руската федерация се опитва да поддържа една балансирана политика в усилията, които полага в борбата със заплахата от тероризъм. В нейната основа лежи схващането, че трябва да бъдат премахнати всички бариери – религиозни, идеологически или политически между държавите, които се сблъскват с терористични престъпления, за да може да бъде организиран ефективен отговор на всички прояви на тероризма и екстремизма, както и създаден общ международен антитерористичен фронт.¹¹

ЛИТЕРАТУРА

1. *Consolidating Intelligence Analysis: Governmental Affairs Committee Hearing on the President's Proposal for a Terrorism Threat Integration Center*. Joint Statement of the Terrorism Integration Center Senior Steering Group Winston P. Wiley, Chair. February 26, 2003.
2. Марков, М. *Тероризм как глобална угроза и как инструмент мировой политики*. [online], 25.04.1996. www.agentura.ru
3. Разузнавателни ведомства на САЩ. [online] <https://bg.wikipedia.org>
4. Страница Европейския съвет. www.consilium.europa.eu
5. Страница на Европейски съвет. www.coe.int
6. Страница на Европейски съвет. www.consilium.europa.eu
7. *Русия в борбата срещу тероризма*. Национален комитет за борба с тероризма, 2019. <https://bg.public-welfare.com>
8. *До 20 години затвор получиха организаторите на метежа в Андижан*. news.bg, 14.11.2005. www.agentura.ru
9. ШОС ще пресича опитите за външна намеса. *Русия днес, Светът*, 23-30.12.2021, стр. 4. [online] <https://www.rusiadnes.bg/index.php/bg/>
11. ред. Димитрова, Р. *Русия обеща да подпомага САЩ в борбата срещу тероризма*. Darik News, 20.02.2020 [online] www.dariknews.bg

REFERENCES

1. *Consolidating Intelligence Analysis: Governmental Affairs Committee Hearing on the President's Proposal for a Terrorism Threat Integration Center*. Joint Statement of the Terrorism Integration Center Senior Steering Group Winston P. Wiley, Chair. February 26, 2003.
2. Markov, M. *Terrorism kak globalnaya ugroza i kak instrument mirovoy politiki*. [online] 25.04.1996, www.agentura.ru
3. Razuznavatelni vedomstva na SASHT. [online] <https://bg.wikipedia.org>
4. Stranitsa Evropeyskiya savet. www.consilium.europa.eu
5. Stranitsa na Evropeyski savet. www.coe.int
6. Stranitsa na Evropeyski savet. www.consilium.europa.eu
7. *Rusiya v borбата sreshthu terorizma*. Natsionalen komitet za borba s terorizma, 2019. <https://bg.public-welfare.com>
8. *Do 20 godini zatvor poluchiha organizatorite na metezha v Andizhan*. news.bg, 14.11.2005. www.agentura.ru
9. ШОС shte presicha opitite za vanshna namesa. *Rusiya dnes, Svetat*, 23-30.12.2021, str. 4. [online] <https://www.rusiadnes.bg/index.php/bg/>
11. red. Dimitrova, R. *Russia obeshtha da podpomaga USA v borбата sreshthu terorizma*. Darik News, 20.02.2020 [online] www.dariknews.bg

ИЗПОЛЗВАНЕ НА ТЕХНИКИТЕ НА ВОЕННАТА ЗАБЛУДА В УКРАИНСКИЯ КОНФЛИКТ

полковник доц. д-р Калин Градев

Военна академия „Г. С. Раковски“, kgradev@abv.bg

майор гл. ас. д-р Кръстю Кръстев

НВУ „Васил Левски“ – Велико Търново, kikrastev@nvu.bg

Резюме: Целта на настоящия доклад е на базата на разработената теория за военната заблуда да се определят използваните способности и техники във военния конфликт на територията на Украйна. Методологията на изследване обхваща използване на методите на системния анализ, синтез, сравнение, изследване на опита, експертни мнения, анализи и изследвания на информационни материали от открити източници.

Ключови думи: *военна заблуда; военен конфликт; Украйна*

USE OF MILITARY DECEPTION TECHNIQUES IN THE UKRAINIAN CONFLICT

Colonel Assoc. Prof. Kalin Gradev, PhD

Rakovski National Defence College

Sofia, Bulgaria

E-mail: kgradev@abv.bg

Major Krastyu Krastev, PhD

Vasil Levski National Military University

Veliko Tarnovo, Bulgaria

E-mail: kikrastev@nvu.bg

Abstract: The purpose of this article is based on the developed theory of military deception to determine the methods and techniques used in the military conflict on the territory of Ukraine. The research methodology covers the use of the methods of systematic analysis, synthesis, comparison, research of experienced expert's opinions, analysis and research of information materials gathered from open sources.

Keywords: *military delusion; military conflict; Ukraine*

*„Хиляди пътища водят към заблудението,
към истината – само един.“*

Жан-Жак Русо

Въведение

Ескалацията на конфликта в Украйна е най-актуалната към момента тема за изследвания по сигурността. Основните проблеми пред сигурността на Европа според съвременните специалисти (Георгиев, Г. П., 2018) са регионалната нестабилност, неустойчивото развитие, появата и изострянето на конфликти на етническа и религиозна основа¹³ и свързаните с тях форми на тероризъм^{6, 7, 13}. Затова управлението на кризи от невоенен характер се превръща в един от основните подходи за гарантиране на международната и националната сигурност и стабилност. В тази област са концентрирани усилията на ООН, НАТО, ЕС и ОССЕ за разширяване на сътрудничеството и взаимопомощта както по проблемите на сигурността, така и по въпросите за предотвратяване и ликвидиране на последствията от бедствия³, промишлени аварии и кризи от невоенен характер и честите природни бедствия¹⁵, съдържащи в себе си потенциал на антропогенни катастрофи^{5, 12, 15, 16}.

Дали ООН, НАТО, ЕС и ОССЕ бяха готови за такова развитие и бърза ескалация на конфликта от невоенен във военен?

Според оценки на американски и украински разузнавателни служби през януари 2022 г. повече от 150 000 руски войници обграждат Украйна от три страни като подкова. Белият дом неведнъж е предупреждавал

давал, че руският президент Владимир Путин може да започне пълномощабно нахлуване в Украйна по всяко време²¹.

На 15 февруари Путин заяви, че връща част от войските си в базата след приключване на ученията и че е готов да намери дипломатически изход от ситуацията. Това твърдение е посрещнато скептично от западните служители, последвано от разочарование, когато САЩ заявяват, че вместо да намали силите си, Русия тихомълком мобилизира още няколко хиляди души. Държавният секретар на САЩ Антъни Блинкен предупреждава, че САЩ не са забелязали непосредствени признаци за изтегляне на руските военни, като отбелязва, че за съжаление има разлика между това, което Русия казва и това, което прави^{18, 19, 20}.

НАТО повиши готовността на силите си за бързо реагиране, а страните членки вдигнаха в бойна готовност войските си и изпратиха в региона батальони, самолети и кораби. САЩ наредиха изпращането на още 3000 военнотслужещи в Полша, с което общият брой на подкрепленията, изпратени в Европа през последните седмици, достига около 5000 души. САЩ заявяват, че нямат намерение да изпращат войски в Украйна, която не е член на НАТО²⁷.

Москва е обвинявана, че води хибридна война срещу Украйна, като използва кибератаки, икономически натиск и пропаганда за провокиране на напрежение. В началото на февруари Държавният департамент на САЩ заяви, че Русия е готова да изфабрикува „претекст за инвазия“ чрез видеоклип под фалшив флаг. Въпреки това намеренията на Кремъл в страната оставаха до голяма степен загадка. В своите аргументи Путин ясно заяви, че вижда в разширяването на НАТО на изток екзистенциална заплаха за Русия³².

Очакван или не, военният конфликт на територията на Украйна от 24.02.2022 г. е факт. Това, което със сигурност можем да очакваме е, че това противопоставяне ще създаде условия за широко използване на военната заблуда в различни количествени и качествени измерения – от тактическа дезинформация до стратегическа измама^{9, 10}.

Целта на настоящия доклад е на базата на анализа на национални и чуждестранни публикации и съществуващите литературни източници да се изследват техниките за военна заблуда, използвани в конфликта в Украйна.

За постигането на тази цел са поставени за решаване следните научно-изследователски задачи:

- да се обобщи теорията за военната заблуда и определят видовете военна заблуда, определени за изследване;
- да се изследват наличните отворени източници на информация относно техниките за военна заблуда, използвани от въоръжените сили на Украйна;
- формулиране на изводи относно използваните техники за военна заблуда в съвременните конфликти.

В хода на изследването са използвани основно методите на системния анализ, синтез, сравнение, изследване на опита, експертни мнения, анализи и изследвания на информационни материали от открити източници.

Анализ на понятието и дефиниране на военната заблуда

1.1. Определение за военна заблуда

При анализа на наличната литература добре формулирано и прецизно определение за заблудата във военните операции срещаме в Доктрината на Сухопътните войски на САЩ, където е отразено, че „заблудата е дейност, предназначена за подвеждане на противника чрез манипулации, изкривяване или фалшифициране на доказателства с цел да бъде принуден да реагира по начин, който е във вреда на собствения му интерес“³³. Тук обаче липсва описанието на основните действащи лица в бойните действия и се обръща внимание единствено и само на похватите, които могат да бъдат използвани⁹.

Според руските специалисти военната заблуда е дефинирана като „действия, предназначени да заблудят врага или да го накарат да действа безразсъдно, които не нарушават нормите на международното хуманитарно право“. Тези действия са приложими при въоръжен конфликт и не попадат в категорията „вероломство“, тъй като не се възползват от доверието на другата страна по отношение на защитата, предвидена в тези норми. Представените примери за военна хитрост са използването на маскировка (камouflаж), примамки, заблуждаващи операции и дезинформация¹².

В Доктрината на въоръжените сили на Република България определението за маскировка е „комплекс от мероприятия и действия, насочени към скриване от разузнаването на противостоящи сили и

въвеждането му в заблуждение за истински състав, бойно построение, бойна готовност и боеспособност, замисъл и характер на действие на силите, както и към осигуряване на внезапност на действие на собствените войски и сили и повишаване на тяхната живучест⁹, което далеч не изчерпва понятието „военна заблуда“, а разглежда само един от неговите аспекти – маскировката⁹.

Като отчитаме нюансите, отразяващи същността на военната заблуда, приликите и разликите в теориите на анализаторите, както и липсващите елементи, неотдаващи значение на цялостния процес по планиране и провеждане на военната заблуда като най-всеобхватно определение за военната заблуда за нуждите на настоящия доклад приемаме следното определение: „Военната заблуда представлява комплекс от процеси, действия, дейности, мерки и мероприятия, осъществявани с цел умишлено подвеждане на даден опонент да предприеме действия в ущърб на собствените си интереси чрез манипулиране процеса му за вземане на решение за отговор, посредством целенасочено и съзнателно довеждане до негово знание на комплекс от истинска, манипулирана, непълна и/или невярна информация“¹⁰.

Така представеното определение дава достатъчно информация за това към кого е насочена, защо се прилага и по какъв начин ще се прилага военната заблуда. Обхващането на широкия кръг от съставни на военната заблуда предоставя възможност тя да бъде класифицирана по различни признаци, както и да се представят основните принципи, които следва да се спазват при необходимост от нейното прилагане.

1.2. Класификация и видове

Изследванията по темата показват, че разработените теории по проблематиката на военната заблуда, споменати в предходния раздел, не отчитат значително количество фактори и представените в тях класификации не обхващат напълно целия спектър показатели и критерии, по които да се характеризират⁹.

В зависимост от мащаба, в който се провежда военната заблуда, тя се подразделя на:

- военна заблуда **на стратегическо ниво**;
- военна заблуда **на оперативно ниво**;
- военна заблуда **на тактическо ниво**.

Военна заблуда на стратегическо ниво. На стратегическо ниво целта е да се повлияе върху способността на противниковите стратегически решения успешно да се противопоставят на собствените национални интереси и цели. Стратегическата заблуда се провежда, за да повлияе на възможността противниковите национални лидери и висши военни командири да вземат точни решения. Цел на стратегическата заблуда е създаването на благоприятни условия за постигане на стратегическите цели на войната. Желаният резултат за противниковите стратегическите цели, политики и операции, които са в полза на собствените и приятелските интереси. Тя се явява отговорност на военнополитическото и военностратегическото ръководство.

Военна заблуда на оперативно ниво. Тук целта на военната заблуда е да повлияе на способността на противниковите оперативни нива при вземането на решения за успешно провеждане на военни операции. Фокусът е да се подкопае способността на противниковите оперативни командири да вземат решения и да провеждат операции. Оперативната заблуда влияе върху решенията на противниковите командири преди, по време и след операцията, така че постигнатият тактически резултат да може да бъде използван на оперативно ниво. Оперативната военна заблуда се използва за скриване на подготовката за провеждане на операция от фронтови или армейски мащаб, въвеждането на противника в заблуждение относно замисъла, главните и други направления, целите и задачите на операцията, а така също и състоянието, разположението и готовността на войските. Осъществяването на военната хитрост на оперативно ниво е задължение на командирите/командващите и щабовете на видовете въоръжени сили и на съвместно ниво⁹.

Военна заблуда на тактическо ниво. Фокусира се върху възможността да се повлияе върху способността на противниковите тактически командири да направят точни и навремени преценки. Целта е да се повлияе на способността на противостоящите командири да вземат решения относно провеждането на боеве и сражения, както и по всякакъв възможен начин да бъдат манипулирани преди и по време на бойните действия. Голяма част от изненадата в хода на бойните действия се постига чрез заблудата. Може да се твърди, че тези два основни компонента са неразривно свързани във военното дело. Тактическата военна заблуда трябва да подпомага и подкрепя оперативните усилия в тази насока.

В зависимост от вида на задачите операцията по въвеждане на противостоящите сили в заблуждение се решават чрез способите – **скриване, имитация, демонстрация и дезинформация**.

Скриването се състои в използване на мероприятия и начини на маскировка, които изключват или затрудняват противостоящите сили в откриването на демаскиращите признаци, а по тях и на самите формирания, техните действия и обекти. Може да се използва за скриване на подготовката на бойните действия и въвеждане на противника в заблуждение относно наличността, състоянието и готовността на подразделенията, частите и съединенията, тяхното въоръжение, способности за използване на огневите средства и водене на бойните действия.

Имитацията представлява възпроизвеждане на демаскиращите признаци, присъщи на реални обекти. Тя предвижда създаването на лъжливи позиции и райони за разполагане на формиранията, лъжливи обекти с използване на макети на техниката и други маскировъчни средства чрез устройване на лъжливи съоръжения, както и чрез обозначаване на признаци за дейност на формиранията, частите и подразделенията.

Демонстрацията (демонстративните действия) е комплекс от преднамерено показване на придвижвания, прегрупиране, съсредоточаване и водене на бой с реални войскови единици. Провежда се с цел сковаване силите на противостоящите сили на второстепенни направления или представяне (показване) на съсредоточаване на голямо количество сили и средства в определени райони. Обикновено се изпълнява с ограничени сили и средства, отделени от съединенията, частите и подразделенията. Провеждащите демонстративни действия формирания могат и да не знаят истинската цел на своите задачи. Това се прави за максимална реалност в демонстрацията.

Дезинформацията има за цел да бъдат предоставени на противника неверни и подвеждащи сведения от най-различен характер. Тя е едно от най-силните средства на оперативната маскировка и това се дължи на големия брой средства и способности за тяхното използване. Дезинформацията се осъществява в строго съответствие със замисъла на командира за провеждане на операцията и въвеждането на противника в заблуждение.

В зависимост от вида на обекта военната заблуда може да бъде **колективна и индивидуална**.

Колективната военна заблуда е насочена към широка аудитория, като целта може да е сричане на моралния дух и волята на противостоящите сили за борба, оказване на влияние върху населението и др.

Индивидуалната военна заблуда е насочена срещу отделни компоненти, от които органите за вземане на решение на опонента да добият информация.

В зависимост от периода на провеждане се подразделят:

- преди провеждането на реалните действия;
- едновременно с реалните действия;
- след приключване на реалните действия.

В зависимост от възприятията, върху които трябва да въздейства, военната заблуда се подразделя на:

- **визуална** – когато е насочена към промяна на визуалните възприятия, снимки, видео и т.н.;
- **звукова** – когато е насочена към изопачаване на данните на звуковото (сигналното) разузнаване;
- **светлинна** – използва се предимно нощем с цел предоставяне на нереални данни или заслепяване;
- **топлинна** – използва се за изопачаване на данните за несъществуващи или за промяна на информация за реални обекти;
- **аналитична** – когато чрез документи, карти или други средства се цели промяна в решенията на органите за управление на противостоящите сили;
- **електронна** – целенасочена промяна на параметрите в електромагнитния спектър;
- **информационна** – когато е насочена към изменение на реалните данни в медии, интернет, киберпространство и т.н.;
- **комбинирана** – между споменатите възприятия.

2. Анализ на използваните техники за военна заблуда в конфликта в Украйна

2.1. На стратегическо ниво

Анализът на използваните видове военна заблуда на стратегическо ниво се фокусира върху официалните изявления на представителите на противостоящите страни – Русия и Украйна, както и на длъжностни лица на НАТО, ЕС, ООН и САЩ.

На 15.02.2022 г. Русия обяви, че изтегля част от силите си край украинската граница към постоянните им бази в потенциална първа сериозна стъпка към деескалация на продължаващата седмици криза със Запада. Решението идва на фона на интензивни дипломатически усилия за осуетяване на предполагаема руска инвазия в Украйна след струпването на над 100 000 руски бойци до общата граница. Кризата достигна пика си след като американски официални лица предупредиха, че пълномасщабна руска атака, включително срещу столицата Киев, е възможна в рамките на дни. На 15.02.2022 г. говорителят на руското военно министерство Игор Конашенков заяви, че част от руските сили край Украйна са приключили своите учения и започват да се изтеглят, като отбеляза, че контингентите от Южния и Западния военен окръг вече са започнали да се товарят за транспортиране и ще се върнат в постоянните си пунктове на дислокация в следващите дни: „След приключването на мероприятията по бойната подготовка войските, както винаги, ще извършват комбинирани маршове към пунктовете на постоянна дислокация“. Ето пример за колективна информационна стратегическа военна заблуда, извършена преди началото на активните действия.

На 19.02.2022 г. CNN излъчи изявление на президента на САЩ Джо Байдън, че Русия се готви да атакува Украйна в следващите дни. Изявлението е направено в Белия дом след проведен телефонен разговор с лидерите на страните членки на НАТО. Според Байдън САЩ имат всички основания да смятат, че Русия ще нахлуе в Украйна през следващите дни. САЩ смятат, че руските войски ще се насочат към украинската столица Киев, град с 2,8 милиона невинни жители. Според САЩ Москва изпраща фалшива информация към руското общество, като се опитва да го заблуди, че Украйна планира офанзива в Донбас. За това няма никакви реални доказателства и противоречи на логиката. Киев няма да предприеме каквито и да било военни действия в региона, докато Русия трупа все повече и повече войски по границата.

На 22.02.2022 г. Съветът за сигурност на ООН се събра спешно заради ситуацията в Украйна. Според генералния секретар на ООН Антониу Гутереш Русия е нарушила териториалната цялост и суверенитета на Украйна чрез признаването на двата отцепили се региона за независими „държави“. Според говорителя Стефан Дюжарик: „ООН, придържайки се към съответните резолюции на Общото събрание, изцяло подкрепя суверенитета, независимостта и териториалната цялост на Украйна в рамките на международно признатите граници на страната. Генералният секретар разглежда решението на Руската федерация като нарушение на териториалната цялост и суверенитета на Украйна, което не съответства на принципите на Устава на ООН“²².

В указа от 21 февруари, с който Владимир Путин призна двете „народни републики“ за независими, не се посочва дали това се отнася само за контролираните от сепаратистите територии или за всички тези, към които те имат претенции. Руските представители, които коментираха въпроса през следващите дни, даваха неясни или дори противоречащи си отговори на въпроса какво точно призна Москва²⁴.

Говорителят на Кремъл Дмитрий Песков каза, че двете образувания са признати в „границите, в които съществуват и в които са провъзгласени“. Тези две граници обаче не съвпадат – сепаратистите имат претенции за територии, които са далеч отвъд тези, които в действителност контролират²⁷.

По-късно говорителката на руското външно министерство Мария Захарова каза, че това е „въпрос за бъдещето“. „Няма нищо изненадващо във факта, че има суверенни държави, чиито граници не са решени или просто не са определени“, каза Захарова. „Това е въпрос за бъдещето, който ще бъде разрешен.“²⁹.

При анализа на статута на Украйна като държава се установи съобщение, че на 07.04.2014 г. Генералният секретар на ООН Бан Ки Мун е направил изявление, чието разпространение е забранено в украинските медии и в интернет. На заседанието на Съвета за сигурност на ООН е повдигнат конфликтът между двете държави – Русия и Украйна. От него беше направен следният извод: Украйна не е регистрирала границите си от 25.12.1991 г. Регистрацията на границите на Украйна като суверенна държава не е извършена в ООН. Следователно може да се предположи, че Русия не извършва никакви нарушения по отношение на Украйна. Според договора за ОНД територията на Украйна е административен район на СССР. Следователно никой не може да бъде виновен за сепаратизъм и насилствена промяна на границите на Украйна. Според международното право страната просто няма официално признати граници. За да разреши този проблем, Украйна трябва да финализира демаркацията на границата със съседните страни и да получи съгласието на съседните страни, включително Русия, за тяхната обща граница. Необходимо е всичко да се документира и да се подпишат споразумения с всички съседни държави. Според Будапещенския меморандум и други споразумения няма граници с Украйна т.е. държавата Украйна не съществува и никога не е съществувала „de jure“³².

При търсене на отговор на въпроса къде е бил Бан Ки Мун, който заема поста на генерален секретар на ООН между 2007 и 2016 г., на 7 април 2014 г. резултатите показват, че той е бил в Руанда по повод 20-годишнината от геноцида в страната. Украйна не е спомената в публикуваното от ООН изказване на Бан по време на церемонията.

Позовавайки се на датата „07.04.2014 г.“, подвеждащата публикация изглежда напуска, че ситуацията в Украйна е била в основна тема на заседанието на Съвета за сигурност на ООН същия ден. Според официалния дневен ред на заседанията и резолюциите на Съвета за сигурност на ООН на 7 април 2014 г. обаче не е имало заседание³².

Дали Украйна е суверенна държава с признати граници е ключов въпрос, който може да разкрие същността на военния конфликт в Украйна – война или военна операция. До произнасянето на ръководните компетентни органи в световен аспект, мненията на специалистите ще са разнородни, в зависимост от характера на приведените аргументи и доказателства.

Анализът на използваните техники за военна заблуда на стратегическо ниво разкрива широкото използване на способите за комбинирани техники на колективна информационна, електронна и административна дезинформация, фокусирани върху основните линии на операциите, а именно – политически, икономически, инфраструктурен, социален, военен и културен аспект.

2.2. На оперативнo ниво

На оперативнo ниво анализът на използваните техники за военна заблуда се базира на фактологията на действията на противопоставящите се страни. Още в първите часове на активните действия като основна среда за прилагане на техниките за военната заблуда бе използвано киберпространството и по-специално приложенията и платформите на социалните мрежи. Възможно е да определим, че от страна на руските въоръжени сили най-често се използват средствата за масова информация (СМИ) – радио и телевизионни канали, докато украинците разчитат повече на социалните мрежи^{27, 29}.

Ежедневно по руските национални телевизии се изнася брифинг от говорителя на руското министерство на отбраната с детайлна информация относно изпълнението на поставените задачи от страна на руските военни формирования, докладва се броят на установените загуби на противниковите сили, както и периодично – броят на загубите в жива сила и техника на собствените сили³¹.

Оперативното построение на руските военни формирования ни позволява да определим оперативните способности, чрез които се цели постигането на желаното крайно състояние, а именно – настъпление на широк фронт, чрез дълбоко вклиняване и териториално разделяне на зоната за провеждане на операцията на т.нар. „котли“. По този начин, след като се формират отделните „котли“ следва тяхното свързване в единна обсадна система.

На оперативнo ниво наред с достоверните публикации за войната в Украйна в социалните мрежи има и много слухове, фалшиви новини и неверифицирани снимки и видеоматериали. Снимки и видеа на ранени хора, ракетни нападения, разрушени сгради, танкове и военни автомобили, преминаващи по улиците. От началото на войната в Украйна социалните мрежи са пълни с подобни публикации на потребители от цял свят. Голяма част от тях могат да бъдат верифицирани, но други изглеждат съмнително. На пръв поглед често е трудно да се установи дали става дума за истина или фейк. При повечето снимки и видеа могат да се проведат проверки, с които се идентифицира мястото, на което са направени. Често е възможно да се направи и сравнение с други кадри. Така например бе доказано, че още преди заповедта на Владимир Путин за нападение специални системи за разминиране вече са се намирали в Украйна³³.

За да могат да бъдат разпознати фалшивите новини, е необходимо специалистите да имат медийна компетентност, както и готовност за критично обмисляне на съдържанията. Оценките на източниците на дезинформация показват и друго: че често само заглавията са подвеждащи – след което в самия материал съдържанието е представено до голяма степен коректно. Затова е важно и това: да се четат не само заглавията, а целите материали.

Ето пример за едно от фалшивите видеа за войната в Украйна:

Нападащи изтребители във вечерното небе, огнени залпове и превъзбуденото заглавие: „Господи!!! Русия нападна Украйна! Вижте това видео!“.

Повечето потребители бяха убедени, че виждат нападение на руски бойни самолети срещу украинската войска долу на земята. Специалистите установиха, че кадрите са от компютърната игра „Arma 3“. Не за пръв път кадри от компютърни игри се използват като софтуер за дезинформация³⁴.

В мащабната кампания за фабрикуването на лъжи и манипулация са въвлечени не само руските медии на властта, но и неговите най-приближени хора, които се готови на всичко, за да сеят смут не само сред световните политически елити, страх и паника сред жителите на европейските страни. Според украинците е очевидно, че планове на руския главнокомандващ за бърза и решителна окупация на Украйна са се провалили. Затова сега той е решен да спечели тази война не с оръжие, а със силата на масова дезинформация и манипулации, с мръсни психологически атаки да пречупи устрема на украинската армия и твърдостта на украинския политически елит, които категорично заявиха, че ще брани страната и народа си до последната капка кръв, да смачкат решителността на украинския народ, готов докрай да защитава своята свобода и независимост³⁶.

При анализа на използваните техники на военна заблуда на оперативно ниво се установи, че широко намират приложение самостоятелни и комбинирани техники на индивидуална и колективна информационна, електронна и административна дезинформация, с помощта на социалните мрежи в киберпространството – Youtube, Twitter, TikTok, Instagram, Facebook и др.

2.3. На тактическо ниво

На тактическо ниво широко приложение имат техниките на военната заблуда – способите скриване, имитация, демонстрация и дезинформация. В повечето случаи се манипулират данните за получените загуби в личен състав, техника и въоръжение, като периодично от изявленията на различни представители информацията се различава драстично.

Най-сериозен опит за дезинформация от страна на президента на Украйна Владимир Зеленски бе съобщението за „чудовищната агресия“ от страна на руски военен кораб спрямо украински граничен пункт, разположен на Змийския остров. Видео съобщението бе излъчено за Guardian News и в последствие публикувано в платформата Youtube на 25.02.2022 г., като към 13.03.2022 г. видеото има 1 231 110 преглеждания. В изявлението си Зеленски, наред с информацията за 137 загинали украински военнорслужещи и 316 ранени, с подobaваща доза трагизъм обяви всички граничари на Змийския остров за „геройски загинали“ и посмъртно ги награди със звание „Герой на Украйна“. Впоследствие се оказа, че никой от намиращите се на острова граничари не е пострадал, както и бе уточнен техният брой 82, а не обявените от Зеленски 14 „герои“³⁷.

В официалният брифинг на министерството на отбраната на Русия обяви нанесените на Украинските въоръжени сили щети, а именно 3593 обекта и съоръжения от военната инфраструктура, 98 самолета, 61 хеликоптера, 126 БЛС, 1159 танкове и бронирани машини, 118 артилерийски системи за залпов огън, 436 артилерийски оръдия и минохвъргачки, 973 единици специална военна техника³⁸.

Заклучение

Вследствие на извършените анализи и проучвания по темата е възможно да се формулират следните изводи:

1. В условията на разрастващия се конфликт в Украйна се установи широко използване на способите и техниките на военната заблуда на всички нива – стратегическо, оперативно и тактическо, целящи постигането на конкретни цели – формиране на обществени нагласи в политическо, икономическо, социално, военно, инфраструктурно и културно отношение.

2. Особеностите на използваните методи за военна заблуда при всяка отделна операция с нейните географски, икономически и военни характеристики в динамичната среда поставят пред военните формирования различни по обем и съдържание задачи, в много случаи и неочаквани, което изисква постоянна готовност и разнообразни ресурси.

3. Необходимо е провеждането на задълбочено специализирано изследване на всяка една от използваните техники на военната заблуда във военния конфликт в Украйна с цел установяване на тенденциите за водене на съвременните психологически и информационни операции, които оказват непосредствено влияние на оперативните и тактическите резултати.

ЛИТЕРАТУРА

1. Атанасова-Кръстева, Невена Цветкова. Необходимостта от адаптивни екипи за действие в екстремални ситуации. В: *Сборник научни доклади – Пети национален конгрес по психология*, брой 1-4, с. 700 – 707, София: „Изток-Запад“. 2008. ISSN 0861-7813.

2. Атанасова-Кръстева, Невена Цветкова. *Психология на кризиса*. Велико Търново: ИК на НВУ „Васил Левски“, 2019. стр. 330. ISBN 978-954-753-290-8.
3. Георгиев, Георги Петров. Взаимодействие между областната и общинската администрация с Българската армия в управлението при бедствия и аварии. В: *Годишник на Военна академия „Г.С.Раковски“: Факултет „Командно-щабен“*, 2018 – с. 400 – 408, ISSN 1312-2991.
4. Георгиев, Георги Петров. *Взривни технологии в аварийно-спасителни работи*. София: Военна академия „Г.С.Раковски“, 2016, стр. 216.
5. Георгиев, Георги Петров. Защита на обекти от критичната инфраструктура от терористични заплахи. В: *Сборник доклади от Международна научна конференция „Сигурност – образование, наука, индустрия“ – втора част*. София: Военна академия „Г. С. Раковски“, 2020, с. 154 – 159, ISBN 978-619-7478-58-7.
6. Георгиев, Георги Петров. Перспективи за използване на формирования от Българската армия за овладяване и/или преодоляване на последствията от бедствия. В: *Сборник материали от военна научна конференция на факултет „Командно-щабен“ на Военна академия „Г. С. Раковски“*. *Годишник на Военна академия „Г.С.Раковски“: Факултет „Командно-щабен“* 2/2014, с. 81 – 89. ISSN 1312-2991.
7. Георгиев, Георги Петров; Филипов, Х.; Георгиев, Г.; Петров, К. *Организиране и провеждане на операции по търсене и спасяване*. София: Военна академия „Г. С. Раковски“, 2012, стр. 123.
8. Георгиев, Христо Александров. Участие и специфични задачи на ССО в операции по преодоляването на кризи в мирно време. В: *Сборник с материали от конференция на факултет „Артилерия, ПВО и КИС“*. Шумен, 2019, стр. 118-124, ISSN 2367-7902
9. Градев, Калин Веселинов. *Военната заблуда като част от военното изкуство*. София: Военна академия „Г. С. Раковски“, 2015, стр. 162. ISBN 978-954-9348-65-1.
10. Градев, Калин Веселинов. Подход за разработване на вариант за действие при планиране на операциите. В: *Сборник доклади от международна научна конференция „Сигурност – образование, наука, индустрия“*. *Втора част*. с. 26-29. ISBN 978-619-7478-58-7
11. Кокудева, Петрана Тошкова, Теорията на системите в епохата на платформите. В: *Сборник доклади от Международна годишна научна конференция на НВУ „Васил Левски“*, 27-28 май 2021 г., Велико Търново: ИК на НВУ „Васил Левски“, с. 1084-1090. ISSN 2367-7481.
12. Кръстев, Кръстю Иванов. *Тактическо разузнаване във военните формирования*. Велико Търново: ИК на НВУ „Васил Левски“, 2021, стр. 161. ISBN 978-954-753-326-4.
13. Маринов, Петър Господинов. *Тероризмът – абстракции и реалности*. София: „Изток – Запад“, 2016, стр.295. ISBN 619152866-3.
14. Петков, Йордан Методиев. Основни насоки за повишаване на уменията на личния състав на разузнавателните формирования. В: *Сборник с материали от конференция на факултет „Артилерия, ПВО и КИС“* – Шумен, 2019, с. 106 – 111. ISSN 2367-7902
15. Радева, Николина Радкова. *Актуални аспекти на защитата на населението при бедствени ситуации*. Варна: Степно, 2019, стр. 141.
16. Романова, Христиана Ангелова. *Потенциални антропогенни екокатастрофи във Варненски регион. Стратегия за защита на населението и запазване на биоразнообразието*. Варна: МУ-Варна, 2014.
17. Atomic Heritage Foundation. *The U.S. Nuclear Weapons Complex Map*. [online] <https://www.atomicheritage.org/location/us-nuclear-weapons-complex-map>, last accessed 21:42, 13 Mar 2022.
18. Axios.com. <https://www.axios.com/ukraine-civilian-deaths-russia-invasion-a9879347-36ed-433a-ba43-6c80dc7d2699.html>
19. Borrell, Josep. *EU to help Ukraine with intelligence from own satellite centre*-EU's Borrell. [online] <https://www.devdiscourse.com/article/technology/1941820-eu-to-help-ukraine-with-intelligence-from-own-satellite-centre-eus-borrell>, Reuters | Brussels | Updated: 28-02-2022 20:30 IST | Created: 28-02-2022 20:30 IST.
20. CBS News. *Russian forces close in on Ukraine's capital as death toll mounts*. <https://www.cbsnews.com/live-updates/russia-ukraine-news-kyiv-war-putin-invasion-talks-today/>
21. Corera, G. *Ukraine invasion: Putin puts Russia's nuclear forces on „special alert“*. 28.02.2022. [online] <https://www.bbc.com/news/world-europe-60547473>
22. Jerome Socolovsky; Jonathan Franklin. *A million people have fled Ukraine as Russia nears takeover of port city*. [online] <https://www.npr.org/>
23. JP3-13.4 Military Deception,
24. Many Ukrainian Nuclear Power Reactors No Longer Produce Electricity. *The New York Times* [online] nytimes.com
25. Maps of Russia's invasion of Ukraine. [online] <https://www.washingtonpost.com/>
26. Natalia Zinets; Editing by Mark Potter, Reuters. *Ukraine Receives Shipment of Machine Guns and Surveillance Gear From Canada*. [online] <https://www.usnews.com/news/world/articles/2022-02-19/ukraine-receives-shipment-of-machine-guns-and-surveillance-gear-from-canada>, Feb. 19, 2022, at 2:27 p.m.
27. O'Falk, Thomas. *How realistic is Vladimir Putin's nuclear threat?* [online] <https://www.aljazeera.com/news/2022/3/3/how-realistic-is-vladimir-putins-nuclear-threat>, 3 Mar 2022, last accessed 21:42, 13 Mar 2022)
28. OPS(EADRCC)(2022)0013-REV1 – NU – RiA – UKRAINE.
29. OPS(EADRCC)(2022)0016 – NU – Enclosure 1 – UCPM table of offers.
30. OPS(EADRCC)(2022)0016 – NU – Ukraine Situation Report #2.
31. Radio Free Europe. *Second Round Of Talks Set To Take Place As Russia Continues Shelling Ukrainian Cities*. [online] <https://www.rferl.org/>
32. *Russia invades Ukraine live updates: 2nd round of talks ends with one agreement: to meet again*. [online] <https://www.npr.org/live-updates/russia-ukraine-kherson-refugees>

33. Russia-Ukraine conflict 2021 – 2022 – statistics & facts. [online] <https://www.statista.com/>
34. Scribner, H. Gitanjali Poonia. Russia-Ukraine updates: Hundreds of Ukrainian troops evacuated from Mariupol steel plant. [online] <https://www.deseret.com/>
35. U.S. Sanctions Against Russia: Summary as of Wednesday, March 1, 2022. [online] <https://www.jdsupra.com/>
36. USMC Major Jessica Meyeraan, USAF Joint Forces Staff College. Military deception: Hiding the real – showing the fake major Mark Johnson. Joint and Combined Warfighting School, 7 March 2003.
37. Vardhan Harsh. Canada's Space Company To Provide Intelligence To Ukraine Via Satellites To Resist Russia. [online] <https://www.republicworld.com/world-news/russia-ukraine-crisis/canadas-space-company-to-provide-intelligence-to-ukraine-via-satellites-to-resist-russia-articleshow.html>, Last Updated: 11th March, 2022 21:10 IST.
38. Watts, William. Here's the technology being used to watch Russian troops as Ukraine invasion fears linger. [online] <https://www.marketwatch.com/story/how-fears-of-russian-invasion-of-ukraine-put-open-source-intelligence-in-spotlight-11645033603?mod=home-page>, Last Updated: Feb. 17, 2022 at 6:36 a.m. ET, First Published: Feb. 16, 2022 at 12:46 p.m. ET.

REFERENCES

1. Atanasova-Krasteva, Nevena Tsvetkova. Neobходимостта от адаптивни екипи за действие в екстремални ситуации. In: *Сборник научни доклади – Петти национален конгрес по психологија*, брой 1-4, с. 700 – 707, София: „Изток-Запад“. 2008. ISSN 0861-7813.
2. Atanasova-Krasteva, Nevena Tsvetkova. *Психологија на кризата*. Велико Тарново: IK на НВУ „Васил Левски“, 2019. стр. 330. ISBN 978-954-753-290-8.
3. Georgiev, Georgi Petrov. Vzaimodeystvie mezhdu oblastnata i obshtinskata administratsiya s Balgarskata armiya v upravlenieto pri bedstviya i avarii. In: *Godishnik na Voenna akademiya „G.S.Rakovski“: Fakultet „Komandno-shtaben“*, 2018 – с. 400 – 408, ISSN 1312-2991.
4. Georgiev, Georgi Petrov. *Vzrivni tehnologii v avariyno-spasitelni raboti*. Sofia: Voenna akademiya „G.S.Rakovski“, 2016, стр. 216.
5. Georgiev, Georgi Petrov. Zashchita na obekti ot kritichnata infrastruktura ot teroristichni zaplahi. In: *Sbornik dokladi ot Mezhdunarodna nauchna konferentsiya „Sigurnost – obrazovanie, nauka, industriya“ – vtora chast*. Sofia: Voenna akademiya „G. S. Rakovski“, 2020, с. 154 – 159, ISBN 978-619-7478-58-7.
6. Georgiev, Georgi Petrov. Perspektivi za izpolzvanie na formirovaniya ot Balgarskata armiya za ovladavane i/ili preodolyavane na posledstviyata ot bedstviya. *Sbornik materialy ot voennonauchna konferentsiya na fakultet „Komandno-shtaben“ na Voenna akademiya „G. S. Rakovski“*. In: *Godishnik na Voenna akademiya „G.S.Rakovski“: Fakultet „Komandno-shtaben“ 2/2014*, с. 81 – 89. ISSN 1312-2991.
7. Georgiev, Georgi Petrov, Filipov, H., Georgiev, G. & Petrov, K. *Organizirane i provezhdane na operatsii po tarsene i spasyavane*. Sofia: Voenna akademiya „G. S. Rakovski“, 2012, стр. 123.
8. Georgiev, Hristo Aleksandrov. Uchastie i spetsifichni zadachi na SSO v operatsii po preodolyavaneto na krizi v mirno vreme. In: *Sbornik s materialy ot konferentsiya na fakultet „Artileriya, PVO i KIS“ – Shumen*, 2019, стр. 118-124, ISSN 2367-7902
9. Gradev, Kalin Veselinov. *Voennata zabluda kato chast ot voennoto izkustvo*. Sofia: Voenna akademiya „G. S. Rakovski“, 2015, стр. 162. ISBN 978-954-9348-65-1.
10. Gradev, Kalin Veselinov. Podhod za razrabotvane na variant za deystvie pri planirane na operatsiite. In: *Sbornik dokladi ot mezhdunarodna nauchna konferentsiya „Sigurnost – obrazovanie, nauka, industriya“*. Vtora chast, с. 26-29. ISBN 978-619-7478-58-7
11. Kokudeva, Petrana Toshkova. Teoriyata na sistemite v epohata na platformite. *Sbornik dokladi ot Mezhdunarodna godishna nauchna konferentsiya na НВУ „Васил Левски“*, 27-28 may 2021 г., Велико Тарново: IK на НВУ „Васил Левски“, с. 1084-1090. ISSN 2367-7481.
12. Krastev, Krastyu Ivanov. *Takticheskoto razuznavane vav voennite formirovaniya*. Veliko Tarnovo: IK на НВУ „Васил Левски“, 2021, стр. 161. ISBN 978-954-753-326-4.
13. Marinov, Petar Gospodinov. *Terorizmat – abstraktsii i realnosti*. Sofia: „Изток – Запад“, 2016, стр. 295. ISBN 619152866-3.
14. Petkov, Yordan Metodiev. Osnovni nasoki za povishavane na umeniyata na lichniya sastav na razuznavatelните formirovaniya. In: *Sbornik s materialy ot konferentsiya na fakultet „Artileriya, PVO i KIS“ – Shumen*, 2019, с. 106 – 111. ISSN 2367-7902
15. Radeva, Nikolina Radkova. *Aktualni aspekti na zashchitata na naselenieto pri bedstveni situatsii*. Varna: Steno, 2019, стр. 141.
16. Romanova, Hristiana Angelova. *Potentsialni antropogenni ekokatastrofi vav Varnenski region. Strategiya za zashchita na naselenieto i zapazvane na bioraznoobrazieto*. Varna: MU-Varna, 2014.
17. Atomic Heritage Foundation. *The U.S. Nuclear Weapons Complex Map*. [online] <https://www.atomicheritage.org/location/us-nuclear-weapons-complex-map>, last accessed 21:42, 13 Mar 2022.
18. Axios.com. <https://www.axios.com/ukraine-civilian-deaths-russia-invasion-a9879347-36ed-433a-ba43-6c80dc7d2699.html>
19. Borrell, Josep. *EU to help Ukraine with intelligence from own satellite centre*-EU's Borrell. [online] <https://www.devdiscourse.com/article/technology/1941820-eu-to-help-ukraine-with-intelligence-from-own-satellite-centre-eus-borrell>, Reuters | Brussels | Updated: 28-02-2022 20:30 IST | Created: 28-02-2022 20:30 IST.
20. CBS News. *Russian forces close in on Ukraine's capital as death toll mounts*. <https://www.cbsnews.com/live-updates/russia-ukraine-news-kyiv-war-putin-invasion-talks-today/>
21. Corera, G. *Ukraine invasion: Putin puts Russia's nuclear forces on „special alert“*. 28.02.2022. [online] <https://www.bbc.com/news/world-europe-60547473>

22. Jerome Socolovsky, Jonathan Franklin. *A million people have fled Ukraine as Russia nears takeover of port city*. [online] <https://www.npr.org/>
23. JP3-13.4 Military Deception,
24. Many Ukrainian Nuclear Power Reactors No Longer Produce Electricity. *The New York Times*. [online] [nytimes.com](https://www.nytimes.com)
25. Maps of Russia's invasion of Ukraine. [online] <https://www.washingtonpost.com/>
26. Natalia Zinets, Mark Potter (ed.). *Ukraine Receives Shipment of Machine Guns and Surveillance Gear From Canada*. Reuters. [online] <https://www.usnews.com/news/world/articles/2022-02-19/ukraine-receives-shipment-of-machine-guns-and-surveillance-gear-from-canada>, Feb. 19, 2022, at 2:27 p.m.
27. O'Falk, Thomas. *How realistic is Vladimir Putin's nuclear threat?* [online] <https://www.aljazeera.com/news/2022/3/3/how-realistic-is-vladimir-putins-nuclear-threat>, 3 Mar 2022, last accessed 21:42, 13 Mar 2022)
28. OPS(EADRCC)(2022)0013-REV1 – NU – RiA – UKRAINE.
29. OPS(EADRCC)(2022)0016 – NU – Enclosure 1 – UCPM table of offers.
30. OPS(EADRCC)(2022)0016 – NU – Ukraine Situation Report #2.
31. Radio Free Europe. *Second Round Of Talks Set To Take Place As Russia Continues Shelling Ukrainian Cities*. [online] <https://www.rferl.org/>
32. Russia invades Ukraine live updates: 2nd round of talks ends with one agreement: to meet again. [online] <https://www.npr.org/live-updates/russia-ukraine-kherson-refugees>
33. *Russia-Ukraine conflict 2021 – 2022 – statistics & facts*. [online] <https://www.statista.com/>
34. Scribner, H., Gitanjali Poonia. *Russia-Ukraine updates: Hundreds of Ukrainian troops evacuated from Mariupol steel plant*. [online] <https://www.deseret.com/>
35. *U.S. Sanctions Against Russia: Summary as of Wednesday, March 1, 2022*. [online] <https://www.jdsupra.com/>
36. USMC Major Jessica Meyeraan, USAF Joint Forces Staff College. *Military deception: Hiding the real – showing the fake* major Mark Johnson. Joint and Combined Warfighting School, 7 March 2003.
37. Vardhan Harsh. *Canada's Space Company To Provide Intelligence To Ukraine Via Satellites To Resist Russia*. [online] <https://www.republicworld.com/world-news/russia-ukraine-crisis/canadas-space-company-to-provide-intelligence-to-ukraine-via-satellites-to-resist-russia-articleshow.html>, Last Updated: 11th March, 2022 21:10 IST.
38. Watts, William. *Here's the technology being used to watch Russian troops as Ukraine invasion fears linger*. [online] <https://www.marketwatch.com/story/how-fears-of-russian-invasion-of-ukraine-put-open-source-intelligence-in-spotlight-11645033603?mod=home-page>, Last Updated: Feb. 17, 2022 at 6:36 a.m. ET, First Published: Feb. 16, 2022 at 12:46 p.m. ET.

ОПЕРАТИВНИ СПОСОБНОСТИ НЕОБХОДИМИ НА СИСТЕМАТА ЗА КОМАНДВАНЕ И УПРАВЛЕНИЕ ЗА СПРАВЯНЕ С ПРЕДИЗВИКАТЕЛСТВОТА, ПРОИЗХОЖДАЩИ ОТ БЪДЕЩАТА ОПЕРАТИВНА СРЕДА

майор Кръстьо Парасков

Военна академия „Г. С. Раковски“, k.paraskov@rmdc.bg

Резюме: Бъдещото развитие и оперативна съвместимост на системата за командване и управление в интегрираната система за противовъздушна и противоракетна отбрана на НАТО изисква генериране на бойни и технически оперативни способности, които са необходими за справянето с предизвикателствата, произхождащи от бъдещата оперативна среда.

Ключови думи: *система за командване и управление; оперативна съвместимост; оперативни способности; оперативна среда*

OPERATIONAL CAPABILITIES REQUIRED BY THE COMMAND AND CONTROL SYSTEM TO DEAL WITH THE CHALLENGES ORIGINATING FROM THE FUTURE OPERATIONAL ENVIRONMENT

Major Krastyo Paraskov

Rakovski National Defence College

Sofia, Bulgaria

E-mail: k.paraskov@rmdc.bg

Abstract: The future development and interoperability of the command and control system of NATO's integrated air and missile defense system requires the generation of the combat and technical operational capabilities needed to meet the challenges posed by the future operational environment.

Keywords: *command and control system; interoperability; operational capabilities; operational environment*

Визията на НАТО за бъдещата оперативна среда¹ предвижда бърз растеж и непрекъсната промяна в технологиите през следващите двадесет години, което ще създаде нестабилна, несигурна, сложна и неопределена среда. Алиансът ще бъде изправен пред разнообразие от непредсказуеми заплахи във всички пространства (въздух, космос, суша, море, кибер- и социално) в целия спектър от противоборства. Въвеждането на нови технологии е потенциално решение за справяне с предизвикателствата пред НАТО и осигуряване на желаните оперативни способности на системата за командване и управление (СКУ). Текущите технически и социални иновации ще доведат до експоненциални промени в конфликтите през следващите години, създавайки различни среди за реализация на възможностите на СКУ в бъдещата оперативна среда².

Експертен екип от Центъра за изследване, изграждане и усъвършенстване на способности на НАТО за командване и управление (Command and Control Centre of Excellence – C2COE) дефинира определени оперативни способности, необходими на оперативно ниво за изпълнение на поставените задачи и съответните необходими технологични развития за осигуряването им, с което се постига необходимата оперативна съвместимост между всички елементи от Интегрираната система за противовъздушна и противоракетна отбрана на НАТО. Тези оперативни способности и технологични развития представляват селекция от възможности, които определят настоящата оперативна среда. Извършен е анализ между всяка оперативна способност и технологичния „реализиращ елемент“, който трябва да бъде изпълнен³.

Въз основа на извършен Делфи-анализ и изследване на съответните оперативни способности се определи нивото на изпълнение на способностите на СКУ на българските Военновъздушни сили и системите за командване и управление на страните, членки на НАТО, в настоящия момент и необходимите способности

през 2035 г. Оценява се до каква степен способността е изпълнена сега и какви ще бъдат очакванията за изпълнение през 2035 г. по скала от 0 (изобщо) до 5 (напълно), всички резултати са осреднени и са изобразени в графика за всяка една оперативна способност.

Това изследване и последващият анализ мохдй да послужат като „списък с желания“ за необходимите оперативни способности и да ръководят придобиването и развитието на бъдещи технологии, които да се прилагат в щабове на оперативно ниво⁴. Необходимите оперативни способности са:

● **Оперативна способност 1** – планиране и провеждане на операции от различни дислокации (мобилност на системата), като основни реализиращи елементи са:

- използване на публични комуникационни мрежи, включително Интернет, за обмен на информация, което ще осигури мрежовата взаимосвързаност на всички елементи, без значение къде се намират;
- автоматизиран обмен на информация между специализирани военни мрежи и публични мрежи;
- силно защитена и криптирана комуникация;
- въвеждане на технологии с виртуална и разширена реалност (BPP) в работните процеси.

● **Оперативна способност 2** – възможност за развързване на специализирани елементи за връзка и взаимодействие, за да се даде възможност за непрекъснатост на управлението и да се поддържат връзките и взаимодействието, включително и с гражданския сектор, когато е необходимо, като основни реализиращи елементи са:

- използване на публични мрежи като средство за обмен на информация;
- автоматизиран обмен на информация между специализирани военни мрежи и публични мрежи;
- силно защитена и криптирана комуникация;
- въвеждане на BPP технологии в работните процеси.

● **Оперативна способност 3** – възможност за свързване на елементи (участници и платформи) в мрежова среда и осигуряване на гъвкава, сигурна и устойчива инфраструктура за постигане на комуникация от точка до точка чрез автоматизирана комуникационна информационна система, като основни реализиращи елементи са:

- специализирани мрежови технологии;
- адаптивен контрол на достъп към мрежите;
- стандартизация на мрежи и протоколи;
- използване на изкуствен интелект (ИИ) за полуавтоматизирана поддръжка при процеса за вземане на решение за динамично мрежово планиране, топография и конфигуриране.

● **Оперативна способност 4** – постигане на необходимо ниво на информационна осведоменост, необходимо за командване и управление на въздушните операции, като непрекъснато се наблюдават и следят следните елементи: опозната картина на въздушната обстановка, разузнаване, граждански сектор, комуникационно-информационна система, електромагнитен спектър, екология, медицина и киберпространство, като основни реализиращи елементи са:

- съхранение на данни в облачни пространства;
- автоматизирано интегриране на различни сензори;
- автоматизирано интегриране на обработената информация в обща оперативна картина;
- персонализирани информационни дисплеи;
- блокчейн* технология, приложена към данните от сензорите;
- използване на технология за разширена реалност (PP), за вътрешните работни процеси в управлението.

● **Оперативна способност 5** – съхраняване, обработване, съвместяване и използване на получените изображения, данни, и разузнавателна информация съгласно изискванията и нуждите на потребителите, като основни реализиращи елементи са:

- съхранение на данни в облачни пространства;
- автоматизирано интегриране на различни сензори;
- автоматизирано интегриране на обработената информация в обща оперативна картина;

* Блокова верига или блокчейн е метод за съхранение на информация в компютърна мрежа, който представя непрекъснато растящ списък от компютърни записи, наречени „блокове“, свързани помежду си и кодирани криптографски. // Narayanan, Arvind, Bonneau, Joseph, Felten, Edward. Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton, Princeton University Press, 2016.

- персонализирани информационни дисплеи;
- блокчейн технология, приложена към данните от сензорите;
- специализиран персонал за анализ на данни;
- ИИ, поддържащ дейността на анализаторите на данни;
- прогнозиране на събития.

● **Оперативна способност 6** – възможност за обединяване на всички налични способности за анализ и обработка на данни от разузнавателна информация, наблюдението и разузнаването, за да се осигури ефективно разпределение на задачите, съвместяване на други възможности за събиране, обработка и разпространение на информация до потребителите, като основни реализиращи елементи са:

- съхранение на данни в облачни пространства;
- автоматизирано интегриране на различни сензори;
- алгоритми за машинно обучение за съвместяване;
- използване на ИИ за автономно планиране и използване на сензори;
- разпространение на информация сред потребителите съгласно нивата на достъп.

● **Оперативна способност 7** – планиране, синхронизиране и координиране на съвместна огнева поддръжка, установяване и управление на процеса по определяне на вероятни цели за въздействие, включително чувствителни спрямо времето цели по полуавтоматизиран способ, като основни реализиращи елементи са:

- използване на ИИ за подпомагане работата на операторите за огнева поддръжка;
- използване на ИИ, осигуряващ правнонормативната уредба;
- полуавтономно планиране на въздействието въз основа на вероятностни модели;
- симулация на синхронизация на въздействието;
- сформирание на екипи човек-машина за развитие на варианти за действие;
- използване на технологии за BPP за подпомагане на работните процеси.

● **Оперативна способност 8** – провеждане на кибер- (компютърни и мрежови) атаки срещу про-тивникови компютърни информационни системи, компютърни мрежи, персонални електронни устройства и инфраструктура като част от процеса на определяне на вероятни цели за въздействие, като основни реализиращи елементи са:

- използване на киберсензори за откриване на уязвимост на противостоящите сили;
- създаване на разбираема картина на кибер пространството;
- използване на ИИ за подпомагане на синхронизирането на кибер въздействието с физическото въздействие;
- автоматизирано генериране и изпълнение на варианти за действие, свързани с кибер пространството.

● **Оперативна способност 9** – използване на социалните медии за разузнавателни цели (като източник), системата за командване и управление (като средство за споделяне на информация) и стратегическите комуникации (като средство за масова информация). Реализиращи елементи са:

- класификация на мрежовата сигурност;
- свързаност в мрежата базирана на ниво експертиза;
- използване на ИИ за определяне на вариантите за действие за използване на стратегически комуникации.

● **Оперативна способност 10** – използване, управление и координиране на специализирани програми (ботове*) за социалните медии, като основни реализиращи елементи са:

- използване на ИИ-алгоритми за разпознаване на шаблони в информацията от социалните медии;
- откриване и уведомяване при наличие на неприятелски намерения (заплахи и др.);
- визуализация на разпознати снимки и обекти.

● **Оперативна способност 11** – извършване на процеси по оценка на операцията и тя да се използва, при необходимост при анализа на по-горното и по-долното ниво, като основни реализиращи елементи са:

- съхранение на информация в облачно пространство;
- използване на симулационни системи;
- специализиран персонал за анализ на данни;
- използване на ИИ, подпомагащ персонала за анализ на данни;

- прогнозен анализ въз основа на натрупани данни и експертни модели;
- адаптивни алгоритми за генериране и оценка на варианти за действие.

● **Оперативна способност 12** – оценка на въздействието на цивилното население върху военните операции и оценка на ефектите на военните операции върху цивилното население, като основни реализиращи елементи са:

- динамичен анализ на социалната мрежа, показващ (симулирани) ефекти от действията;
- постоянно наблюдение;
- използване на ИИ за извършване на прогнозен анализ, базиран на експертни и специфични модели.

● **Оперативна способност 13** – планиране, внедряване, поддръжка и експлоатация на стабилна и многослойна комуникационна мрежа, способна да предава по защитен и незащитен начин, при необходимост, всички данни за основните и функционалните услуги, глас, видео, виртуална реалност и изображения с разширена реалност, за да се осигури комуникация със сили и средства на НАТО, съюзници извън НАТО и оторизирани невоенни елементи, като основни реализиращи елементи са:

- динамична класификация на нивата на сигурност в мрежата;
- използване на ИИ-алгоритми за приоритизиране на комуникациите;
- използване на адаптивни протоколи;
- преобразуване на текст-реч/реч-текст;
- използване на технологии за BPP за подпомагане на работните процеси.

● **Оперативна способност 14** – осигуряване на ефективно и ефикасно управление на информацията чрез разпределено търсене, архивиране на данни, използване на социални мрежи, база данни и когнитивно изчисление. Информацията трябва да бъде откриваема, достъпна, постижима, запазвана, за еднократна употреба, обозначена, проследима и възпроизвеждима, за да се даде възможност за вземане на решения чрез споделяне на информация в рамките на НАТО и между нациите и съответните общности по интереси, като основни реализиращи елементи са:

- прогнозно търсене;
- съхранение на информация в облачно пространство;
- класификация и управление на информацията;
- използване на ИИ за сформирание на екипи човек-машина за конструиране на персонализирани информационни модели въз основа на поставените задачи;
- инструменти за анализ на информация (извличане на факти, извличане на намерения, класифициране на обекти, автоматично прехвърляне на метаданни);
- използване на технологии за BPP за подпомагане на работните процеси.

● **Оперативна способност 15** – откриване на компютърни мрежови атаки срещу собствени компютърни информационни системи, компютърни мрежи, лични електронни устройства и инфраструктура и интегриране на ефективна киберзащита, за да се сведе до минимум уязвимостта, да се поддържа степента на непрекъснатост на операцията приемлива за командира по време на провеждане на бойни действия и за възстановяване на оперативни способности след въздействие, като основни реализиращи елементи са:

- използване на ИИ за откриване на аномалии в мрежовия трафик;
- специализирани алгоритми, подпомагащи обучението за откриване на неприятелски кибер атаки.

● **Оперативна способност 16** – поддържане целостта на информацията, като се гарантира, че тя остава некомпрометирана в непрекъсната линия от подателя до получателя чрез технологични и/или други средства, като основни реализиращи елементи са:

- инструменти за киберзащита, включително валидиране на информационни канали;
- квантова комуникация*;
- адаптивен контрол на достъп към мрежите, следене кой и какъв достъп има до информация.

● **Оперативна способност 17** – осигуряване на подходящо ниво на защита на силите, интегриране и използване на средства и процедури за защита на силите, включително прилагане на оперативна

* Бот (от „робот“) се нарича компютърна програма, която използва мрежови услуги, предназначени за хората, с цел да извършва автоматични действия, например обработка на данни. Използването на бот позволява иначе трудоемки задачи да бъдат решени автономно. <https://bg.wikipedia.org/wiki/Бот>

сигурност, информационна сигурност, комуникационна сигурност, химическа, биологична, радиационна и ядрена защита, защита от импровизирани взривни устройства и политики и стандарти за защита на здравето, като основни реализиращи елементи са:

- алгоритми за обучение за откриване на модели на защита;
- уведомяване на командването за нарушения на правилата, политиките и стандартите въз основа на получена информация от сензорите (физични, физиологични, биологични, химични и др.).

От изложеното дотук може да се отбележи, че съществуват няколко реализиращи елементи, показващи че някои технологични разработки са от значение за множество оперативни способности. Най-значимите технологични разработки са:

- мрежови технологии за съхранение и обмен на информация;
- интегриране на информация от различни видове сензори;
- приложения и инструменти за поддръжка на ИИ (машинно обучение, предвиждащи модели, вероятностни модели, експертни модели);
- анализ и разпространение на информация;
- технологии за съвместяване на човек-машина процеси;
- симулационни технологии, поддържани от ИИ.

Тези реализиращи елементи най-често трябва да подобрят достъпа до информация, информационната осведоменост, оперативната съвместимост, подпомагане на разузнаването, надеждността и гъвкавостта на комуникационната система и сигурността. Това пояснява баланса, който трябва да бъде намерен между стандартизирани и сигурни (затворени) системи, от една страна, и гъвкави и отворени системи, от друга.

На фигура 1 са визуализирани в обща графика всичките необходими оперативни способности, посочени по-горе.

Очаква се за способностите, при които се наблюдава най-голяма разлика, НАТО и страните-членки да положат значителни усилия за подобряването им. Въвеждането и спазването на стандартите е от решаващо значение за достигане на необходимите оперативни способности за цялостното изпълнение на въздушните операции. Тези резултати може да не се приемат за стандарт, но те дават индикация и направление кои способности на страните-членки на НАТО и други партньори все още може да се развият, за да се подобрят настоящите способности и да се осигури по-доброто справяне с прогнозираната бъдеща оперативна среда.

Една от най-значимите способности за СКУ е способността „мобилност“ или работата от различни дислокации. Командирът трябва да запази способностите си в театъра на военните действия и да може да изпълнява задълженията си от всяка една позиция, на която е дислоциран.

Използването на публични мрежи и обменът на криптирана информация по автоматичен начин, между мрежи с различна класификация ще бъде от решаващо значение. Ще бъде необходимо да се разчита на взаимодействие чрез технологии за BPP, за да се гарантира контакт между всички участници в зоната за отговорност.

Способността за обмен на информация с всички участници на оперативно ниво по гъвкав, сигурен и контролиран начин, както и за постигане на адекватна степен на информационна осведоменост в различните области, ще бъде важна за оперативния командир, като тази способност ще бъде осигурена от система за контрол на достъпа и ИИ технологията. Използването на криптиращи технологии, за да се гарантира достоверността на информацията, на база на която се вземат решения, ще бъде от решаващо значение в бъдеще⁵.

* Квантова комуникация е бързоразвиваща се авангардна област с гарантирано бъдеще в направлението на информационните и комуникационните технологии, която се базира на квантово споделяне на секретни ключове при криптирането на данните. Целта им е да осигурят високоскоростно, надеждно и сигурно предаване на информационни трафични потоци между комуникиращите страни с помощта на квантово криптиране и декриптиране в реално време. Тяхното най-голямото предимство е, че се гарантира защитата срещу подслушване и копиране при предаване на секретна информация на сравнително големи разстояния. Чрез иманентна обратна връзка в сплетената фотонна система при неототоризирано проникване в канала потокът от данни се преустановява или продължава със заблуждаващ реверс. [online] <https://www.inrme.bas.bg/index.php/project-quasar>

1. Мобилност;
2. Развързване на специализирани елементи за връзка и взаимодействие;
3. Свързаност в мрежова среда;
4. Информационна осведоменост;
5. Съхраняване, обработване, съвместяване и използване на получените изображения, данни, и разузнавателна информация;
6. Обединяване на всички налични способности за анализ и обработка на данни;
7. Съвместна огнева поддръжка;
8. Провеждане на кибер атаки;
9. Използване на социалните медии, командването и управлението и стратегическите комуникации;
10. Използване, управление и координиране на специализирани програми (ботове);
11. Оценка на операцията;
12. Оценка на въздействието на военните операции върху цивилното население;
13. Планиране, внедряване, поддръжка и експлоатация на стабилна и многослойна комуникационна мрежа;
14. Управление на информацията;
15. Откриване на компютърни мрежови атаки;
16. Цялост на информацията;
17. Защита на силите.



Фиг. 1. Необходими оперативни способности на СКУ

Възможността за извършване на процеса по оценка на операцията въз основа на по-точни и актуализирани данни означава, че командирът може да използва по-ефективно своите сили и средства. Очаква се това да оптимизира продължителността на операцията⁶.

Функциите, от които СКУ на оперативното ниво ще се нуждае в бъдеще, няма да се различават съществено от тези, които съществуват в момента. Това, което се променя, е начинът на изпълнение на тези функции, структурата на групите и отделите, съвместните екипи и връзката между тях, всичките те взаимосвързани и работещи като система от системи с новите технологии⁷. Бъдещите технологии за СКУ, по-специално на оперативното ниво, са насочени към подпомагане на командирите и персонала да получават по-бързо информация с по-високо качество, да я обработват ефективно и да им помагат да вземат ефективни решения въз основа на тази информация.

Очаква се около 2035 г. екипи от хора и инструменти от ИИ да си партнират, за да водят бъдещите операции по-ефективно. Новите технологии, като изкуствения интелект, притежават потенциала да подобрят СКУ на всички нива. Тъй като в СКУ ситуационната осведоменост и вземането на решения се заключават в процеса по разбиране и определяне на действията, които трябва да се предприемат, използването на ИИ е очевиден избор в СКУ⁸.

ЛИТЕРАТУРА

1. Strategic foresight analysis ACT, 2017.
2. NATO's long term military transformation. Read Ahead for Long-term Military Transformation. Workshop, 2016.
3. The Future of the Command Post, Part 1. A NATO Command and Control Centre of Excellence Study, 2019.

4. Пак там.

5. Избор на критерии за качество и оптималност на планирането на авиационна система при планиране на композитна въздушна операция. Въздушният суверенитет и единно европейско въздушно пространство. В: *Сборник доклади от научна конференция на Военна академия „Г. С. Раковски“, Фондация „Български ВВС“ и катедра „ВВС и ПВО“*, 09.10.2019. София: Военна академия „Г. С. Раковски“, стр. 78-92. ISBN 978-619-7478-36-5.

6. Command and control operational requirements and system implementation. *Information and Security, An International Journal*, Vol.5, 2000.

7. Кокудева, П. Сложните системи и системата от системи в сигурността. Въздушният суверенитет и единно европейско въздушно пространство. В: *Сборник доклади от научна конференция*, 9 октомври 2019. София: Военна академия „Г. С. Раковски“, стр. 143-153. ISBN 978-619-7478-36-5.

8. The Future of the Command Post. Part 2. *A NATO Command and Control Centre of Excellence Study*, 2019.

REFERENCES

1. Strategic foresight analysis ACT, 2017.

2. NATO's long term military transformation. *Read Ahead for Long-term Military Transformation*. Workshop, 2016.

3. The Future of the Command Post, Part 1. *A NATO Command and Control Centre of Excellence Study*, 2019.

4. ibidem

5. Избор на критерии за качество и оптималност на планирането на авиационна система при планиране на композитна въздушна операция. Въздушният суверенитет и единно европейско въздушно пространство. In: *Сборник доклади от научна конференция на Военна академия „Г. С. Раковски“, Фондация „Български ВВС“ и катедра „ВВС и ПВО“*, 09.10.2019. София: Военна академия „Г. С. Раковски“, стр. 78-92. ISBN 978-619-7478-36-5.

6. Command and control operational requirements and system implementation. *Information and Security, An International Journal*, Vol.5, 2000.

7. Kokudeva, P. Slozhnite sistemi i sistemata ot sistemi v sigurnostta. Vazdushniyat suverenitet i edinno evropeysko vazdushno prostranstvo. In: *Sbornik dokladi ot nauchna konferentsiya*, 9 oktombri 2019. Sofia: Voenna akademia „G. S. Rakovski“, str. 143-153. ISBN 978-619-7478-36-5.

8. The Future of the Command Post. Part 2. *A NATO Command and Control Centre of Excellence Study*, 2019.

РУСКИТЕ ХИПЕРЗВУКОВИ ОРЪЖИЯ

доц. д-р Пламен Богданов

Университет по библиотекознание и информационни технологии, София,
p.bogdanov@unibit.bg

Резюме: В доклада се анализират причините и основните направления за разработване на хиперзвукови оръжия в Русия. Изследвани са резултатите от тестовете, възможностите, приемането на въоръжение и очакваното развитие на различните видове хиперзвукови оръжия – с наземно, въздушно и морско базиране, през второто и началото на третото десетилетие на XXI век.

Ключови думи: *Русия; хиперзвуково оръжие; хиперзвуков планер; хиперзвукова крилата ракета; балистична ракета; скорост; маневреност*

RUSSIAN HYPERSONIC WEAPONS

Assoc. Prof. Plamen Bogdanov, PhD

University of Library Studies and Information Technologies

Sofia, Bulgaria,

E-mail: p.bogdanov@unibit.bg

Abstract: The paper analyzes the reasons and main directions for the development of hypersonic weapons in Russia. The results of the tests, capabilities, adoption of armaments and the expected development of the different types of hypersonic weapons – ground, air and sea based, during the second and the beginning of the third decade of the 21st century have been studied.

Keywords: *Russia; hypersonic weapon; hypersonic glider; hypersonic cruise missile; ballistic missile; speed; maneuverability*

Въведение

Развитието на технологиите и стремежът да се противодейства на оръжията на противника доведе до създаването в наши дни на нов клас оръжие – хиперзвуковото.

Хиперзвуковите оръжия се движат със скорост 5 и повече пъти по-голяма от тази на звука (331 м/сек.), могат да маневрират в полет и да носят достатъчно експлозив. С тях могат да се атакуват множество цели, което прави оцеляването на танкове, кораби и бомбардировачи все по-трудно. Скоростта на хиперзвуковите оръжия, тяхната маневреност и защита срещу откриване, от друга страна, намаляват вероятността за унищожаването им.

Хиперзвуковото оръжие има две разновидности – хиперзвукови крилати ракети и хиперзвукови планери (безпилотни планиращи летателни апарати, глайдъри).

Хиперзвуковата крилата ракета е задвижвана от двигател и се издига до определена височина и достигане на определена скорост монтирана на балистична ракета (на мястото на бойните глави) или подкачена на свръхзвуков изстребител или бомбардировач. Хиперзвуковият планер достига горните слоеве на атмосферата монтиран на балистична ракета (на мястото на бойните глави), където се отделя от нея.

Тези оръжия се разглеждат и като хиперзвукови маневриращи бойни блокове, поставени на мястото на бойните глави на балистичните ракети или подкачени на самолети. Възможността за повишаване способностите на оръжията, благодарение на хиперзвуковите технологии, предизвиква нова надпревара във въоръженията след Студената война. Русия, Китай и САЩ вече имат определени резултати в края на второто десетилетие на XXI век.

За Русия разработването на хиперзвукови оръжия е средство за пробиване на американската противоракетна отбрана и за възстановяване на двустранните ядрени връзки на основата на уязвимостта. Първите изпитания на хиперзвуков блок в Русия са проведени през 2001 г. на космодрума Плесецк. Според изявление на руския президент Путин от септември 2020 г. Русия е била принудена да създаде

хиперзвуково оръжие, след като САЩ се оттеглят от Договора за противоракетната отбрана през 2002 г. и в отговор на развърщането на американската система за стратегическа противоракетна отбрана, която е можела да неутрализира целия руски ядрен арсенал¹. Освен това според Москва еволюцията на американската стратегическа доктрина през последните години, с кулминация излизането от Договора за съкращаване на ядрените ракети със среден и малък обсег (1987 г.) през 2019 г., подчертава смяната на съществуващата доктрина за „Взаимно гарантирано унищожение“ с развитие на способности за първи удар. Това дава допълнителни основания на Русия да развива хиперзвукови програми.

Хиперзвуковите оръжия са сред шестте нови оръжейни системи от ново поколение, които президентът Путин обявява пред Федералното събрание на Русия на 1 март 2018 г.

1. Наземни хиперзвукови оръжия

През 2018 г. е извършен първият тест на *хиперзвуковия планер „Авангард“*. Той се изстрелва от междуконтинентална балистична ракета (МБР) с няколко бойни глави (MIRV) и е представен като имащ неограничен обхват. На практика „Авангард“ е ракетен комплекс със стратегическо предназначение, който използва МБР с планираща бойна част (боен блок). Хиперзвуковият планер (бойният блок) се изстрелва до горните слоеве на атмосферата с балистичната ракета, където се отделя от нея и се насочва към своята цел, извършвайки маневри по пътя си.

Първият тест на хиперзвуковия планер „Авангард“ през 2018 г. е извършен с използване на снетите от въоръжение ракети УР-100Н (SS-19 Stiletto). Ракетата, изстреляна от полигона Домбаровский, достига цел, разположена на отдалечение 6000 км в ракетния тестов полигон Кура. Според съществуващата информация планерът е достигнал скорост 27 пъти по-голяма от скоростта на звука (Mach 27 – над 32 000 км/ч), което означава приблизително 1800 – 2000° С температура на повърхността².



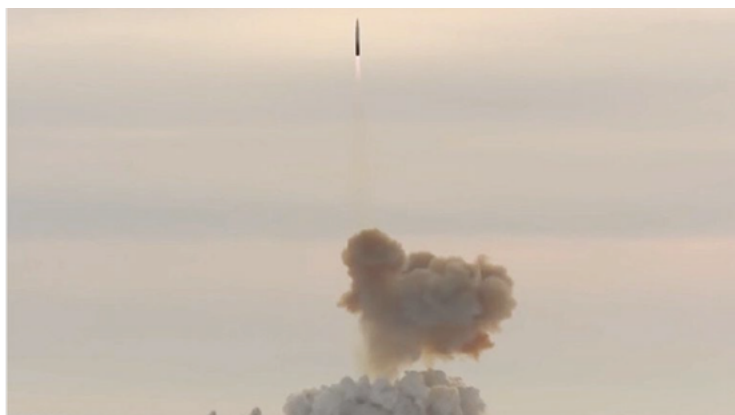
Фиг. 1. Мобилна пускова установка от комплекса „Авангард“

Този хиперзвуков планер, за който се съобщава, че може да носи конвенционални и ядрени бойни глави, е приет на въоръжение и според съобщение на руското Министерство на отбраната на 27 декември 2019 г. е застъпил в бойно дежурство в състава на първия ракетен полк, въоръжен с новия комплекс. Този полк е включен в състава на Домбаровската ракетна дивизия в Оренбургска област в Урал³. В бъдеще „Авангард“ вероятно ще бъде носен от МБР РС-28 „Сармат“ (SS-X-30).

За първи път за комплекса „Авангард“ съобщава руският президент пред Федералното събрание през 2018 г. Той казва, че тези ракети на практика са непобедими и сравнява „Авангард“ със създаването на първия изкуствен спътник на Земята. Другото руско оръжие, също представено от Путин като непобедимо, е споменатата като потенциален носител на хиперзвуковия планер „Авангард“ – МБР от пето поколение РС-28 „Сармат“. Новите ракети (с обсег 18 000 км) влизат поетапно на въоръжение от 2022 г. и заменят най-мощните в света стратегически ракети с шахтно базиране Р-36М2 „Воевода“⁴ (известни и като РС-20В, по класификацията на НАТО SS-18 Satan), които имат обсег 11 000 км.



Фиг. 2. Изстрелване на хиперзвукова ракета „Авангард“



Фиг. 3. Хиперзвукова ракета „Авангард“ в полет след изстрелване

Според анализатори в ядрен вариант една ракета „Сармат“ е достатъчна да нанесе на САЩ гарантирано неприемливи поражения. В неядрен вариант ракетата ще стане супероръжие, съчетаващо колосалната скорост на МБР и точността на маневриращата хиперзвукова бойна глава на „Сармат“, която достига до няколко метра. Счита се, че „Сармат“ ще може да атакува цели, например в САЩ, от Космоса не по най-късата права, а от всяко направление, включително през Северния и Южния полюс. Траекторията се прокарва така, че да се избегнат районите с масирано разположени средства за ПРО. Освен това тази ракета не лети по класическа балистична, а по ниска траектория, с което времето за долитане до целта се съкращава, а хиперзвуковата маневрираща бойна глава ще лети в атмосферата по-дълго и така ще се увеличат възможностите за бойното ѝ използване. Най-главното е, че се очаква новият боен блок на „Сармат“ (наричан в Русия 4202, а в САЩ – U-71) да бъде управляем по време на цялата траектория на своя полет⁵.

Освен това се очаква, че РС-28 „Сармат“, подобно на някои от съществуващите руски ракети, като например Р-36М2 „Воевода“, ще разполага освен с бойни блокове и с блокове оборудвани с касети с многобройни имитатори, предназначени за заблуждаване на противниковите радары. Докато радарите търсят реалните цели сред множеството лъжливи, бойните блокове влизат в траекториите за поразяване на определените цели. Всеки от тях има двигател за маневриране в космическото пространство и плоскости (крила) за управление на полета в атмосферата.



Фиг. 4. Ракетен комплекс с наземно шахтно базиране РС-28 „Сармат“ с тежка МБР „Сармат“

Според наблюдатели комплексът „Авангард“ поставя край на американската военна доктрина за така наречения „Бърз глобален удар“⁶. Концепцията „Конвенционален бърз глобален удар“, както вече беше казано, е приета в САЩ през 2007 г., в резултат на което през 2009 г. е формирано Командване на глобалните удари на ВВС на САЩ с цел повишаване ефективността на управлението на националните ядрени сили.

2. Авиационни хиперзвукови оръжия

Друго руско хиперзвуково оръжие е *изстрелваната от въздуха балистична ракета* Х-47М2 „Кинжал“, която може да носи ядрени бойни глави. За нея са обявени скорост Mach 10, обхват 2000 км и тегло 4 т.

„Кинжал“ е най-новият руски авиационен комплекс, в чийто състав влиза самолета-носител МиГ-31К и хиперзвукова ракета. „Кинжал“ е авиационен вариант на балистичните ракети „повърхност-повърхност“ от оперативно-тактическия ракетен комплекс 9К720 „Искандер“. След приемане на въоръжение през декември 2017 г. системата постига Пълни оперативни способности през март 2018 г. и е развърната в Южния военен окръг. Пускове над Баренцово море от МиГ-31, базиран в Оленя (Оленегорск), полуостров Кола, подсказват, че е възможно системата „Кинжал“ да е развърната и в Северния военен окръг.



Фиг. 5. Балистична ракета „Кинжал“, подкачена на изстребител МиГ-31К

Руското Министерство на отбраната информира, че само в началото на 2018 г. са извършени повече от 250 полета, за да се прецизира работата на ракетните системи⁸. Агенция ТАСС, като се позовава на двама източници от военнопromишления комплекс на Русия, съобщава за тестово изстрелване на хиперзвуковата ракета „Кинжал“ в Арктика в средата на ноември 2019 г. Ракетата е достигнала скорост Mach 10 (над 12 000 км/ч)⁹. Според заместник-министъра на отбраната на Русия, ракетната система „Кинжал“ може да унищожава движещи се големи морски цели като самолетоносачи, разрушители и крайцери¹⁰.

За създаването и на комплекса „Кинжал“ за първи път съобщава руският президент на 1 март 2018 г. В началото на 2020 г. се носи опитно-бойно дежурство в Южния военен окръг с една ескадрила МиГ-31К с хиперзвукови ракети.



Фиг. 6. Изстребител МиГ-31К в полет с ракета „Кинжал“

Освен това, в началото на 2020 г. става ясно, че се планира руските свръхзвукови стратегически ракетноносци Ту-160 също да бъдат въоръжени с хиперзвуковите ракети „Кинжал“, като разработката на проекта трябва да завърши до края на 2020 г. Този бомбардировач може да носи до 12 стратегически крилати ракети¹¹.



Фиг. 7. Бомбардировач за далечно действие Ту-160

Според друга информация от руския военнопromишлен комплекс от юли 2018 г. са планирани тестови пускове на хиперзвукови ракети и от бомбардировача с далечен обseg Ту-22М3.



Фиг. 8. Бомбопускане от бомбардировачи за далечно действие Ту-22М3

3. Морски хиперзвукови оръжия

Русия разработва и хиперзвукови оръжия, изстрелвани от морски съдове. Такова е **хиперзвуковата крилата ракета 3М22 „Циркон“**, изстрелвана от кораб, която може да достигне скорост от Mach 6 до Mach 8 и да атакува морски и земни цели на дистанция от 500 до 1000 км в зависимост от режима на изстрелване.

Според руската агенция ТАСС „Циркон“ може да се изстрелва от вертикална изстрелваща система, монтирана на няколко типа платформи, включително бойните крайцери „Петър Велики“ и „Адмирал Нахимов“, корветите Проект 20380, подводниците Проект 885 клас „Yasen“ и фрегатите проект 22350 (с водещ кораб фрегатата „Адмирал Горшов“). На 27 юли 2020 г. президентът Путин заявява, че руският флот ще бъде въоръжен с хиперзвукови оръжия за ядрени удари. По-рано руското Министерство на отбраната обявява, че „Циркон“ е във финална фаза на тестване, а според източници от американското разузнаване се очаква ракетата да бъде в оперативна готовност през 2023 г.¹².



Фиг. 9. Основни данни на хиперзвукова ракета „Циркон“

Съобщава се и за друго изстрелване на „Циркон“ през 2020 г., в което успешно е поразена крайбрежна цел на разстояние 350 км, а ракетата е развила скорост над Mach 8.

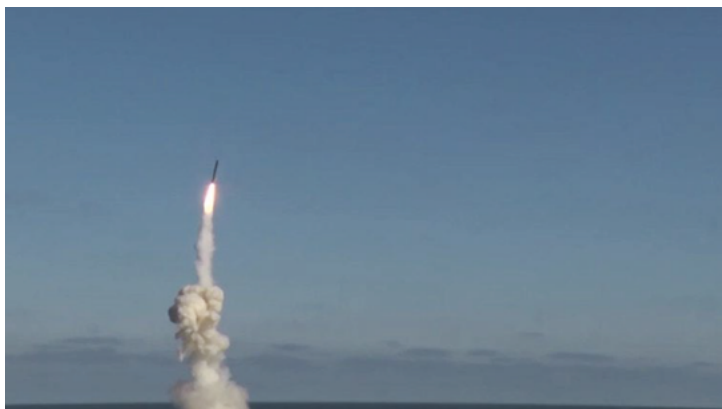
Очаква се, че Русия ще бъде първата държава, която ще приеме на въоръжение и хиперзвукови ракети с подводно базиране. За това пише в края на 2020 г. в американското издание The National Interest експертът Калев Ларсон. [13] Подводниците с хиперзвукови ракети са особено опасни, защото те могат да останат под вода продължително време и са много трудни за откриване.



Фиг. 10. Хиперзвукова ракета „Циркон“ след изстрелване

Заклучение

Технологиите напредват и позволяват на света да постига нови еволюционна нива¹⁴. Хиперзвуковите ракети и планери са високоманеврени и по-често се отнасят към ракетите, въпреки че концепцията за хиперзвуковите оръжия в действителност е по-широка, тъй като обхваща и планери. Предимствата на хиперзвуковите оръжия са съчетаване на скоростта на балистичните ракети с маневреността и точността на крилатите ракети.



Фиг. 11. Изстрелване на хиперзвукова ракета „Циркон“

През последните години Китай и САЩ отделят значителни средства за разработване и интензивно провеждат тестове на различни видове хиперзвукови оръжия. В някои отношения те прилагат различни концептуални подходи от тези в Русия. Изследванията в САЩ пък са насочени само към неядрени хиперзвукови планери и крилати ракети, за разлика от тези в конкурентите.

В последната Стратегия за национална сигурност на Русия намира място констатацията, че нараства значението на военната сила като инструмент за постигане от субектите на международните отношения на своите геополитически цели. Като задачи в стратегията се поставят снабдяването на руските въоръжени сили със съвременно въоръжение, военна и специална техника и иновативното развитие на

отбранително-промишления комплекс на страната, запазване на лидерството в разработването и производството на нови (перспективни) образци (комплекси и системи) въоръжения, военна и специална техника¹⁵.

Така Русия продължава мащабно да разработва и тества и открито обявява възможностите на своите хиперзвукови оръжия. С това демонстрира нарасналите си военни способности с оръжия от ново поколение, за които твърди, че все още няма създадена система, която да им противодейства.

ЛИТЕРАТУРА

1. БНТ 1 Новини – интернет страница. Путин: Създадохме хиперзвукови ракети в отговор на отбраната на САЩ, 19.09.2020 [онлайн], <https://bntnews.bg/>
2. Tilenni, G. Hypersonic Developments. *European Security & Defence International Security and Defence Journal*, 10/2020, p. 60.
3. Руските хиперзвукови ракети са вече на бойно дежурство. *Клуб Z*, 27.12.2019. <https://clubz.bg/> – достъпно на 26.01.2021.
4. Первый полк новых МБР «Сармат» заступит на боевое дежурство к концу года. *Интерфакс*, 8 января, 2022. <https://www.interfax.ru/Russia/814303/> – достъпно на 25.02.2022.
5. Иванджийски, К. Хипервойната в хиперетап. *strogosekretno.com*, юни 2017. <https://strogosekretno.com/> – достъпно на 21.05.2020.
6. „Авангард“ лети с 34 000 км/час. След него летят другите хиперзвукови ракети. *От упор*, 4 януари 2020. [онлайн] <https://otupor.com/> – достъпно на 26.01.2021.
7. Tilenni, G. Hypersonic Developments. *European Security & Defence International Security and Defence Journal*, 10/2020, p. 60.
8. Русия с успешно изпитание на новата свръхзвукова ракета „Кинжал“. [онлайн] *news.bg*, 11.03.2018. <https://news.bg/> – достъпно на 26.01.2021.
9. Русия за първи път изпита в Арктика новата свръхзвукова ракета „Кинжал“. *news.bg*, 30.11.2019. [онлайн] <https://news.bg/> – достъпно на 26.01.2021.
10. Русия се хвали: Ракетата „Кинжал“ може да потапя самолетоносачи. *news.bg*, 12.03.2018. [онлайн] <https://news.bg/> – достъпно на 26.01.2021.
11. ТАСС: Въоръжават Ту-160 с хиперзвукови ракети, 10 февруари 2020. [онлайн] <https://focus-militarynews.net>, 16 февруари 2020 – достъпно на 15.01.2021.
12. Tilenni, G. Hypersonic Developments. *European Security & Defence International Security and Defence Journal*, 10/2020, p. 60.
13. Изпревари ли Русия в разработването на хиперзвуково оръжие САЩ? *Актуално*, 10.11.2020. [онлайн] <http://www.actualno.com/> – достъпно на 26.01.2021.
14. Кокудева, П. Сложните системи и системата от системи в сигурността (Системна теория и военна наука). В: *Сборник доклади от научна конференция „Въздушният суверенитет и единно европейско въздушно пространство“ на Военна академия „Г. С. Раковски“*, 9 октомври 2019 г., София: Военна академия „Г. С. Раковски“, 2019, с. 143.
15. *Стратегия на национальной безопасности Российской Федерации*, утвърдена Указом Президента Российской Федерации от 2 июля 2021 г. № 400, с. 13.

REFERENCES

1. BNT 1 Novini – internet stranitsa. Putin: Szazadohme hiperzvukovi raketi v otgovor na otbranata na USA, 19.09.2020 [onlayn], <https://bntnews.bg/>
2. Tilenni, G. Hypersonic Developments. *European Security & Defence International Security and Defence Journal*. 10/2020, p. 60.
3. Ruskite hiperzvukovi raketi sa veche na boyno dezhurstvo. *Klub Z*, 27.12.2019. <https://clubz.bg/> – dostapno na 26.01.2021.
4. Pervay polk novayh MBR «Sarmat» zastupit na boeovoe dezhurstvo k kontsu goda. *Interfaks*, 8 yanvary, 2022. <https://www.interfax.ru/Russia/814303/> – dostapno na 25.02.2022.
5. Ivandzhiyski, K. Hipervoyната v hiperetap. *strogosekretno.com*, yuni 2017. <https://strogosekretno.com/> – dostapno na 21.05.2020.
6. „Avangard“ leti s 34 000 km/chas. Sled nego letyat drugite hiperzvukovi raketi. *Of upor*, 4 yanuari 2020. [onlayn] <https://otupor.com/> – dostapno na 26.01.2021.
7. Tilenni, G. Hypersonic Developments. *European Security & Defence International Security and Defence Journal*. 10/2020, p. 60.
8. Russia s uspešno izpitatie na novata svrazhzhukova raketa „Kinzhal“, [onlayn] *news.bg*, 11.03.2018. <https://news.bg/> – dostapno na 26.01.2021.
9. Russia za parvi pat izpita v Arktika novata svrazhzhukova raketa „Kinzhal“. *news.bg*, 30.11.2019. [onlayn] <https://news.bg/> – dostapno na 26.01.2021.
10. Russia se hvali: Raketata „Kinzhal“ mozhe da potapya samoletonosachi. *news.bg*, 12.03.2018. [onlayn] <https://news.bg/> – dostapno na 26.01.2021.
11. TASS: Vaorazhavat Tu-160 s hiperzvukovi raketi, 10 fevruari 2020. [onlayn] <https://focus-militarynews.net>, 16 fevruari 2020 – dostapno na 15.01.2021.
12. Tilenni, G. Hypersonic Developments. *European Security & Defence International Security and Defence Journal*, 10/2020, p. 60.
13. Izprevari li Rusiya v razrabotvaneto na hiperzvukovo orazhie USA? *Aktualno*, 10.11.2020. [onlayn] <http://www.actualno.com/> – dostapno na 26.01.2021.

14. Kokudeva, P. Slozhnite sistemi i sistemata ot sistemi v sigurnostta (Sistemna teoriya i voenna nauka). In: *Sbornik dokladi ot nauchna konferentsiya „Vazdushniyat suverenitet i edinno evropeysko vazdushno prostranstvo“ na Voenna akademiya „G. S. Rakovski“*, 9 oktomvri 2019 g., Sofia: Voenna akademiya „G. S. Rakovski“, 2019, s. 143.
15. *Strategiya natsionalnoy bezopasnosti Rossiyskoy Federatsii*, utverzhdena Ukazom Prezidenta Rossiyskoy Federatsii ot 2 iyulya 2021 g. № 400, s. 13.

ФАКТОРИ, ВЛИЯЕЩИ НА ИЗПОЛЗВАНЕТО НА РАЗУЗНАВАТЕЛНИ ФОРМИРОВАНИЯ В ОПЕРАЦИИ ПРИ БЕДСТВИЯ И АВАРИИ

подполковник Добромир Дамаков, докторант
Военна академия „Г. С. Раковски“, damakov@abv.bg

Резюме: Целта на настоящия доклад е на базата на анализа на националния и чуждестранния опит и съществуващите литературни източници да се изследват условията, при които се използват разузнавателни формирования при бедствия и аварии, и да се набележат насоки за подобряване на практическата им подготовка за участие в такива операции.

Ключови думи: бедствия; аварии; разузнавателни формирования; използване

FACTORS AFFECTING THE USE OF INTELLIGENCE FORMATIONS IN DISASTER AND ACCIDENT OPERATIONS

Lieutenant Colonel Dobromir Damakov, PhD Student
Rakovski National Defence College
Sofia, Bulgaria
E-mail: damakov@abv.bg

Abstract: The purpose of this article is to analyze the conditions under which intelligence agencies are used in disasters and accidents and to identify guidelines for improving their practical preparation for participation in such operations, based on the analysis of national and foreign experience and existing literature sources.

Keywords: disasters; accidents; reconnaissance units; use

Въведение

През последното десетилетие се утвърдиха редица позитивни промени в международните отношения. Основните проблеми пред сигурността според съвременните специалисти³ са регионалната нестабилност, неустойчивото развитие, появата и изострянето на конфликти на етническа и религиозна основа¹² и свързаните с тях форми на тероризъм и честите природни бедствия¹⁴, съдържащи в себе си потенциал на антропогенни катастрофи^{5, 12, 14, 15}. Затова управлението на кризи от невоенен характер се превръща в един от основните подходи за гарантиране на международната и националната сигурност и стабилност. В тази област са концентрирани усилията на ООН, НАТО, ЕС и ОССЕ за разширяване на сътрудничеството и взаимопомощта както по проблемите на сигурността, така и по въпросите за предотвратяване и ликвидиране на последствията от бедствия³, промишлени аварии и кризи от невоенен характер³. С подкрепата на ООН в НАТО бе създаден Евроатлантически съвет за партньорство и постояннодействащ Евроатлантически център за координиране на действията при бедствия с цел съсредоточаване на усилията и координиране на действията за оказване на навременна и ефективна помощ на населението¹⁴ чрез формиране на адаптивни екипи¹ за действие при възникналите екстремални ситуации^{1, 2, 14}.

Като се има предвид широкият спектър от области и сфери на приложение на силите и средствата за разузнаване, ще огранича предмета на изследване за целите на настоящия доклад в направление особености в подготовката на разузнавателни формирования определени за участие при бедствия и аварии и респективната подготовка за достигане на оптимални резултати при използването им.

Същността на разузнаването в операции при бедствия и аварии е добиване, обработване и разпространение на информация, която осигурява изпълнението на целите на операцията при минимален риск за участващите в нея формирования. Както отбелязват специалистите^{9, 11, 13}, този процес е неразделна част от самите операции и е елемент от особена важност при тяхната предварителна подготовка^{9, 11, 13}.

Целта на настоящия доклад е на базата на анализа на националния и чуждестранния опит и съществуващите литературни източници да се изследват условията, при които се използват разузнавателни формирования при бедствия и аварии, и да се набележат насоки за подобряване на практическата им подготовка за участие в такива операции.

За постигането на тази цел са поставени за решаване следните научно-изследователски задачи:

- формулиране на основни принципи и изисквания към разузнаването при участие в операции при бедствия и аварии;

- да се изследва опитът и възможностите на разузнавателни формирования при провеждане на операции вследствие на бедствия и аварии.

- формулиране на основни насоки за подобряване и усъвършенстване на практическата подготовка на формированията за добиване на информация при участие в операции при бедствия и аварии.

В хода на изследването са използвани основно методите на системния анализ, синтез, сравнение, изследване на опита, експертни мнения, анализи и изследвания вследствие на натрупаният опит от участие на формирования от Българската армия за защита на населението при бедствия, аварии и катастрофи.

1. Обща характеристика на факторите, влияещи върху разузнавателните формирования при участие в операции вследствие на бедствия и аварии. Възникналите у нас през последните години проблеми в резултат на природни бедствия, свързани с човешки жертви и огромни материални загуби, определиха необходимостта от засилване на ефективността при справянето с кризи от невоенен характер.

Изпълнението на тези задачи е свързано с отчитане влиянието на множество фактори, с реализацията на професионални умения от различни области на практиката и предполага проявата на творчески усилия с висока степен на сложност, значимост и риск. Участието на войскови формирования в кризи от невоенен характер и анализът на натрупания опит през последните години показва, че са налице съществени постижения в тази насока. В същото време в контекста на гражданско-военните отношения е необходимо да се подчертае, че армията е продукт и функция на обществото. Това показва, че армията има ресурс в личен състав и техника, които могат и трябва да бъдат използвани, когато населението на страната има нужда от помощ.

Участието в управлението на кризи от невоенен характер е относително ново предизвикателство за формированията от Българската армия³. Това е така, защото е свързано с изпълнението на несвойствени за тях задачи.

1.1. Фактори, свързани с правнонормативната база: основополагащи нормативни документи; меморандуми, двустранни и многостранни договори; законодателството на страната домакин; оперативни и други регламентиращи документи, обособяващи правната рамка за инициране и провеждане на съответната операция;

1.2. Фактори, свързани с подготовката и способностите на формирането: степен на оперативна съвместимост; комуникационни възможности; роля и място в общата информационна мрежа на съвместния разузнавателен щаб; възможности за осигуряване и поддръжка на разузнавателните елементи; оперативни, тактически и технологични възможности на силите и средствата за разузнаване; състояние и възможности на националните разузнавателни системи и платформи за оказване на съдействие и др.¹⁰

1.3. Природни фактори: земетресения, наводнения, снежни бури и снегонавявания, градушки, прашни бури, свлачища и пожари. Районът на Балканския полуостров е най-земетръсната територия в Европа. Статистика показва, че за период от 1000 години 98% от територията на България ще бъде подложена на въздействие с интензивност от 7-а и по-висока степен. В тези райони попадат 94 населени места с население около 6 340 000 души, представляващо 80% от населението на страната и могат да бъдат разрушени частично или напълно 26% от сградния фонд.

1.4. Техногенни фактори, свързани с промишлените аварии и катастрофи: важен рисков фактор, който може да повлияе на сигурността в национален и регионален план.

Благоприятното геостратегическо положение на България е предпоставка за оживен автомобилен, железопътен, въздушен и воден транспорт. Това създава условия за транспортни произшествия,

свързани с разливане или разсипване на опасни товари, което води до замърсяване на околната среда и застрашаване живота и здравето на хората^{14, 15}.

Стопанската дейност в страната е свързана с функционирането на много обекти от енергийната, химическата, нефтопреработвателната, металургичната и фармацевтичната промишленост, повечето от които работят с взривоопасни, леснозапалими, горими и силно токсични вещества, като живак, барий, фосген, амоняк, сярна киселина, при което под заплахата могат да се окажат 120 населени места с население над 800 000 души.

Като се изхожда от горепосочените фактори и необходимостта от висока степен на ефективност, задачите се приоритизират по важност, степен на изпълнимост и време за изпълнение, с което се постига в максимална степен изпълнението на изискванията към разузнаването, предадени от командира в различните етапи на операцията. Във всеки конкретен случай ще се определят и съответните допълнителни разузнавателни органи от други структури, допустимите способности за разузнаване, сроковете за изпълнение на поставените задачи, реда за докладване и разпространяване на разузнавателната информация.

2. Задачи по разузнаването при участие в операции при бедствия и аварии. Съгласно Конституцията на страната на въоръжените сили не могат да се възлагат задачи от вътрешнополитически характер, но те имат своята вътрешна функция и тя се заключава в тяхната стабилизираща роля в обществото и в готовността за защита на населението при природни бедствия и катастрофи. Този тип действия се включва в термина „управление на кризи от невоенен характер“.

Изпълнението на задачи от такъв характер разузнавателните формирования извършват под ръководството на местната администрация, органи на други ведомства или специализирани държавни органи⁴, като във взаимодействие със силите на другите видове въоръжени сили, други ведомства териториалните органи на изпълнителната власт³ и органите на местното самоуправление изпълняват задачи по: наблюдение и прогнозиране на бедствени ситуации; осигуряване на ред и сигурност в застрашения район; оказване помощ на населението; въздействие върху елементите на бедствието за неговото овладяване; действия за ликвидиране на последствията от него^{3, 4, 5, 6}.

Главната задача на въоръжените сили при участие в провеждане на спасителни операции при бедствия и аварии във всички условия на политическата и стратегическата обстановка е да се осигури безопасността и сигурността на населението. Всички подразделения от Сухопътните войски и в частност разузнавателните формирования водят подготовка и поддържат готовност за действия по защита на личния състав, въоръжението, техниката, обектите на Министерството на отбраната, населението и националната инфраструктура при инциденти и кризи от невоенен характер.

За участие на разузнавателните формирования при възникване на кризи от невоенен характер се води планова специализирана подготовка на личния състав за участие в действия при възникване, развитие, овладяване или ликвидиране на последствията, предизвикани от бедствия и аварии^{11, 13}. Организиран се и се провеждат тренировки и учения за усвояване на планове. Води се инженерно разузнаване, наблюдение и контрол. Поддържа се готовност за оповестяване.

При заплахата от инцидент се усилява наблюдението върху елементите на бедствието в съответствие с възможностите на силите и средствата, събират се данни, анализира се и се прогнозира характерът и ходът на проявление на бедствието и обстановката, която може да възникне. Уточняват се планове за действие при управление на кризи от невоенен характер. Определят се необходимите сили и средства за овладяване на бедствието.

При възникване на бедствие се предприемат незабавни мерки за защита на личния състав, въоръжението, техниката и имуществата, ако са застрашени, и се привеждат в готовност определените за участие сили и средства. При поискване от държавните органи за управление, определените сили и средства вземат участие в действията за овладяване на инциденти и кризи от невоенен характер и преодоляване на последствията от тях съгласно разработените планове.

При ликвидиране на последствия от аварии и природни бедствия, освен типичните за разузнавателните формирования задачи, се изпълняват и задачи по изясняване на радиационната, химическата, биологическата, екологичната, пожарната, хидрометеорологичната и друга обстановка в райони на бедствия, провеждане на мероприятия по възстановяване на околната среда и други. Конкретните задачи и

дейности зависят както от характера и мащабите на бедствието, така и до голяма степен от възможностите на разузнавателните формирования.

Голяма част от задачите са общи както за бойната дейност, така и за участие в операции за разрешаване на кризи от невоенен характер. Най-близки до бойните си задачи, при участие в операции породени от природни бедствия, ще изпълняват разузнавателните формирования от инженерни войски.

Подготовката за водене на бойни действия е главната задача на бойната подготовка на разузнавателните формирования от Сухопътни войски. Върху качествата на тази подготовка оказват влияние много фактори, един от които е подготовката и участието в операции по ликвидиране на последствията от бедствия и аварии.

Задачите на разузнавателните формирования при участието им в спасителни операции вследствие на бедствия и аварии се определят от възможностите на отделните подразделения и модули и зависят от комплектуването им с личен състав и техника, състава и състоянието им, обстановката, създадена от природното бедствие, условията на местността, времето като сезон, денонощие и количество, замисъла за действие и други.

Въз основа на функциите, ролята и мястото се определят и задачите, които трябва да изпълняват формированията от Българската армия при разрешаването на кризи, възникнали вследствие на бедствия и аварии.

Тези задачи са:

- поддържане на готовност за хуманитарна помощ и спасителни действия на територията и акваторията на страната и извън нея в съответствие с националното законодателство и международните договори, по които Република България е страна;

- подготовка и обучение на разузнавателни единици за провеждане на спасителни и неотложни аварийно-спасителни работи при природни бедствия, промишлени аварии, катастрофи и опасни замърсявания;

- разузнаване на райони и маршрути – тази задача се изпълнява от разузнавателни дозори, които се придвижват в зоната на поражение с транспортни средства. Те водят разузнаване за изясняване на обстановката в най-силно засегнатите от бедствието райони и обекти, работещи или съхраняващи промишлени отрови, взривоопасни и пожароопасни вещества, входни и изходни магистрали, булеварди, крупни промишлени предприятия, болнични заведения, обществени сгради и други.

В хода на изпълнение на тази задача разузнавателните органи следва да установят:

- най-кратките и безопасни маршрути за движение на силите и средствата към участъците и обектите за работа;

- степента и характера на пораженията;

- местонахождение на бедстващи хора и степен на заплашващите опасности;

- най-удобните места за подход към наводнените участъци, а също така и пътища за евакуиране на населението при нужда;

- състоянието на мостовите и пропускателните им възможности;

- условията за провеждане на спасителни и възстановителни работи от силите на Главна дирекция „Гражданска защита“ и формированията от Сухопътни войски и възможности за използване на специална и друга техника;

- наличието на заразени участъци от промишлени отрови и други;

- наличието на инертни и други материали за последващо изграждане на диги и други възпиращи водната стихия съоръжения;

- устройване на преходи за въвеждане на силите; устройването на временни места за преминаване по пътното платно на улиците и пътищата се прилага както при земетресения, така и при ликвидиране на последствията от свлачища, срутища и наносни елементи след големи наводнения;

- търсене и спасяване на пострадали от разрушения, на хора останали затрупани под разрушени сгради, започва веднага в процеса на разузнаването и въвеждането на спасителните и аварийно-възстановителните команди в огнищата на поражение чрез пълно обследване на територията;

- гасене на пожари и спасяване на хора от горящи сгради в процеса на спасителните и аварийно-възстановителните работи, за да се създадат условия за откриване и спасяване на затрупаните хора.

Данните от разузнаването се използват за вземане на решение по организиране на защитата на населението и силите за действие, а също така и по провеждане на спасителни и аварийно-възстановителни работи в района на бедствието. Конкретните задачи на силите и средствата за разузнаване силно зависят от обстановката и вида на съответната операция. Задачите, които може да изпълняват разузнавателните подразделения, най-често включват устройване на наблюдателни и контролно-пропускателни пунктове, патрулиране в пеши строй или на машини в зависимост от поставена задача, въздушно наблюдение и фотографиране и др.

Освен това разузнавателните подразделения може да изпълняват и задачи по осигуряване на сигурността. Това включва прилежащия район, осигуряване на сигурността на улици и кръстовища в населени места, патрули, конвои, ескортиране на важни личности и др.

Всичко това ясно показва, че офицерите от структурите и органите за управление и ръководство на разузнаването, както и всички командири на разузнавателни формирования, трябва много добре да познават както възможностите на наличните технически средства за разузнаване, така и процедурите, правилата и условията за тяхното използване в операции от невоенен характер.

Въпреки определените успехи, постигнати в тази област, съществуват и проблеми, които не са развити в необходимата цялост и пълнота и затрудняват или биха могли да бъдат пречка в изпълнението на тези, все още нови за въоръжените сили, задачи.

Един от проблемите, който не е получил досега задоволително разрешение, е начинът за събиране, получаване и разпределение на информация за бедствията и аварията, в управлението на които са ангажирани разузнавателните формирования. Отговорност за своевременното подаване на информацията за възникнали инциденти и бедствия и за нейната достоверност носят Националната система за управление, областните управители и кметовете. Комуникационно-информационната система за управление се изгражда на база мрежите на далекосъобщителните оператори и на обособените информационни мрежи на Министерския съвет, Министерството на вътрешните работи, Министерството на отбраната, на другите централни и териториални органи на изпълнителната власт.

От опита, който добихме след наводненията през лятото на 2005 г. и пролетта на 2006 г., се оказва, че информационният поток, който би следвало да тече между ведомствата, не се осъществява с пълна сила. Няма яснота по въпроса кой каква информация ще добива и ще предоставя за обобщаване и за взимане на решение за действие. На този етап действащите модулни формирования разчитат предимно на събраната и обобщена информация от своите разузнавателни органи включени в състава на формированията. Като най-подходящи в случай на природни бедствия се явяват органите за инженерно разузнаване.

За изпълнение на тази задача е целесъобразно да се сформират разузнавателни групи, в които да се включат инженерни специалисти, а при наличието на опасност от радиационно или химическо замърсяване – и специалисти от подразделенията за ЯХБЗ и Е. Те добиват информация за подходите към района на бедствието, общата инженерна обстановка в района, наличие и състояние на съоръженията, организират и водят ядрено и химическо разузнаване по основните маршрути за евакуация и подвоз на материални средства и изпълняват задачи по радиометричен анализ на проби от почва, вода, въздух, хранителни продукти и други.

Особено важно в такава ситуация е взаимното информиране, тясното взаимодействие и съгласуваност на действията между формированията на Сухопътни войски, формированията на главна дирекция „Гражданска Защита“, главна дирекция „Пожарна безопасност и спасяване“, Министерство на отбраната, органите на местната администрация и местното самоуправление³.

За непрекъснато и устойчиво управление е необходимо предвидените формирования от Българската армия за участие в аварийно-спасителни работи да се комплектуват с радиосредства, работещи и съвместими по технически характеристики с тези на ВВС, Гражданска защита, МВР и Военна полиция.

За повишаване ефективността на управлението на сборните отряди и модулните формирования е целесъобразно да бъде изградена устойчива система и среда за комуникации, отговарящи на съвременните изисквания и преодоляващи несъвършенствата на системите и платформите за осигуряване на управлението¹⁰.

3. Сили и средства за разузнаване при участие на войски формирования в операции вследствие на бедствия и аварии.

Силите и средствата от Сухопътни войски за участие в операции по защита на населението при бедствия, аварии и катастрофи се определят ежегодно със заповед на Министъра на отбраната на Република България, в която се определят и модулните формирования от подразделения на инженерните войски. Всички сили от Българската армия, независимо от тяхната принадлежност към конкретна командна структура, вид въоръжени сили и степен на комплектност, участват в действия по овладяване на кризи от невоенен характер в определените им зони за отговорност. Разузнавателните сили и средства, определени за участие в дейностите по оказване помощ на населението при бедствия, аварии и катастрофи, би следвало да се организират в модулни формирования с конкретно предназначение, при което е необходимо да са оборудвани с техника и да водят подготовка съобразно предназначението си, като са разпределени на териториален принцип.

Целесъобразно е при формиране на разузнавателни формирования да се изхожда от задачите, които те трябва да изпълняват и това следва да залегне в системата на тяхната подготовка, обучение и използване. В зависимост от изпълняваните задачи и предназначението им разузнавателните формирования могат да имат различен състав и окомплектуване.

Едновременно с това разузнавателните формирования трябва да заделят сили за изолиране района на бедствието, организиране контролно-пропускателни пунктове (КПП) на подходите и изходите към района, осигуряване конвои с хуманитарна помощ, организиране на лагери за бедстващото население. За тази цел ще бъдат използвани формирования от механизирани подразделения в зависимост от това в коя зона се работи по овладяване на кризата.

Групировката от сили трябва да отговаря на замисъла на предстоящите действия и да осигурява: разузнаване, своевременно изнасяне, развързване и въвеждане в зоната на бедствено положение; непрекъснато водене на спасителни и неотложни аварийно-възстановителни работи (СНАВР) при най-пълно използване възможностите на силите; нарастване усилията и осигуряване възможности за маневър; удобство в управлението; поддържане на непрекъснато взаимодействие; спазване мерките за безопасност и др. Групировката за провеждане на спасителни и неотложни аварийно-възстановителни работи (СНАВР) включва разузнавателни подразделения, отряд за осигуряване на движението, главни сили и резерв; отряди за логистично осигуряване.

Разузнавателните формирования разузнават маршрутите за изнасяне към зоната на бедствено положение; определят размерите, характера, степента и последиците от разрушенията, степента на радиация, вида на ОБ, местата, размерите и посоката на разпространение на пожарите, наводненията, заразените райони; откриват затрупани (поразени) хора и ги обозначават; докладват данните от разузнаването. Желателно е разузнавателните органи да могат да преценяват на място обективната обстановка и при изготвянето на докладите си да дават своето мнение какви сили и средства е желателно и могат да бъдат използвани при създамата се обстановка. За постигане на цялостна картина от разузнаването в състава на разузнавателната група е целесъобразно да се включи и химически разузнавателен дозор. Разузнавателен дозор за осигуряване на движението се създава за осигуряване изнасянето на основните сили за изпълнението на поставените им задачи. Съставен е преди всичко от сили и средства на МВР и инженерни войски.

Главните сили имат задача своевременно да се развърнат и започнат СНАВР в заповяданите райони при взаимодействие с щатни сили на Гражданска защита и доброволни формирования. Разузнавателният резерв е предназначен за нарастване усилията, за разширяване фронта на работите и за извършване на частична или пълна смяна на силите от главните сили. В неговия състав обикновено се включват сили, имащи по-ниска степен на готовност, включително и подразделения на Гражданска защита, подразделения за ЯХБЗ и Е и инженерни подразделения. Използва се и за решаване на внезапно възникнали задачи. Отрядите за медицинско и логистично осигуряване извършват цялостното медицинско и логистично осигуряване на СНАВР.

Най-важните задачи в хода на СНАВР са придвижването на силите и средствата до зоната на бедствието; своевременно и ефикасна помощ за спасяване живота и запазване здравето на хората; ограничаване размерите на щетите за околната среда и на материалните загуби; локализиране на зоните на

бедствената ситуация; прекратяване действието на опасните фактори; изтегляне на силите и средствата от зоната на бедствието. В зависимост от изпълняваните задачи и предназначение разузнавателните формирования могат да имат различен състав и комплектуване.

Разузнавателните формирования за гасене на пожари могат да бъдат в състав около 8 – 12 души до взвод, снабдени с автомобили с повишена проходимост, линейка, инженерна машина БАТ-М, специален автомобил АРС-14, моторни помпи, автокран, огнеупорни жилетки, защитно облекло и каски и др. Към този тип формирование биха могли да се включват и вертолети Ми-17 снабдени с баки за вода.

Разузнавателните формирования за действие в зимни условия при обилни снеговалежи и бедствия могат да бъдат в състав от около 12 – 15 души, снабдени с автомобили с повишена проходимост, верижни транспортъори, влекачи, инженерна машина БАТ-М, автомобилна ремонтна машина, линейка, походна кухня, електроагрегат, возим шансов инструмент и др.

Разузнавателните формирования за действие при наводнения могат да бъдат в състав от около 8 – 12 души до рота, снабдени с автомобили с повишена проходимост, линейка, инженерна машина БАТ-М, моторни помпи, автокран, гумени надуваеми лодки, спасителни жилетки и пояси, защитно гумирано облекло, возим шансов инструмент и водолази.

Разузнавателните формирования за действие при земетресение могат да бъдат в състав около 8 – 12 души до рота, снабдени с автомобили с повишена проходимост, автокранове, ескаватори, компресори, булдозери, линейки, електроагрегати, водоноски и полеви кухни. Освен това следва да се планират и заделят материални средства и имущества, необходими за устройване на полеви лагери за настаняване на населението от бедствените райони.

Разузнавателните формирования за действие при промишлени аварии може да бъдат в състав до 12 – 15 души, снабдени с товарни автомобили, специализирани автомобили от типа АРС-14, ДКВ, ДЦА, Маяк, линейки, противопожарен автомобил, защитно облекло, противогази.

Разузнавателният модул, като цяло, би могъл да се формира в състав 60 – 80 човека, при което би следвало да включва всички видове специалисти от родовете и специалните войски – механизирани, артилерийски, инженерни, разузнавателни, свързочни, химически и т.н., както и лица от местното население, познаващи района и особеностите на местността. Добиването на разузнавателна информация представлява изключително деликатна и специфична дейност, която трябва да се ръководи, координира и реализира внимателно от специално обучен състав. Това налага необходимостта от обединяване на усилията в единен орган, който да ръководи, координира и управлява всички тези дейности. Ето защо при участие на войскови формирования в спасителни операции вследствие на бедствия и аварии е целесъобразно да се създаде разузнавателен щаб или разузнавателна клетка, който да е в състояние да организира, координира и управлява дейността на всички сили и средства за разузнаване, привлечени за участие в конкретната операция, и да ръководи добиването, обработването и разпространяването на разузнавателна информация.

Заклучение

Вследствие на извършените анализи и проучвания по темата е възможно да се формулират следните изводи:

1. В зависимост от вида на конкретната операция при бедствия и аварии, целите, които се дефинират за постигане, могат да бъдат различни, в повечето случаи те се свеждат до овладяване на кризи, възникнали на основа на икономически, екологични и други фактори, водещи до създаване на опасност за живота на населението. Крайната цел на всяка една операция е възстановяване на ефективни граждански структури, способни да решават проблемите на обществото.

2. Всяка операция с нейните географски, икономически и военни характеристики в динамичната среда поставят пред разузнаването различни по обем и съдържание задачи, в много случаи и неочаквани, което изисква разнообразен разузнавателен ресурс.

3. Опитът показва, че не винаги щатните средства за разузнаване и екипировка са достатъчни. С оглед на това е целесъобразно прилагане на модулния принцип при формиране на разузнавателни структури, които да притежават комплексни способности, снабдени с всякакъв вид съвременни средства за ориентиране и наблюдение.

4. От съществено значение за успеха се явява познаването от командирите и щабовете на процедурите и моделите за своевременно планиране, творческо и ефективно водене на разузнаването, което ще позволи да се привеждат в изпълнение решения и мероприятия, адекватни на всяка конкретна ситуация. В този аспект на разузнаването следва да се гледа като на една жизненонеобходима система от взаимносвързани дейности от изключителна важност.

ЛИТЕРАТУРА

1. Атанасова-Кръстева, Невена Цветкова. Необходимостта от адаптивни екипи за действие в екстремални ситуации. В: *Сборник научни доклади. Пети национален конгрес по психология*, брой 1-4, с. 700 – 707. София: Изток-Запад, 2008. ISSN 0861-7813.
2. Атанасова-Кръстева, Невена Цветкова. *Психология на кризиса*. Велико Търново: ИК на НВУ „Васил Левски“, 2019. стр. 330. ISBN 978-954-753-290-8.
3. Георгиев, Георги Петров. Взаимодействие между областната и общинската администрация с Българската армия в управлението при бедствия и аварии. В: *Годишник на Военна академия „Г. С. Раковски“*. Факултет „Командно-щабен“, 2018, с. 400 – 408, ISSN 1312-2991.
4. Георгиев, Георги Петров. *Взривни технологии в аварийно спасителни работи*. София: Военна академия „Г. С. Раковски“, 2016, стр. 216.
5. Георгиев, Георги Петров. Защита на обекти от критичната инфраструктура от терористични заплахи. В: *Сборник доклади от Международна научна конференция „Сигурност – образование, наука, индустрия“, втора част*. София: Военна академия „Г. С. Раковски“, 2020, с. 154 – 159, ISBN 978-619-7478-58-7.
6. Георгиев, Георги Петров. Перспективи за използване на формирования от Българската армия за овладяване и/или преодоляване на последствията от бедствия. В: *Сборник материали от военна научна конференция на факултет „Командно-щабен“ на Военна академия „Г. С. Раковски“*. Годишник на Военна академия „Г. С. Раковски“: Факултет „Командно-щабен“ 2/2014, с. 81 – 89, ISSN 1312-2991.
7. Георгиев, Георги Петров, Филипов, Х., Георгиев, Г. & Петров, К. *Организиране и провеждане на операции по търсене и спасяване*. София: Военна академия „Г. С. Раковски“, стр. 123, 2012.
8. Георгиев, Христо Александров. Участие и специфични задачи на ССО в операции по преодоляването на кризи в мирно време. В: *Сборник с материали от конференция на факултет „Артилерия, ПВО и КИС“ – Шумен*, 2019, стр. 118-124. ISSN 2367-7902
9. Градев, Калин Веселинов. Подход за разработване на вариант за действие при планиране на операцияте. В: *Сборник доклади от международна научна конференция „Сигурност – образование, наука, индустрия“, Втора част*, с. 26-29. София: Военна академия „Г. С. Раковски“. ISBN 978-619-7478-58-7.
10. Кокудева, Петрана Тошкова. Теорията на системите в епохата на платформите. В: *Сборник доклади от Международна годишна научна конференция на НВУ „Васил Левски“*, 27 – 28 май 2021, с. 1084 – 1090. Велико Търново: ИК на НВУ „Васил Левски“. ISSN 2367-7481.
11. Кръстев, Кръстю Иванов. *Тактическо разузнаване във военните формирования*. Велико Търново: ИК на НВУ „Васил Левски“, 2021, стр. 161. ISBN 978-954-753-326-4.
12. Маринов, Петър Господинов. *Тероризмът – абстракции и реалности*. София: „Изток -Запад“, 2016. стр. 295, ISBN 619152866-3.
13. Петков, Йордан Методиев. Основни насоки за повишаване на уменията на личния състав на разузнавателните формирования. В: *Сборник с материали от конференция на факултет „Артилерия, ПВО и КИС“ – Шумен*, 2019, с. 106 – 111. ISSN 2367-7902.
14. Радева, Николина Радкова. *Актуални аспекти на защитата на населението при бедствени ситуации*. Варна: Стено, 2019, стр. 141.
15. Романова, Христиана Ангелова. *Потенциални антропогенни екокатастрофи във Варненски регион. Стратегия за защита на населението и запазване на биоразнообразието*. Варна: МУ – Варна, 2014.

REFERENCES

1. Atanasova-Krasteva, Nevena Tsvetkova. Neobходимостта от адаптивни екипи за deystvie v ekstremalni situatsii. In: *Sbornik nauchni dokladi. Peti natsionalen kongres po psihologiya*, broj 1-4, s. 700 – 707. Sofia: Iztok-Zapad, 2008. ISSN 0861-7813.
2. Atanasova-Krasteva, Nevena Tsvetkova. *Psihologiya na krizisa*. Veliko Tarnovo: IK na NVU „Vasil Levski“, 2019. str. 330. ISBN 978-954-753-290-8.
3. Georgiev, Georgi Petrov. Vzaimodeystvie mezhdu oblastnata i obshtinskata administratsiya s Balgarskata armiya v upravlението pri bedstviya i avarii. In: *Godishnik na Voenna akademiya „G. S. Rakovski“*. Fakultet „Komandno-shtaben“, 2018, s. 400 – 408, ISSN 1312-2991.
4. Georgiev, Georgi Petrov. *Vzrivni tehnologii v avariyno spasitelni raboti*. Sofia: Voenna akademiya „G. S. Rakovski“, 2016, str. 216.

5. Georgiev, Georgi Petrov. Zashchita na obekti ot kritichnata infrastruktura ot teroristichni zaplahi. In: *Sbornik dokladi ot Mezhdunarodna nauchna konferentsiya „Sigurnost – obrazovanie, nauka, industriya“, vtora chast*. Sofia: Voenna akademiya „G. S. Rakovski“, 2020, s. 154 – 159, ISBN 978-619-7478-58-7.
6. Georgiev, Georgi Petrov. Perspektivi za izpolzvanie na formirovaniya ot Balgarskata armiya za ovladyavane i/ili preodolyavane na posledstviyata ot bedstviya. In: *Sbornik materialy ot voennonauchna konferentsiya na fakultet „Komandno-shtaben“ na Voenna akademiya „G. S. Rakovski“*. Godishnik na Voenna akademiya „G. S. Rakovski“: Fakultet „Komandno-shtaben“ 2/2014, s. 81 – 89, ISSN 1312-2991.
7. Georgiev, Georgi Petrov, Filipov, H., Georgiev, G. & Petrov, K. Organizirane i provezhdane na operatsii po tarsene i spasyavane. Sofia: Voenna akademiya „G. S. Rakovski“, str. 123, 2012.
8. Georgiev, Hristo Aleksandrov. Uchastie i spetsifichni zadachi na SSO v operatsii po preodolyavaneto na krizi v mirno vreme. In: *Sbornik s materialy ot konferentsiya na fakultet „Artileriya, PVO i KIS“ – Shumen*, 2019, str. 118-124. ISSN 2367-7902
9. Gradev, Kalin Veselinov. Podhod za razrabotvane na variant za deystvie pri planirane na operatsiite. In: *Sbornik dokladi ot mezhdunarodna nauchna konferentsiya „Sigurnost – obrazovanie, nauka, industriya“, Vtora chast*, s. 26-29. Sofia: Voenna akademiya „G. S. Rakovski“. ISBN 978-619-7478-58-7.
10. Kokudeva, Petrana Toshkova. Teoriyata na sistemite v epohata na platformite. In: *Sbornik dokladi ot Mezhdunarodna godishna nauchna konferentsiya na NVU „Vasil Levski“*, 27 – 28 may 2021, s. 1084 – 1090. Veliko Tarnovo: IK na NVU „Vasil Levski“. ISSN 2367-7481.
11. Krastev, Krastyu Ivanov. *Takticheskoto razuznavane vav voennite formirovaniya*. Veliko Tarnovo: IK na NVU „Vasil Levski“, 2021, str. 161. ISBN 978-954-753-326-4.
12. Marinov, Petar Gospodinov. *Terorizmat – abstraktsii i realnosti*. Sofia: Iztok - Zapad, 2016. str. 295, ISBN 619152866-3.
13. Petkov, Yordan Metodiev. Osnovni nasoki za povishavane na umeniyata na lichniya sastav na razuznavatelните formirovaniya. In: *Sbornik s materialy ot konferentsiya na fakultet „Artileriya, PVO i KIS“ – Shumen*, 2019, s. 106 – 111. ISSN 2367-7902.
14. Radeva, Nikolina Radkova. *Aktualni aspekti na zashchitata na naselenieto pri bedstveni situatsii*. Varna: Steno, 2019, str. 141.
15. Romanova, Hristiana Angelova. *Potentsialni antropogenni ekokatastrofi vav Varnenski region. Strategiya za zashchita na naselenieto i zapazvane na bioraznoobrazieto*. Varna: MU – Varna, 2014.

ОРГАНИЗИРАНЕ И ПРОВЕЖДАНЕ НА ЕВАКУАЦИЯ НА БЕДСТВАЩО НАСЕЛЕНИЕ

полковник доц. д-р Георги Георгиев

Военна академия „Г. С. Раковски“, georgi.georgiev@rndc.bg

Резюме: За територията на Република България са характерни почти всички познати природни бедствия, но е възможно и възникването на производствени аварии съпроводени със спиране или сериозно нарушаване на производствения процес, с взривове, с пожари, със замърсяване на околната среда, разрушения, жертви или заплаха за сигурността на хора и имущество. Освен това катастрофите са често срещани явления.

За осигуряване на защита на живота и здравето на населението и неговото имущество, за опазването на околната среда при бедствия, аварии и катастрофи в Република България се изпълняват дейности по евакуация и са създадени държавни и обществени органи и организации със съответните сили и възможности на бързо и ефективно реагиране и ограничаване на последствията.

Ключови думи: *евакуация; бедствие; авария; катастрофа; процес на управление; защита при бедствие.*

ORGANIZATION AND CONDUCT OF THE EVACUATION OF DISASTER STRICKEN POPULATION

Colonel Assoc. Prof. Georgi Georgiev, PhD

National Defence College "G. S. Rakovski"

Sofia, Bulgaria

E-mail: georgi.georgiev@rndc.bg

Abstract: Almost all types of natural disasters are characteristic for the territory of the Republic of Bulgaria, but it is also possible that industrial accidents occur, that cause serious disruptions of the production process, with explosions, fires, environment pollution, destruction, casualties and threats for the safety of both people and property. Apart from that catastrophes are also not uncommon.

In order to protect the lives and health of people and their property, to protect the environment in case of disasters, accidents and catastrophes in the Republic of Bulgaria, different activities related to the evacuation are performed. State and municipal bodies and organizations with the relevant capabilities are created in order to manage in a fast and effective way the reaction and consequence management.

Keywords: *evacuation; disasters; accidents; catastrophe; management process; disaster protection*

Ежегодно в света, в резултат на стихийни бедствия, аварии, катастрофи, нещастни случаи в бита и в производството, загиват и получават травми хиляди хора, а материалните загуби оказват сериозно влияние върху икономиката на страните. Прилагането на нови правила и норми за реагиране при бедствия, аварии и катастрофи със сигурност ще спомогне за ограничаване и намаляване на жертвите и щетите.

Процесът по организиране, управление и провеждане на защита от бедствие е свързан с познаване на характера, динамиката на неговото развитие и ескалация. Борбата за преодоляване на бедствията трябва да започва на възможно най-ранна фаза, да се използват разнообразни методи за управление, както и гъвкавото им подменяне с оглед резките изменения на обстановката. Очевидно, трябва да се реагира своевременно на динамичния характер на бедствията, аварията и катастрофите. Именно по този начин е възможно рязкото снижаване на броя на човешките жертви.

Съгласно Закона за защита при бедствия (ЗЗБ), който урежда осигуряването на защитата на живота и здравето на населението, опазване на околната среда и имуществото при бедствия, дейностите по евакуация и/или разсредоточаване се извършват само при обявяване на бедствено положение или при възникване на опасност от бедствие.

В ЗЗБ са дефинирани понятията **евакуация, разсредоточаване, бедствие, бедствено положение, авария и ликвидиране на последствията от бедствия.**

„Евакуация е организирано извеждане на хора и животни от застрашени райони и настаняването и осигуряването им в безопасни места“. Евакуацията се счита за завършена, когато всички подлежащи на евакуация хора и животни са изведени зад границата на зоната на действие на поразяващите фактори на източника на бедствие, авария или катастрофа в безопасни райони.

„Разсредоточаването представлява организирано изнасяне на културни и материали ценности от застрашени райони и преместването и опазването им в безопасни места“. На разсредоточаване още подлежат и ценни исторически и архивни документи, научна и техническа документация, лекарствени средства, медицински изделия, кръв и кръвни продукти, медицинска апаратура и болнично имущество електронноизчислителна, комуникационна и информационна техника и програмни продукти, резервни части, инструменти, ценно оборудване, суровини и готова продукция, промишлени отрови, химикали, източници на йонизиращи лъчения, взривни вещества и горивно-смазочни материали, ценни книжа, парични знаци и скъпоценности, съхранявани в кредитни институции, други движими материални ценности, включени в разчетите за евакуация и разсредоточаване на планове за защита при бедствия.

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

„Бедствено положение е режим, който се въвежда в зоната на бедствието от определените в закона органи, свързан с прилагането на мерки за определен период от време с цел овладяване на бедствието и провеждане на спасителни и неотложни аварийно-възстановителни работи“.

„Авария е внезапна технологична повреда на машини, съоръжения и агрегати, съпроводена със спиране или сериозно нарушаване на технологичния процес, с взривове, образуване на пожари, замърсяване на околната среда, разрушения, жертви или заплахи за живота и здравето на гражданите“.

„Ликвидиране на последствията от бедствия и аварии са спасителни и неотложни аварийно-възстановителни работи, насочени към спасяване на живота и опазване на здравето на хората, намаляване размерите на щетите на околната среда и на материалните загуби, а така също локализиране на зоните на бедствено положение и прекратяване действието на характерните за тях опасни фактори“.

Условията и редът за провеждане на евакуация и разсредоточаване са от изключително важно значение за намаляване на последствията и броя на жертвите при възникване на определено бедствие. Всички особености свързани с условията и реда за провеждане на евакуация и разсредоточаване са оповестени в Наредба, приета с ПМС № 337 от 20.12.2012 г. и влязла в сила от 28.12.2012 г.

В зависимост от времето за подготовка и оповестяване евакуацията и разсредоточаването могат да бъдат два вида – незабавни и след предупреждение и оповестяване. Незавадна евакуация или разсредоточаване се извършва при регистриране на земетресение, ядрена или радиационна обстановка, инциденти с опасни вещества и материали, самолетни катастрофи, горски пожари и други опасности. Евакуация и разсредоточаване след предупреждение и оповестяване се извършва при наводнения, урагани, бури, снегонавявания и обледенявания. Съгласно дефинициите на закона в зависимост от ситуацията може да не се извършва евакуация и разсредоточаване, а да се осъществи само временно извеждане на лица, домашни и селскостопански животни, без настаняване и изнасяне на имущество на безопасни места.

Основна роля за успешното провеждане на евакуация и разсредоточаване е свързана с познаването и стриктното спазване на всички дейности при обявяване на бедствие или бедствено положение. Тези дейности се заключават в пет основни точки:

1. Вземане на решение за провеждане на евакуация и разсредоточаване.
2. Ранно предупреждение и оповестяване.
3. Извеждане и транспортиране на хора и животни, изнасяне и преместване на културни и материални ценности.
4. Настаняване и осигуряване на условия за живот и съхранение на културни и материални ценности.
5. Връщане на евакуираното население, животни, културни и материални ценности.

Провеждането на евакуация е основен способ за запазване на човешкия живот и намаляване жетровите от дадено неблагоприятно събитие. Именно поради този факт от съществено значение е спазването на определени правила и изисквания при осъществяване на тази дейност, а именно:

1. Своевременно реагиране при възникване на ситуации, налагащи евакуация и разсредоточаване.
2. Използване на всички възможности за оповестяване и информиране на населението.
3. Точно изпълнение на задълженията от участващите в провеждането на евакуацията и разсредоточаването.
4. Ефективно използване на наличните ресурси при провеждане на евакуация и разсредоточаване.
5. Наличие на актуални бази данни, необходими за провеждане на евакуация и разсредоточаване.
6. Единно ръководство и управление на евакуацията и разсредоточаването.

В зависимост от нуждите евакуираното население може да бъде настанено в сборни евакуационни пунктове (СЕП), евакуационни центрове (ЕЦ) или места за настаняване (МН). При провеждане на евакуация и разсредоточаване юридическите лица и едноличните търговци, включени в разчетите за евакуация и разсредоточаване, предоставят при поискване планираната помощ, докато физическите лица са длъжни да спазват установения ред за провеждане на евакуация и разсредоточаване и да оказват съдействие.

Планирането е целенасочен процес по обосноваване на определено управленско решение и разпределение на ресурсите за неговото изпълнение с цел създаване на благоприятни условия за успешно решаване на поставените задачи и рационалното използване на ресурсите. Основен момент при провеждането на всяка една дейност е изготвянето на план за действие. Именно чрез него организирането на дейностите, необходими за преодоляване на определено събитие или ситуация, се осъществява по-бързо, по-ефективно и се постига най-добър резултат. Планирането на евакуация и разсредоточаване се осъществява на три основни нива – общинско, областно и национално.

Основен момент тук е, че към съответните части от планове за защита при бедствия по чл. 9 от ЗЗБ се изготвят разчети. Те включват следните уточнения:

- начините и способите за оповестяване;
- местата на СЕП, ЕЦ и МН;
- отговорниците и състава на СЕП, ЕЦ и МН и техните задължения при провеждане на евакуация и разсредоточаване;
- транспортните средства, необходими за провеждането на евакуацията и разсредоточаването;
- основните и резервните маршрути за евакуация и разсредоточаване и организацията на движението;
- реда за настаняване и осигуряване на евакуираните лица и за съхранение на разсредоточените културни и материални ценности;
- мерките за осигуряване на обществен ред и опазване на имуществото на евакуираните;
- реда за връщане на евакуираните по местата за постоянно местоживее и на разсредоточените културни и материални ценности.

В СЕП се осигуряват условия за регистрация и разпределение на подлежащите на евакуация, минимални хигиенно-битови условия и подпомагане с храна и вода. В ЕЦ се осигуряват условия за регистрация на евакуираните, консултиране, комуникации, услуги и раздаване на продукти от първа необходимост. В МН се осигуряват условия за подслон, предоставяне при необходимост на храна, вода, дрехи, одеяла, комуникации, достъп до медицинска помощ и други.

Настаняването на евакуираните лица и съхранението на разсредоточените културни и материални ценности по възможност се планира на територията на съответната или на най-близката съседна община (област). При наличие на бедствие или обявяване на бедствено положение кметът на съответната община е длъжен да изготви разчети за евакуация и разсредоточаване за съответните части на общинския план за защита при бедствия съвместно с представители на ведомствата и юридическите лица, имащи отношение към тази дейност на територията на общината.

Областният управител изготвя разчети за евакуация и разсредоточаване за съответните части на областния план за защита при бедствия съвместно с териториалните звена на администрацията на централните органи на изпълнителната власт и кметовете на общините. Централните органи на изпълнителната власт в планове за защита при бедствия за изпълнение на задълженията им, предвидени в Националния план за защита при бедствия (чл. 9, ал. 6 ЗЗБ), разработват разчети за изпълнение на задълженията им, предвидени в Националния план за защита при бедствия. Средствата за покриване на разходите по провеждането на евакуацията и разсредоточаването са в рамките на общинските бюджети и/или бюджетите на отговорните ведомства за местни дейности.

Плановете за защита при бедствия се изготвят по части за всяка от опасностите, специфични за съответната територия, като частите за земетресение, наводнение и ядрена и радиационна авария са задължителни. Основната част от съдържанието на плана за защита при бедствия е свързана с:

- анализ и оценка на риска от бедствия;
- мерките за предотвратяване или намаляване на риска от бедствия;
- мерките за защита на населението;
- разпределението на задълженията и отговорните органи и лица за изпълнение на предвидените мерки;
- средствата и ресурсите, необходими за изпълнение на дейностите;
- начина на взаимодействие между съставните части на единната спасителна система;
- реда за ранно предупреждение и оповестяване на органите на изпълнителната власт, на съставните части на единната спасителна система и населението при опасност или възникване на бедствия;
- информация за екипите и средствата на съставните части на единната спасителна система;
- време за готовност за реагиране на съставните части на единната спасителна система.

Планът за разсредоточаване и евакуация на обект от националното стопанство се състои от две части – текстуална, графическа и приложения.

Текстуалната част на плана включва: обем на евакуационните мероприятия; списък на евакуационните органи; ред за привеждане в готовност на евакуационните органи; оповестяване за началото на разсредоточаването и евакуацията; разчет на подлежащите на разсредоточаване и евакуация; организация на управлението, свързката и оповестяването; защита и осигуряване на разсредоточаващите се (евакуираните) и приложения – схема на маршрута, схема на сборно евакуационни пунктове, схема за свързките, разчет на марша, разчет на евакуацията и др.

Графическата част на плана се разработва върху план-схема на обекта и карта. На план-схемата на обекта се нанасят сборно евакуационни пунктове, които ще се използват при провеждането на евакуацията и разсредоточаването. Върху картата се нанася обектът, местата за настаняване, маршрутите за изнасяне (основни и запасни), местата за почивките, бензиностанциите, медицинските, техническите и снабдителните пунктове.

Органите за управление при бедствия, аварии и катастрофи осъществяват наблюдение на рискови фактори, анализ, оценка и прогнозиране на потенциални бедствия, аварии и катастрофи, извършват планиране и подготовка за предотвратяване и управление в извънредни условия, подготвят решения и провеждат действия в конкретни бедствени ситуации. Основните отговорности при евакуацията и разсредоточаването са свързани с вземане на решение за евакуация. Това се осъществява от кмета на съответната община, областния управител, както и от Министерския съвет.

При вземането на решение за евакуация се имат предвид всички фактори, влияещи върху обстановката, включително недостатъчната информация, нивото на информираност на населението за характера на опасността и подходящите защитни действия, възможните рискове при придвижването и др.

Ръководството на евакуацията и разсредоточаването на територията на повече от една област се осъществява от Националния щаб по чл. 62а, ал. 2 от ЗЗБ. Ръководството на евакуацията и разсредоточаването на областно и общинско ниво се осъществява от областните управители и кметовете на общини, които се подпомагат от щабове по чл. 64, ал. 1, т. 10 и чл. 65, ал. 1, т. 7 от ЗЗБ. За изпълнение на дейностите по евакуация и разсредоточаване тези щабове:

- организират оповестяването за евакуация и разсредоточаване;
- организират извеждането (транспортирането) на подлежащите на евакуация и разсредоточаване хора, животни и имущество;
- организират посрещането и настаняването на евакуираните, както и съхраняването на разсредоточеното имущество на съответната територия;
- организират логистичното осигуряване на евакуираните и защитата на разсредоточеното имущество на съответната територия;
- осъществяват непосредственото ръководство на СЕП, ЕЦ и МН;
- организират охраната на територията, от която е извършена евакуацията и разсредоточаването;
- организират и координират получаването и раздаването на хуманитарни помощи;
- предоставят информация за проведената евакуация и разсредоточаване;

– извършват и други дейности във връзка с провеждането на евакуацията и разсредоточаването.

Организацията на движението по маршрутите за евакуация и разсредоточаване се извършва от Министерството на вътрешните работи (МВР), Министерството на транспорта, информационните технологии и съобщенията, Министерството на регионалното развитие и благоустройството, Министерството на отбраната и съставните части на единната спасителна система. Министерството на транспорта, информационните технологии и съобщенията организира евакуацията и разсредоточаването с железопътен транспорт и съдейства за организирането с автомобилен, воден и въздушен транспорт. Кметовете на общините съвместно с превозвачите, които притежават лиценз за извършване на превоз на пътници или товари, уреждат необходимите транспортни средства, включени в разчетите за евакуация и разсредоточаване.

Оказването на спешна медицинска помощ в СЕП, по маршрутите за евакуация, в ЕЦ и в МН се организира и извършва от Министерството на здравеопазването (МЗ) чрез централите за спешна медицинска помощ и други лечебни и здравни заведения предвидени в съответните планове за защита при бедствия. Хигиенно-противоепидемичните мероприятия в МН се организират от съответната регионална здравна инспекция. При провеждане на евакуация на територията на повече от една област, МЗ координира медицинското осигуряване на населението съгласно областните планове за защита при бедствия.

Контролът по храните в СЕП, маршрутите за евакуация, ЕЦ и МН се осъществява от Българската агенция по безопасност на храните и от областните дирекции по безопасност на храните към Министерството на земеделието и храните.

Общественият ред по време на евакуация и разсредоточаване се осигурява от МВР. Логистичното осигуряване на евакуацията и разсредоточаването се извършва от кмета на общината.

Населението се оповестява за началото на евакуацията и разсредоточаването по реда на Наредбата за условията и реда за функциониране на Националната система за ранно предупреждение и оповестяване на органите на изпълнителната власт и населението при бедствия и за оповестяване при въздушна опасност, приета с Постановление № 48 на Министерския съвет от 2012 г.

Оповестяването на населението в застрашени райони се извършва чрез:

– Националната система за ранно предупреждение и оповестяване на органите на изпълнителната власт и населението. Наблюдението, ранното предупреждение и оповестяването се основават на информация и данни, предоставени от физически лица, организации и институции, информация и данни от системи за мониторинг на метеорологични, хидрологични, сеизмологични, химически, биологични, радиологични, ядрени, екологични и други обекти и явления, информация и данни, получени в централите на Националната система за спешни повиквания с единен европейски номер 112 и други;

– локалните системи за оповестяване в обектите;

– електронните съобщителни мрежи и/или услуги на предприятия, осъществяващи електронни съобщения по заявка на МВР

– комуникационната среда на МВР и други ведомства и организации.

– ресурсите на Единната спасителна система и местните средства за масово осведомяване;

– други средства за оповестяване.

Съобщението за евакуация трябва да съдържа:

– издаващ орган;

– дата и час на издаване;

– точно описание на бедствието или опасността и район, който е или е вероятно да бъде засегнат;

– указания за евакуация съгласно разчетите – СЕП, евакуационни маршрути и ЕЦ, както и какво евакуиращите се да вземат със себе си;

– време на следващото съобщение.

Способите за евакуация и срокът за нейното провеждане зависят от мащабите на бедствието или аварията, числеността на оказалото се в опасната зона население, наличието на транспорт и други конкретни условия. Населението се евакуира с транспорт, пеш или по комбиниран способ, основан на съчетаване на извеждане на максимално възможно количество хора с наличния транспорт. При това транспортът се планира да извози като правило население, което не може или трудно се придвижва пеш.

Пеша евакуация се планира на разстояние за едноминутен преход, извършван за 10 – 12 часа движение, като се отчита изходът от зоната на бедствието. За осигуряване на организирано движение

и управление се формират колонии с численост от 500 до 1000 човека по производствено-териториален признак и се назначават началници (отговорници) на колоните от ръководния състав.

Средната скорост на движение на колоните е 4 – 5 km в час. Разстоянието между колоните е до 500 метра. По време на движение се организират малки почивки с продължителност 10 – 15 минути. Те се дават за пешите колонии през всеки 1 – 1,5 часа движение. Големи почивки с продължителност 5 – 6 часа се дават за пешите колонии в началото на втората половина на денонощния преход.

За организация на движението в пеши марш в колоните се създават групи за управление с началници на маршрутите за евакуация, назначени с решение на органите на местното самоуправление, най-често от състава на пътните служби.

В състава на групите за управление влизат:

- звено за свързка – 3 – 4 човека;
- постове за регулиране на движението – 5 – 8 човека;
- отделение за осигуряване на движението – 8 – 10 човека;
- единичен пост – 3 човека.

Основните задачи на групите за управление по маршрутите за евакуация в пеши ред са:

- организирано начало на марша на пешите колонии;
- поддържане на ред и осигуряване на управление по маршрута;
- подготовка и поддържане на маршрута в изправно състояние;
- водене на радиационно, химическо и бактериологично разузнаване по маршрута;
- оказване на медицинска помощ на болелите.

Основният недостатък на този способ е продължителното време за изнасяне на разсрещочаващото и евакуиращото се население. Евакуацията на населението с транспорт се извършва организирано в колонии от машини. Дистанциите между отделните колонии и машините в колоната може да бъдат 25 – 50 метра. При движение в условията на ограничена видимост, прашни пътища, лоши терени, метеорологични условия и повишена скорост дистанциите се увеличават и могат да стигнат до 100 – 150 метра.

Денонощният преход (средно за движение в едно денонощие се приемат 10 – 12 часа) може да бъде до 400 km и повече. В планинско-гориста местност и при лоши условия (прашни пътища, ограничена видимост, поледица, наличие на стръмни наклони и завои) – 200 – 250 km, а понякога и по-малко.

Средната скорост за движение при марш зависи от състоянието на маршрута, подготовката на шофьорите, както и от организацията и осигуряването на марша. Без да се взема под внимание времето за почивките, тя може да бъде за автомобилни колонии – 30 – 40 km/h и повече. В планинско-гориста местност и при други неблагоприятни условия средната скорост за движение може да бъде и до 20 km/h. Във всички случаи маршът трябва да се извършва с възможно максималната за дадените условия скорост.

При извършване на марш с автомобилен транспорт за хранене и почивка на хората се определят малки и големи, дневни и нощни почивки. В хода на марша малки почивки с продължителност до 1 час се определят през 3 – 4 часа движение и една почивка с продължителност до 2 часа във втората половина на денонощния преход. Денуването (нощуването) се дава в края на всеки денонощен преход, а при извършване на марш на големи разстояния при необходимост може да се определи и денонощна почивка. За дневна (нощна) почивка, както и за почивка с продължителност до 2 часа, трябва да се избират райони с достатъчни и проверени водоизточници.

Изнасянето с транспорт е най-ефективният способ, тъй като се провежда в кратки срокове, запазват се силите и здравето на хората. На извозване подлежат майките с деца до 7 годишна възраст, болните и възрастните хора, личният състав на министерствата, ведомствата, на обектите от националното стопанство (степенувани по важност), медицинският персонал на болничните заведения, детските ясли и градини, разплодните животни, материалните и културните ценности.

Организирането на дейностите по извеждане и транспортиране на хора и животни, изнасяне и преместване на културни и материални ценности се извършва от СЕП непосредствено след оповестяването. В СЕП се извършват регистрация и разпределение на евакуиращите се по маршрути и ЕЦ и осигуряване на условия за временен престой. В СЕП се създава организация за оптимално използване на превозните средства, включително на личните автомобили.

Основните места, където се разполагат сборните евакуационни пунктове, са в близост до железопътни гари, морски и речни пристанища, летища, както и в непосредствена близост до маршрутите за

пеша евакуация в места, осигуряващи условия за събиране на хора. Приоритетно се евакуират деца, болни и възрастни хора. Хората от социални, лечебни и здравни заведения се евакуират, като се полагат изискванията се за тях грижи от персонала на съответното заведение. Евакуацията от зони със степен на радиационно и химическо замърсяване и биологическо заразяване се извършва след провеждане на деконтаминация.

В Евакуационни центрове (ЕЦ) се извършва регистрация на евакуираните, оказване при необходимост на психологическа помощ, консултиране, раздаване на продукти от първа необходимост и разпределение по места за настаняване (МН). При разпределение по места за настаняване не се разделят семейства и се отчитат нуждите на групи с определени специални нужди и с различни културни, етнически или религиозни идентичности. В МН се предоставя подслон, снабдяване с храна, вода, дрехи и одеяла и при необходимост се оказва медицинска и психологическа помощ.

Щабовете за изпълнение на планове за защита при бедствия предоставят на Националния щаб по чл. 62а, ал. 2 от ЗЗБ информация за проведената евакуация и разсредоточаване. Органът, разпоредил евакуацията и разсредоточаването, със заповед организира връщането по местата за постоянно местоживее.

Осигуряването на разсредоточаването и евакуацията е комплекс от мероприятия, провеждани в мирно време, през степените на готовност и в хода на разсредоточаването и евакуацията. То има за цел да се създадат най-благоприятни условия за провеждане на разредоточаването и евакуацията и намаляване на загубите.

Защитата на населението от бедствия, аварии и катастрофи е една от основните задачи на държавата. Тази дейност е приоритетна в цивилизованите страни. Организацията на обединените нации обявя десетилетието за предотвратяване и намаляване на последствията от стихийни бедствия, което е осъзнат израз на заплахата, която те представляват за човечеството. В Европа и страната има природни и производствени рискови фактори, които засягат сигурността на хората, производствата и собствеността и обуславят необходимостта от надеждна защита на населението, провеждане на превантивни дейности за недопускане или намаляване на загубите и вредните последствия при бедствия, аварии и катастрофи.

За територията на Република България са характерни природни явления като земетресения, суша, свлачища и срутища, горски и полски пожари, градушки, наводнения, морски щорм, снежни бури и овладявания, огнища на заразни болести по хората, животните и растенията. Нерядко възникват крупни производствени аварии, които представляват внезапни повреди на машини, механизми и агрегати по време на тяхната експлоатация, съпроводени със спиране или сериозно нарушаване на производствения процес, с взривове, образуване на огнища на пожари, замърсяване на околната среда, разрушения, жертви или заплаха за сигурността на хора и имущество, катастрофите са чести срещани явления.

За борба с бедствията, аварията и катастрофите в Република България са създадени държавни и обществени органи и сили за защита на населението и националното стопанство при критични ситуации с възможности на бързо и ефективно реагиране и ограничаване на последствията от тях.

ЛИТЕРАТУРА

1. Балева, Д. Икономически аспекти на защитата при бедствия. *Годишник на факултет „Командно-щабен“, Военна академия „Г. С. Раковски“*, 2/2012, стр. 173 – 179. ISSN 1312-2991.
2. Балева, Д. Повишаване на защитата на населението при бедствия в Република България чрез развитие на доброволни формирования за защита. В: *Научна конференция „Актуални проблеми на сигурността“*, 26-27 октомври, 2017 г., Велико Търново. ISSN 2367-7465.
3. Дуганова, Д. Оценка на ефективността на взаимодействието между Министерството на отбраната, държавната и местната власт при бедствия, аварии и катастрофи. В: *Сборник материали от Международна научна конференция на Военна академия „Г. С. Раковски“ – „Дългосрочни предизвикателства за развитие на средата за сигурност и изграждане на способности на въоръжените сили“*, втора част, 12 – 14 ноември 2019, стр. 257 – 268. ISBN 978-619-7478-35-8
4. Закон за защита при бедствия. *Държавен вестник*, бр. 102 от 19.12.2006, изм. и доп. бр. 60 от 07.07.2020.
5. Закон за Министерството на вътрешните работи. *Държавен вестник*, бр. 53 от 27 Юни 2014, доп. бр. 20 от 9 март 2021.
6. Закон за отбраната и въоръжените сили на Република България. *Държавен вестник*, бр. 35 от 12.05.2009, изм. и доп. бр. 23 от 19.03.2021, в сила от 1.09.2021, попр. бр. 25 от 26.03.2021.
7. Наредба за условията и реда за провеждане на евакуация и разсредоточаване. Приета с ПМС № 337 от 20.12.2012 г. *Държавен вестник*, бр. 103 от 28 Декември 2012.
8. Недевски, Д. *Изясняване и оценка на екологичната обстановка след техногенни аварии*. София: Военна академия „Г. С. Раковски“, 2018.

9. Недевски, Д. *Системи за мониторинг, ранно предупреждение и оповестяване за бедствия и аварии*. София: Военна академия „Г. С. Раковски“, 2010.

REFERENCES

1. Baleva, D. Ikonomicheski aspekti na zashtitata pri bedstviya. *Godishnik na fakultet „Komandno-shtaben“*, Voenna akademiya „G. S. Rakovski“, 2/2012, str. 173 – 179. ISSN 1312-2991.
2. Baleva, D. Povishavane na zashtitata na naselenieto pri bedstviya v Republika Bgariya chrez razvitie na dobrovolni formirovaniya za zashtita. In: *Nauchna konferentsiya „Aktualni problemi na sigurnostta“*, 26-27 oktomvri, 2017 g., Veliko Tarnovo. ISSN 2367-7465.
3. Duganova, D. Otsenka na effektivnostta na vzaimodeystviето mezhdu Ministerstvoto na otbranata, darzhavnata i mestnata vlast pri bedstviya, аварии i katastrofi. In: *Sbornik materialy ot Mezhdunarodna nauchna konferentsiya na Voenna akademiya „G. S. Rakovski“ – „Dalgosrochni predizvikelstva za razvitie na sredata za sigurnost i izgrazhdane na sposobnosti na vaorazhenite sili“*, vtora chast, 12 – 14 noemvri 2019, str. 257 – 268. ISBN 978-619-7478-35-8
4. Zakon za zashtita pri bedstviya. *Darzhaven vestnik*, br. 102 ot 19.12.2006, izm. i dop. br. 60 ot 07.07.2020.
5. Zakon za Ministerstvoto na vatreshnite raboti. *Darzhaven vestnik*, br.53 ot 27 Yuni 2014, dop. br. 20 ot 9 mart 2021.
6. Zakon za otbranata i vaorazhenite sili na Republika Bgariya. *Darzhaven vestnik*, br.35 ot 12.05.2009, izm. i dop. br.23 ot 19.03.2021, v sila ot 1.09.2021, popr. br 25 ot 26.03.2021.
7. Naredba za usloviyata i reda za provezhdane na evakuatsiya i razsredotochavane. Prieta s PMS № 337 ot 20.12.2012 g. *Darzhaven vestnik*, br. 103 ot 28 Dekemvri 2012.
8. Nedeovski, D. *Izysnyavane i otsenka na ekologichnata obstanovka sled tehnogenni аварии*. Sofia: Voenna akademiya „G. S. Rakovski“, 2018.
9. Nedeovski, D. *Sistemi za monitoring, ranno preduprezhdenie i opovestyavane za bedstviya i аварии*. Sofia: Voenna akademiya „G. S. Rakovski“, 2010.

ДОКТРИНАЛНИ АСПЕКТИ НА ОСИГУРЯВАНЕТО И ПОДДРЪЖКАТА

доц. д-р Светослав Велев

Военна академия „Г. С. Раковски“, s.velev@rmdc.bg

Резюме: Докладът е посветен на развитието на схващанията и разбиранията за определена част от доктриналната база на въоръжените сили, свързана с осигуряването и поддръжката при провежданите от тях операции. „Доктринална база“ е обобщаващо понятие. В изследването са използвани и коментирани и някои основни моменти от стратегически и концептуални документи, както и такива от по-ниско ниво и архивни издания.

Ключови думи: доктрина; операция; осигуряване; поддръжка; развитие

DOCTRINAL ASPECTS OF COMBAT SUPPORT

Assoc. Prof. Svetoslav Velev, PhD

Rakovski National Defence College

Sofia, Bulgaria

E-mail: s.velev@rmdc.bg

Abstract: The report is dedicated to the development of perceptions and understandings of a certain part of the doctrinal base of the Armed Forces, related to the provision and support of their operations. „Doctrinal basis“ is a generalizing concept. The study also uses and comments on some key points from strategic and conceptual documents, as well as lower-level ones and archival publications.

Keywords: doctrine; operation; provision; support; development

Направените промени, започнали с издадените през 1996 г. бойни устави, преминали от доктрините на видовете въоръжени сили през 2000, 2001 и 2002 г. и Наставлението за служба на щабовете (2002 г.)¹ до актуализиращите се и в момента Доктрина на въоръжените сили на Република България и свързаните с нея базови и поддържащи доктрини и приложни документи очертават непрекъсната тенденция за създаване на общоприета основа, съвместима с доктриналната база и стандарти в НАТО. Изданията от първите няколко години на новото хилядолетие са изпълнили своята до голяма степен символична роля след един период на неяснота и липса на актуална база за практическо ръководство и управление на войските. Необходимостта от такава теоретична основа е неоспорима, защото от нея пряко зависи военната мощ на страната. Нейният трети компонент е *концептуалният* и в него влизат именно *доктрините и концептуалното мислене*. Предназначението на доктрините е „да предостави насоки за ефективно провеждане на военните операции, както и да *стандартизира терминологията и да уеднакви разбиранията...*“, те са един от компонентите на отбранителните способности.²

Влагането на еднакъв смисъл и единно разбиране за съдържанието на използваните термини при планирането и провеждането на операциите е все още е предизвикателство. То е породено от липсата на последователност при изследването на процесите и обектите в областта на военната мощ. Нарушен е подходът *описание, разкриване, разбиране и възприемане*.

Представянето на външните характеристики на процеса или обекта, който стои зад определен термин (*описанието*), трябва да е последвано от *разкриване* на причинно-следствените връзки, за което са необходими специфични понятия. Следва *разбирането*, което, за да е единно, трябва да се основава на мисловните стереотипи, на схващанията на широкия кръг експерти, ангажирани в настоящия случай с разнообразните военни операции. *Възприемането* се базира на личен подход и индивидуалната теоретична подготовка. Като преминава през различните равнища, обективното описание се трансформира в *субективно възприемане*.³

Специфичните понятия, първоначално използвани за *разкриване* на причинно-следствените връзки, не са общоприети. В началния етап на създаване на „новите“ регламентиращи документи се въвежда меха-

нична съвкупност от действащите дотогава термини заедно с такива, които са буквално преведени и често неточни, зависещи от владенето на съответния чужд език или индивидуалното виждане на авторите за същността им. От тук произтича и нееднозначното им възприемане, което е обяснимо, тъй като опитът и подготовката на специалистите, използващи терминологията, не са на едно ниво. Естествено липсата на обективното описание води до такова субективно възприемане, което затруднява работата на експертите, използващи различните публикации.

Споменатият подход включва и още едно, пето равнище – *направляването*, което е способността за въздействие на базата на постигнатите до този момент резултати. Понеже резултатите са доста спорни, се оказва изключително трудно те да бъдат използвани в практиката или пък като основа за бъдещо развитие.

1. Осигуряване

1.1. Възникване и развитие на осигуряването

Армиите възникват заедно с държавата и в определен исторически период са нейната най-важна институция. Съществува пряка зависимост между военната техника, формите на организация на въоръжените сили и начините на провеждане на военните операции. Оръжието е факторът, който определя развитието и изграждането на въоръжените сили и начините за водене на войната. Новите системи предизвикват и появата на специфични видове бойни действия, свързани освен с използването им и със защитата от тях. За осъществяването им се променя организационната структура и цялостното изграждане на въоръжените сили, създават се и нови видове.

Единното разбиране за вложения смисъл и за съдържанието на анализираното понятие изисква и разглеждането на неговата семантика.* „Осигурявам“ означава *„правя нещо да бъде напълно възможно, правя сигурно съществуването, осъществяването на нещо“*.*

1.1.1. Възникване на осигуряването

Осигуряването като съвкупност от бойни дейности по естествена и логична необходимост възниква и се развива едновременно с войските. Първоначално е свързано с охраната им, като целта му е да „изключи внезапно противниково нападение“, но прогресът на оръжейните технологии, организацията и способите за използване на войските налагат необходимостта от „намаляване на ефективността на противниковите удари“ и създаване на „благоприятни условия за подразделенията и частите едновременно да влизат в бой и успешно да го водят“⁴. Съпоставката с формулирания в речника смисъл на думата „осигуряване“ показва коректното използване и точност на влагането в понятието съдържание от военните експерти. Видовете осигурявания *„правят възможно“* постигането на желания краен резултат, *„осъществяването на нещо“* – на изпълнението на задачите, на целите на операцията, на успеха на мисията...

Началото на процеса на групирането и класификацията на бойните дейности без все още да бъдат обобщени в един термин може да се проследи чрез няколко примера. Постепенно в уставите се регламентира организацията на дейности свързани със създаване на условия за изпълнение на задачите от формираната. Те са свързани с охрана, разузнаване и защита от все по-модерните въоръжения и техника.

В издадения през 1912 г. „Устав на полската служба“⁵ в раздел „Охранителна служба“ е регламентирано, че нейната цел е: „а) да се предвдварят войските от ненадежности, б) да се препятства на неприятелските разузнаващи части да проникват към нашите войски в) да се дава време на нашите войски да се приготвят за изпълнение на дадените разпоредби“. Въведеният по-късно раздел „Свързка, разузнаване и охрана“⁶ разширява сферата на дейностите, необходими за ефективното използване на формираната. Изброените примери потвърждават логическата връзка между описаните дейности, тяхната цел и разбирането за тяхната същност, която напълно се вписва в „осигуряване“-то.

Като обобщение на резултатите от развитието на изследваната функционална област (осигуряването) може да бъде възприето съдържанието на Глава V „Охрана“ от „Английски правилник за бойната служба“ (Field service regulations, vol. II, operations – general, 1935).⁷ Правилникът е преведен и допълван от български военни експерти през 1935, 1936 и 1937 г.

* Семантика – наука, която изследва значенията на езиковите единици и отношението към назоваваните предмети; значение, смисъл. *Съвременен тълковен речник на Българския език*. Велико Търново: „Абагар“ ООД, 2000.

В него до голяма степен е представено развитието на въоръжените сили в навечерието на Втората световна война, отчетени са новите фактори, влияещи върху подготовката и воденето на боя и са предложени адекватни на настъпилите промени решения. На първо място прави впечатление класификацията на различните формирования. Родовете войски са разделени на такива, „чийто главна задача е да влязат в допир с противника, да превземат и овладеят изгодни точки или да ги отбраняват“ – това са бронираните войски, конница и пехота. Другите са „войски, чийто главна задача е да подкрепят първите в техните действия“ – т. е. „*правят нещо да бъде напълно възможно*“. Те са класифицирани още като „спомогателни“ – артилерия, инженерни и свързочни войски.

В правилника са коментирани и правилата за „снабдителната и подкрепителна служба“. Очевидно е, че групирането и класификацията са направени по функционални критерии. В Българската армия в края на двадесетте години на 20 век родовете войски са: пехота, погранична стража, артилерия, конница и инженерни войски (в чийто състав са и свързочните формирования до 1938 г.). Създават се два нови рода „Газова служба“ (предшестваща химическата служба и в следствие – химически войски, през 1928 г.) и противовъздушна отбрана през 1929 г.⁸ Съпоставката с формулировката в тълковния речник отново дава възможност да се перифразира, че споменатите войски и служби „правят възможно осъществяването на задачите; правят сигурно съществуването на останалите“. Термините „поддръжка“ и „осигуряване“ все още не се използват, но на практика такива задачи се изпълняват.

Развитието на оръжейните системи и способите за използването им са причината за появата на поредния аспект на защитата – от бронираните средства на противника. Смесово тя също попада в „осигуряването“ – тя е инструмент за „намаляване на ефективността на противниковите удари“.

1.1.2. Развитие на осигуряването

Периодът на Втората световна война не се характеризира с развитие на теоретичните основи на тактиката и оперативното изкуство на Българската армия. Натрупаният в него практически опит става основа на следващия етап (края на четиридесетте и началото на петдесетте години на 20 век) на осъвременяване на схващанията за подготовката и провеждането на боя и операцията. Те са отразени в „Устав за щабната служба – Част I, Пехотен полк“⁹, в който се регламентират взаимоотношенията на щаба на полка със специалистите по видовете осигурявания. Разузнаването, наблюдението, противотанковата и противовъздушната отбрана, инженерното осигуряване, противохимическата защита и организацията на свързките вече са обособени като „осигуряване на боя“. Аналогично е представянето им в част II – „Дивизия и армия“. Формално може да се приеме, че това е първото използване на термина в широкия контекст на съвременното му значение. Той обаче не съвпада с приетия по-късно „бойно осигуряване“.

В следващите издания – „Наставление за полевата служба на щабовете в Българската народна армия“¹⁰ е използвано понятието „обезпечаване“. В него са включени: разузнаване на противника и местността; охранение на войските; организация на противовъздушната, противодесантната и противотанковата отбрана; противохимическата защита и маскировка. Прави впечатление, че, въпреки разликата във формулировките и разширения поради новите средства на въоръжение обхват, няма разлика между целта на „охранението“ в сравнение с 1912 г.

В „Наставление за полевата служба на щабовете“¹¹ анализират функционална област отново е озаглавена „Осигуряване на бойните действия на войските“. Тя включва разузнаване, защита от оръжията за масово поразяване (ЗМП), охранение, инженерно осигуряване, маскировка, борба с радиоелектронните средства на противника и защита на своите радиоелектронни средства, хидрометеорологично, топогеодезично осигуряване, тилово, шурманско, радиотехническо и инженерно-авиационно осигуряване.

Изключително разширеният обхват на дейностите не променя същността на осигуряването и се запазва вложенят в думата смисъл – то „прави нещо да бъде напълно възможно, прави сигурно съществуването, осъществяването на нещо“ или от военна гледна точка е насочено към „намаляване на ефективността на противниковите удари“, създава „благоприятни условия за подразделенията и частите едновременно да влизат в бой и успешно да го водят“.

Благоприятните условия са акцентът в осигуряването на действията и на друг вид въоръжени сили – военноморските.¹² То „... има за цел да се създадат най-благоприятни условия за изпълнението на поставената им бойна задача“. Непрекъснатата модернизация и технологични нововъведения във въоръженията и способите за прилагането им изискват и създаване на организация за ефективното им използване. Следствие от промените е и групирането на дейностите в рамките на осигуряването – по-

вяват се видовете осигурявания – бойно, техническо (специално техническо) и тилово, регламентирани в бойните устава от 1984 г.¹³ Тази класификация се запазва до 1993 г. Оттогава датира проекта на „Боев устав – механизирани (танков) батальон“.¹⁴ В него осигуряването на бойните действия е разделено на бойно и материално-техническо, тилово и медицинско осигуряване.

Интерес представлява въвеждането на понятието „бойна поддръжка“. С него са обозначени част от формированията, чиито функции са свързани с осъществяването на дейностите по осигуряване на бойните действия на батальона – „Използване на подразделенията за бойна поддръжка и осигуряване...“. Въвежда се и терминът „огнева поддръжка“ като функция на минохвъргачната батарея и противотанковия взвод.

Проектът се реализира през 1996 г. като част от група нови публикации^{15, 16}, в които обхватът на осигуряването приема вида: бойно осигуряване, информация и връзки с обществеността и специално техническо, техническо, тилово и медицинско осигуряване. Новост е терминът „логистично осигуряване“¹⁷, а доктрината за логистиката на Българската армия е част от поредица, в която започва използването на актуална терминология – процес, който продължава и в момента.

За логиката и последователността в налагането на новите понятия може да се съди от споменатата доктрина за логистиката. Само година по-рано (2000 г.) тя е предшествана от проект на „Доктрина за материално-техническото осигуряване на Българската армия“. Нещо повече – в Доктрината за логистиката се подчертава, че е разработена в съответствие с „... концепцията за единно материално-техническо осигуряване на Българската армия“. Липсва обосновка на връзката между „материално-техническо осигуряване“ и „логистика“, което е красноречив пример за „импровизацията“ в работата на колективите.

В друга доктрина, за Съвместните операции¹⁸ в Приложение 6 т. 4 е озаглавена „Осигуряване на операцията“. В нея са посочени „Концепция за материално-техническото осигуряване“ и „Стандарти и изисквания на материално-техническото осигуряване“, въпреки че в основната част (раздел 6 „всестранно осигуряване“) става дума за „логистично осигуряване“. И двете доктрини са приети на съвети на Началник-щабове при началника на Генералния щаб на Българската армия в период от двадесет дена... На практика изброените документи не са осигурили това, за което са предназначени – да въведат система от официално приети възгледи и принципи за планиране, осигуряване и провеждане на операции от въоръжените сили.

В публикуваната през 2001 г. Доктрина на Сухопътните войски¹⁹ няма определение за това какво представлява осигуряването. В главата наречена „Осигуряване на операциите, сраженията, бойните действия и боевете“ са изброени разузнаване (основна бойна функция от бойните операционни системи), комуникационно-информационно осигуряване (система от дейности), оперативна маскировка (комплекс от мероприятия), сигурност (комплекс от мероприятия), инженерно осигуряване, ЯХБЗ и Е (комплекс от мероприятия), топогеодезично осигуряване (съвкупност от дейности), хидрометеорологично осигуряване, материално-техническо (а не логистично) и медицинско осигуряване (комплекс от дейности). В доктрината на Военновъздушните сили (ВВС)²⁰ ясно е посочено, че то е комплекс от мероприятия за поддържане на формированията във висока бойна готовност и боеспособност и създаване на благоприятни условия за изпълнение на задачите им. Разделено е на бойно, логистично и психологическо, както е и в доктрината на Военноморските сили (ВМС)²¹.

В периода 2011 – 2014 г., когато е издадена следващата поредица от доктрини, Република България вече е член на НАТО. В тази група публикации осигуряването е представено и от друга гледна точка. В Доктрината на въоръжените сили на Република България²², най-високото ниво в йерархичната структура на доктриналните документи, осигуряването, е определено като част от физическия компонент на военната мощ. На него вече се гледа като на „инструмент“ за *съхраняване* на потенциала на силите. В термина вече се влага нов смисъл, свързан с дейностите за организацията и осигуряването на материалните, финансовите и човешките ресурси за поддържане на способностите²³. Това е съвсем различно определение, в понятието на практика се влага ново съдържание, без да има обективни основания за това.

В доктрините от различните периоди, както и в различните им варианти, не са възприети единни критерии, чрез които да се определи кои дейности представляват осигуряване и кои – поддръжка. Като пример за непоследователност може да бъде посочено, че в доктрината на въоръжените сили на Република България (2011 г.) военното контраразузнаване е определено като осигуряване, а в нейния

вариант (А) от 2017 г. то е поставено в раздела „Поддръжка“. Регламентираните в „Доктрина за сухопътните операции“²⁴ бойни функции са посочени като инструментът, описващ всички аспекти на боя. Една от тях е „бойно осигуряване и поддръжка“, „Бойно осигуряване“ обаче никъде не се използва като понятие по-нататък в публикацията.

В Доктрина за планиране на операции от 2013²⁵ г. в раздела „Разработване на план за операция“ като една от дейностите в процеса е посочена „планиране на подготовката и всестранното осигуряване на силите“. В следващото издание на доктрината – А, от 2018 г. осигуряването е обозначено като функционална област, заедно с маньовъра, огневото поразяване, командването и управлението, разузнаването, защитата на силите и гражданско-военното сътрудничество.

Мотивите за цитираните промени са неясни. Те в никакъв случай не допринасят за единно разбиране и това в крайна сметка е препятствие пред уеднаквяването на възприятията и стандартизацията на терминологията. Причината за това е, че разнообразните дейности, мероприятия, функции и съвкупностите от тях не са коректно описани и не е разкрита тяхната същност. Като се използват предоставените в документите описания на елементите, съставлящи осигуряването на войските и силите следва да се изведе основният резултат от тяхното осъществяване, който ги групира в тази категория.

Крайният продукт от военноеографското, метеорологично и хидрографско осигуряване е оценена от гледна точка на конкретната операция *информация* за терена и хидрометеорологичната обстановка. Нейното предназначение е да послужи при вземането на решения или за тяхната корекция при промяна в ситуацията.

Резултатът от дейностите за разкриване, предотвратяване и противодействие на заплахите срещу военнотбранителните способности, каквато е функцията на военното контраразузнаване, е постигане на *състояние на сигурност* в определена област. Целта е намаляване на уязвимостта на въоръжените сили при изпълнение на техните мисии.

Военнополицейското осигуряване е комплекс от дейности, в резултат на които се постига свобода на действие и мобилност при движението на войските, сигурност и дисциплина в зоната на операцията, т. е. отново крайният продукт е някаква форма на сигурност. Контраразузнаването и военнотбранителното осигуряване реално създават благоприятни условия за организацията и провеждането на операцията.

Логистика е комплекс от дейности, резултатът от които е снабдяването на въоръжените сили с ресурси и тяхното правилно използване. В доктрината точният термин е „материални ресурси“, но освен тях тук могат да бъдат приобщени и човешките ресурси, тъй като чрез дейностите по медицинското осигуряване се запазва, укрепва и възстановява здравето на личния състав.

Спопоставката между значенията на думата „осигурявам“ (*„правя нещо да бъде напълно възможно, правя сигурно съществуването, осъществяването на нещо“*) и смисъла, вложен в описанието на дейностите показва, че те съвпадат. Същността на елементите, съставлящи осигуряването, може да се определи и на базата на ефектите, получавани в резултат на този тип дейности.

„Ефектите са елементи от причинно-следствена последователност, състояща се от задачи, действия, резултати, цели на операцията и крайното състояние.“²⁶ Ефектът е физическото или поведенческо състояние на система, в резултат от действие, набор от действия или друга причина. Той е резултатът, изходът, следствието.²⁷

В зависимост от ефекта върху функционирането на обекта тактическите действия биват поразяващи и градивни. Първите водят до прекратяване или затрудняване функционирането на обекта на въздействие, а вторите – до възстановяване или подобряване функционирането му. От тази гледна точка се вижда, че ефектът от действията по осигуряването се постига при градивни тактически действия, в резултат от тях се повишават способностите на формированията.

След направения обзор на развитието на термина „осигуряване“ и вложения в него смисъл може да се обобщи, че осигуряването на войските и силите е възприето като съвкупност или система от дейности, комплекс от мероприятия или бойна функция от бойните операционни системи. На по-високо ниво то се възприема като част от физическия компонент на военната мощ.

Първоначално резултатът от осъществяване на дейностите е създаване на условия за успешно изпълнение на задачите от военните формирования в рамките на участието им в различните видове операции. В актуалните регламентиращи документи дейностите в рамките на функцията „осигуряване“ са променени, а нейната цел е насочена към съхраняване на потенциала на силите.

Аргументи за промяната не са представени, няма и критерии, по които една бойна функция, функционална област или вид бойна дейност попадат в категорията „осигуряване“. Анализът на ефектите от всички изброени от тях до момента показва, че те са резултат от градивни тактически действия, което не може да се каже за дейностите и мероприятията, изграждащи поддръжката.

2. Поддръжка

2.1. Възникване и развитие на поддръжката

2.1.1. Възникване на поддръжката

Първото използване на термина „поддръжка“ в контекста на актуалното му възприемане е в цитирания в предходната глава проект на „Боеен устав – механизирани (танков) батальон“ във връзка с използването на подразделенията за бойна поддръжка и осигуряване. В него като функция на минохвъргачната батарея и противотанковия взвод на батальона се въвежда и „огневата поддръжка“.

До този момент поддръжката се свързва именно със задачите на конкретни формирования – „поддържащи сили и средства – подразделения (части, кораби), съединения, назначени от старшият началник – командир за изпълнение на бойни задачи в интерес на тези подразделения (части, съединения, обединения) на Сухопътните войски (ВМС), които решават основните задачи в боя (операцията)“. Очевидно като критерии са използвани взаимоотношенията, регламентирани от старшият командир при организацията на изпълнението на задачите на операцията, тъй като „за разлика от придадените сили и средства поддържащите сили и средства остават в подчинение на преките си началници“²⁸. В този случай поддръжката не се разглежда като функция – бойна или съвместна.

В „Боеен устав на Сухопътните войски“²⁹ се уточнява, че батальонът или ротата се поддържа в боя от артилерийски дивизион или батарея. Отново е валидно правилото, че поддържащите остават в подчинение на старшият командир (началник). В случай че са „придадени“, те са подчинени на командира на батальона, но на практика същността на техните действия не се променя, те изпълняват сходни задачи. Разликата не е във функциите им, а в организацията на използването им. Командирите едновременно могат да бъдат поддържани и да действат като поддържащи. И тук изясняването на съдържанието на термина започва със семантиката на думата.

В „Български тълковен речник“ смисълът на „поддържам“ е „оказвам някому подкрепа“. От своя страна подкрепата се разглежда като морална или материална³⁰, съдействие³¹. Това е едната гледна точка, приемана донякъде и в настоящите условия – „... в случай, че военно формирование трябва да подпомогне, защити или допълни друго формирование, като изпълни задачи в негов интерес“.³²

Донякъде, защото споменаването в този контекст е сравнително ограничено. Освен като задачи, изпълнявани от формирования със специфични способности в актуалните публикации, в същността на поддръжката се влага и друг смисъл, който ще бъде обект на отделен анализ. Посоченият цитат показва, че няма промяна в схващанията от тридесетте години на двадесети век, когато войските са разделяни на такива „чията главна задача е да влязат в допир с противника, да превземат и овладеят изгодни точки или да ги отбраняват“ (т. е. изпълняват основните задачи) и „войски, чията главна задача е да подкрепят първите в техните действия“³³ (т. е. изпълняват на бойни задачи в техен интерес). Справка с речника на термините и дефинициите, използвани в НАТО³⁴, показва аналогично възприемане на същността на термините, съдържащи в себе си „поддръжка“.

В едно от тях като support/поддръжка е определено действието на дадена сила или част от нея, която подпомага, защитава, попълва или поддържа всяка друга сила. Осигуряван командир (supported commander) е този, приемащ въоръжени сили или друга подкрепа от един или повече подкрепящи командири (supporting commander), който пък предоставя на осигурявания командир въоръжени сили или друга поддръжка....

Интересното в това определение е, че двата аспекта на един и същи процес са обозначени с еднакви термини на английски (supporting – supported, разликата е в глаголните времена) и с различни на български език: осигуряван – подкрепящ.

2.1.2. Развитие на поддръжката

Налагането на това понятие започва с Доктрината на Сухопътните войски от 2001 г. Първоначално в доктрината „поддръжката“ е определена като „бойна“. Целта на тази дейност е подпомагане, защита, осигуряване или допълване на бойната мощ на поддържаното формирование по време на операциите. Състои се от огнева поддръжка и оперативно подпомагане³⁵.

Когато едно формирование е назначено да поддържа друго без да е прикрепено към него или пък да е под негово командване, формата на поддръжката е „придаване“. „Преподчиняване“ е вариант на поддръжката, при който относително временна организационна структура има пълни права над поставено в нея формирование.

Действията на формирование, подпомагащо, предпазващо, допълващо или осигуряващо с материални средства друго са „поддръжане“, а *непосредствената поддръжка* се осъществява при поискване. *Усилване за обща поддръжка* се осигурява като цяло за изпълнение на конкретна задача. *Общата поддръжка* не е в интерес на конкретно формирование, а на поддържаните войски и сили въобще.

Независимо от вида на поддръжката във всички цитирани примери става дума за организационни взаимоотношения при съвместно изпълнение на задачите в операцията. Това обстоятелство рязко се променя с въвеждането на публикациите от 2011 г. и по-специално – с Доктрината на въоръжените сили на Република България.³⁶ В нея се поддръжката е насочена към операциите, за разлика от осигуряването, което е „на войските и силите“: „Поддръжката и осигуряването се разделят на поддръжка на операциите и осигуряване на войските и силите“.

Доколкото операцията е действие или поредица от координирани действия, може да се приеме, че поддръжката е насочена към действието, за разлика от осигуряването, насочено към конкретни обекти (войски, сили). Според определението в доктрината поддръжката на операциите е „комплекс от действия, целящи добиване на достоверна информация за противостоящите сили, снижаване на тяхната боеспособност и защита на собствените войски“. То не се променя и в изданието от 2017 г.

Това определение представя ново виждане за поддръжката – изпълняване на специфични дейности, мероприятия, процедури, чието осъществяване не е задължително обвързано с конкретни родове и специални войски. Основната част от тях, разбира се, се осъществява от специално подготвени и екипирани формирования, снабдени с необходимото въоръжение и техника. Като критерий обаче не са избрани взаимоотношенията. Те могат да бъдат и придадени, но същността на тяхната дейност е насочена към едно – да създадат условия или да подкрепят действията на тези, които осигуряват или към които са придадени.

Елементите на поддръжката според изданието на доктрината от 2017 г. са разузнаване, информационно осигуряване и разузнавателна поддръжка, военно контраразузнаване, огнева поддръжка, противовъздушна и противоракетна отбрана, защита на войските и силите, специфични отбрани и защиты на ВМС, електронна война, военноинженерно осигуряване, комуникационно-информационна поддръжка на системата за командване и управление, ядрена, химическа и биологическа защита, маскировка, противодействие на импровизирани взривни устройства, неутрализиране на невзривени бойни припаси, сигурност на информацията и киберотбрана и военнопотребителска поддръжка.

В предходния вариант от 2011 г. военноеографското, метеорологичното и хидрографското, военното контраразузнаване и военнопотребителското осигуряване са част от видовете осигурявания. Какво налага промяната в класификацията и прехвърлянето им в раздел „поддръжка“? Този въпрос не засяга само промените в периода 2011 – 2017 г. Защо дейности, чието същност и краен резултат не се променят са обединени в друга функционална група? Озадачаващ е и фактът, че няколко от елементите на „поддръжката“ съдържат думата „осигуряване“ в наименованията си, а именно – военноинженерното и информационното осигуряване. Отново се налага анализ на целите и ефектите при осъществяването на изброените видове поддръжка, за да се установи има ли промяна в тяхната същност. Като критерий може да се използва целевата устойчивост на военните системи – дали дейностите повишават устойчивостта на собствената военна система или понижават тази на противодействащата. Ефектите от разузнаването, защитата на силите, маскировката и, до голяма степен – инженерното осигуряване се постигат с градивни действия и повишават устойчивостта на собствената военна система.

Увеличаването на реките въздействия по противостоящата система води до унищожаване или елиминирание на нейните ресурси, което снижава целевата ѝ мощност. Именно чрез деструктивни действия за подавяне, неутрализиране и унищожаване или намаляване на ефективността на противостоящите сили постигат целите си огневата поддръжка, съвместната огнева поддръжка, противовъздушната и противоракетна отбрана или противодействието на импровизирани взривни устройства.

Оказва се, че в една група се поставят дейности, които са коренно различни от гледна точка на ефекта от тях и на влиянието им върху военните системи. Стремешът към преодоляване нормативния дефицит в Българската армия е съпроводен с редица несъответствия, които трябва да бъдат отстранени. Успехът на

съюзните и коалиционните операции зависи пряко от оперативната съвместимост, условие за която е доктриналната съвместимост. Единното възприемане на използваните в публикациите понятия и изясняване на връзките между тях са една от възможностите за преодоляване на това предизвикателство.

ЛИТЕРАТУРА

1. *Наставление за служба на щабовете*. София: Генерален щаб на Българската армия, 2002.
2. *Национална отбранителна стратегия*. София, 2016.
3. Давутоглу А. *Стратегическа дълбочина*. София: Изток – Запад, 2015. ISBN: 978-619-152-674-1.
4. Резниченко, В. Г., Воробьев, И. Н., Мирошченко, Н. Ф., Надиров, Ю. С., Сидоренко, А. А. *Тактика*. София: Военно издателство, 1988.
5. *Устав на полската служба*. София: печатница „Военен журнал“, 1912.
6. *Устав за обучение и действие на българската пехота*. София: печатница „Военен журнал“, 1917.
7. *Английски правилник за бойната служба – Том II, операции – общи положения*. София: Военна библиотека, 1939.
8. Станчев, С.; Николов, Р. *История на сухопътните войски на България, том II*. София: Фондация Българско военно историческо наследство, 2017. ISBN 978-954-92859-3-2.
9. *Устав за щабната служба – Част I, Пехотен полк*. София: Печатница при Генералния щаб, 1947.
10. *Наставление за полевата служба на щабовете в Българската народна армия*. София: Държавно военно издателство, 1952.
11. *Наставление за полевата служба на щабовете*. София: Държавно военно издателство, 1965.
12. *Боев устав на военноморския флот на НРБ, кораб – бригада – дивизия*. София: Държавно военно издателство, 1967.
13. *Боев устав на Сухопътните войски, Част I – дивизия, бригада, полк; Част II – батальон, рота; Част III – взвод, отделение, танк*. София: Военно издателство, 1984.
14. *Боев устав – механизирани (танков) батальон*, проект, №967/94.
15. *Боев устав на механизирани (танков) батальон*. София: Министерство на отбраната, 1996.
16. *Боев устав на механизирани (танкова) бригада*. София: Министерство на отбраната, 1996.
17. *Доктрина за логистиката на Българската армия 4.0, Генерален щаб на Българската армия*. София: Военно издателство ЕООД, 2001.
18. *Доктрина за съвместните операции 3.0, Генерален щаб на Българската армия*. София: Военно издателство ЕООД, 2001.
19. *Доктрина на Сухопътните войски, Генерален щаб на Българската армия, Главен щаб на Сухопътните войски*. София: Военно издателство ЕООД, 2001.
20. *Доктрина Военновъздушните сили, Генерален щаб на Българската армия, Главен щаб на Военновъздушните сили*. София: Военно издателство ЕООД, 2001.
21. *Доктрина Военноморските сили, Генерален щаб на Българската армия, Главен щаб на Военноморските сили*. София: Военно издателство ЕООД, 2001.
22. *Доктрина на въоръжените сили на Република България, ноември 2011 г.*
23. *Доктрина за провеждане на операции, издание (А), ноември 2018 г.*
24. *Доктрина за сухопътните операции*. Н. П. – 3.2. (А), 2020 г., С
25. *Доктрина за планиране на операцията, Национална публикация на въоръжените сили на република България НП – 05*. София: Министерство на отбраната, 2013.
26. *Доктрина за планиране на операцията, Национална публикация на въоръжените сили на република България НП – 05 (А)*. София: Министерство на отбраната, 2018.
27. *Joint Publication 3-0 – Joint Operations*, 2017.
28. *Военный энциклопедический словарь*. Москва: Военное издателство, 1984, стр. 156.
29. *Боев устав на Сухопътните войски, Част II – батальон, рота*. София: Военно изда-телство, 1984.
30. *Български тъловен речник*. София: Наука и изкуство, 1976.
31. *Български тъловен речник*. София: Наука и изкуство, 2003.
32. *Доктрина за провеждане на операции, Национална публикация на въоръжените си-ли на република България НП – 3 (А)*. София: Министерство на отбраната, 2018.
33. *Английски правилник за бойната служба. Том II, Операции – общи положения*. София: Военна библиотека.
34. *AAP – 06. Речник на термините и дефинициите, използвани в НАТО (на английски и български език)*. Публикация на офиса на НАТО по стандартизация (NSO), 2021.
35. *Доктрина на Сухопътните войски, Генерален щаб на Българската армия, Главен щаб на Сухопътните войски*. София: Военно издателство ЕООД, 2001.
36. *Национална публикация на въоръжените сили на Република България НП – 04. Доктрина на въоръжените сили на Република България*. София: Министерство на отбраната, 2011.

REFERENCES

1. *Nastavlenie za sluzhba na shtabovete*. Sofia: Generalen shtab na Balgarskata armia, 2002.
2. *Natsionalna otbranitelna strategia*. Sofia, 2016.
3. Davutoglu A. *Strategicheska dalbochina*. Sofia: Iztok – Zapad, 2015. ISBN: 978-619-152-674-1.

4. Reznichenko, V. G., Vorobyov, I. N., Miroshchenko, N. F., Nadirov, Yu. S., Sidorenko, A. A. *Taktika*. Sofia: Voenno izdatelstvo, 1988.
5. *Ustav na polskata sluzhba*. Sofia: pechatnitsa „Voenen zhurnal“, 1912.
6. *Ustav za obuchenie i deystvie na balgarskata pehota*. Sofia: pechatnitsa „Voenen zhurnal“, 1917.
7. *Angliyski pravilnik za boynata sluzhba – Tom II, operatsii – obshti polozhenia*. Sofia: Voenna biblioteka, 1939.
8. Stanchev, S., Nikolov, R. *Istoria na suhopatnite voyski na Bulgaria, tom II*. Sofia: Fondatsia Balgarsko voenno istoricheskoto nasledstvo, 2017. ISBN 978-954-92859-3-2.
9. *Ustav za shtabnata sluzhba – Chast I, Pehoten polk*. Sofia: Pechatnitsa pri Generalnia shtab, 1947.
10. *Nastavlenie za polevata sluzhba na shtabovete v Balgarskata narodna armia*. Sofia: Darzhavno voenno izdatelstvo, 1952.
11. *Nastavlenie za polevata sluzhba na shtabovete*. Sofia: Darzhavno voenno izdatelstvo, 1965.
12. *Boen ustav na voennomorskia flot na NRB, korab – brigada – divizia*. Sofia: Darzhavno voenno izdatelstvo, 1967.
13. *Boen ustav na Suhopatnite voyski, Chast I – divizia, brigada, polk; Chast II – batalyon, rota; Chast III – vzvod, otdelenie, tank*. Sofia: Voenno izdatelstvo, 1984.
14. *Boen ustav – mehaniziran (tankov) batalyon, projekt, №967/94*.
15. *Boen ustav na mehaniziran (tankov) batalyon*. Sofia: Ministerstvo na otbranata, 1996.
16. *Boen ustav na mehanizirana (tankova) brigada*. Sofia: Ministerstvo na otbranata, 1996.
17. *Doktrina za logistikata na Balgarskata armia 4.0, Generalen shtab na Balgarskata armia*. Sofia: Voenno izdatelstvo EOOD, 2001.
18. *Doktrina za savmestnite operatsii 3.0, Generalen shtab na Balgarskata armia*. Sofia: Voenno izdatelstvo EOOD, 2001.
19. *Doktrina na Suhopatnite voyski, Generalen shtab na Balgarskata armia, Glaven shtab na Suhopatnite voyski*. Sofia: Voenno izdatelstvo EOOD, 2001.
20. *Doktrina Voennovazdushnite sili, Generalen shtab na Balgarskata armia, Glaven shtab na Voennovazdushnite sili*. Sofia: Voenno izdatelstvo EOOD, 2001.
21. *Doktrina Voennomorskite sili, Generalen shtab na Balgarskata armia, Glaven shtab na Voennomorskite sili*. Sofia: Voenno izdatelstvo EOOD, 2001.
22. *Doktrina na vaorazhenite sili na Republika Bulgaria, noemvri 2011 g.*
23. *Doktrina za provezhdane na operatsii, izdanie (A), noemvri 2018 g.*
24. *Doktrina za suhopatnite operatsii. N. P. – 3.2. (A), 2020 g., S*
25. *Doktrina za planirane na operatsiite, Natsionalna publikatsia na vaorazhenite sili na republika Bulgaria NP – 05*. Sofia: Ministerstvo na otbranata, 2013.
26. *Doktrina za planirane na operatsiite, Natsionalna publikatsia na vaorazhenite sili na republika Bulgaria NP – 05 (A)*. Sofia: Ministerstvo na otbranata, 2018.
27. *Joint Publication 3-0 – Joint Operations*, 2017.
28. *Voenniy entsiklopedicheskiy slovar*. Moskva: Voennoe izdatelstvo, 1984, str. 156.
29. *Boen ustav na Suhopatnite voyski, Chast II – batalyon, rota*. Sofia: Voenno izdatelstvo, 1984.
30. *Bulgarski talkoven rechnik*. Sofia: Nauka i izkustvo, 1976.
31. *Bulgarski talkoven rechnik*. Sofia: Nauka i izkustvo, 2003.
32. *Doktrina za provezhdane na operatsii, Natsionalna publikatsia na vaorazhenite si-li na republika Bulgaria NP – 3 (A)*. Sofia: Ministerstvo na otbranata, 2018.
33. *Angliyski pravilnik za boynata sluzhba. Tom II, Operatsii – obshti polozhenia*. Sofia: Voenna biblioteka.
34. *AAP – 06. Rechnik na terminite i definitsiite, izpolzvani v NATO (na angliyski i balgarski ezik)*. Publikatsia na ofisa na NATO po standartizatsia (NSO), 2021.
35. *Doktrina na Suhopatnite voyski, Generalen shtab na Balgarskata armia, Glaven shtab na Suhopatnite voyski*. Sofia: Voenno izdatelstvo EOOD, 2001.
36. *Natsionalna publikatsia na vaorazhenite sili na Republika Bulgaria NP – 04. Doktrina na vaorazhenite sili na Republika Bulgaria*. Sofia: Ministerstvo na otbranata, 2011.

РАЗУЗНАВАТЕЛЕН АНАЛИЗ НА ТРАНСФОРМАЦИЯТА НА СТРУКТУРАТА И ФУНКЦИИТЕ НА ПОСТМОДЕРНИТЕ ТЕРОРИСТИЧНИ ОРГАНИЗАЦИИ

доц. д-р инж. Добрин Анастасов

Военна академия „Г. С. Раковски“, *andreife17@hotmail.com*

Резюме: Разгледани са основните характеристики на транснационалните терористични организации и са посочени подходите за използване на инструментариума на разузнавателния анализ за оценка на техния кадрови, идеен и организационен потенциал. Формулирани са възможностите за използване на класифицирана и от открити източници разузнавателна информация.

Ключови думи: *разузнавателен анализ; транснационални терористични организации; бойни и логистични терористични клетки*

INTELLIGENCE ANALYSIS OF THE TRANSFORMATION IN THE STRUCTURE AND FUNCTIONS OF POSTMODERN TERRORIST ORGANIZATIONS

Assoc. Prof. Eng. Dobrin Anastasov, PhD

Rakovski National Defence College

Sofia, Bulgaria

E-mail: *andreife17@hotmail.com*

Abstract: Analyzed are the main characteristics of the transnational terrorist organizations and are formulated the means of using the craft of the intelligence analysis in estimating their member, ideological and organizational potential. Formulated are the possibilities to make the best use of classified and open-source intelligence information.

Keywords: *intelligence analysis; transnational terrorist organizations; militant and logistic terrorist cells*

Активните действия на разузнавателните и силовите структури в борбата с различните ислямистки, националистически и религиозни организации породиха определени промени в техните цели и „модус операнди“ и наложиха трансформация на структурите им. В това отношение основно влияние оказват бързите промени във военнополитическата, военната, икономическата и политическата обстановка в регионите с най-характерно проявление на тези организации.

Характерните за периода на „разцвет“ на „Ислямска държава“, „Ал Кайда“ и останалите по-малки терористични организации силови действия, активна пропаганда, глобални призови за „джихад“ бяха постепенно, а в определени случаи и много бързо, заменени с подходи и действия, които дават представа за темпото им на адаптация към новите условия. Основното внимание беше насочено към укрепване на главните структури на организациите и осигуряване на тяхната функционалност и автономност, независимо от това дали са йерархични или мрежови. Това се изрази в редица промени на характеристиките на бойните, логистичните и „спящите“ клетки на терористичните организации:

- активно използване на форми и методи за скриване на личностните си данни и особености и прилагане на различни подходи за приспособяване към окръжаващата действителност, даващо възможност за активни действия и определяне на целите за атака;

- ускорена адаптация и трансформация към промените в обстановката, регионална и около и в обектите за атака;

- използване в различна степен на преимуществата и преодоляване на недостатъците на съществуващите йерархични и мрежови структури на организациите и гъвкаво прилагане на хибридни форми на организация в съответствие с конкретните цели;

- промяна в използването на човешкия потенциал – подбират се лица от различни националности, възраст, пол, религия, като се прилагат критерии, пряко оценяващи тяхната пригодност за определена

позиция в организацията, различните клетки или в интерес на един или друг аспект на планираните бойни и информационни действия, необходимост и времетраене на обучението и проверката в симулирани бойни условия;

- широко и активно използване на интернет и социалните мрежи за насочване, изучаване и вербовка на нови членове на клетките, разработване и прилагане на адаптирани към различните по произход и местоживееене лица схеми на установяване и закрепване на контактите;

- провеждане на целенасочени дейности по създаване в необходимата степен на прикрития за членовете на организацията и нейните структури, без оглед на териториална, идейна, материална или расова принадлежност;

- активно разграничаване на вида, качеството и времевите характеристики на прикритията в зависимост от конкретните изпълнители, използваните бойни и разузнавателни средства и условията за укриването им след изпълнение на задачата;

- осигуряване на хомогенност и управляемост на различните структури при подготовката на терористичната атака с готовност за непрекъснато следене и реагиране на промените в оперативната среда и нивото на „твърдост“ на планираните за атака основни и спомагателни цели;

- за преодоляване на въздействието на разузнавателните органи и словите структури върху организациите като цяло и отделните техни структури и членове се прилагат форми на целенасочено създаване и поддържано убеждение в членовете на съответните клетки и отделни терористи-смъртници в тяхната принадлежност към мощна и неуязвима организация, която защитава истински и непреходни ценности;

- формиране и поддържане на колективна и индивидуална зависимост между отделните членове на клетката и готовност за взаимопомощ и саможертва, слъпо изпълнение на заповедите на полевия командир чрез внимателно формулиране на вида и характера на вербалната комуникация и активно прилагане на различни форми на психологическа и психическа индоктринираност и дори медикаментозна обработка и закрепване на императиви;

- строго съблюдаване на дисциплината, активно отработване на отделните етапи и отговорности на конкретните групи и изпълнители, строго спазване на характера на прикритията за недопускане предварителното осветяване на целите и задачите на клетката в процеса преди и след провеждане на конкретната терористична операция;

- ограничаване на достъпа на членовете на организацията до лица извън организацията за недопускане на влияние на идеи и разбирания, които противоречат или внасят съмнение, вяра и убежденост в правотата на собствените си действия и отхвърляне или тотално неприемане на други идеи и морални възгледи;

- внедряване в обществени групи и предварително подбрани населени места или градски райони, които да осигуряват свободно и продължително пребиваване на членовете на клетката, особено ако тя е „спяща“, без да са налага да се вземат специални мерки за отклоняване на вниманието на разузнавателните или полицейските органи;

- при подготовката за провеждане на терористична операция върху членовете на клетката се налагат строги мерки за спазване на конспирацията и характера на използваните прикрития за осигуряване на пълно сливане със средата за действие и маскировка на избраните позиции за осъществяване на нападението и отхода от района на базиране и дейност;

- внасят се необходимите корекции и маскировка на дейностите по получаване на финансиране, обучение, легенди (индивидуални и групови), привличане на съмишленици и нови членове, като се полагат усилия за такова позициониране на членовете на терористичната организация, което да не е свързано с прекалена афишираност и в същото време да дава възможност за комуникация и осигуряване на жизнеспособността и функционалността на клетката като цяло;

- поддържане на убежденост в изключителността на отделната клетка и нейните членове, както и определена степен на дистанцираност както вътре между отделните индивиди, така и спрямо реалната обстановка;

- поддържане на комуникации по вертикала, а при определени условия и съгласуваност с други клетки, групи на организираната престъпност, мафиотски структури;

- търсене и използване на форми за финансиране, които да се различават от традиционните и станалите известни на разузнавателните органи схеми и начини на укриване и трансфериране на средствата;

- засилване на вниманието и разнообразяване на подходите за вербовка на лица, чрез които организацията си набавя оръжия и боеприпаси, транспортни средства, легализационни документи, осигурява конспиративни квартири и условия за тренировка и обучение на бойните клетки;

- сериозна промяна се осъществява в медийното покритие на дейността на транснационалните терористични организации, като се формулират и прилагат подходи за пропагандиране на „общочовешки ценности“, „грижи за братята, потискани и онеправдани от режимите в страните, в които живеят“ и т.н.;

- активно техническо превъоръжаване и използване в пълна степен на възможностите на модерните технологии в сферата на комуникациите, въоръжението и разузнаването за осигуряване на непрекъснато ръководство на структурите, вкл. и от различни териториални дестинации;

- активизиране на изучаване на формите и методите на работа на разузнавателните и антитерористичните организации, целенасочено обучение на членовете на клетките в различни тактики и похвати за противодействие и поведение при арест и разпити, както и информиране на съмишленици и симпатизанти за прилагането им;

- активно се контролират стремежите и необходимостта на отделните членове на организацията от връзки с роднини и познати, както и вътре в организацията и отделните клетки в рамките на целия жизнен цикъл на организацията и членовете ѝ;

- рязкото увеличаване на обема и обхвата на използване на средствата и похватите на информационната война за постигане на дългосрочни политически, икономически и военни цели и противодействие на мероприятията и дейностите на международните и националните силови структури.

Обща характеристика на така формулираните особености на проявление и дейност на транснационалните терористични организации е рязкото увеличаване на темпото на промяна и приспособяване на структурата и кадровия им потенциал към координираните и с широк национален и международен обхват действия на разузнавателните и антитерористичните организации. Анализирането на така формулираните характеристики и дейност на транснационалните терористични организации и дисперсните форми на изграждането и функционирането им дава основание да се оцени наличието на активен процес на изграждането на адекватна на съвременната среда за действие терористична структура, която можем да определим като постмодерна. Тази структура се формира на базата на утвърдени подходи за организационно и кадрово изграждане, но целенасочено привлича и използва форми и методи, заимствани от противостоящите национални и международни организации и интерпретирани съобразно своите конкретни идейни, идеологически, религиозни и политически постановки.

Допълнителен характерен елемент на постмодерните терористични организации е дуализмът в тяхното проявление. Като използват дисперсния си структурен характер, те създават явни структури, стремящи се да развият дейност, която в максимална степен да отклонява вниманието на разузнавателните и силовите органи от вътрешната, законспирирана структура на организацията. Тази структура се формира от ограничени по състав отделни многофункционални звена-клетки, които могат да бъдат използвани и ръководени както йерархично, така и мрежово, като техните членове са подготвени и снабдени с документи и легенди, позволяващи придвижване и проникване в различни страни и региони и действия при различни оперативни условия.

На практика обаче това означава определено разконспириране на членовете, структурите, командните и управленските форми и вериги, наличието на сътрудничество с местни структури за снабдяване с оръжие и боеприпаси, както и използване на местен транспорт, комуникационни и информационни системи. Следва да се има предвид и участието на членове и/или групи от терористичната организация в процеса на насочване, изучаване, привличане или вербуване на местни лица от различни социални и професионални групи. В провеждането на тези дейности могат и се проявяват индивидуалните особености на членовете на клетката в едно или друго направление, което в определени случаи нарушава скритостта и намалява ефективността на прилаганите конспиративни форми и методи на работа.

В рамките на тези констатации се оформят и придобиват определеност и използваемост възможностите на разузнавателния анализ на наличната и добиваната класифицирана и от всички явни източници информация за разкриване на законспирираните членове на организацията и ограничаване във въз-

можната степен на ефективността на водената от тях пропагандна и терористична дейност. Ефективното използване на инструментариума на разузнавателния анализ налага формулирането на онези аспекти от работата по добиването на необходимия обем и качество информация, която след обработка в рамките на разузнавателния цикъл да бъде своевременно предоставена на оперативните сили за ограничаване и в пределна степен минимизиране на възможностите на терористичната организация да реализира ефективна операция.

Основното изискване е да се добива информация чрез осъществяване на комплексна разузнавателна дейност в следните направления:

- изваждане на членовете на бойната и логистичните клетки от нелегалните позиции на действие и определяне характера и вида на конспиративната квартира или квартири;
- ефективно контролиране на дейността на разкрити или в процес на установяване членове на „спящи“ клетки, съмишленици и лица от диаспората, оказващи доброволно или принудително съдействие;
- засилване на контрола и охраната на предполагаемите обекти за терористична атака при спазване на необходимата конспирация и легендировка на провежданите в това отношение мероприятия;
- конкретизиране на целите и задачите на всички видове техническо и агентурно разузнаване;
- ускоряване на процесите на добиване на целева информация от явни източници, разкриване и дешифриране на комуникациите в даркнета и използване на хакери за проникване в сайтове и интернет мрежи и клубове, социалните мрежи и отделни компютърни конфигурации, неутрализация на текстови и графични файлове и програми, за които се счита или подозира, че се използват от съответната терористична организация, без да се разкрива характера, извършителя или поръчителя на тази дейност;
- ускоряване на работата по вербовката на оперативно интересни лица от състава на клетката или организацията и завършване на внедряване в клетките на вербовани местни лица или специално подготвени оперативни работници.

Също така следва да се използват активно информационни и психологически операции, дезинформационни операции, потенциалът на съответните контрразузнавателни и антитерористични сили, информатори и сътрудници на местните сили за сигурност. Значителна роля в постигането на успех в добиването на разузнавателна информация следва да играе активното сътрудничество между разузнавателните и правоохранителните органи на всички заинтересовани страни.

Събраната по този начин информация ще бъде подложена на активна аналитична дейност за извличане на онези елементи, които позволяват да се формулират отделните аспекти, характеризиращи плановете и конкретната подготовка за провеждане на терористична операция. По същество това ще обхваща:

- определянето на точното местоположение на конспиративната квартира и броя на укриващите се там членове на клетката;
- вид и характер на готвената терористична операция, евентуално време за подготовка и приблизителното време за началото ѝ, наличието на основен и допълнителен вариант, въоръжение и средства за въздействие върху охраната и защитата на обекта за атака;
- оценка на личностните и бойните качества на членовете на клетката и полевия командир, национална принадлежност, участие в други операции или в поддържане на връзки с други организации, разкриване на слабост в мотивацията на отделни членове на клетката – изготвяне на профили и очаквани реакции на промени в хода на операцията или при загуба на определен брой терористи;
- определяне на степента на надеждност на комуникацията между всички участници в терористичната операция, използваните комуникационни средства, наличие на криптирана връзка с друга клетка или по вертикала, възможности за легендирано смущаване или тотално заглушаване на индивидуалните и колективни средства за връзка на терористичната клетка;
- осигуряване на възможности за защита и мотивирано извеждане на наша агентура и сътрудници от състава на клетката в периода на непосредствената подготовка и провеждане на терористичната операция, като в този процес следва да се създават предпоставки за по-нататъшното ѝ използване в състава на друга клетка или структура на организацията;
- разкриване наличието на допълнителни източници на оръжие и боеприпаси, транспортни и резервни комуникационни средства, достъп до допълнително материално, финансово и легализационно осигуряване, резервни маршрути за напускане на региона и страната;

– наличие на потенциална опасност от използване на оръжие за масово поразяване, ракетно въоръжение, летателна техника, дроне;

– очаквани варианти на маскировка на членовете на клетката при подхода към обекта и изчакване началото на атаката, сигнали и координация на действията на допълнителните сили и средства.

Реализирането на тези задачи изисква привличането на голям кадрови потенциал в рамките на разузнавателната организация и ангажирането на значителен финансов, материален и енергиен ресурс. Определено може да се оцени, че това ще изисква голям обем работно и машинно време, своевременно докладване на междинни оценъчни документи, поставяне на нови и продължаващи задачи на добиващите органи, целево разпределение на исканията за допълнителна информация от партньорски и съюзнически разузнавателни органи при защита на собствената информация и закриване на източниците ни. Наред с това ще възникват и трудности от различен и неочакван характер, както и административни ограничения, които допълнително ще усложняват и забавят темпото на разузнавателния анализ, изготвянето на крайния разузнавателен продукт, неговото разпространение и оценка и поставянето на искания за допълнителен анализ и добиване в тази връзка за информация.

Борбата с терористичната заплаха и неутрализирането на постмодерните терористични организации изисква непрекъснатост и създаване и съхраняване на голяма база данни, който да бъде оперативно достъпен и постоянно и целенасочено обогатяван и прецизиран.

За ефективното използване на добиваната агентурна и закрита информация е необходимо да се поддържат и усъвършенстват протоколи за защита от преднамерено или неволно изтичане на информация или проникване в източниците и тяхното осветяване. Следва да се подчертае, че терористичните организации и особено самостоятелно действащите клетки и терористи-камикадзе имат предимството на изненадата, когато успеят да запазят анонимността си до и след провеждането на терористичната операция или акт и принудят разузнавателните и силовите структури да действат прибързано и с намалена ефективност.

Силата на разузнавателния анализ ще може да бъде използвана в пълна степен тогава, когато дейността по добиване на релевантна информация от всички източници се води координирано, по определени и съгласувани на базата на анализа критерии и при пълното спазване на конспирация и бдителност. В това отношение мерките трябва да бъдат безкомпромисни и да не допускат разкриване на характера и обхвата на провежданата добиваща дейност. Необходимо е да се търси и добива такава информация, с чиято помощ да се създават информационни масиви от конкретни данни, които да бъдат използвани за разширяване достъпа до основните клетъчни ядра на съответната организация, формиране на оценки за кадровия потенциал, системата за набиране на членове, форми на проверки и обвързване на отделните членове, психологически профили на основните лица в йерархията на организацията и създаване на предпоставки за вербовката на „най-уязвимия член“ и провеждане на мероприятия и дейности по разлагане и подкопаване на мотивацията на членовете на клетките.

Тази дейност от страна на отделните структури в системата за защита на националната сигурност ще осигури нарастващата ситуационна и операционална информираност за дейността на терористичните организации и ускоряване на реакцията и своевременно разкриването на планираните или провежданите от тях мероприятия на територията на нашата страна. Наред с това ще може да бъде осигурена и необходимата информация за евентуални съвместни действия с други терористични организации и такива на международната организирана престъпност, която своевременно да бъде предадена на заинтересованите съюзнически и партньорски организации.

Необходимо е да се подчертае, че допълнителни условия за трансформиране на транснационалните терористични организации в постмодерни терористични организации възникнаха в резултат на оформящото се възраждане на ислямизма след поражението на водещите ислямистки организации и наличието на нови политически, икономически и военни реалности в Близкия изток. Освен в този регион, терористичните организации в азиатски и африкански страни действат активно за трансформация на структурите си и формиране на дуалистични организационни формации. Оценката, че ислямизмът и екстремизмът са получили тежък удар и не са в състояние да формират структури, които сериозно да застрашат съответните режими, все по-определено се разминава с реалностите в анализирания регион. Процесите на консолидация и преструктуриране вече имат своите проявления и то под формата на

постмодерни терористични организации, разчитащи и получаващи материална, финансова помощ и в определена степен – политическа закрила, конкретно в Магреба, Ирак, Сирия и Афганистан. По същество това изисква значително по-целенасочено и обемно добиване на разузнавателна информация от всички източници, следене на откритите проявления на ръководствата на тези терористични организации и комплексен разузнавателен анализ на целия спектър от данни, свързани с дисперсното изграждане на организациите и конвергенцията им с различни по политическа, социална, икономическа и религиозна характеристика национални или регионално представени организации структури.

НАПРАВЛЕНИЯ ЗА ПОВИШАВАНЕ УСТОЙЧИВОСТТА НА ПЪТНАТА МРЕЖА ВЪВ ВОЕНЕН КОНФЛИКТ

подполковник д-р Данаил Петев

Военна академия „Г. С. Раковски“, d.petev@mdc.bg

Резюме: Докладът отразява моментните условия за организирането и изпълнението на задачите по подготовка на пътна мрежа в хода на придвижване на войските във военен конфликт и осигуряване на оптимално устойчивото им движение. В доклада са разгледани моментните способности, дейността и задачите, изпълнявани от инженерно-пътните формирования от Българската армия, и са предложени направления за повишаване устойчивостта на пътна мрежа във военен конфликт.

Ключови думи: *пътна мрежа; подготовка на пътища; възстановяване на военни пътища; оптимално и устойчиво движение по пътна мрежа; повишаване устойчивостта на пътна мрежа във военен конфликт*

DIRECTIONS FOR INCREASING SUSTAINABILITY OF ROAD NETWORK IN MILITARY CONFLICT

Lieutenant Colonel Danail Petev, PhD

Rakovski National Defence College

Sofia, Bulgaria

E-mail: d.petev@mdc.bg

Abstract: This report presents the conditions for organizing and implementation of the tasks related to the preparation of road network in the course of the movement of troops in military conflict and providing their optimal movement. The report examines the momentary capabilities, activities and tasks performed by combat engineer units of the Bulgarian army and are suggested directions for increasing the sustainability of the road network in military conflict.

Keywords: *road network; road preparation; restoration of military roads; optimal and sustainable movement on the road network; increasing the stability of the road network in military conflict*

В съвременните условия най-характерна и най-сложна задача е подготовката на пътищата в хода на придвижване на войските. Това на първо място се отнася за условията на настъпление и преследване. Често има и случаи, когато пътищата за маршове, за изнасяне към рубежите за развързване, а понякога и част от пътищата в отбранителната полоса, ще трябва да се подготвят в процеса на придвижване на войските.

Условията за организиране и изпълнение на задачите по подготовка на пътищата в хода на придвижване на войските се характеризират със следните особености:

- необходимите темпове на подготовка на пътищата се диктуват от скоростите на придвижване на войските;

- пътищата се подготвят обикновено с използване на съществуващите почвени пътища и само на малки участъци (главно на местата за заобикаляне на разрушените пътни участъци) – по целина. Основните пътни работи в тези условия се съсредоточават на отделни обекти и участъци със сравнително малка дължина. Обектите за работа се появяват с придвижване на войските, а честотата на появяването се определя от скоростта на придвижването и от обема на разрушенията на пътищата;

- времето за изпълнение на работите на отделните обекти се определя от режима на придвижване на войските и от мястото на инженерно-пътното подразделение в бойните редове;

- крайно ограничен е изборът на пътнотроителни материали, поради това използването на табелните и на предварително изготвените пътно-мостови конструкции има решаващо значение за своевременната подготовка на пътищата;

- налага се да се вземат мерки за запазване на потенциалните възможности на инженерно-пътните подразделения за решаване на нови, а понякога – и на внезапно възникващи задачи.

Като се имат предвид големият обем от пътни и мостови работи при строителството на съществуващ път следва, че по-голямо значение имат мероприятията, провеждани от мирно време и застрашаващият период.

За определяне обема на възстановителните работи по пътната мрежа се налага изчисляването на минималната интензивност на движението, която се явява един от военнотехническите параметри. Възстановяването на движението по пътната мрежа е основен фактор за определяне на комплексната устойчивост на обектите. Намирането на начин за изчисляване стойностите на необходимата минимална интензивност спомага за комплексното решаване на задачата – повишаване устойчивостта на пътната мрежа във военен конфликт. От необходимата минимална интензивност на движението се определят видът на възстановителните работи, изборът на вариант за възстановяване, а от там – силите и средствата.

Върху стойностите на минималната интензивност на движението оказват влияние множество параметри, които характеризират подготовката и воденето на военния конфликт:

- видът на бойните действия – отбрана или настъпление;
- мястото на пътя (обекта) в полосата, зоната в която се намира;
- срокът за използване на пътя от войските;
- общото количество на машините в съединенията, частите, подразделенията, които използват пътя;
- количеството на оборудваните в полосата пътища;
- общото съотношение на силите, собствени войски и противник и др.

Всеки един от тези показатели се изменя в определени граници, които зависят най-много от решението на командирите (началниците) за подготовка и водене на бойните действия. Планирането на използването на пътната мрежа се състои в определяне на направленията и границите за движение на войските, подвоза на материалните средства и всички видове евакуация.

Очертанието на мрежата от военни пътища е непостоянно, най-малкото има множество варианти, които са в зависимост от:

- театъра на военните действия (ТВД);
- периода на развързване на Въоръжените сили и зоната, в която се намират войските;
- направлението за съсредоточаване на усилията на противника и др. Различните варианти изискват мероприятията, които се провеждат за изграждане на една устойчива пътна мрежа, да се провеждат на различни места и обекти за всеки конкретен случай, който може да възникне във военния конфликт. Планирането на тези мероприятия значително се усложнява и изисква **нов подход** при подготовката на пътната мрежа за осигуряване воденето на успешни бойни действия.

Основа на новия подход е прогнозирането на въздействието на противника по пътната мрежа в мирно време и особено в застрашаващия период. Освен това се налага проиграване на най-вероятните варианти за определяне количеството и мястото за складиране на материални средства и конструкции, необходими за възстановяване на движението по пътната мрежа след въздействие на противника. Тази задача може да се реши с изграждането на модел на военния конфликт и с помощта на симулации се проиграват основните варианти. След анализ на получените резултати се определят мястото и количеството на силите и средствата, необходими за подготовка и поддържане на пътната мрежа и техническо прикритие на обекти от нея. Прогнозирането на въздействието на противника и планирането на използването на пътната мрежа изискват постоянна информация за състоянието на обектите с отчитане на факторите, влияещи върху устойчивостта им. Такава информация съществува в щабовете на съединенията и частите на въоръжените сили, както и в Министерството на транспорта.

Основно изискване към пътната мрежа е тя да бъде устойчива. Под устойчивост в най-общия смисъл се разбира **способността на дадена система или обект да запази количествените и качествените си характеристики при въздействие на едни или други негативни фактори**. Това изискване придобива особено значение при използване на високоточни оръжия, които притежават голяма далекобойност и висока точност на поразяване и при промишлени аварии и природни бедствия. Това внася твърде важни, качествено нови черти в съдържанието на понятието устойчивост на пътната мрежа.

Отделните компоненти (мероприятия), от които зависи осигуряването на оптимално и устойчиво движение по пътната мрежа във военен конфликт, се групират условно на:

– организационно-планировъчни – за които е характерно изразходването на умствена енергия от командирите, които разработват мероприятията за повишаване устойчивостта на пътната мрежа. Огромна организаторска работа се осъществява по схемата планиране – организация на изпълнението – контрол

и отчетност. Нуждата от материални, трудови, енергийни и финансови ресурси е сравнително малка. Мероприятията, свързани с този компонент обаче, са базови за останалите четири компонента на устойчивостта и за бързото преминаване на пътната мрежа от мирно на военно положение. В тази група спадат: планиране на използването на пътната мрежа; разработване на прогнози, концепции, специални модели; научноизследователска работа в интерес на военновременната устойчивост; планиране, организиране и извършване на контрола и отчетността за всички етапи;

– материално-енергетични – осигуряване на потребните материални средства за създаване и поддържане на цялата дейност при повишаване устойчивостта на пътната мрежа. Изпълнението на мероприятията е свързано с много капиталовложения, разходи на време, материални и трудови ресурси. Към тези мероприятия се отнасят: строителството и реконструкцията на съществуващи пътища; плановете за техническо прикритие; подготовката и поддържането на пътната мрежа; рекогносцировката и други. Както се вижда, материално-енергетичният компонент е с най-голямо значение за повишаване устойчивостта на пътната мрежа;

– инженерно-технически – включват проектирането, изграждането, поддържането и подобряването на имащите военно значение пътни съоръжения и участъци. Към този компонент се отнасят и опитно-конструкторската и инженерно-внедрителската дейност в интерес на устойчивостта на пътната мрежа във военно време;

– специфично отбранителни – имат за цел да се запазят от противника физически уязвимите за пътната мрежа места. Изразява се в охрана и отбрана на важни обекти, мероприятия по маскировката и други.

Високата устойчивост на пътната мрежа във военен конфликт ще се постигне с провеждането на комплекс от мероприятия в три основни направления:

- при предварителната подготовка на ТВД (в мирно време);
- при непосредствената подготовка на ТВД (в застрашаващия период);
- в хода на военния конфликт.

По време на последните две направления се извършва стратегическото развързване на въоръжените сили на Република България. Пътната мрежа в тези периоди трябва да създава благоприятни условия за създаването и бойните действия на отбранителни и контраударни групировки.

За съоръженията от пътната мрежа, като обекти от националното стопанство, се различават няколко основни вида устойчивост:

– физическа устойчивост – способността на инженерно-техническия комплекс (пътно платно и различни видове съоръжения) да издържи на взривове, пожари, наводнения, заразяване и други, като в зависимост от състоянието ѝ тя още е фактическа, критическа и оптимална. Последната в идеалния случай съвпада с фактическата устойчивост, най-често веднага след построяването на пътя и съоръженията. За осигуряването на бойните действия на групировки е необходимо знание за фактическата, а за пътновъзстановителните работи – параметрите на критическата устойчивост;

– устойчивост на производствените връзки – отразяват всички видове дейности изпълнявани по пътната мрежа като едно неразделно цяло за осигуряване на движение с определени характеристики и включват: противниковите въздействия; изпълнение на мероприятия за повишаване на устойчивостта; използването на пътната мрежа от въоръжените сили; материално-техническото и финансовото осигуряване в мирно и военно време и други;

– морално-психическа устойчивост на личния състав при решаването на производствените и други задачи в сложна и тежка обстановка.

Указаните три вида устойчивост се синтезират в общата устойчивост на обекта. Те насочват вниманието към нейното целенасочено и диференцирано изследване и повишаване.

Под устойчивост на пътната мрежа се разбира **способността ѝ да осигурява непрекъснатост на планираното движение в условия на въздействие от противника с всички средства за нападение**. Устойчивостта в голяма степен зависи от подготовката и възможностите на пътностроителните части и подразделения да извършват определен обем от работи под въздействие на противника, с което осигуряват нормалната пропускателна способност на пътната мрежа.

Основни направления, които биха повишили устойчивото движение по пътната мрежа във военен конфликт следва да бъдат:

• Директивност и нормативност. Да се създаде единна, всеобхватна система от нормативни актове – решения на съответните държавни и стопански органи (Министерски съвет, Министерство на отбраната, държавни стандарти, ведомствени нормативи и други), за ръководството, организацията и съдържанието

на мероприятията за повишаване устойчивостта на пътната мрежа. Спазването на принципа предполага да се познават и прилагат от съответните длъжностни лица постановките и изискванията на официалните документи, за да може на практика да се осъществят планираните мероприятия.

- **Отчитане влиянието на противника.** При планирането и осъществяването на мероприятията по устойчивостта на пътната мрежа във военно време трябва да се отчитат пълно реалните и прогнозните възможности на противника да въздейства по съоръженията и участъците от пътната мрежа, както и възможните последици от ударите по тях. Това става от органите на генералния щаб на Българската армия, който под различна форма ги свежда до знанието на съответните административни, стопански и други ръководства в касаещия ги обем.

- **Повсеместност.** Мероприятията по военновременната устойчивост трябва да се провеждат по цялата пътна мрежа, както и във всички отговорни за изпълнението на тази задача звена. Повсеместността се явява и като резултат от пълното, правилното и навременното изпълнение на системата от мероприятията по пътната мрежа.

- **Плановост и своевременност.** Мероприятията по военновременната устойчивост на движението по пътната мрежа намират място в плановите за отбрана на страната, както и в плановите за транспортното развитие на националното стопанство. За тях е необходимо да се мисли отрано и да се работи постоянно, тъй като устойчивостта на пътната мрежа във военно време се изгражда основно в мирновременния период, а се проявява като особено важно качество в хода на военния конфликт.

- **Диференцираност.** Принципът изисква мероприятията да се осъществяват диференцирано по място, време и задачи по обекти и участъци от пътната мрежа. С приоритет трябва да се ползват онези от тях, които имат пряко отношение към осигуряване действията на въоръжените сили. По този начин се дава преднина на дейностите по създаване на предпоставки за успешен ход и завършек на военния конфликт.

- **Компенсирание на загубите.** Мероприятията по военновременната устойчивост на движението по пътната мрежа на територията на страната е необходимо да се планира така, че с излизане от строя на отделен обект или участък от път с оцелелите да се изпълнят планираните транспортни дейности. Това означава незасегнатите пъти направления да са в състояние да поемат част от движението чрез резерв от пропускателна способност или преустройство на организацията на движението.

- **Ефективност на мероприятията.** Това предполага провежданите мероприятия за повишаване устойчивостта на пътната мрежа да спомагат за осигуряване на непрекъснато движение при спазването на определени изисквания във военен конфликт. Мероприятията трябва да осигуряват и ликвидирането на отрицателните последици от природни бедствия и крупни производствени аварии в мирно и военно време. С други думи мероприятията трябва да са в съответствие с интересите на въоръжените сили, трудовите колективи и научно-техническия прогрес. Това налага в значителна степен те да бъдат икономически целесъобразни както за военно време, така и за мирно време. Такива са обходите на населени места с натоварено движение, усъвършенстване на „тесните“ места по пътната мрежа, подземно строителство, въвеждане на авангардни технологии и други.

Съществено важно условие пътната мрежа да е устойчива е правилният подбор на участъците, които влизат в нея. Колкото по-малко са неустойчивите обекти по пътната мрежа, толкова повече сили ще са необходими за извършване на разрушения и заграждения от противника. Пътища с малко неустойчиви обекти се поддържат с по-малко сили и средства.

ЛИТЕРАТУРА

1. Андреева, Г. & Петров, К. *Методика за прогнозиране поразяването на обекти от транспортните комуникации във военен конфликт*. София: Издателство на Министерството на отбраната „Св. Георги Победоносец“, 1998.
2. Бахчеванов, Г. В. и др. *Един метод за определяне устойчивостта на обект от пътната мрежа*. В: *Трудове на академията*, 1996.
3. Колектив. *Контролен пример. Автоматизирани технологии за оценка на обема разрушения на конкретните транспортни обекти по железопътната мрежа, автомобилните, морските и речни пътища на 4-те ТВД*. София, 1995.
4. *Организация на пътното осигуряване на операциите. Част първа и втора*. София: Военно издателство, 1981.
5. *Основи на устойчивостта на народното стопанство за работа във военно време*. София: Военно издателство, 1986.
6. Колектив. *Пояснителна записка. За обема разрушения на конкретните обекти по транспортните комуникации на 4-те ТВД*. София, 1995 г.

REFERENCES

1. Andreeva, G. & Petrov, K. *Metodika za prognozirane porazyavaneto na obekti ot transportnite komunikatsii vav voenen konflikt*. Sofia: Izdatelstvo na Ministerstvoto na otbranata „Sv. Georgi Pobedonosets“, 1998.
2. Bahchevanov, G. V. i dr. *Edin metod za opredelyane ustoychivostta na obekt ot patnata mreza*. In: *Trudove na akademiata*, 1996.
3. Kolektiv. *Kontrolen primer. Avtomatizirani tehnologii za otsenka na obema razrushenia na konkretnite transportni obekti po zhelezopatnata mreza, avtomobilnite, morskite i rechni patishta na 4-te TVD*. Sofia, 1995.
4. *Organizatsia na patnoto osiguruvane na operatsiite. Chast parva i vtora*. Sofia: Voenno izdatelstvo, 1981.
5. *Osnovi na ustoychivostta na narodnoto stopanstvo za rabota vav voenno vreme*. Sofia: Voenno izdatelstvo, 1986.
6. Kolektiv. *Poyasnitelna zapiska. Za obema razrushenia na konkretnite obekti po transportnite komunikatsii na 4-te TVD*. Sofia, 1995 g.

УСТОЙЧИВОСТ И НЕПРЕКЪСВАЕМОСТ НА РАБОТАТА НА ВЕДОМСТВА И ОРГАНИЗАЦИИ ПРИ БЕДСТВИЯ

гл. ас. д-р Даниела Балева

Военна академия „Г. С. Раковски“, d.baleva@rmdc.bg

Резюме: Устойчивостта и непрекъсваемостта на работния процес във ведомствата и организациите, особено на тези, които са пряко свързани със сигурността на обществото, е основна предпоставка за намаляване на жертвите и загубите при възникване на различни по вид и мащаб бедствия. В тази връзка в настоящия доклад са анализирани не само методите, които могат да повишат устойчивостта и непрекъсваемостта на работата при бедствия, но и основните фактори, които влияят върху тях.

Ключови думи: *устойчивост; непрекъсваемост; бедствия*

SUSTAINABILITY AND CONTINUITY OF THE WORK PROCESS OF DEPARTMENTS AND ORGANIZATIONS IN CASE OF DISASTERS

Assist. Prof. Daniela Baleva, PhD

Rakovski National Defence College

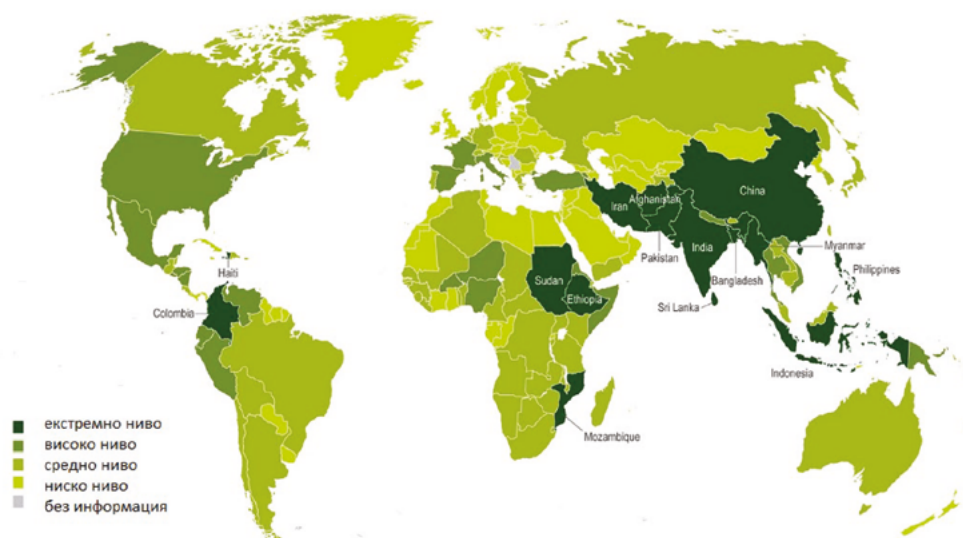
Sofia, Bulgaria

E-mail: d.baleva@rmdc.bg

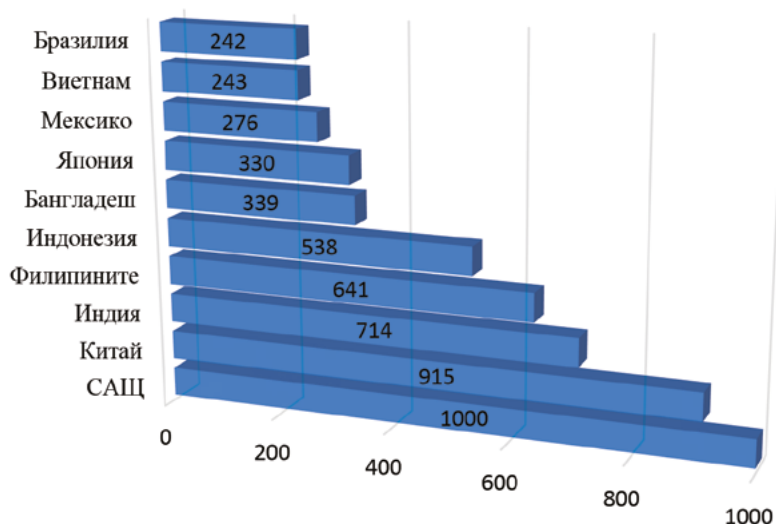
Abstract: Sustainability and continuity of the work process of departments and organizations, especially of those directly related to the safety of the society, is the main prerequisite for decreasing the number of victims and the losses in case of disasters of different nature and scale. In this relation the present report analyses not only the methods for increasing the sustainability and continuity of the work in time of disasters but also the main factors that influence them.

Keywords: *sustainability; continuity; disasters*

Бедствията се характеризират със значително нарушаване на нормалното функциониране на обществото, което надвишава капацитета му да се справи с възникналата ситуация със собствените си ресурси.¹ Този вид събития се съпровождат от жертви, човешко страдание, материални, икономически и екологични загуби.



Фиг. 1. Риск от бедствия



Фиг. 2. Най-често засягани от бедствия държави в глобален мащаб, 1950 – 2020 г.

Бедствията влияят в значителна степен на социалното и икономическото развитие и на Република България. Въпреки че липсва ясна тенденция на нарастване на кризисните събития (включително природни бедствия като пожари, свлачища, земетресения, наводнения, бури и градушки, катастрофи, замърсявания с опасни вещества и епидемии по животните и хората) през периода 2010 – 2020 г., е необходимо да се отчита, че както средната годишна сума на щетите и публичните разходи във връзка с дейностите по защита (над 200 млн. лв), така и екстремните стойности, достигани през годините, са изключително високи (таблица 1).⁵

Таблица 1. Кризисни събития в Република България

	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
брой кризисни събития	4 571	8 268	10 826	2 728	4 356	4 008	3 577	1 594	1 420	1 066	1 220
установени щети, хил. лв.	100 594	487 254	106 160	443 067	190 218	191 820	65 243	148 305	44 694	34 833	174 517
средства за възстановяване	74 047	424 127	36 167	399 240	59 916	23 854	20 709	15 481	227 699	22 123	23 543
разходи за спасителни и неотложни аварийни работи, хил. лв.	7 513	11 726	104 228	21 814	21 632	7 736	23 177	4 812	5 553	5 353	10 855
Общо щети и разходи за СНАВР, хил. лв.	108 107	498 980	210 388	464 881	211 850	199 556	88 420	153 117	50 247	40 186	185 372

Устойчивост на социално-икономическите субекти

С оглед ограничаване на негативните ефекти при възникване на бедствия усилията на обществата се насочват все повече към повишаване на тяхната устойчивост при възникване на бедствия.

Устойчивостта се дефинира най-общо като способността на система или отделен субект, изложени на рискове, да устоят на негативно влияние и да запазят възможността си да функционират, а ако това е невъзможно, да се ограничат времето и ресурсите, необходими за тяхното възстановяване.

От основно значение за повишаване на устойчивостта на социално-икономическите субекти с оглед ограничаване на загубите при възникване на бедствия е определянето на факторите, които ѝ влияят. Като основни такива могат да се посочат:

- устойчивост на физическите обекти, която зависи основно от надеждността на оборудването, сградите и съоръженията;

- качеството на техническото обслужване – стратегия за ремонт и профилактика, структура на ремонтните дейности, качество на диагностиката, снабдяване с резервни части и пр.;

- качество на човешките ресурси. Изразява се в способностите им за прогнозиране на възможни бедствия и ефективността на дейностите по предотвратяване, ограничаване или възстановяване на щетите;

- структура на икономиката. В рамките на този фактор се разглежда по-голямата уязвимост на отделни стопански отрасли, взаимовръзките между тях и отделните икономически субекти;

- система за управление, включително организационна структура, технически възможности за управление, принципи на управление, алгоритми и процедури за управление, система за управление на качеството, интегрирана информационно-управленска система.

Повишаването на устойчивостта на социално-икономическата система при бедствия може да стане чрез повишаване на устойчивостта на отделните ѝ елементи или чрез реализирането на такива мерки, чрез които да се повиши устойчивостта на системата като цяло.

Устойчивостта на отделните елементи на системата се определя от техния вид, съществуващите взаимовръзки между тях и зависимостта им от функционирането на различни обекти от критичната инфраструктура. Повишаването на устойчивостта на всеки отделен елемент води до повишаване на устойчивостта на системата като цяло.

Устойчивостта на цялата социално-икономическа система може да се повиши така, че тя да бъде по-висока от устойчивостта на отделните ѝ елементи. Това може стане като се използват следните подходи:

- диверсификация на икономиката – развиват се различни сектори от икономиката, диверсифицират се пазари, доставчици и пр.;

- усъвършенстване на системата за управление и в частност – системата за управление при бедствия. Това би дало възможност за осъществяване на превантивна дейност, благодарение на което да се ограничат потенциалните загуби при бедствия и се съкрати времето за възстановяване нормалната работа на субектите.

Възможно е и комбинирането на двата подхода (повишаване на устойчивостта на отделните елементи и повишаване устойчивостта на социално-икономическата система като цяло).

Непрекъсваемост на работата на ведомствата и организациите при бедствия

Непрекъснатостта на работния процес във ведомствата и организациите и особено на тези, които са пряко свързани със сигурността на обществото, е основна предпоставка за намаляването на жертвите и загубите при възникването на различни по вид и мащаби бедствия.

Прекъсването на работния процес при възникване на бедствия може да бъде в резултат от различни причини, основните от които са:

- разрушаване на активи, необходими за изпълнение на задачите;

- загуба на ключови служители от различните нива в организациите;

- разрушаване на комуникационните връзки, в резултат на което организациите не могат да бъдат управлявани, т.е. не може да се получава достоверна информация по отношение на необходимите мерки и/или да се свеждат задачите до изпълнителските екипи.

В тази връзка, с оглед осигуряването на непрекъснатост на работния процес във ведомствата и организациите, се налага:

- повишаване на устойчивостта на критичните за организациите активи;

- повишаване на сигурността на личния състав в организацията, особено при възникване на извънредни ситуации;

- осигуряването на постоянен обмен на информация.

Непрекъсваемостта на работата на ведомствата и организациите при бедствия е в пряка връзка с тяхната устойчивост. Както по отношение на социално-икономическата система като цяло, така и по отношение на отделните организации, повишаването на устойчивостта им може да стане, от една страна, чрез повишаване на устойчивостта и качеството на всеки отделен обект и елемент от нея или чрез реализирането на такива мерки, чрез които устойчивостта на системата да стане по-голяма от тази на отделните ѝ елементи.

Повишаване устойчивостта на ведомствата и организациите така, че устойчивостта им да бъде по-висока от тази на отделните им елементи може да стане чрез:

- създаване на относително самостоятелни сегменти в тяхната организационна структура, така че спирането на работата в една част от организацията да не доведе до спирането на работата в други нейни части или негативните ефекти от спирането на работата в един относително самостоятелен сегмент да доведе до ограничени негативни последици за организацията като цяло.

- дублиране на структури. Осъществява се като се добави такава структура, която може да изпълнява същите задачи като основната и се включва в работа на организацията при поразяване на основната. Този подход води до съществено увеличаване на разходите, но значително повишава сигурността на организациите.

С оглед предотвратяване на потенциалните щети, които могат да възникнат поради прекъсване на дейността на ведомствата и организациите в резултат от възникване на бедствия, е целесъобразно въвеждането и използването на стандарти, улесняващи управлението на риска и на организациите като цяло при възникване на извънредни ситуации.

Такъв е например стандартът „Сигурност и устойчивост. Системи за управление на непрекъснатостта на дейността. Изисквания“ (ISO 22301: 2019). Посредством този стандарт се определят изискванията към планирането, установяването, въвеждането и мониторинга, поддръжката и непрекъснатото подобряване на система за управление, която да предпазва от или да намалява вероятността от прекъсване на работния процес във ведомствата и организациите, да ги подготви за работа в неблагоприятни условия, а така също и за своевременното възстановяване на дейността в случай, че прекъсването ѝ не е могло да бъде предотвратено. Изпълнението на мерките в този стандарт е насочено към това да позволи на организацията да продължи да извършва критично важните си дейности, дори и при възникването на различни извънредни ситуации, които затрудняват нормалното ѝ функциониране.

Въпреки факта, че стандартът представя подход за планиране и реализиране на мерки за намаляване на риска от прекъсване на дейността в организациите, той не дава единен универсален вариант на решение на проблемите, свързани с осигуряването на непрекъснатост на процесите. В основата на представения подход стои идеята за необходимост от оценка на всяка конкретна организация, нейната устойчивост и съществуващите рискове за дейността ѝ.

Мерките и дейностите за осигуряване на непрекъснатост на дейностите в организациите съгласно стандарта са насочени към някои от следните основни техни елементи, които имат отношение към устойчивостта им: човешки ресурси, комуникации, оборудване, финанси, информационни и комуникационни технологии, производство, верига за доставки.

По отношение на **човешките ресурси** могат да се открият някои основни добри практики, които да намалят риска от прекъсване на работата на организациите, например:

- разработване на план за заместване, особено на ключовите и ръководните кадри в организацията;
- обучаване на резервен персонал за изпълнението на ключови за организацията дейности;
- запознаване на служителите със задълженията им в контекста на осигуряването на непрекъснатост на дейността на организациите при извънредни ситуации;
- осигуряване на възможност за работа от разстояние или на алтернативни локации при необходимост;
- осигуряване на необходимите условия за непрекъснат процес на комуникация;

По отношение на **комуникацията**, основните направления, в които може да постави акцент при планирането на непрекъснатостта на дейностите са:

- изготвяне на стратегия за прозрачна комуникация със заинтересованите от дейността на организацията страни;
- изясняване предварително на каналите за получаване на достоверна информация и комуникация в рамките на организацията;
- планиране и осигуряване на резервни канали за комуникация, в случай че основните се претоварят и/или спрат да функционират.

В областта на **финансите** някои от основните мерки, които могат да се посочат за запазване непрекъснатостта на работата в организацията са:

- осигуряването на ликвидност (това е финансово-счетоводен термин, свързан със способността на активите да бъдат максимално бързо превърнати в парични средства при минимум загуби, включително достатъчно касова наличност с оглед гарантиране извършване на плащанията в срок);
- оценяване влиянието на прекъсването на доставките върху дейността и финансовите потоци в организацията.

По отношение на **информационните и комуникационните технологии** в най-голяма степен следва да се предприемат мерки, целящи гарантиране на сигурността на информацията и осигуряването на необходимия капацитет за нормално протичане на информацията при допълнително натоварване на системите при възникването на извънредни ситуации.

В сферата на **производството** мерките за осигуряване на непрекъснатост на дейността са насочени към:

- оценяване на минималното количество ресурси от всеки вид за работа в критични за организацията сфери;
- определяне възможността за работа на място или дистанционно;
- определяне кои аспекти на дейността на организацията ще бъдат засегнати от извънредната ситуация;
- определяне на това, кои продукти или услуги реализирани от организацията ще бъдат засегнати;
- определяне на ключовите потребители на продуктите или услугите на организацията и създаване на планове за задоволяване на техните потребности;
- разработване на план с конкретни критерии за това кога и как да се активират алтернативните варианти за доставки до потребителите;
- определяне на алтернативни източници за критично важни суровини, материали и резервни части;
- осигуряване на транспорт на ключови служители до и от работните места.

По отношение на **веригата за доставки** важни насоки за ограничаване на риска от прекъсване на дейността на организацията са свързани с:

- определяне на външните субекти, от които е зависима организацията и идентифициране на основните доставчици;
- регулярно получаване на информация за ситуацията в страните и регионите, в които са ситуирани основните доставчици с оглед прогнозиране на възможни проблеми със снабдяването с ключови за организацията ресурси.

Други дейности, които биха способствали за ограничаване на риска от прекъсване на дейността на организацията обхващат също така:

- създаване и актуализиране при всяка съществена промяна на средата на план за управление при извънредни ситуации с ясно разпределени роли и отговорности;
- регулярно проиграване на плановите с оглед запознаване на личния състав със задълженията им при възникване на подобни ситуации и своевременно откриване на пропуски в подготовката.

Така описаните дейности не предполагат едно и също съдържание на предприеманите мерки, а по-скоро изискват предварителното извършване на специфични оценки на риска от прекъсване на дейността за всяка една конкретна организация и внедряването на подходящи за нея добри практики.

Повишаването на устойчивостта на органите за управление при бедствия и осигуряването на непрекъсваемостта на тяхната работа са основна предпоставка за защитата на интересите на обществото, тъй като непрекъснатото функциониране на тези структури е предварително условие за успешното про-

веждане на планираните дейности за защита. Поради тези причини в рамките на ведомствата и в част от организациите (особено тези, които стопанисват обекти от критичната инфраструктура) се създават специализирани звена, които отговарят за предотвратяване негативното въздействие на различните по вид и мащаби бедствия върху дейността на организациите и възстановяването на работния процес, тогава, когато бедствието е довело до неговото прекъсване.

ЛИТЕРАТУРА

1. International Federation of Red Cross and Red Crescent Societies. *What is a disaster?* [online] 10.03.2022, 13:05. <https://www.ifrc.org/what-disaster>
2. Закон за защита при бедствия. *Държавен вестник*, бр.102 от 19 Декември 2006г., изм. и доп. *Държавен вестник*, бр.60 от 7 Юли 2020.
3. Asia most at risk from natural disasters. *The New Humanitarian*, 31 May 2010. [online] 10.03.2022, 13:09. <https://www.thenewhumanitarian.org/news/2010/05/31>
4. *Global Occurrences from Natural Disasters, 1950 to 2020*. EM-DAT, CRED/UCLouvain, Brussels, Belgium. [online] 10.03.2022, 13:14. www.emdat.be
5. Национален статистически институт. *Възникнали кризисни събития*. [онлайн] 10.03.2022, 12:20. <https://www.nsi.bg/sites/default/files/files/data/timeseries/Crisis1.1.xls>
6. *Сигурност и устойчивост. Системи за управление на непрекъснатостта на дейността*. Изисквания. (ISO 22301:2019).
7. *Какво трябва да включва Планът за непрекъсваемост на бизнес процесите при пандемия съгласно ISO 22301?* [онлайн] 10.03.2022, 13:18. <https://www.consejo.bg/какво-трябва-да-включва-планът-за-непрекъсваемост-на-бизнес-процесите-при-пандемия-съгласно-iso-22301~252>

REFERENCES

1. International Federation of Red Cross and Red Crescent Societies. *What is a disaster?* [online] 10.03.2022, 13:05. <https://www.ifrc.org/what-disaster>
2. *Zakon za zashtita pri bedstvia*. *Darzhaven vestnik*, br.102 ot 19 Dekemvri 2006 g., izm. i dop. *Darzhaven vestnik*, br.60 ot 7 Yuli 2020.
3. Asia most at risk from natural disasters. *The New Humanitarian*, 31 May 2010. [online] 10.03.2022, 13:09. <https://www.thenewhumanitarian.org/news/2010/05/31>
4. *Global Occurrences from Natural Disasters, 1950 to 2020*. EM-DAT, CRED/UCLouvain, Brussels, Belgium. [online] 10.03.2022, 13:14. www.emdat.be
5. *Natsionalen statisticheski institut. Vazniknali krizisni sabitia*. [onlayn] 10.03.2022, 12:20. <https://www.nsi.bg/sites/default/files/files/data/timeseries/Crisis1.1.xls>
6. *Sigurnost i ustoychivost. Sistemi za upravlenie na neprekasnatostta na deynostta*. *Iziskvania*. (ISO 22301:2019).
7. *Kakvo tryabva da vklyuchva Planat za neprekasvaemost na biznes protsesite pri pandemia saglasno ISO 22301?* [online] 10.03.2022, 13:18. <https://www.consejo.bg/kakvo-tryabva-da-vklyuchva-planat-za-neprekasvaemost-na-biznes-protsesite-pri-pandemia-saglasno-iso-22301~252>

БЕДСТВИЯ – МИГРАЦИЯ И БЕЖАНЦИ

гл. ас. д-р Даниела Балева

Военна академия „Г. С. Раковски“, *d.baleva@rndc.bg*

Резюме: В доклада е представено влиянието на бедствията върху миграционните процеси в рамките на засегнатите държави и извън тях. Анализирани са основните проблеми, свързани с тези процеси и факторите, които влияят върху техните мащаби.

Ключови думи: *бедствия; мигранти; бежанци*

DISASTERS – MIGRANTS AND REFUGEES

Assist. Prof. Daniela Baleva, PhD

Rakovski National Defence College

Sofia, Bulgaria

E-mail: *d.baleva@rndc.bg*

Abstract: The report presents the influence of disasters on migration processes in the affected counties and beyond. The main problems concerning these processes and the factors that influence their scale are analyzed.

Keywords: *disasters; migrants; refugees*

Миграцията най-общо представлява преместване на хора с цел смяна на местоживеенето. Съществуват различни видове миграция в зависимост от критериите, които се използват за нейната класификация.

Така например в зависимост от това дали се пресичат държавни граници, може да се обособят два вида – вътрешна и външна миграция. По отношение на трайността и миграцията може да бъде временна или трайна, а в зависимост от причините, които я пораждат – продиктувана от субективни или от обективни причини.

Въпреки че най-често причините за миграцията са субективни – икономически, образователни, семейни и др., обективните причини за мигриране на големи групи от хора, включително такива като войни или бедствия, предизвикват значителни сътресения в общественото развитие, които надхвърлят непосредственото влияние върху засегнатите личности.

Акцент при настоящия анализ е поставен върху миграционните процеси в контекста на възникването на бедствия. Основните причини за това са, че, от една страна, миграцията при бедствия е свързана с наличието на множество проблеми, които е необходимо да бъдат решени, не само с оглед опазването на живота и здравето на хората пряко засегнати от бедствията, но и с цел повишаването на сигурността на обществото като цяло. От друга страна, следва да се отчита и фактът, че факторите, влияещи върху мащабите на проблемите са различни, а инструментите за решаването им (включително и по отношение на приетото законодателство) в някои случаи – силно ограничени.

1. Особенности на миграционните процеси при бедствия.

Бедствията се характеризират с нарушаване на нормалното функциониране на обществото в мащаб, който надвишава капацитета му да се справи със възникналата ситуация със собствените си ресурси. В тази връзка и като пряк резултат от съществуващите рискове за живота и здравето им и същественото намаляване на качеството на живот, вследствие на възникналите бедствия, големи групи от хора мигрират в рамките на родните си страни или извън тях.

Връзката между миграцията, социалното развитие и природните бедствия е комплексна (Таблица 1).¹

Проблемите, пред които са изправени мигрантите в и извън родните им страни при възникване на бедствия, са разнообразни. Те могат да бъдат обособени в отделни групи, като например:

– *проблеми свързани с логистиката.* Тази група обхваща разнообразни проблеми, свързани най-вече с изхранването, придвижването и настаняването на засегнатите от бедствие;

– *проблеми, свързани с медицинското осигуряване.* Обикновено, освен рутинната нужда от медицински грижи за населението, при възникване на бедствия хората търпят различни по характер и тежест травми, които следва да бъдат третирани. Често възниква необходимост и от оказване на първа психологична помощ на засегнатите от бедствия и конфликти;

– *проблеми по осигуряване на обществен ред.* Силите на реда по време на бедствие са ангажирани с различни дейности, включително по осигуряване на безпрепятственото придвижване на спасителните екипи към мястото на бедствието, евакуацията на хората от застрашените райони и др. Особено внимание тук следва да се обърне на мерките по предотвратяване на мародерство.

Върху мащабите на тези проблеми свързани с миграцията при бедствия влияят различни фактори. Основните са:

- мащабът на самото бедствие;
- наличието на съответната социална инфраструктура, посредством която да се посрещнат проблемите на мигрантите;
- времето, за което хората са принудени да напуснат домовете си и родните си места;
- пресичането на международни граници;
- наличието на културно-религиозни различия между населението, което мигрира, и приемащото го общество.

2. Динамика на миграционните процеси.

Изменението на климата и природните бедствия, обичайно в краткосрочен период, създават условия за вътрешно разселване на засегнатите лица.

В световен мащаб нито причините, пораждащи вътрешна миграция, нито нейните мащаби са равномерно разпределени (фиг. 1).² За периода 2008 – 2020 г. вътрешно разселени лица в резултат от бедствия са повече от 318 млн. души при приблизително 9600 регистрирани за същия период бедствия (фиг. 2).³ Почти половината от всички засегнати от бедствия хора са разселени в резултат от наводнения (фиг. 3). В тази връзка през последните години все по-често се говори за „климатични бежанци“ и „екологични бежанци“.

В тази връзка използването на понятието „климатичен бежанец“ или „екологичен бежанец“ не е напълно обосновано от правна гледна точка. Въпреки това понятието „климатичен бежанец“ се използва все повече със значението на човек, който е принуден да напусне своята страна вследствие на това, че климатична катастрофа или глобалното затопляне са засегнали мястото на пребиваването му. Определението на понятието „екологичен бежанец“ е по-широко, а именно: човек, принуден да напусне местообитанието си временно или за постоянно, поради разрушаване на околната му среда (поради причини, свързани с човешка дейност или природни бедствия), което застрашава съществуването му или значително намалява качеството на живота му. Съгласно това разбираме в рамките на обхвата на понятието не са включени хора, които мигрират по политически или икономически причини.⁴ Въпреки все по-широката употреба на тези понятия, липсата на приета международна правна дефиниция води до това, че тези лица не могат да се ползват от специални права и закрила.

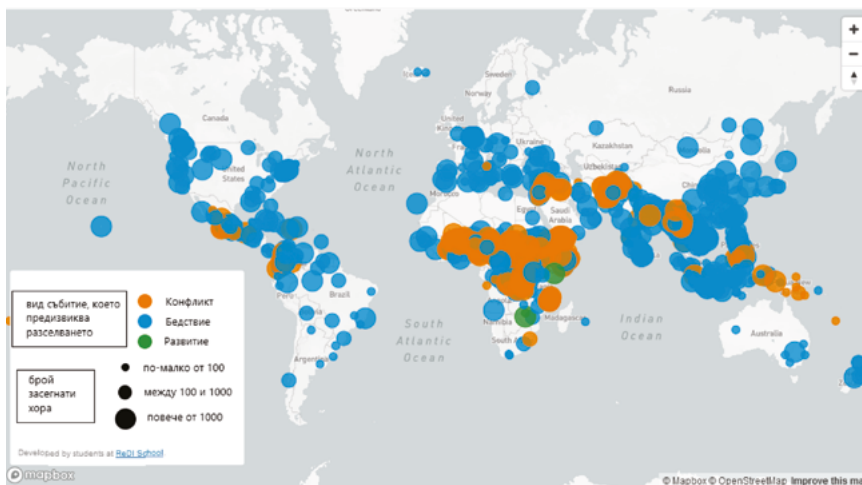
Бежанците или тези, които вече са били вътрешно разселени поради други причини (особено във връзка с развитието на военни конфликти), са особено уязвими при възникване на бедствия. Основните причини за това се крият във факта, че тези групи от хора се заселват в райони, които се характеризират с по-голям риск при възникване на бедствия и са с ограничени възможности да реагират при възникване им. Те, като правило, имат и силно ограничени ресурси и на практика в кратък срок – никаква възможност да се върнат в родните си места.

Пример в това отношение е кризата в Сахел, която се утвърждава като най-бързо развиващата се криза с разселени лица в световен мащаб. В този район насилието осъществявано от различни въоръжени групировки принуждава приблизително три милиона души да мигрират както в рамките на родните си страни, така и извън тях. В този контекст разрастващата се хуманитарна и криза на сигурността изострят съществуващите по-рано предизвикателства, пред които били изправени хората от района, включително тези, породени от изменението на климата.^{5, 6}

Таблица 1

**Влияние и взаимовръзки между миграцията,
социално-икономическото развитие и природните бедствия**

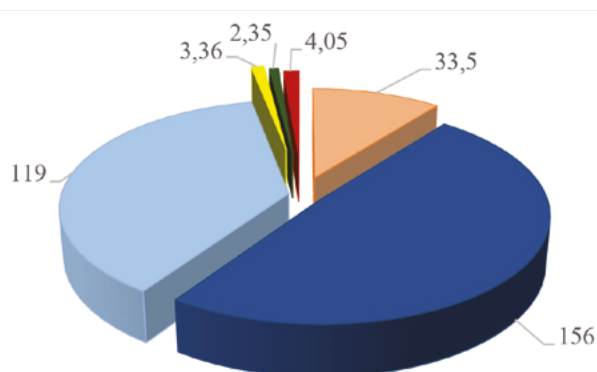
Независими/ зависими променливи	Миграция	Развитие	Природни бедствия
Миграция		– влияе положително върху социално-икономическото развитие, например посредством изплащането на финансови помощи, завръщането на високо-квалифицирани специалисти в родината; – влияе негативно, например поради изтичането на мозъци	– влияе косвено положително или отрицателно върху ефектите от бедствието чрез влиянието върху социално-икономическото развитие; – посредством изплащането на помощи от националната диаспора, живееща в чужбина може да смекчи ефектите от бедствието и да подпомогне възстановяването
Развитие	– по-ниската степен на развитие създава предпоставки за увеличаване на миграцията; – определено ниво на развитие е необходимо, за да се мигрира. По тази причина най-бедните слоеве от населението обикновено не са в състояние да мигрират		– развитието може да смекчи потенциалния ефект от възникването на бедствия, като способства за осигуряване на по-голяма устойчивост и защита
Природни бедствия	– природните бедствия могат да повлияят негативно на социално-икономическото развитие и да предизвикат миграционни потоци; – бедствията могат да доведат и до миграционни потоци в посока на засегнатото от бедствие място, вкл. близки и роднини на засегнатите или хора, търсещи работа в процеса са възстановяване	– природните бедствия влияят негативно на развитието най-малко по отношение на отделните индивиди и засегнатите общности. Понякога и на национално ниво, когато става въпрос за мащабни или повтарящи се във времето бедствия	



Фиг. 1. Събития, свързани с вътрешно разселване на лица за период от 180 дни през 2021 г.



Фиг. 2. Вътрешно разселени лица в резултат от бедствия в световен мащаб за периода 2008 – 2020 г.



Фиг. 3. Вътрешно разселени лица по причини, млн. души

* * *

Бедствията и войните предизвикват значими миграционни потоци в световен мащаб. Подпомагането на вътрешно разселените лица, бежанците и имигрантите предполага не само познаването в дълбочина на проблемите, пред които те са изправени, но и наличието на необходимите ресурси, нормативна рамка и организация. Липсата им води до увеличаване на жертвите, загубите и човешкото страдание.

REFERENCES

- 1 Migration, Development and Natural Disasters: Insights from the Indian Ocean Tsunami. *IOM Migration Research Series*. International Organization for Migration. [online] <https://www.un-ilibrary.org/content/books/9789213630228/read>
- 2 *Global map: Internal displacement updates*, <https://www.internal-displacement.org/global-displacement-map>
- 3 *IDMC Query Tool – Disaster*, <https://www.internal-displacement.org/database/displacement-data>
- 4 *Environmental Refugees*, Essam El-Hinnawi, United Nations Environment Programme, ISBN: 92-807-1103-2, <https://digitallibrary.un.org/record/121267>
- 5 *Humanitarian Needs And Requirements Overview Sahel Crisis*. Humanitarian Program Cycle 2021, published in april 2021, <https://reliefweb.int/sites/reliefweb.int/files/resources/2021%20Sahel%20Crisis%20HNRO%20EN.pdf>
- 6 *Climate change and disaster displacement*. <https://www.unhcr.org/climate-change-and-disasters.html>

КОМУНИКАЦИЯ ПРИ БЕДСТВИЯ

гл. ас. д-р Даниела Дуганова

Военна академия „Г. С. Раковски“, d.duganova@rndc.bg

Резюме: В доклада е разгледана комуникацията като едно от решаващите предизвикателства при природни и причинени от човека бедствия и възможностите за надеждни и достъпни комуникационни и информационни системи, имащи ключово значение за устойчивостта на общността. Разкрити са и начините за получаване на информация от медиите и обществеността при бедствия.

Ключови думи: бедствия; комуникация; управление на информацията и комуникацията

DISASTERS COMMUNICATION

Assist. Prof. Daniela Duganova, PhD

Rakovski National Defence College

Sofia, Bulgaria

E-mail: d.duganova@rndc.bg

Abstract: The report examines communication as one of the crucial challenges in case of natural and man-made disasters, as well as the opportunities for reliable and accessible communication and information systems that are key to the sustainability of the community. The ways of obtaining information by the media and the public in case of disasters are also revealed.

Keywords: *disasters; communication; information and communication management*

Има убедителни доказателства, че броят и сериозността на бедствията се увеличават и че бедните страни и бедните общности са непропорционално засегнати. Бедствията са убили по-малко хора през последните две десетилетия, отколкото преди, отчасти поради по-ефективните международни усилия за реагиране, но броят на бедствията, броят на хората, които те засягат, и имуществените загуби, които причиняват, нарастват драстично всяко десетилетие, откакто съществуват надеждни записи около 1960 година¹.

Едно от решаващите предизвикателства при природни и причинени от човека бедствия е комуникацията. Комуникацията по време и непосредствено след бедствие е важен компонент от реакцията и възстановяването, тъй като свързва засегнатите хора, семейства и общности с лицата, които се отзовават, системите за подкрепа и други членове на семейството. Надеждните и достъпни комуникационни и информационни системи също са от ключово значение за устойчивостта на общността. Симулационните възможности на информационните системи могат да позволят откриване на зараждащи се инциденти, рискове и заплахи².

Бедствията се случват неочаквано, с различни нива на тежест, което представлява голямо предизвикателство за ефективен обмен на информация и координация. Повторяемостта на тези събития в продължение на дълги периоди обаче заставя правителствата да отчитат възможността за тяхното възникване и да провеждат политика в областта на защитата на населението, която да намали потенциалните неблагоприятни последици³. При бедствия животите са разбити завинаги, поминъкът е разрушен и хората са разселени, като много от тях не могат да се върнат към нормалния си живот преди бедствието – ситуация, която представлява огромно социално-психологическо предизвикателство за жертвите. Въздействието не е само за тях – семейства, приятелите на жертвите, лицата, които се отзовават, и полагащите грижи също се сблъскват с много нежелани ситуации. Колосалният характер на бедствията доведе до осъзнаването, че комуникационните и стратегиите за управление при бедствия трябва да бъдат по-съгласувани и ефективни.

Когато бедствията са чести и засягат големи части от населението, намаляването на риска започва да се налага в дневния ред за развитие. Налице е паралелен процес с безпрецедентни усилия на хуманитарните агенции и агенциите за развитие да си сътрудничат, за да намерят начини да се отдалечат от разчитането на краткосрочни спешни реакции при продължителна несигурност към дългосрочно ориен-

тирани към развитието, които включват по-тясно партньорство с правителствата. Изключително важно значение за успешната защита на населението имат превантивните дейности и особено тези, които позволяват да се прогнозира появата и развитието на бедствията, както и за отстраняване на предпоставките за възникването им⁴.

Политиците са едновременно помощ и пречка при предоставянето на информация на обществеността преди, по време и след бедствия. При бедствия те изпитват сериозна заплаха за основните структури или фундаменталните ценности и норми на системата, които във времето на натиск и силно несигурни обстоятелства налагат вземането на жизненоважни решения.

Една от задачите на комуникацията е да бъде създадена увереност и доверие в условията на несигурност и нестабилност⁵. Не бива да се пропуска и изострената обществена чувствителност при различните бедствия, която прави аудиторията извънредно податлива на фалшиви новини и паника.

Има изобилие от примери за политически последващи кризисни комуникации както вербални, така и невербални, от министри и правителствени ръководители. Един от тях е изявлението на Ангела Меркел „Wir schaffen das“ в пика на сирийската бежанска криза в края на лятото на 2015 г. – съдбоносен и променящ „играта“ морален и политически ангажимент Германия да получи най-големия приток на бежанци в Европа след Втората световна война.

Въпреки че ролята на политическите лидери и представянето на политическото лидерство по време на бедствия все още е донякъде слабо развита изследователска област, има основателни причини да ѝ се обръща постоянно внимание. От обществена гледна точка изследването на политиката на управление и комуникация по време на бедствия генерира жизненоважно знание за функционирането на социалните и политическите институции. По-специално в демократичните политически системи бедствията тестват стабилността на тяхната институционална структура и отговорността, която имат към населението. Освен това гласовете на политическите лидери не са единствените, които се излъчват и слушат. Техните изявления често биват оспорвани от леко или радикално различни интерпретации, предлагани от техните политически опоненти, както и потенциално – от други политически заинтересовани страни, жертви, журналисти, коментатори, адвокати и др.

Възможностите на държавата да предотвратява и овладява бедствия, както и да преодолява последици от тях, се определят от наличието на функционираща система за управление, позволяваща да се получава постоянна информация за рисковете от възникването им и от поддържането на подготвени и добре екипирани професионални и доброволни формирования за действие⁶. Предоставянето на информация за риска на общностите, живеещи в райони застрашени от бедствия, ще осигури по-добри резултати във всички етапи, но по-важното е, че ще им позволи да поемат контрол над живота си, като им се предоставя ценна информация, която може да се използва за предприемане на мерки за намаляване на риска и подобряване на стратегиите за преодоляване на последствията.

Изграждането на комуникационна стратегия по време на извънредна ситуация се свързва с набор от решения, често пъти взети в условията на съкратено време и динамично променяща се среда⁷. Прессъобщения и пресконференции, технически бюлетени, интервюта със специалисти, посещения на мястото на бедствието, срещи с редакционни екипи, институционални уеб сайтове, съобщения за обществени услуги и образователни материали са някои от начините за получаване на информация от медиите и следователно – обществеността при бедствия.

Интервютата са друг начин за достигане до медиите. Те предоставят възможност директно да се обясни, от гледна точка на експертите, затрудненото положение на засегнатото население, действията, предприети от здравния сектор, и постигнатият напредък в усилията за оказване на помощ. Това е идеален начин за предоставяне на по-задълбочена информация по конкретни или по-сложни теми. Интервютата също могат да повишат осведомеността на медиите за тяхната роля по време на извънредна ситуация или бедствие.

Управлението на информацията между различни заинтересовани страни в природни и причинени от човека бедствия е от основно значение за ефективните операции за помощ при бедствия. Процесът на комуникация по време и непосредствено след бедствие е жизненоважна част от реакцията и възстановяването, тъй като свързва жертвите на бедствие с лицата за първа помощ, системите за подкрепа и други членове на семейството. Като такива, надеждните и достъпни комуникационни системи са от решаващо значение за устойчивостта на общността.

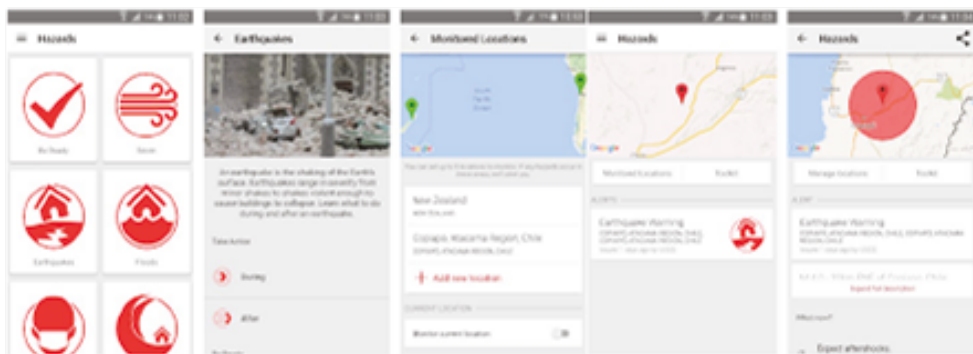
Хуманитарната информация и данни също трябва да бъдат направени достъпни за всички хуманитарни участници чрез прилагане на лесни за използване формати и чрез превод на информация на общи

или местни езици, когато е необходимо. Информацията, използвана за хуманитарни цели, трябва да бъде широко достъпна чрез различни онлайн и офлайн канали за разпространение, включително медиите.

Докато традиционните медии, като телевизията и вестниците, продължават да играят важна роля в информирането на масовата аудитория за рисковете, развитието на информационните и комуникационните технологии осигурява по-голям достъп до информация чрез интернет-базирани комуникационни инструменти, като социални мрежи и уебсайтове. Социалните медии преструктурират комуникацията като бързовъзникваща, без географски граници и интерактивна както в социален, така и в индивидуален план. Бързата комуникация е предизвикателство за управление и това предизвикателство се изостря в най-неотложните ситуации: извънредни ситуации и бедствия, които трябва да бъдат управлявани от организации в публичния сектор. В допълнение, напредъкът в технологиите направи възможно интуитивното визуализиране на сложна информация като въздействия, уязвимости и рискове, които могат да бъдат споделяни широко онлайн. Използването на интернет, освен ситуационно обусловено, има и чисто рационално обяснение. То дава възможност за осигуряването на постоянен информационен поток към целевите групи, от една страна, и към традиционните медии, от друга⁸.

Нараства разбирането, че двупосочната комуникация е по-ефективна, което увеличава участието на широката общественост като заинтересована страна в процеса на вземане на решения. Повечето организации за защита на гражданите в света насърчават цели общности да участват в програми и дейности, които могат да направят техните семейства, домове и региони по-безопасни при извънредни ситуации⁹. Мобилните телефони, мобилните приложения и платформите за социални медии станаха популярни за такава двупосочна комуникация. Те могат да се използват за изпращане на конкретна информация до обществеността въз основа на местоположението на техните мобилни телефони. В случай на извънредна ситуация само тези хора, които са на определено разстояние от бедствието, ще получат информация, която е от значение за тях в момента.

Като положителен пример може да се посочи приложението Hazard за смартфони, което Червеният кръст на Нова Зеландия разработи, за да помогне на хората да се подготвят и да реагират при бедствия (фиг. 1). Приложението е предварително „заредено“ с информация за наводнения, земетресения, цунами, пожари и др. Това приложение позволява на потребителите да подготвят домовете и семействата си за бедствие, да намерят помощ и да уведомят другите, че са в безопасност. Вградената система за предупреждение позволява получаването на сигнали въз основа на местоположението и вида на опасността, която се наблюдава. Чрез приложението се получават официални предупреждения за извънредни ситуации и сигнали от участващите агенции според местоположението. Така гражданите имат контрол върху местоположенията, видовете опасности и нивото на сигналите, които наблюдават в приложението. Сигналите са насочени към конкретни географски области, а потребителите могат да контролират и нивото на сигналите, които искат да получават.

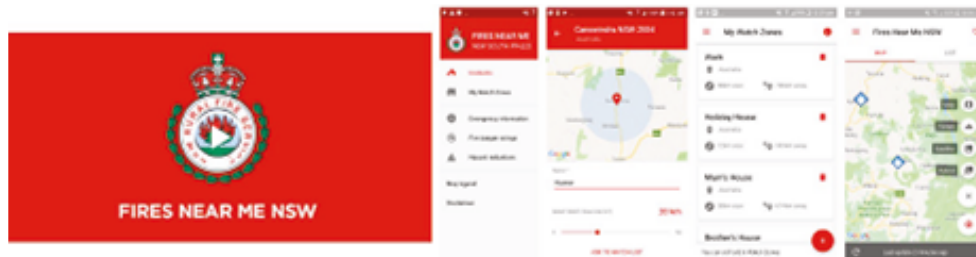


Фиг. 1. Приложението Hazard в Нова Зеландия.

Комуникацията по каналите в социалните медии често е единствената възможност, която „оцелява“ след въздействието на бедствията. Използването на социални медии като телефонни разговори, системи за кратки съобщения (SMS), Facebook, Twitter, имейл се увеличава по време на бедствия. Хората използват тези платформи, за да изпращат и получават информация за различни аспекти по отношение на бедствието.

Горските пожари на 17 октомври 2013 г. в Сините планини, Нов Южен Уелс, унищожават и нанасят щети на няколкостотин къщи, а стотици ученици биват хванати в капан в училищата си в Уинмали, докато пожарите се разпространяват. Много от жителите тогава разчитат на мобилните си телефони, за да получат бърза и надеждна информация. Противопожарната служба на NSW Rural използва приложение за смартфони, наречено Fires Near Me (фиг. 2), изтеглено близо 200 000 пъти по време на бедствието, а в пика на пожара страницата във Facebook регистрира над милион гледания на час. Неговият Twitter нарасна от 20 000 на 37 000 последователи. По същество тези платформи помогнаха да се предупредят хората за възможностите за обезопасяване и опасните зони около тях.

Днес социалните медии безспорно предоставят възможности за работа в мрежа и взаимодействие с хора по време на бедствие чрез разпространение на свързана информация и събиране на публикувана.



Фиг. 2. Приложението Fires Near Me

Може да се използват и по-традиционни начини на комуникация, като стационарен телефон, ако комуникационната инфраструктура все още е непокътната.

На местно ниво комуникацията може да бъде още по-фокусирана върху заинтересованите страни, участващи в оценката на риска, и върху прилаганите методи за смекчаване. Комуникацията за риска на местно ниво има за цел:

- информирание на хората за риска в техния район;
- повишаване на знанията им за възможни природни бедствия и как да се подготвят за тях;
- промяна на отношението им към готовността за бедствия;
- в крайна сметка да променят поведението си за намаляване на риска от бедствия и изграждане на устойчивост;
- създаване на диалог за алтернативи за намаляване на риска от бедствия.

Начинът, по който съобщенията и сигналите се разпространяват в действителност, е от решаващо значение и трябва да се проучи подробно, включително използването на алтернативни форми на комуникация в случай на първична системна повреда на използваните технологии. Необходима е система с удобен за потребителя интерфейс за наблюдение и предупреждение и е важно да се установят ясни процедури, така че отговорните страни да разберат какво трябва да направят на всяка стъпка от събитието. Тези процедури трябва да бъдат документирани на ясен, лесен за разбиране език и да бъдат лесно достъпни, в идеалния случай поставени на видно място.

Обичайно е системите за ранно предупреждение да използват няколко нива на предупреждение, като всяко ниво увеличава степента на неотложност и довежда предупреждението до повече хора, за да могат да предприемат по-нататъшни действия. Фалшивите предупреждения обаче могат да имат обратен ефект, тъй като твърде много от тях ще накарат общностите да игнорират предупрежденията в бъдеще, с потенциално катастрофални последици.

Управлението при бедствия е процес на координиране на усилията на различните структури на Единната спасителна система (ЕСС) и тяхната съвместна работа за постигането на общата цел – овладяване на възникнало бедствие и защита на живота и здравето на хората, имуществото и околната среда¹⁰. Управлението е ефективно, когато се изпълнява комбинация от задачи: възникващата криза се открива бързо и реагиращите разбират какво се случва, критичните решения се вземат от точните хора и усилията на реагиращите са организирани (вземане на решения и координация), правителството, длъжностните лица и агенциите са в състояние да оформят възприятието и оценката на обществото за това, което се случва, какво се прави за справяне с него и какви могат да бъдат последиците от него за тях. В същото

време са създадени процедури за отчетност, а настъпилото събитие се използва като точка от данни и задействане за колективно самоизследване и подобрене (учене).

При бедствия населението очаква от отговорните лица да намалят несигурността и да предоставят авторитетен отчет за това какво се случва, защо се случва и какво трябва да се направи. Правителствените елити могат да се радват на някои априорни предимства, предвид техният достъп до жизненоважна информация, до широко използвани и доверени комуникационни канали и до подкрепата на специализирани съветници. В същото време може да се окаже, че тяхната лична или институционална достоверност сред (части от) обществото е ниска и допълнително отслабена от настъпването на бедствието.

В политически план ключов въпрос, който възниква рано или късно в хода на всяко бедствие, е кой носи отговорността и какви ще са последствията за тези, които се смятат за отговорни. В рамките на всяка демократична политика способността да се търси отговорност от длъжностните лица е жизненоважна за легитимността и доверието, предоставено на политически и административни участници и институции. Терминът „отчетност“ се отнася както до добродетел, която трябва да се преследва (активно поемане на отговорност), така и до механизмите и институционалните договорености, осигуряващи на участниците стимули да преследват тази добродетел¹¹. В основата му лежи комуникацията. Марк Бовенс авторитетно дефинира отчетността като „комуникативно взаимодействие между действащо лице (лице или организация) и форум за отчетност, в който се оценява поведението на първия (в най-широк смисъл на думата)“¹².

Проблемите с комуникацията са широко разпространени при всички извънредни ситуации. Изследванията показват, че всички бедствия регистрират някакъв вид комуникационни проблеми. Това може да бъде външна комуникация с жертвите и обществеността и/или вътрешна комуникация между отговорните органи и лица. Прекъсванията в комуникационните системи, инфраструктурата и електроснабдяването значително ще попречат на ефективната реакция и възстановяването, както и други усилия за подкрепа при бедствия. Въпреки че много бедствия са неизбежни, въздействието и страданията могат да бъдат намалени чрез въвеждане на подходящи системи за управление и разпространение на информация и системи за ранно предупреждение за предстоящи бедствия. Навременното разпространение на прецизни и разбираеми предупреждения за бедствия до населението в риск и до съответните органи за реагиране при бедствия може да сведе до минимум загубите и щетите. Освен това общностите, живеещи в зони на бедствие, трябва да имат достъп до комуникационно оборудване при всички атмосферни условия по време на бедствие. Отговорните органи и лица на различните нива трябва да бъдат оборудвани с няколко начина на комуникация, които включват факсове, електронни сателитни радиостанции и УКВ радиостанции и телефони. Ако една система се повреди, населението следва да може да разчита на други системи за комуникация. Други инициативи трябва да включват подходящо обучение на отговорните лица, които управляват приемниците, и да гарантират, че обществеността е правилно информирана относно номерата за спешни случаи, вероятно чрез мобилни мрежи. Координацията между заинтересованите страни при бедствия, като държавни агенции, неправителствени организации и хуманитарни агенции, е от решаващо значение за осигуряване на ефективни усилия за оказване на помощ при бедствия. Поради това трябва да се обърне голямо внимание на осигуряването на ефективни канали за комуникация между тези заинтересовани страни.

Управлението на информацията и комуникацията трябва да бъде част от планираното проектиране и изпълнение и да бъде интегрално в планове за управление на риска и бедствия на организацията. Импровизираната комуникация може да струва скъпо и да има незадоволителни резултати.

Работата в екип е от съществено значение, ако управлението на информацията и комуникацията са успешни. Експертите по бедствия, комуникаторите или администраторите не могат да работят изолирано и работата на тези с една специализация трябва да допълва работата на другите. Тези, които отговарят за комуникацията, трябва да имат ясно разбиране за бедствията. По същия начин експертите по управление на бедствия ще вземат по-добри решения, когато приемат информация от специалистите по комуникации. Инвестицията в управлението на информацията и комуникацията е междусекторно начинание и трябва да бъде неразделна част от работата на експертите и организациите по управление при бедствия.

Информацията е основният елемент в процеса на оценка на щетите и нуждите на засегнатото население и е основата за координация и вземане на решения при извънредни ситуации. Тя има

силно въздействие върху начина, по който се мобилизират националните и международните ресурси. Това е от съществено значение за анализа, оценката и извлечените поуки. Управлението и обменът на информация трябва да се основават на система за сътрудничество, партньорство и споделяне. Трябва да има висока степен на участие и ангажираност от множество заинтересовани страни, особено представители на засегнатото население. Информацията трябва да бъде точна, последователна и базирана на солидни методологии, валидирана от външни източници и анализирана в подходяща контекстуална рамка.

В днешния глобализиран и взаимосвързан свят информацията за въздействието на бедствие или извънредна ситуация е почти невъзможно да бъде скрита от обществеността. В крайна сметка извънредната ситуация ще бъде „разкрита“. Ето защо, за да се предотвратят слухове и дезинформация, най-добре е информацията да се обяви възможно най-рано. Поддържането на доверието на обществеността по време на бедствия изисква прозрачност, т.е. комуникация, която е откровена, лесно разбираема, пълна и точна с факти. Прозрачността характеризира взаимоотношенията между отговорните лица и обществеността. Това позволява на населението да види процесите на събиране на информация, оценката на риска и вземане на решения, които са свързани с контрол на рисковете. Прозрачността сама по себе си обаче не може да гарантира доверие.

ЛИТЕРАТУРА

1. White, P., Pelling, M., Sen, K., Seddon, D., Russell, S., Few, R. *Disaster Risk Reduction: a development concern*. London: Overseas Development Group, 2005.
2. Георгиев, Г. Защита на обекти от критичната инфраструктура от терористични заплахи. В: *Сборник доклади от Международна научна конференция „Сигурност – образование, наука, индустрия“ – втора част, Военна академия „Г. С. Раковски“*. София, 2020, стр. 154 – 159.
3. Балева, Д. Бюджет за защита на населението при бедствия. *Икономическа мисъл*. Книжка 5, 2016, стр. 136 – 148.
4. Георгиев, Г. Перспективи за използване на формирования от Българската армия за овладяване и/или преодоляване на последствията от бедствия. В: *Годишник на Военна академия „Г. С. Раковски“, Факултет „Командно-щабен“, 2/2014*, стр. 81 – 89.
5. Събева, Я. Политическата комуникация в условията на криза в България в периода 2001 – 2005 г. *Политически хоризонти*, бр. 3, 2019, стр. 64 – 73.
6. Георгиев, Г. Взаимодействие между областната и общинската администрация с Българската армия в управлението при бедствия и аварии. Военнонаучна конференция с международно участие „Съвременни аспекти на сигурността – предизвикателства, подходи, решения“, 20 – 21 юни 2018 г. В: *Годишник на Военна академия „Г. С. Раковски“, Факултет „Командно-щабен“, 2018*, стр. 400 – 408.
7. Събева, Я. *Кризис и политическата комуникация в България в периода 2001 – 2005 г. Преходът и политическите езици*. София: Център за исторически и политологически изследвания, Българска асоциация по реторика, Фондация „Солидарно общество“, 2019, стр. 204 – 212.
8. Събева, Я. Реторически аспекти и комуникационни специфики на протестите от 2020 г. *Политически хоризонти*. бр. 6, 2020, стр. 179 – 185.
9. Филипов, Х. Подготовка на населението за защита при извънредни ситуации. В: *Сборник с доклади от юбилейна международна научна конференция „Сигурност и икономика в несигурния свят – дилеми и предизвикателства“*. ВУСИ Пловдив, 2018, стр. 181 – 187.
10. Закон за защита при бедствия. *Държавен вестник*, бр. 102 от 19.12.2006, посл. изм. и доп. *Държавен вестник*, бр. 60 от 7.07.2020.
11. Bovens, M., Schillemans, T., Robert, E., Goodin, R. *Public Accountability*. Oxford: Oxford University Press, 2014.
12. Bovens, M. Analysing and Assessing Accountability: A Conceptual Framework. *European Law Journal*, vol. 13, No. 4, 2007, pp. 447–468.

REFERENCES

1. White, P., Pelling, M., Sen, K., Seddon, D., Russell, S., Few, R. *Disaster Risk Reduction: a development concern*. London: Overseas Development Group, 2005.
2. Georgiev, G. Zashchita na obekti ot kritichnata infrastruktura ot teroristichni zaplahi. In: *Sbornik dokladi ot Mezhdunarodna nauchna konferentsia „Sigurnost – obrazovanie, nauka, industrija“ – vtoro chast, Voenna akademija „G. S. Rakovski“*. Sofia, 2020, str. 154 – 159.
3. Baleva, D. Byudzhet za zashchita na naselenieto pri bedstvia. *Ikonomicheska misal*. No 5, 2016, str. 136 – 148.
4. Georgiev, G. Perspektivi za izpolzvanе na formirovania ot Balgarskata armia za ovladyavane i/ili preodolyavane na posledstviyata ot bedstvia. In: *Godishnik na Voenna akademija „G. S. Rakovski“, Fakultet „Komandno-shtaben“, 2/2014*, str. 81 – 89.

5. Sabeva, Ya. Politicheskata komunikatsia v usloviyata na kriza v Bulgaria v perioda 2001 – 2005 g. *Politicheski horizonti*, br. 3, 2019, str. 64 – 73.
6. Georgiev, G. Vzaimodeystvie mezhdu oblastnata i obshtinskata administratsia s Balgarskata armia v upravlението pri bedstvia i avarii. Voennonauchna konferentsia s mezhdunarodno uchastie „Savremenni aspekti na sigurnostta – predizvikatelstva, podhodi, reshenia“, 20 – 21 yuni 2018 g. In: *Godishnik na Voenna akademia „G. S. Rakovski“*, Fakultet „Komandno-shtaben“, 2018, str. 400 – 408.
7. Sabeva, Ya. *Krizi i politicheskata komunikatsia v Bulgaria v perioda 2001 – 2005 g. Prehodat i politicheskite ezitsi*. Sofia: Tsentar za istoricheski i politologicheski izsledvania, Balgarska asotsiatsia po retorika, Fondatsia „Solidarno obshtestvo“, 2019, str. 204 – 212.
8. Sabeva, Ya. Retoricheski aspekti i komunikatsionni spetsifiki na protestite ot 2020 g. *Politicheski horizonti*. br. 6, 2020, str. 179 – 185.
9. Filipov, H. Podgotovka na naselenieto za zashtita pri izvanredni situatsii. In: *Sbornik s dokladi ot yubiley na mezhdunarodna nauchna konferentsia „Sigurnost i iekonomika v nesigurnia svyat – dilemi i predizvikatelstva“*. VUSI Plovdiv, 2018, str. 181 – 187.
10. Zakon za zashtita pri bedstvia. *Darzhaven vestnik*, br. 102 ot 19.12.2006, posl. izm. i dop. *Darzhaven vestnik*, br. 60 ot 7.07.2020.
11. Bovens, M., Schillemans, T., Robert, E., Goodin, R. *Public Accountability*. Oxford: Oxford University Press, 2014.
12. Bovens, M. Analysing and Assessing Accountability: A Conceptual Framework. *European Law Journal*, vol. 13, No. 4, 2007, pp. 447–468.

АДАПТИВНОСТ НА РАЗУЗНАВАТЕЛНИЯ ЦИКЪЛ

доц. д-р Елислав Иванов

Военна академия „Г. С. Раковски“, e.ivanov@rndc.com

Резюме: В съвременната среда за сигурност съвременните заплахи се развиват с бързи и непредвидими темпове и направления. Те стават все по-сложни и злонамерени, като кибернетичните заплахи са с особена значимост. Целта на доклада е да предостави кратко въведение в непосредствените предизвикателства и проблеми, пред които е изправено „разузнаването на киберзаплахите“, да разгледа ролята и мястото на разузнаването при откриване и идентифициране на тези заплахи и предоставянето на пътища и инструменти за тяхното противодействие. Въз основа на преглед на етапите от разузнавателния цикъл и наложените промени в него, в резултат на кибернетичните заплахи, се извежда на преден план важноста и значението за предоставяне на качествена разузнавателна информация в областта на кибернетичните заплахи, кибернетичните атаки и кибертероризма като цяло.

Ключови думи: *разузнаване; разузнавателен цикъл; етапи; риск; заплаха; киберзаплахи*

ADAPTABILITY OF THE INTELLIGENCE CYCLE

Assoc. Prof. Elislav Ivanov, PhD

Rakovski National Defence College

Sofia, Bulgaria

E-mail: e.ivanov@rndc.com

Abstract: In today's security environment, today's threats are evolving at a rapid and unpredictable pace and direction. They are becoming more complex and malicious, with cyber threats of particular importance. The purpose of the report is to provide a brief introduction to the immediate challenges and problems facing "cyber threat intelligence", to examine the role and place of intelligence in detecting and identifying these threats and to provide ways and tools to counter them. Based on an overview of the stages of the intelligence cycle and the changes imposed in it as a result of cyber threats, it highlights the importance and significance of providing quality intelligence in the field of cyber threats, cyber-attacks and cyber terrorism in general.

Keywords: *intelligence; intelligence cycle; stages; risk; threat; cyber threats*

„Всеки успешен военен план и операция разчитат на разузнаването“.

Дейвид Шед, бивш заместник-директор на
Агенцията за отбранително разузнаване (DIA)¹

Още в самото начало е необходимо да бъдат поставени определени ограничения по отношение на разузнавателния цикъл с цел по-голяма яснота и постигане на разбираемост. Разузнаването и по-конкретно – разузнавателният цикъл, ще се разглежда на стратегическо ниво и значението му на геостратегическо, а в частност и на национално ниво. Необходимо е да се говори за единен разузнавателен процес, който е в интерес на националната и международната сигурност. Същността на приложимостта на разузнаването на стратегическо ниво се изразява основно в способността му да прави стратегически прогнози и да предлага варианти за стратегически решения.

Разузнавателният цикъл е гръбнакът на разузнаването. На сегашния етап няма наложена общоприета единна схема на разузнавателните общности. Отделните страни приемат и използват свои варианти в зависимост от необходимостта и поставените задачи. По този начин на един етап са засилени разузнавателните проявления в една фаза/етап, а в последствие – на друга фаза/етап, което води до различен разузнавателен потенциал в рамките на страните, членки на ЕС и НАТО.

В това направление от особена важност са изградените разузнавателни способности за разкриване и превенция срещу съвременните рискове и заплахи за сигурността. Следователно основната цел е общото разбиране на международните заплахи и рискове и тяхното значение за международната сигурност.

На този етап от изследването би следвало да се обърне внимание именно на институционалните и когнитивните детерминанти, които са в основата за постигане на единно становище за етапите на разузнавателния цикъл. Необходимо е да се отчита и фактът, че според условията съвременната информация търпи непрекъснати промени и се модифицира чрез допълнителни елементи на всяка фаза от цикъла, отличаващи се с кратковременен или продължителен характер. Разглеждането на елементите от разузнавателните етапи на национално ниво ще даде възможност да се структурират правилно отделните елементи в тяхната особеност, за да се получи една обща, съвместима и разбираема позиция, която да е лесно приложима в съвременната среда за сигурност. Направените констатации са лични съображения и не засягат позиции или становища залегнали в доктринални или други регламентиращи документи.

Целта на аналитичната информация, придобита по време на различните етапи на разузнавателния процес, е да се анализират рисковете и заплахите за сигурността чрез преценки и предложения за решения посредством прилагането на научни методи и технологии, които произвеждат знание, спомагащо за разкриване на агресивни замисли и намерения.

Тук е необходимо да бъде направено едно уточнение от гледна точка на използваните понятия с цел тяхното уеднаквяване. Понятието „разузнаване“ ще бъде използвано като обединяващо понятие на отделните видове разузнавания. Става въпрос за разделяне дейността на аналитичното разузнаване на стратегическо ниво от информационно-аналитичната и прогностична дейност на национално ниво.

Преди да пристъпим към анализиране, същността и функционалното значение на понятието „цикъл на разузнаването“, е необходимо да се спрем на дефиницията на понятието „цикъл“ като цяло. Общо казано цикълът е система от хомогенни и хетерогенни елементи, които са в определена последователност, за да се реши или реализира определен проблем. В контекста на разузнавателната дейност неговият основен продукт е информацията и съответно основният принцип на разузнаването е използването на отделните етапи/фази на разузнавателния цикъл, включващи последователност от действия, чрез които информацията се получава, преобразува в разузнавателна и се предоставя на заинтересованите страни.

Най-общо казано разузнавателният цикъл може да се определи като планиран процес, по време на който определени участници, въз основа на анализ и оценка на налична или целенасочено добита разузнавателна информация, обработват, съпоставят с наличните данни (информации), натрупват или трансформират в разузнавателни информации/анализи и я предоставят на оторизираните ръководители за вземане на решения и прогнозиране за бъдещо развитие или противодействие.

Етапите на разузнавателния цикъл

Има няколко подхода за разделяне етапите на разузнавателния цикъл. Основният е разделянето на цикъла на шест етапа: планиране, събиране на информация, обработка на получената информация, оценка, разпространение и получаване на обратна връзка. Според разработеното от Женевския Център за управление на сектора за сигурност (*Geneva Centre for Security Sector Governance DCAF*) справочно пособие², се изтъква, че шестте етапа представляват един общ гъвкав процес и няма строго определени граници между тях. Тази обща детерминанта може да служи като един общ модел за концептуализиране на процеса на разузнаване.

Цикълът на разузнаването е набор от дейности, състоящ се от много цикли, които работят на различни нива и с различна скорост. Няколко цикъла могат да възникнат едновременно. Някои задачи в тях се припокриват, съвпадат и често се изпълняват едновременно, а не последователно. Ще разгледаме един разузнавателен цикъл и последователността на неговото функциониране. В най-общи линии той се разглежда в шест стъпки.

Първата стъпка – „Възлагането на задачи“/„Планиране и ръководство“. За успешното изпълнение на задача трябва да се определят приоритетите на разузнавателния процес, като се има предвид, че изискванията невинаги отговарят на наличните възможности. Разпределят се ресурсите в съответствие с оценените заплахи. Важен фактор при този етап е разбирането кой ще ползва крайния продукт – дали това е екип от експерти/анализатори или ръководител, който има нужда от общ поглед и тенденции, помагачи му при вземането на решения.

Втората стъпка – „Събиране“ – директното събиране на необработени данни в операционното пространство, които са зададени на първия етап. Най-добре е данните да бъдат от широк спектър от източници. Използват се както открити, така и закрити/секретни източници за събиране на информация за хора, места, събития и различни дейности. Могат да бъдат *вътрешни* като налична, регистрирана информация, съдържаща различни събития, или анализи на минали събития и реакции по тях, а така също и *външни* източници – социални медии, отворени или тъмни мрежи (злонамерени IP адреси и др.) или други технически източници.

Третата стъпка – „Обработка“ – преобразуването на събраните данни в установени, удобни формати, позволяващи визуализация, по-нататъшно използване, съхранение и разпространение на обработените данни. Извършва се сортиране на добитата информация, проверява се нейният произход и предназначение и се подготвя за провеждане на аналитична дейност. С други думи – протича процес на структуриране на данните, което улеснява следващия аналитичен процес.

Четвъртата стъпка – „Анализ“ – подготовка на материалите и обработване/анализиране. На този етап се осмислят обработените данни и се реализира превръщането на информацията в аналитичен продукт, съдържащ точна, обективна, своевременна, разбираема и реална информация по поставената за изпълнение задача. Според Нинов „Традиционният анализ на документите и информацията се съсредоточава върху смисловата интерпретация на източниците – каква е логиката, същността, основната идея, истинност и кои са смисловите акценти в тях“.³ В анализа се посочват факти, източници, оценки, ключови предположения, алтернативни сценарии и предложения, улесняващи вземането на решения. На тази стъпка се взема решение как точно да се използва добитата и обработена информация.

Петата стъпка – „Разпространение“ – включва навременна доставка на информация до заявителите в необходимия формат с помощта на комуникационните канали. Тя трябва да достигне до точните хора в точното време. Важно е разпространяваната информация да е кратка и ясна, за да се избегне претоварване на командира/ръководителя. На този етап е важно решението кой ще има достъп до този или друг разузнавателно-информационен продукт.

Шеста стъпка – „Използване и обратна връзка“ – оценка на изпълнението на задачата и препоръки за бъдещи насоки, необходими за планиране и ръководство и готовност за изпълнение на нов разузнавателен цикъл. Това е последната стъпка, цикълът на разузнаването е завършил пълния кръг, което го прави тясно свързан с първоначалната фаза на планиране и насочване. След като получи готовия разузнавателен продукт заявителят го преглежда и определя дали на въпросите му е отговорено задоволително и изчерпателно. В зависимост от това се задейства нов цикъл или се подготвя план за такъв, който да реагира при нови задачи.

Описаните стъпки са необходими за придобиване на ситуационна осведоменост и улесняване вземането на решения. Пренебрегването на една стъпка води до нарушаване на цикличността и ритмичността на процеса, а слабостта ѝ отслабва цялата верига.

Извършването на аналитична дейност се определя като един от важните етапи. Често срещана терминология за този етап е названието „аналитично разузнаване“. Не са редки случаите, когато на даден етап заявителят внася съществени корекции в своята заявка, свързана с информационните му потребности. И разузнавателният цикъл се повтаря. В това се заключава и едно от важните свойства на съвременната разузнавателна дейност – цикличност, непрекъснатост, умение да се приспособява към изпълнението на поставените задачи. Процесът на аналитичното разузнаване е непрекъснат. Той трябва да се осъществява постоянно, а не периодически, във връзка с поставянето на нова задача, защото новата задача изисква нов цикъл, а вече веднъж започнат, така или иначе, той действа.

Поради финансови и организационно-щатни причини, разузнавателният цикъл може да се сведе и до изпълнение **само на четири основни етапа**: управление, събиране, обработка и разпространение. Най-широко приложим сред страните, членки на ЕС и НАТО, е разузнавателен **цикъл от пет етапа**, като основно внимание и значение се отдава на 2-ри и 3-ти етап. Изискванията към разузнаването се определят от лицето, вземащо решение, за да се постигнат неговите/нейните цели. Във федералното правителство на Съединените щати изискванията могат да бъдат издадени от Белия дом или от Конгреса. В НАТО командирът използва изисквания (понякога наричани „Основни елементи на разузнаването“ (*Essential Elements of Intelligence* – EEI))⁴, за да инициира цикъла на разузнаването.

Разузнавателният цикъл и съвременните рискове и заплахи

Цикълът е необходимо да бъде разглеждан като многоетапен, цикличен процес, а не като задача, която трябва да бъде изпълнена в дадения момент. Осигуряването на постоянен мониторинг върху заплахите ще даде възможност да бъде определен техният потенциален и действителен характер. Така ще могат да бъдат управлявани уязвимости и анализирани рисковете за сигурността и избраната. Ясно е, че рисковете, свързани с това потенциално развитие, са очевидни, погледнати през призмата на увеличаващите се и намиращи все по-голямо приложение хибридни заплахи. Не на последно място по значимост са и перспективите за усъвършенстване на процеса на вземане на решения и непрекъснато подобряване на жизнения цикъл на бъдещите разузнавателни процеси, а така също – подобряване на инструментите за разузнаване на заплахите. Разузнаването на заплахи може да предостави достатъчно информация, спомагаща за вземане на информирано решение, по което може да се предприеме действие.

Съвременната среда за сигурност се характеризира с нов вид заплахи, (хибридни, киберзаплахи) налагащи нови концепции и доктрини, а „съвременните концепции за постигане на стратегически цели и налагане на воля се основават на съгласувано използване на множество разнообразни, хибридни и асиметрични модели на поведение“⁵. Всичко това изисква нови методи и способности за откриване, познаване и превенция от страна на разузнаването. Това налага и определени промени в жизнения разузнавателен цикъл. Според Столтенберг „...на този етап най-съществени и опасни са кибератаките, които са невидими, агресивни, атакуват уязвимости и със значителни, а понякога и невъзвратими последствия“⁶. По тази причина и разузнавателният цикъл при функции за разузнаване на киберзаплахи ще има **седем етапа**: планиране, съхраняване, развитие, съпоставяне, анализ, отчитане и разпространение.

Някои изследователи на киберзаплахите изразяват мнение, че последният етап трябва да бъде „прогнозиране“, други са на мнение, че той трябва да е „обратна връзка“, тъй като след всяко предупреждение за заплахата от решаващо значение е да се анализират отново целите, които застрашават сигурността. Заплахата е възможността за нежелана или дори опасна дейност, която причинява щети, а в дигиталния свят заплахите са навсякъде. Въздействието върху отделни субекти може да бъде огромно.

Същност на „разузнаване на киберзаплахите“⁸

„Разузнаването на киберзаплахите“ (*Cyber Threat Intelligence* – CTI) трябва да бъде разбираемо и операционализирано, за да подпомага при вземането на политико-стратегически решения“⁹. Днес цифровите технологии намират приложение навсякъде. Разузнаването на заплахите е превенция – да се предотвратят или смекчат атаките. Разузнаването на заплахите – това са данните, които се добиват, обработват и информират за техните проявления. Това дава възможност да се разбере кой извършва атаката, каква е неговата мотивация и възможности и какви индикатори за компромис в системите могат да се реализират, за да има възможност за вземане на решения относно сигурността. Необработените или т.нар. „сурови данни“ се добиват от множество източници, наблюдавани както от експерти, така и от автоматизирани инструменти.

Този целият процес представлява разузнавателния цикъл, тъй като в хода на развитието на разузнаването се идентифицират нови въпроси и пропуски в знанията и това води до поставяне на нови задачи и изисквания за добиване на нови данни. Чрез експертни човешки изследвания и анализи, подпомагани от различни технически средства и апаратури, включително и от изкуствен интелект, този набор от данни се превръща в подобрени емисии за разузнаване на рисковете и заплахите, които да се използват от екипи и платформи за сигурност.

Своевременното изучаване на произхода, естеството и техните проявления дава възможност за планиране и прилагане на защитни тактики и стратегии срещу злонамерено цифрово или открито поведение. Това позволява на екипите по сигурността бързо да оценяват рисковете и въздействията, да приоритизират дейностите и да концентрират своите по-ефективно. По този начин това спомага за намаляване на негативни въздействия, предотвратяване на пробиви на данни и избягване на финансови и ресурсни въздействия.

Добиване, съхраняване и обработка на данните за съвременните рискове и заплахи

Създаването на широка база от данни, комулирани от различни специализирани източници, включително и от човешкото разузнаване, предоставя възможности за обработката и анализирането на тези

данни с автоматизирани машини, а така също – и процеси управлявани от изкуствен интелект. Освен създаването на необходимата база данни за рисковете и заплахите, съществува определен интерес и нужда от специалисти, които да могат да обработят тези данни и да притежават подходяща аналитична експертиза. Това налага разработване и прилагане на подходящ инструментариум за разузнаване и анализ на заплахите чрез различни платформи, включително и в областта на софтуера и хардуера.

„Днес индустрията за киберсигурност е изправена пред многобройни предизвикателства – все по-постоянни и непредвидими заплахи, ежедневен поток от данни, пълни с чужда информация и фалшиви тревоги в множество несвързани системи за сигурност и сериозен недостиг на квалифицирани специалисти“¹⁰ Всичко това води до една неопределеност и несигурност. Хибридните заплахи стават все по-агресивни, трудно откриваемы и неопределими.

Нарастващата сложност и динамика на контекста на военните операции, както и непредсказуемостта на противника, създават голямо търсене на ефективност и ефикасност на процеса на разузнаване за доставяне на технологии, които могат да бъдат внедрени в този процес.

Заклучение

Тенденциите в съвременната среда за сигурност, наложени от бързото развитие на съвременните технологии, изискват нов дизайн на разузнавателния цикъл, нови условия и нови методи за бъдещи начини за водене и реализиране на разузнавателния цикъл, като предоставят нова перспектива за използване на съвременните технологии, автоматизации и прилагането на изкуствен интелект в тази изключително важна сфера.

От практикоприложна гледна точка, с цел подобряване на разузнавателния процес, могат да бъдат дадени известен брой направления, които биха спомогнали бъдещата информационно-организационна дейност на разузнавателните агенции с цел по-добра адекватност в новите условия. Те се изразяват както следва:

- рационализиране на усилията и възможностите;
- намаляване на дублирането на едни и същи функции;
- предоставяне на по-последователна разузнавателна картина, т.е. да не се „работи на парче“;
- активиране на нови разузнавателни функции;
- окомплектоване с личен състав и оптимизиране на оборудването и техническите функции;
- постигане на сигурност и защита на системите, непозволяваща противникови атаки върху уязвимости свързани с разузнавателните структури;
- изграждане на доверие в партньорите и съюзниците;
- подобряване на съществуващите възможности с цел увеличаване на базата данни, търсенето в нея чрез автоматизирани системи и изкуствен интелект;
- разширяване използването на данни и информации, добивани от наземното наблюдение, радиолокационното, морското, включително и космическото, които да са в почти реално време, с цел подобряване ситуационната осведоменост за средата на сигурност;
- преразглеждане на техническата база и оперативната съвместимост на информационно-технологичните системи и управлението на данни;
- задълбочаване на сътрудничеството между цивилното и военното разузнаване на национално ниво, което ще спомогне за по-последователни, актуални, качествени и своевременни оценки, а така също – и тяхното своевременно предоставяне на вземащите решения;
- постигане на общо становище между службите за сигурност за преодоляване на различията в отделните култури „необходимост от споделяне“ и „необходимост да се знае“, съдържащи се в контекста на крайния техен информационен продукт. Това ще доведе до нова релевантност на разузнавателния процес в новата съвременна среда за сигурност;
- акцентиране върху новите съвременни хибридни и киберзаплахи, които вече придобиват ежедневно присъствие и оказват съществено влияние и значение на съвременната разузнавателна дейност.

Изразените становища по отношение на направленията за бъдеща работа съдържат лично мнение на автора и не ангажират мнението на горепоменатите структури.

ЛИТЕРАТУРА

1. David Shedd [former Deputy Director of the Defense Intelligence Agency (DIA), retired U.S. intelligence officer, 27 and 28 May 2020]. *NATO STO Research Task Group (RTG)*. Available from: <https://www.sto.nato.int/Lists/STONewsArchive/displaynewsitem.aspx?ID=552> [Посетен на 24.01.2022].

2. *Intelligence Services, Roles and responsibilities in good security sector governance*. Available from: https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_BG_12_Intelligence%20Services.pdf, [Посетен на 04.02.2022]
3. Нинов, Мариан. *Военнополитическо прогнозиране чрез анализ на национални доктрини*. София: Авангард Прима, 2020. стр.36. ISBN 978-619-239-479-0.
4. *Joint Publication 2-0, Joint Intelligence*, 22.10.2013, Available from https://irp.fas.org/doddir/dod/jp2_0.pdf
5. Гинев, Д. *Изграждане на граждански способности за отбрана на страната*. София: Алфа визия, 2020, стр.13. ISBN 978-619-7595-00-0.
6. Stoltenberg J. *Cyber Defence Pledge Conference*. London, 23 May 2019, OTAN, Available from: NATO – Opinion: Remarks by NATO Secretary General Jens Stoltenberg at the Cyber Defence Pledge Conference, London, 23-May-2019, [Посетен на 06.02.2022].
7. Available from: <https://img3-freepng.ru, intelligence-cycle-5bDedff82569d1.1414678015277014961533.png>
8. Robiah Yusof, *Cyber Threat Intelligence–Issue and Challenges*. *Indonesian Journal of Electrical Engineering and Computer Science*, Vol. 10, No. 1, April 2018, pp. 371–379 ISSN: 2502-4752, DOI: 10.11591/ijeecs.v10.i1.pp371-379, (PDF) *Cyber Threat Intelligence–Issue and Challenges* Robiah Yusof – Academia.edu
9. *Cyber Threats and NATO 2030: Horizon Scanning and Analysis* A. Ertan, K. Floyd, P. Pernik, T. Stevens, 2020 by NATO CCDCOE Publications, ISBN (pdf): 978-9916-9565-1-9, Available from: *Cyber-Threats-and-NATO-2030_Horizon-Scanning-and-Analysis(2).pdf* [Посетен на 05.02.2022].
10. *Recorded Future, What is Threat Intelligence*. Available from: <https://www.recordedfuture.com/threat-intelligence/>, [Посетен на 20.01.2022]

REFERENCES

1. David Shedd [former Deputy Director of the Defense Intelligence Agency (DIA), retired U.S. intelligence officer, 27 and 28 May 2020]. *NATO STO Research Task Group (RTG)*. Available from: <https://www.sto.nato.int/Lists/STONewsArchive/displaynewsitem.aspx?ID=552> [last visited: 24.01.2022].
2. *Intelligence Services, Roles and responsibilities in good security sector governance*. Available from: https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_BG_12_Intelligence%20Services.pdf, [last visited: 04.02.2022]
3. Ninov, Marian. *Voennopoliticheskoprognozirane chrez analiz na natsionalni doktrini*. Sofia: Avangard Prima, 2020. str.36, ISBN 978-619-239-479-0.
4. *Joint Publication 2-0, Joint Intelligence*, 22.10.2013, Available from https://irp.fas.org/doddir/dod/jp2_0.pdf
5. Ginev, D. *Izgrazhdane na grazhdanski sposobnosti za otrana na stranata*. Sofia: Alfa vizia, 2020, str.13. ISBN 978-619-7595-00-0.
6. Stoltenberg J. *Cyber Defence Pledge Conference*. London, 23 May 2019, OTAN, Available from: NATO – Opinion: Remarks by NATO Secretary General Jens Stoltenberg at the Cyber Defence Pledge Conference, London, 23-May-2019, [last visited: 06.02.2022].
7. Available from: <https://img3-freepng.ru, intelligence-cycle-5bDedff82569d1.1414678015277014961533.png>
8. Robiah Yusof, *Cyber Threat Intelligence–Issue and Challenges*. *Indonesian Journal of Electrical Engineering and Computer Science*, Vol. 10, No. 1, April 2018, pp. 371–379 ISSN: 2502-4752, DOI: 10.11591/ijeecs.v10.i1.pp371-379, (PDF) *Cyber Threat Intelligence–Issue and Challenges* Robiah Yusof – Academia.edu
9. *Cyber Threats and NATO 2030: Horizon Scanning and Analysis* A. Ertan, K. Floyd, P. Pernik, T. Stevens, 2020 by NATO CCDCOE Publications, ISBN (pdf): 978-9916-9565-1-9, Available from: *Cyber-Threats-and-NATO-2030_Horizon-Scanning-and-Analysis(2).pdf* [Poseten na 05.02.2022].
10. *Recorded Future, What is Threat Intelligence*. Available from: <https://www.recordedfuture.com/threat-intelligence/>, [last visited: 20.01.2022]

ЧОВЕШКИЯТ ФАКТОР В АВИАЦИЯТА – ОТ ПЪРВИЯ ПОЛЕТ ДО ДНЕС

д-р Маргарита Куманова

Военна академия „Г. С. Раковски“, *m.kumanova@rmdc.bg*

Резюме: Настоящият доклад представя появата и развитието на идеята за човешкия фактор в авиацията и проследява еволюцията му във времето – от понятие в управлението на риска и безопасността до мета-наука, изучаваща отношението на човешкия елемент в жизнения цикъл на всяка система.

Ключови думи: *авиация; човешки фактор; исторически преглед*

HUMAN FACTORS IN AVIATION – SINCE THE FIRST FLY TILL TODAY

Margarita Kumanova, PhD

Rakovski National Defence College

Sofia, Bulgaria

E-mail: *m.kumanova@rmdc.bg*

Abstract: The paper presents the appearance and development of the idea of the human factors in aviation and traces their evolution over the time – from a concept in risk and safety management to a meta-science that studies the relationship among human and system elements in the life cycle of any system.

Keywords: *aviation; human factor; historical overview*

*„От гледна точка на авиационните инженери, пилотите притежават
неограничени способности да обкръжат нещата.*

*От гледна точка на пилотите, оборудването на пилотските кабини
съдържа неограничен потенциал да им създава неприятности“*

Сидни Декър

Увод

С бегъл поглед към недалечното минало се вижда, че за последните 250 години човечеството преживява революционен период на развитие в обществено-икономическата, производствената и технологичната сфера. Твърде бързо човекът бива въвлечен в бурен вихър от технологии, довчера познати само от научнофантастичните романи. И така внезапно „**съвременният човек се оказва като дете в сложно пространство за игра, в което едва се ориентира, а трябва да гарантира не само собственото си оцеляване, но и съхраняването на средата**“¹, а колкото по-сложна е тя, толкова провалите са по-гръмки и последиците от тях – по-сериозни.

Анализът на причините за възникване на провал; механизмите, по които той се развива; потенциалът за разрушение, който притежава; управлението на риска и безопасността в сложния свят, отдавна прекращват границите на науката, такава каквато я познаваме и налагат да се търсят обяснения и решения в сложни интердисциплинарни взаимовръзки и мета-науки.

Назад в историята

От създаването си до днес авиацията е образец за технологии и въплъщение на бъдещето. Благодарение на човека този сложен конгломерат от технологии, комуникации, правила, разнопосочни цели и конфликти се превръща във функционираща система. Идеята за човешкия фактор имплицитно е заложена хилядолетия назад в зората на разумното човешко битие. Търсенията в тази област се коренят в осъществяването на мечтата на човек да полети (фиг. 1).

Съдържателно съвременната идея за човешкия фактор води началото си от бойната авиация и по-конкретно – от разследването на авиационните произшествия.



Фиг. 1. Назад в историята на човешкия фактор

От първия полет до Първата световна война

По време на Първата Световна война самолетът заема своето място на бойното поле и бързо се превръща от средство за разузнаване в оръжие. Загубата на пилотски състав и летателна техника пряко се отразяват върху способностите на авиационното формование, затова и интервалът на допустимата грешка при изпълнение на бойни летателни задачи е малък. Полетите са сложни по отношение на височини, маневри, брой на летателни апарати в непосредствена близост, използване на авиационно въоръжение, физическо и психическо натоварване (и претоварване), опасности за здравето и живота.

Наблюденията и анализите на мисиите в следвоенния период показват нещо любопитно: едва два процента от жертвите и загубите на техника могат да се класифицират като бойни загуби, около осем процента са загуби поради технически неизправности и почти деветдесет процента са в следствие на „индивидуални недостатъци“ на пилотите. Като под израза „индивидуални недостатъци“ се визират грешки във възприемането, пространствена дезориентация, липса на решение, ненавременни или неточни решения за съответната ситуация. В тези анализи се открива първообразът на човешкия фактор, като в тази си част, съдържателно, понятието се доближава в много голяма степен до авиационна психология, такава, каквато я познаваме днес.

Между двете световни войни

Вторият период в историята на човешкия фактор е белязан с едно събитие от изключителна важност в развитието на авиацията. През 1930 г. Едуин Алберт Линк патентова в Съединените американски щати т. нар. „синя кутия“ – първият симулатор-тренажор за обучение на пилоти. Чрез изобретението на Линк се въвежда принципно нов подход в обучението и практическата подготовка на летците, който е от особено значение, когато е невъзможно провеждането на визуални полети и се налага пилотаж по прибори. При този тип обучение (фиг. 2) значително се подобрява изпълнението на пилотите в полет², осигуряват се способности да се проиграт набор от потенциално възможни комплексни ситуации. Подготовката на летци на симулатор-тренажор осигурява натренираност при определено ниво на реализъм – безопасно, на земята и под наблюдението на вече опитни инструктори. Осигурява се възможност да се идентифицират и коригират своевременно грешки както във възприемането на обстановката, така и във взетите решения и тяхната реализация.

По отношение на развитието на човешкия фактор тази стъпка измества същността на концепта от психология към ергономия. Знанието и изследванията за повишаване на авиационната безопасност за този период са в полето на ергономията и дизайна на работното пространство.



Фиг. 2. Инструктори проследяват обучение в тренажора на Е. А. Линк

От Втората световна война до 1970 година

През 40-те години на миналия век за първи път неофициално Британските кралски военновъздушни сили споменават понятието „**човешки фактор**“, но едва през 1957 г. то е вписано като понятие в официален доклад от разследване на авиационно произшествие.

След Втората световна война се наблюдава период на бурен технологичен подем, авиацията все повече напуска военната и навлиза в гражданската сфера. До презумпцията за съхраняване на способностите на авиационното формование, дори с по-голяма тежест, се нарежда и презумпцията за съхранение на живота. Въпросите за безопасността и надеждността придобиват нови и още по-значими измерения. С всеки следващ превозен пътник или товар цената на безопасността се покачва.

В този период обхватът на човешкия фактор се разширява до по-добър подбор на хората в авиацията, извежда се на преден план идеята, че за безопасното изпълнение в сложната операторска дейност (каквато по същността си е дейността на пилота) е необходимо да бъдат селектирани хора с конкретни когнитивни възможности. Подборът се поставя на научна основа и през 1946 г. се открива първият „Институт по авиация“ към Университета в Илинойс (САЩ). Човешкият фактор отново се обръща към психологията, като фокусът на вниманието остава върху отделния пилот със съответните възможности и ограничения на личността.

Ера на човешкия фактор

В края на 70-те години на миналия век, с развитието на инженерните науки и техниката, обяснимо намалява дялът на авиационните инциденти по технически причини до 15%. Постигнато е приемливо ниво на техническа безопасност, повишава се надеждността на системите и се стига до заключението, че човешката грешка е водеща в причините за летателните произшествия. Статистическият дял на човешката грешка е в интервала между 70 и 80 процента. Изследователите на авиационните инциденти постепенно започват да се фокусират върху специалните мерки за намаляване броя на грешките, допускани от операторите (пилоти, ръководител-полети, авиационен инженерно-технически състав и т.н.). Полагат се множество усилия за елиминирането им, но въпреки това човешкият фактор остава водеща причина за авиационните произшествия. Човекът продължава да е в центъра на вниманието, но вече не само като личност със своите индивидуални особености, а като част от екип/екипаж/група.

Тази осъзната необходимост от изучаване и подобряване на изпълнението на групата се материализира в т. нар. „Управление на ресурсите на екипажа (CRM)“, целящо развиване и усъвършенстване

на нетехническите умения на персонала. Обучението по CRM (Cockpit Resource Management) възниква като система за обучение на летателния състав, а по-късно еволюира в обучение на целия кабинен състав (Crew Resource Management), като обхваща и останалите членове на екипажите в гражданската авиация. Ползата от това знание е оценена и за кратко време обученията се превръщат в норма и стават задължителни дори за авиационния инженерно-технически състав. А Европейската асоциация за авиационна безопасност (EASA) задължава компаниите да имат програми за обучение на екипажите и персонала по допълнителни (нетехнически) умения^{3,4} и стриктно проследява тяхното изпълнение.

Организационна ера

От 1990 година до наши дни идеята за управление на безопасността се развива в посока на управление на грешките и заплахите, присъщи на средата. В основата на тази идея е фактът, че средата със своите сложност и комплексност ще влияе върху поведението на човека-оператор. С „организационната ера“ се свързва разбирането за значението на организацията за осигуряване на авиационната безопасност. Въвежда се формулировката „произшествие по организационни причини“, отчита се влиянието на организационната култура и политика върху безопасността на полета.⁵

Усилията в посока намаляване на човешката грешка чрез системен подход са отразени и в по-известните дефиниции на човешкия фактор в авиацията, като всяка една се опитва максимално подробно и в същото време стегнато и еднозначно да включи многообразието от научни области и посоки на изследване в себе си.

Съгласно определението на Федералните авиационна администрация на САЩ човешкият фактор е „свкупност от мултидисциплинарни **усилия**: събиране, анализиране и прилагане на информация за човешките възможности и ограничения и прилагането на това ново знание в оборудване, системи, съоръжения, процедури, работни места, среда, обучение, персонал и управление на персонала за безопасно, удобно и ефективно функциониране на човека“⁶.

В книгата си Human Factors in Aviation професор Елвин Едуардс определя човешкия фактор като „**технологията**“, оптимизираща връзката между хората и техните дейности чрез интегриране на хуманитарните науки в системното инженерство“⁷.

Международната организация за гражданска авиация дефинира човешкия фактор като **наука** за хората; за хората в средата, в която те живеят и работят, за тяхното взаимодействие с машините, нормативите, окръжаващата среда и не на последно място – за междуличностните им отношения. Целта е по-голяма ефективност и повече безопасност⁸.

Независимо в колебанията в дефинициите дали човешкият фактор е „**усилие**“, „**технология**“ или „**наука**“ в цялостната авиационна система са утвърдени редица модели за изследването му, които да дават възможност за неговия анализ и намират общо в поне две основни направления:

- от една страна, човешкият фактор е свкупност от знания, умения, факти, изследвания и анализи на много хуманитарни науки, които имат за цел да изведат най-доброто по отношение на функциониране на човека-оператор;

- от другата страна са поставени инженерните науки, ергономията с предложенията за най-добрият дизайн, оборудване, правила, процедури и т.н. характеристики на работната среда.

С поглед към бъдещето

В този смисъл, историческата задача на „Човешкият фактор“ да разбере „**защо хората правим това, което правим, с основна цел да се променя и приспособява средата, в която работим и съответно да формираме своите оценки и действия**“⁹ намира решение в различни форми на обучение и тренингови програми, предлагани от авиационните субекти на различни нива.

Все повече са лабораториите, които работят в областта на човешкия фактор, а много университети (основно в САЩ, Великобритания и Германия) вече предлагат интердисциплинарни магистърски програми по „Човешки фактор“ в авиацията (или във високонадеждните организации) за инженери, психолози, медици. Знанията и уменията, които се придобиват в такава магистърска програма надхвърлят пределите на авиационната наука и професия и ще са все по-високо оценени предвид сложния и все по-непредсказуем свят, в който живеем.

Една бъдеща магистърска програма по „Човешки фактор в авиацията“ би била възможност Военна академия „Г. С. Раковски“ да използва ресурса си и съвместно със своите партньори да предложи ново приложно знание на образователния пазар.

Заклучение

В заключение може да се обобщи, че знанията за човешкия фактор отдавна са напуснали пределите на авиацията и се отнасят към всички аспекти на функциониране на една високонадеждна система: идеен проект; дизайн; тестване и оценка на модела; правила и процедури; организация; технология; поддръжка; управление и контрол; обратна връзка; тенденции за развитие. По своята същност човешкият фактор е приложна мета-наука, чиято цел е осигуряване безопасно и надеждно функциониране на високонадеждните системи по отношение на човешкия елемент в жизнения цикъл на всяка система.

ЛИТЕРАТУРА

1. Thomas, M. J. W. *Training and Assessing Non-Technical Skills. A Practical Guide*. Taylor & Francis Group, LLC, 2018.
2. *The Link Flight Trainer. A Historic Mechanical Engineering Landmark*. Roberson Museum and Science Center, Binghamton, New York, 2010.
3. Human Factors In Aviation. FAA/EASA part 147 Aircraft Type Training Company.
4. Aviation non-technical skills. Handbook, 2018.
5. Карева, Р. *Авиационна психология, Среда*. София: Военна академия „Г. С. Раковски“, 2019.
6. FAA Order 9550.8 *Human Factors Policy*.
7. CAP 719 *Fundamental Human Factors Concepts* (previously ICAO Digest No. 1).
8. ICAO, Circular 227.
9. Dekker, S. W. A. *The Field Guild to Understanding Human Error*. Aldershot, UK: Ashgate Publishing, 2006.

REFERENCES

1. Thomas, M. J. W. *Training and Assessing Non-Technical Skills. A Practical Guide*. Taylor & Francis Group, LLC, 2018.
2. *The Link Flight Trainer. A Historic Mechanical Engineering Landmark*. Roberson Museum and Science Center, Binghamton, New York, 2010.
3. Human Factors In Aviation. FAA/EASA part 147 Aircraft Type Training Company.
4. Aviation non-technical skills. Handbook, 2018.
5. Kareva, R. *Aviatsionna psihologia, Sreda*. Sofia: Voenna akademia „G. S. Rakovski“, 2019.
6. FAA Order 9550.8 *Human Factors Policy*.
7. CAP 719 *Fundamental Human Factors Concepts* (previously ICAO Digest No. 1).
8. ICAO, Circular 227.
9. Dekker, S. W. A. *The Field Guild to Understanding Human Error*. Aldershot, UK: Ashgate Publishing, 2006.

ОТБРАНИТЕЛНОТО ПЛАНИРАНЕ ЗА ПОДДЪРЖАНЕ И РАЗВИТИЕ СПОСОБНОСТИТЕ НА ВЪОРЪЖЕНИТЕ СИЛИ НА РЕПУБЛИКА БЪЛГАРИЯ

д-р Ганчо Душков

Военна академия „Г. С. Раковски“, *g.dushkov@rndc.bg*

Резюме: Анализирана е връзката на отбранителното планиране с развитието на отбранителните способности. Направен е анализ на реализирането им до 2020 г. и прогноза за тяхното развитие до 2032 г. в съответствие с констатираните области от дефицит на способности на въоръжени сили. Разгледани са основните инвестиционни и проекти за модернизация до 2020 г. и предстоящите, чиято реализация ще допринесе за развитие на нови способности до 2032 година.

Ключови думи: *отбранително планиране; минимални изисквания към способностите; дефицит от способности; балансиран отбранителни способности*

DEFENSE PLANNING TO MAINTAIN AND DEVELOP THE ABILITY OF THE BULGARIAN ARMED FORCES

Gancho Dushkov, PhD

Rakovski National Defence College

Sofia, Bulgaria

E-mail: *g.dushkov@rndc.bg*

Abstract: The connection of defense planning with the development of defense capabilities is analyzed. An analysis of their implementation by 2020 and a forecast for their development until 2032 has been made, in accordance with the identified areas of deficiency of aircraft capabilities. The main investment and modernization projects until 2020 and the forthcoming ones, the implementation of which will contribute to the development of new capabilities by 2032, are discussed.

Keywords: *defense planning; minimum capability requirements; capability shortages; balanced defense capabilities*

Съвременната среда на сигурност продължава да бъде сложна и динамично променяща се не само от международната обстановка¹, но и в резултат на нови предизвикателства, каквито са световната пандемична ситуация и войната между Русия и Украйна. Съществено влияние върху стратегическата среда на сигурност оказва пандемията от Covid-19. Тя показва глобалната уязвимост от разпространението на инфекциозни заболявания и последващите сериозни и дългосрочни отражения върху държавите, обществата и икономиките. Пандемията създаде предпоставки за рязък спад на икономическите показатели в световен мащаб, благоприятства разрастването на протекционистските политики и наложи преосмисляне на зависимостта на Европейския съюз от външни доставчици в стратегически отрасли.² Този процес продължава да се задълбочава и да придобива непредсказуеми последствия. В резултат на това заплахите за сигурността на страната стават все по-динамични и по-трудно предвидими, като дефинират голяма динамика в промяната на средата на сигурност. Интегрираното въздействие на съвременните предизвикателства създава обективни предпоставки за преосмисляне на съществуващите системи за национална и колективна сигурност и налага поддържане и изграждане на отбранителни способности, адекватни на новите условия. Програмите за превъоръжаване на въоръжените сили на държавите в глобален план с най-новите и върхови постижения в областта на науката и технологиите са показател за запазване ролята на военния инструмент като гарант за сигурността и отбраната.³

Изграждането на съвременни въоръжени сили е продължителен процес, който се реализира чрез отбранителното планиране. Това е основна дисциплина в НАТО и благодарение на този вид планиране се изграждат необходимите бъдещи способности на въоръжените сили и техните възможности за защита на териториалната цялост на страната. Отбранителното планиране се подразделя

на дългосрочно, средносрочно и краткосрочно планиране. Дългосрочното планиране е стратегическо планиране и обхваща продължителен период от време – десет и повече години. Това е комплексен процес, който осигурява рамка за развитие на въоръжените сили.³ Провежда се в обхвата на определен национален процес на отбранително планиране – стратегически преглед на сигурността и отбраната. В процеса на планиране се отчитат възможните предизвикателства на бъдещата среда на сигурност, политико-военните потребности и поетите съюзни ангажменти и възможностите за ресурсно осигуряване в рамките на предвидената ресурсна рамка. Неговото реализиране е трудно, предвид продължителността на периода, който обхваща, и необходимостта от предвиждане на бъдещия състав на въоръжените сили, структура, въоръжение и техника за успешно изпълнение на мисиите на въоръжените сили за защита на териториалната цялост на страната. Несигурността и динамиката на процесите са голямо предизвикателство при реализация на този вид планиране и взиманите решения в условия на недостатъчно определени параметри. Дългосрочното планиране на отбраната и въоръжените сили осигурява съответствие между целите на държавната политика в областта на отбраната с поддържането и изграждането на необходимите балансиран отбранителни способности за бъдещите предизвикателства пред сигурността. Този вид планиране е основата и стратегическата рамка за процесите на средно и краткосрочно планиране, чрез които се реализират зададените дългосрочни стратегически цели. Средносрочното планиране обхваща шестгодишен период и едногодишен период за краткосрочното планиране.

Отбранителните способности на въоръжените сили са основният компонент от системата за национална сигурност, която се определя от националните интереси и се осъществява при условията на колективната отбрана на съюзниците от Организацията на Северноатлантическия договор (НАТО), както и в рамките на Общата политика за сигурност и отбрана на ЕС.⁴ Защитата се осъществява в условията на чл. 5 от Вашингтонския договор и се изпълнява съвместно със сили и средства за колективна отбрана на НАТО (приетия пакет Цели за способности 2017 г.). Съгласно този пакет, ние сме приели за изпълнение до края на 2032 г. цели за способности с повишени изисквания и формирания за колективна отбрана.⁵ Пакетът Цели за способности 2017 от процеса на планиране на отбраната на Алианса осигурява приемственост и последователност с пакет Цели за способности 2013 за развитие на отбранителните способности на въоръжените сили. Фокусът беше поставен върху изграждането на силна колективна отбрана и капацитет за възпиране. Пакет Цели за способности 2017 осигурява изпълнението на операции за колективна отбрана и водене на бойни действия с висок интензитет.⁶ В тази връзка се повишиха изисквания към въоръжените сили, както следва:

- за Сухопътните войски акцент беше поставен върху изграждането на тежка механизирани бригада с необходимото бойно осигуряване и поддръжка;
- за Военновъздушните сили бяха определени като особено важни подготовката на силите за развързване и развитието на способности за системата за командване и управление;
- за Военноморските сили като приоритетни бяха определени развитието на морската ситуационна осведоменост, способностите за надводна борба и защитата на силите;
- за Силите за специални операции акцентът беше поставен върху развитието на способности на системата за командване и управление, а в групата на спомагателните способности – на тези за киберзащита, ЯХБЗ и КИС.

В резултат на променения фокус на Алианса към колективна отбрана вече над половината от декларираните ни сили са в блока от сили на НАТО с висока степен на готовност. Въпреки това ограниченият финансов ресурс предопредели все още да бъдат налични остарели платформи на въоръжение и техника, несъвместими с използваните в страните, членки на НАТО. Необходимо е предприемане на действия по придобиване и използване на съвременни високотехнологични образци от въоръжение и техника. Придобиването на нова транспортна техника ще осигури нормалното функциониране на линиите за логистично осигуряване при провеждане на операции.

В периода на изпълнение на „Програма за развитие на отбранителните способности на Република България 2020“ усилията бяха насочени към поддържане на съществуващите и постепено развитие на нови отбранителни способности, адекватни на тенденциите в развитието на средата на сигурност.⁶ Стартира едновременната реализация на трите основни инвестиционни проекта за модернизация, насочени към преодоляването на дефицита от критично необходими ключови способности.

Инвестиционен проект „Придобиване на нов тип боен самолет“ е във фаза „Изпълнение“. Изпълняват се четири международни договора за неговата реализация и доставка на осем броя самолети F-16 Block 70 с правителството на САЩ, по условията на програмата на САЩ за чуждестранни военни продажби (FMS). Първите два самолета се очаква да бъдат доставени през 2023 г., а останалите шест – през 2024 г.

Инвестиционен проект „Придобиване на многофункционален модул на патрулен кораб за ВМС“ е във фаза „Изпълнение“. На 12.11.2020 г. беше подписан Договор между Министерството на отбраната и Fr. Lürssen Werft за неговата реализация, като той се изпълнява съгласно разработения график. Двата кораба ще бъдат построени в Република България, като първият ще бъде предаден до края на 2025 г., а вторият – до края на 2026 г.

Инвестиционен проект „Придобиване на основна бойна техника за изграждане на батальонни бойни групи от състава на механизирани бригади“ е във фаза „Изпълнение“. Подготвена беше процедура за избор на изпълнител, но беше прекратена поради значителното превишаване в двете оферти на определената финансова рамка. В момента се извършва анализ на възможностите за реализация на проекта в определената финансова рамка без загуба на необходимите способности.

Инвестиционен проект „Придобиване на нови трикоординатни радары“ е от Категория 2 от Портфолиото поради липсата на финансово осигуряване. Той обаче е от изключителен приоритет за Министерството на отбраната и в частност за ВВС. През 2019 г. бяха изпратени запитвания за информация (RFI – Request for Information) към шест фирми, производители на радары. През април 2020 г. бяха изпратени допълнителни RFI до още две компании. В допълнение беше изпратено писмо – заявка (LOR for P&A) до САЩ, за предоставяне на информация за цени и наличности на нови трикоординатни радары. Предстои проектът за инвестиционен разход да бъде внесен за приемане от Министерския съвет и Народното събрание и осигуряване на необходимото финансиране.

Инвестиционен проект „Модернизация на фрегати клас E-71“ е във фаза „Изпълнение“. Към момента същият се изпълнява частично на основата на подписани рамкови споразумения, като няма подписано споразумение за ремонта на въоръжението на двата кораба. Основен проблем е липсата на достатъчно финансиране.

Инвестиционен проект „Криптографски мрежи и системи с интегрирано разпределение на ключови документи за защита на услуги в КИС (криптирани гласови комуникации)“ е във фаза „Изпълнение“. Изготвени са технически спецификации, Документ за инициране на проект (ДИП) и стартира процедура за избор на изпълнител. Основен проблем е липсата на достатъчно финансиране.

Инвестиционен проект „Киберзащита“ е във фаза „Изпълнение“. Основната част ще се реализира по FMF. Сключен беше договор със САЩ за финансиране и изграждане на „Оперативен център за киберотбрана на Министерство на отбраната“. През 2022 г. ще се извърши доставката на оборудването, а през 2023 г. – интегрирането и завършването на първи етап на проекта в съответствие с първия договор. За реализацията на втори етап предстои да се сключи нов договор по FMF.

Осигуряването на ритмично финансиране се очертава като основен проблем за успешната реализация на проектите от портфолиото на Министерството на отбраната. Този факт е индикатор за разминаване между нивото на амбиция по отношение на изграждане и развитие на отбранителни способности и възможностите на бюджета да осигури адекватни финансови ресурси.

Освен работата по основните проекти за превъоръжаване и модернизация на Българската армия, след период на отлагане стартира основният ремонт на танкове Т-72 и танкови мерници-далекомери за танкове Т-72, ремонтът на самолети МиГ-29 и СУ-25, както и капитално-възстановителният ремонт на вертолети Ми-24В и Ми-17. За ремонта на изстребителите МиГ-29, в изпълнение на сключеното на 21.03.2018 г. рамково споразумение с РСК „МиГ“ на стойност близо 81,5 млн. лв. без ДДС със срок на действие 48 месеца, бяха сключени договори, включващи доставка на имущество, ремонти на оборудване и на двигатели РД-33, контролно-възстановителни работи на 3 броя учебно-бойни изстребители МиГ-29УБ и др. Заради забавяне на изпълнението на договорите от страна на руската компания, Министерството на отбраната предава искане за изплащане на неустойки. В изпълнение на договор на стойност около 82,5 милиона лева без ДДС, подписан през 2018 г. с беларуския завод „Барановичи“, през 2020 г. в авиобаза „Безмер“ пристигнаха шест ремонтирани штурмови самолета СУ-25, а през февруари 2021 г. – и последните два. Удълженият с осем години ресурс на самолетите ще позволи воденето на интензивна подготовка на ле-

тателния състав от базата и повишаване на нивото на бойна подготовка. Модернизирани са системите, като са включени възможности за спътникова навигация. Разширени са възможностите за използване на ракетно въоръжение. Радиостанциите са подменени с нови, които позволяват едновременно връзка и прослушване на две честоти, включително и осъществяване на контакт със сухопътен и морски компонент. Това прави самолетите по-боеспособни и по-ефективни в изпълнението на основните задачи по осигуряване на непосредствена авиационна поддръжка, изолиране на района на бойните действия и подпомагане воденето на боя от формированията на сухопътни и военноморски подразделения и части.

На 9 декември 2020 г. Министерският съвет одобри проект за инвестиционен разход „Модернизация на танк Т-72 за нуждите на танковите формирования от Сухопътни войски“. На 16 декември 2020 г. между Министерство на отбраната и „ТЕРЕМ – ХОЛДИНГ“ ЕАД беше сключен договор за модернизация на 44 танка Т-72 за нуждите на танковите формирования от Сухопътни войски. Договорът предвижда и модернизация и на три командно-щабни машини МТ-ЛБ У. С реализацията на проекта се цели преодоляването на технологичното изоставане на танковите формирования по отношение на системите за управление на огъня, защитеност на комуникациите и ситуационната осведоменост. Чрез него също така ще се постигне оперативна съвместимост на силите и средствата както в национален, така и в съюзен формат. Това от своя страна ще доведе до изпълнение на поетите съюзни ангажменти на страната. В периода януари 2019 г. – юли 2020 г. в завод „ТЕРЕМ – Хан Крум“ ЕООД в Търговище бяха извършени ремонти на 13 танка Т-72 и 60 броя танкови мерник-далекомери. Сключени бяха нови споразумения и договори за ремонт и поддръжка на старите съветски самолети, съответно с Руската федерация за МиГ-29 (2016 г. и 2018 г.) и с Беларус за СУ-25 (2018 г.). В контекста на тази негативна оценка следва да се отчитат някои обективни обстоятелства. Въпросните договори бяха сключени с цел поддържане на необходими за въоръжените сили отбранителни способности, за да могат те да продължат да изпълняват конституционните си задължения. До осигуряването и въвеждането на въоръжение на новите самолети F-16 е наложително да бъдат използвани наличните, за да не бъде допуснат дефицит от критично важни способности.

Поставената в Програма 2020 цел да бъде премахната зависимостта на отбранителните ни способности от страни извън НАТО и Европейския съюз не беше изпълнена. През периода на изпълнение на Програма 2020 се запази зависимостта на Република България от Руската федерация за ремонт и поддръжка на останала на въоръжение стара и оперативно несъвместима съветска техника, което е сериозен проблем при поддържане на придобитите способности.

С решение на Министерския съвет № 26/18.01.2019 год. в Република България беше иницииран и проведен Стратегически преглед на системата за защита на националната сигурност и Стратегически преглед на отбраната. Провеждането на този преглед е нормативно изискване^{7,8} в съответствие със Закона за управление и функциониране на системата за защита на националната сигурност и на Закона за отбраната, а и необходимост⁹ определена от промените в средата на сигурност, от членството на страната ни в НАТО и Европейския съюз.

По време на прегледа бяха разработени шест планиращи сценария, покриващи общите ситуации за използване на въоръжените сили при разрешаване на кризи и конфликти. На тяхна база бяха разработени концепциите, които дадоха възможност да бъдат определени задачите на въоръжените сили. Беше разработен „Доклад за резултатите от проведения Стратегически преглед на отбраната“. След приемането му беше създаден основополагащият стратегически документ за развитие на въоръжените сили – „Програма за развитие на отбранителните способности на въоръжените сили на Република България 2032“, чрез която се реализира процесът на стратегическо преосмисляне на отбранителната политика и се поставиха насоките за изграждане на адекватни на предизвикателствата на стратегическата среда отбранителни способности.

Тя определя минимално необходимите отбранителни способности на въоръжените сили за изпълнение на приетото ниво на политическа амбиция за тяхното използване. Зададени бяха параметрите за развитие и основните насоки за изграждане на отбранителните способности на въоръжените сили до 2032 г. чрез ангажиране на политическите, икономическите, технологичните, информационните, военните и гражданските ресурси на страната. Ще продължат да се поддържат императивите на значителна част от изградените способности, като се развият и нови в съответствие с констатираните дефицити по време на прегледа.¹⁰ Дефинираните минимални военни изисквания бяха извършени в съответствие с разработените сценарии, основната мисия на въоръжените сили „Отбрана“ и изискванията на приетия пакет „Цели

за способности – 2017". Те дават възможност да се гарантира успешното изпълнение на задачите по всяка мисия на въоръжените сили. Тези изисквания са формулирани на базата на планиращи сценарии, обхваща областите на използване на въоръжените сили като основен военен инструмент за гарантиране суверенитета в национален формат и защитата на териториалната цялост на страната в съюзен формат. Минималните военни изисквания към въоръжените сили налагат ускоряване на превъоръжаването/модернизацията за постигане на оперативна съвместимост и повишаване на ефикасността на разходваните ресурси за отбрана. Разработената програма интегрира протичащите процеси на стратегическо преосмисляне в НАТО и Европейския съюз и е база за разработване на План за развитие на въоръжените сили.

По време на прегледа, на базата на разработените сценарии и концепции за провеждане на операции по тях, бяха дефинирани 188 минимално необходими способности на въоръжените сили, както и основните военни формирования в тях, които да ги изграждат, развиват и поддържат.¹¹ Предвидено е да бъдат развивани способности за гарантиране на суверенитета, сигурността и независимостта на страната, гарантиране на териториалната цялост и ангажиментите към НАТО. Това ще осигури изграждане и развитие на способности в четирите измерения на бойното пространство, като по отношение на петото – космическото пространство, ще се разчита да бъдат използвани споделени способности на съюзниците от НАТО.

Извършеното остойностяване на дефинираните минимално необходими способности на въоръжените сили, в съответствие със средносрочната прогноза на министерство на финансите, показва че те не могат да бъдат финансово осигурени. Това наложи приоритизиране и разсрочване, като при отчитане на увеличения процент на разходите за отбрана¹² е възможно да бъдат финансово осигурени 38 от дефинираните минимално необходими способности и то до края на 2032 година. В резултат на извършеното проучване на възможностите за използване на допълнителен финансов ресурс по проекти и инициативи на НАТО и Европейския съюз беше предвиден такъв, който, заедно с прогнозния финансов ресурс на национално ниво, даде възможност за включване в „План за развитие на въоръжените сили на Република България до 2026 г.“ на 25 способности за изграждане и развитие. От тези способности с приоритет за въоръжените сили е реализирането на следните проекти:

- придобиване на трикоординатни радары за близко и далечно наблюдение;
- придобиване на дистанционно управляеми системи във видовете въоръжени сили, включително и за осигуряване на системата за командване и управление на стратегическо и оперативно ниво;
- развитие на способностите за участие на Република България в Инициативата за готовност на НАТО;
- изграждане на система за ПВО на механизирена бригада и ПВО на ключови военни инфраструктурни обекти;
- развитие на способностите, включени в предложенията на НАТО за пакет Цели за способности;
- развитие на способностите за поразяване с високоточни оръжия в цялата зона на операцията.

Изграждането, поддържането и развитието на съвременни и боеспособни въоръжени сили може да бъде реализирано с целенасочено и последователно национално планиране за придобиване на съвременни отбранителни способности в сферата на отбраната и сигурността в съответствие с процеса на отбранително планиране на НАТО, процеса на развитие на отбранителни способности в Европейския съюз и адекватно ресурсно осигуряване. Това ще даде възможност за пълна реализация на планираните отбранителни способности на въоръжените сили за изпълнение на задачите по отбрана на страната и на задълженията на Република България в системата за колективна сигурност и отбрана.

ЛИТЕРАТУРА

1. *Strategic Foresight Report*, 2021.
2. Доклад за състоянието на отбраната и въоръжените сили през 2020 г.
3. Концепция за дългосрочно планиране на отбраната. Министерство на отбраната, 2021.
4. Закон за отбраната и въоръжените сили на Република България, чл. 3 (1) и (2) и чл. 4 (1) и (2). *Държавен вестник*, бр. 35 от 12.05.2009.
5. Запрянов, А. *Встъпително слово на конференция на AFCEA Българските задачи и отговорности в европейската сигурност и отбрана*. Секция „София“, 2017. [онлайн] www.afcea-bg.org
6. Оценка за изпълнението на „Програма за развитие на отбранителните способности на въоръжените сили на Република България 2020“, 2021.

7. Закон за управление и функциониране на системата за защита на националната сигурност, чл. 7 (1). *Държавен вестник*, 31 юли 2015.
8. Закон за отбраната и въоръжените сили на Р. България, чл. 27, т.7, *Държавен вестник*, бр. 35 от 12.05.2009.
9. Алашки, М. Стратегически преглед на Системата за защита на националната сигурност в Министерство на отбраната. В: *Сборник с доклади от Международна научна конференция „Дългосрочни предизвикателства за развитие на сигурността и изграждане на отбранителните способности на въоръжените сили“*, I част. София: Военна академия „Г. С. Раковски“, 2019 г. ISSN 978-619-7478-35-8.
10. Душков, Г. И. Надграждане на способностите на въоръжените сили до 2032 год. Научна конференция „Дългосрочни предизвикателства за развитие на средата на сигурност и изграждане на способности на въоръжените сили“, 12 – 14.11.2019 г., Военна академия „Г. С. Раковски“. В: *Сборник доклади от годишната научна конференция на Военна академия „Г. С. Раковски“, втора част*, 2019 г., стр. 24-29, ISBN 978-619-7478-35-8.
11. *План за развитие на въоръжените сили на Република България до 2026 г.*
12. *Национален план за повишаване на разходите за отбрана на 2% от brutния вътрешен продукт на Република България до 2024 г.*, 2017 г.

REFERENCES

1. *Strategic Foresight Report*, 2021.
2. *Doklad za sastoyanieto na otbranata i vaorazhenite sili prez 2020 g.*
3. *Kontseptsia za dalgosrochno planirane na otbranata*. Ministerstvo na otbranata, 2021.
4. Закон за отбраната и vaorazhenite sili na Republika Bulgaria, chl. 3 (1) i (2) i chl. 4 (1) i (2). *Darzhaven vestnik*, br. 35 ot 12.05.2009.
5. Zapryanov, A. *Vstapitelno slovo na konferentsia na AFSEA Balgarskite zadachi i otgovornosti v evropeyskata sigurnost i otbrana*. Sektsia „Sofia“, 2017. [onlayn] www.afcea-bg.org
6. *Otsenka za izpalnenieto na „Programa za razvitie na otbranitelnite sposobnosti na vaorazhenite sili na Republika Bulgaria 2020“*, 2021.
7. Закон за управление i funktsionirane na sistemata za zashtita na natsionalnata sigurnost, chl. 7 (1). *Darzhaven vestnik*, 31 yuli 2015.
8. Закон за otbranata i vaorazhenite sili na R. Bulgaria, chl. 27, t.7, *Darzhaven vestnik*, br. 35 ot 12.05.2009.
9. Alashki, M. Strategicheski pregled na Sistemata za zashtita na natsionalnata sigurnost v Ministerstvo na otbranata. In: *Sbornik s dokladi ot Mezhdunarodna nauchna konferentsia „Dalgosrochni predizvikatelstva za razvitie na sigurnostta i izgrazhdane na otbranitelnite sposobnosti na vaorazhenite sili“*, I chast. Sofia: Voenna akademia „G. S. Rakovski“, 2019 g. ISSN 978-619-7478-35-8.
10. Dushkov, G. I. Nadgrazhdane na sposobnostite na vaorazhenite sili do 2032 god. Nauchna konferentsia „Dalgosrochni predizvikatelstva za razvitie na sredata na sigurnost i izgrazhdane na spo-sobnosti na vaorazhenite sili“, 12 – 14.11.2019 g., Voenna akademia „G. S. Rakovski“. In: *Sbornik dokladi ot godishnata nauchna konferentsia na Voenna akademia „G. S. Rakovski“, vtora chast*, 2019 g., str. 24-29, ISBN 978-619-7478-35-8.
11. *Plan za razvitie na vaorazhenite sili na Republika Bulgaria do 2026 g.*
12. *Natsionalen plan za povishavane na razhodite za otbrana na 2% ot brutnia vatreshen produkt na Republika Bulgaria do 2024 g.*, 2017 g.

ИЗПОЛЗВАНЕ НА ВЪОРЪЖЕНИТЕ СИЛИ В КОНТЕКСТА НА КОЛЕКТИВНАТА ОТБРАНА НА СТРАНАТА

майор Лъчезар Русеков

Военна академия „Г. С. Раковски“, *l.p.rusekov@rmdc.bg*

Резюме: Въоръжените сили са гарант за суверенитета, сигурността и независимостта на страната. В контекста на колективната отбрана българските въоръжени сили участват в съвместни и съюзни операции, като целта е да се реагира адекватно на пълния спектър от заплахи и въздействия от противостоящи сили, посредством нанасяне на ефективно поражение, чрез съчетаване на възможностите на видовете въоръжени сили да влияят на факторите на съвременната оперативната среда.

Ключови думи: *въоръжени сили; Вашингтонски договор; съюзна съвместна операция; национална съвместна операция; съвместни сили; информационни операции стратегическо развързване; използване на въоръжените сили*

USE OF THE ARMED FORCES WITHIN THE CONTEXT OF THE COUNTRY'S COLLECTIVE DEFENSE

Major Rusekov Lachezar

Rakovski National Defence College

Sofia, Bulgaria

E-mail: *l.p.rusekov@rmdc.bg*

Abstract: The armed forces are a guarant for country's sovereignty, security and independence. Within the context of collective defense, Bulgarian Armed Forces participate in joint and allied operations with the aim of responding adequately to the full spectrum of threats and impacts from opposing forces, by inflicting effective strike, by combining the capabilities of the armed forces to impact to operating environment factors.

Keywords: *Armed Forces; Washington Treaty; Allied Joint Operation; National Joint Operation; Joint Forces; Information Operations Strategic Deployment; Use of Armed Forces*

Отбраната е основна държавна дейност, чрез която се гарантира националната сигурност, суверенитетът, териториалната цялост и независимостта на Република България. Тя осигурява създаване, поддържане и използване на необходимите ресурси на страната за формиране на стабилна среда за сигурност посредством ефективно използване на националните отбранителни способности.¹ Ефективната отбрана на страната в съвременни условия се реализира посредством военната мощ², която се създава и поддържа, за да неутрализира военните заплахи. Военната мощ е показател за способността на страната да постига военни цели, а като такава е основен фактор за гарантиране на националната сигурност. Основен инструмент на военната мощ са въоръжените сили, които гарантират суверенитета, сигурността и независимостта, и защитават териториална цялост на Република България, като споделят отговорностите със съюзниците от НАТО и Европейския съюз чрез ефективен принос към колективната отбрана, в условията на чл. 5 от Северноатлантическия договор.³

В контекста на колективната отбрана българските въоръжени сили участват в съвместни и съюзни операции, като целта е да се реагира адекватно на пълния спектър от заплахи и въздействия от противостоящи сили посредством нанасяне на ефективно поражение чрез съчетаване на възможностите на видовете въоръжени сили да влияят на факторите на съвременната оперативната среда. Използването на националните въоръжени сили в рамките на колективната отбрана на страната се осъществява чрез адаптиране на националните схващания за провеждане на операции с тези на НАТО и на страните членки за предприемане на синхронизирани действия съгласно договореностите във Вашингтонския договор⁴.

В рамките на чл. 5 от Вашингтонския договор и според схващанията на НАТО за колективна отбрана всеки акт на агресия срещу страна, членка на Алианса, се възприема като въоръжена атака сре-

щу Съюза и следва ответна реакция. Останалите страни членки предприемат действия, каквито считат за необходими да защитят атакувания съюзник.⁵ Тези действия трябва да бъдат предприети както индивидуално, така и колективно, в рамките на съюзна съвместна операция. По своята същност **съюзната съвместна операция** е *съвкупност от съгласувани и взаимосвързани подчинени бойни и небойни операции и действия, провеждани от многонационалните съвместни оперативни сили по единна концепция и план за изпълнение на определена военна мисия в определени пространствени и времеви рамки*. Провежда се в Зона за съвместни операции, която е временен район, определен от върховния главнокомандващ на съвместните сили. Тази зона може да включва цялата или част от територията, въздушното и морските пространства на една или няколко страни, членки на НАТО, и в нея се водят активни бойни действия. В тази зона назначеният за командващ на съвместните сили планира и изпълнява конкретната мисия.

Съгласно плановете за развърщане за изпълнение на задачи, касаещи колективната отбрана на Алианса на територията на Европа, **съюзната съвместна операция може да бъде обособена в шест фази:**

ФАЗА 1 – Предупреждение и активация. В тази фаза се демонстрира решимостта и единството на Алианса в ранен етап на кризата. Целта е да се вземе решение за военен отговор и да се формират необходимите за това сили.

ФАЗА 2 – Предотвратяване на конфликта. Целта на фазата е развърщане на многонационални съвместни сили на територията на страната домакин за демонстриране на решимостта и единството на Алианса и предотвратяване ескалацията на кризата и на конфликта във възможно най-ранен етап. Развърщането на съюзните сили може да завърши по всяко време при намаляване на напрежението и преодоляване на кризата, след което се преминава директно към заключителна фаза. В случай на по-нататъшно ескалиране на кризата, операцията преминава във ФАЗА 3.

ФАЗА 3 – Разрешаване на кризата посредством развърщане на допълнителни съюзни сили. Фазата може да завърши с преустановяване на агресивните действия срещу страната домакин или с нарушаването на нейната държавна граница, с което операцията навлиза във ФАЗА 4.

ФАЗА 4 – Отбрана. Смисълът на фазата е защита на суверенитета и териториалната цялост на страната домакин. Целта е да се отрази агресията и да се възстанови териториалната цялост на страната домакин, чрез провеждането на съюзна съвместна отбранителна операция. ФАЗА 4 започва с началото на агресията на противостоящите сили и завършва с гарантиране териториалната цялост на страната домакин, с което операцията навлиза във ФАЗА 5.

ФАЗА 5 – Деескалация. За понижаване на напрежението в зоната на операция се прилагат съответните мерки и се създават условия за политическо разрешаване на кризата. Постепенно се намалява степента на готовност на силите като целта е поетапно изтегляне от зоната. Фазата завършва с готовността на силите на НАТО за изтегляне, с което операцията навлиза във ФАЗА 6.

ФАЗА 6 – Изтегляне. Провежда се поетапно изтегляне на силите в техните пунктове за постоянна дислокация.

В рамките на териториалната отбрана на страната въоръжените сили на Република България провеждат Национална съвместна операция, която по своята същност е *съвкупност от съгласувани и взаимосвързани бойни операции и тактически действия, провеждани от националните съвместни сили по единна концепция и план на съвместното командване на силите за изпълнение на определена мисия в заповядани пространствени и времеви рамки*.

Националната съвместна операция може да се провежда за разрешаване на военен конфликт с висока, ниска или средна интензивност. Тя се провежда в Зона за съвместни операции, в която назначеният командващ на съвместните сили планира и изпълнява конкретна мисия. Зоната за съвместни операции включва част или цялата територия, въздушното и морските пространства на страната и в нея се водят активни бойни действия. Размерите на зоната на съвместната операция зависят от характера на задачите на войските и силите, техният състав и способности, от особеностите на местността и вероятните действия на противостоящите сили. Границите на зоната за съвместни операции се определят от върховния главнокомандващ на въоръжените сили на страната. Командващият съвместните сили може да определи и други зони за операции на основните компоненти на съвместните сили и за действия по поддръжка и осигуряване.⁶

Националната съвместна операция, провеждана за разрешаване на регионален военен конфликт със средна и висока интензивност, се подготвя и провежда с цел прикритие и отбрана на застрашен участък от държавната граница, защита на въздушното и морските пространства на страната и създаване на условия за развърщане на съюзни сили и провеждане на съюзни операции за разрешаване на военния конфликт. В този случай, по инициатива на страната, Северноатлантическият съвет активира консултации за предприемане на дипломатически инициативи за предотвратяване на конфликта. Като крайна мярка Северноатлантическият съвет може да развърне превантивно част от Силите за отговор на НАТО. Така изпълнението на задълженията като страна домакин и съвременно интегриране на определените национални сили в съюзните сили ще е от ключово значение за бързото спиране на военните действия и разрешаване на военния конфликт.

Провежданата при тези условия национална съвместна операция може да включва следните етапи:

ЕТАП 1 – Създаване на групировка на националните съвместни сили за прикритие и отбрана на застрашен участък от държавната граница и осигуряване развърщането на съвместните сили на Алианса за разрешаване на военнополитическата криза.

ЕТАП 2 – Водене на задържащи бойни действия от националните съвместни сили за създаване на условия за провеждане на съюзна съвместна операция за разрешаване на военния конфликт.

ЕТАП 3 – Прегрупиране на националните съвместни сили за участие в провеждането на съюзна съвместна операция за разрешаване на военния конфликт.

Съотнесено към горепосочените шест фази на съюзната съвместна операция на НАТО:

ЕТАП 1 на националната съвместна операция трябва да започне преди или в началото на **ФАЗА 1** на операцията на НАТО. През този етап от националната съвместна операция се актуализират плановете за нейното провеждане, сформират се групировките и се заема зоната за прикритие на държавната граница от сухопътния компонент на националните съвместни сили. Тези сили осигуряват развърщането и участват в съвместната подготовка на съюзните сили и тяхното прегрупиране за провеждане на съвместна операция. Провеждането на **ЕТАП 1** от националната съвместна операция завършва с развърщането на съюзните сили и разрешаването на военнополитическата криза или с нарушаване на държавната граница от противника. Ако противникът започне своята агресия преди развърщането на съюзните сили на наша територия, се преминава към **ЕТАП 2** на националната съвместна операция.

През **ЕТАП 2** на националната съвместна операция се водят задържащи бойни действия от националните съвместни сили за създаване на условия за развърщане на съюзните сили и провеждане на съюзна съвместна операция за защита суверенитета и териториалната цялост на страната. **ЕТАП 2** пряко кореспондира с **ФАЗА 2** и **ФАЗА 3** от съюзната съвместна операция. След развърщането на съюзните сили на наша територия се преминава към **ЕТАП 3** на националната съвместна операция.

През **ЕТАП 3** на националната съвместна операция се извършва прегрупиране на силите за участие в провеждането на съюзна съвместна операция за защита суверенитета и териториалната цялост на страната. В зависимост от конкретните условия **ЕТАП 3** може да се отнесе както към **ФАЗА 2** и **ФАЗА 3**, така и към **ФАЗА 4** от съюзната съвместна операция. В зависимост от развитието на обстановката командването на съюзните сили взема решение за актуализиране на плана за провеждането на съюзната съвместна операция или преминаване към изпълнението му. Извършва се прегрупиране на националните сили за участие в съюзната съвместна операция, ако планът го изисква.

След успешното провеждане на операцията по отразяване на агресията се пристъпва към изпълнение на **ФАЗА 5** и **ФАЗА 6** от Съюзната съвместна операция, при които националните въоръжени сили участват в провежданите мероприятия за деескалиране на кризата и преодоляване на последствията, а след това се изтеглят в пунктовете за постоянна дислокация и преминават на подчинение на националния командващ/командир.

Националната съвместна операция, провеждана за разрешаване на ограничен регионален военен конфликт с ниска интензивност, се подготвя и провежда с цел отбрана на част от територията, въздушното и морските пространства на страната, които са обект на въздействие от чужди войски и сили, а при определени условия – и от паравоенни формирования (или терористични групи) и поддържащите ги местни незаконни въоръжени структури. Обичайно за провеждане на Националната съвместна операция в условията на ограничен регионален конфликт с ниска интензивност се използват част от мирновремен-

ните формирования с най-висока степен на готовност, които периодично се ротират в зоната на операцията. В зависимост от това дали действията започват и се развиват преобладаващо по суша, въздух или море, операцията ще има различно съдържание и може да се провежда с водещата роля на войски и сили от сухопътния, военновъздушния, военноморския или на компонента, съставен от командването за специални операции. В зависимост от конкретните условия, разрешаването на ограничен регионален военен конфликт с ниска интензивност може да се отнесе както към **ФАЗИ 1 и 2**, така и към **ФАЗА 3** от съюзната съвместна операция.

При разрешаването на ограничен регионален военен конфликт с ниска интензивност, съгласно чл. 4 от Северноатлантическия договор, държавата може да поиска консултации, ако е възникнала заплаха за териториалната цялост, политическата независимост или сигурността ѝ. В рамките на отбраната на страната, съгласно Доктрината на въоръжените сили на Република България, по мисия „Отбрана“ въоръжените сили изпълняват следните **основни видове операции**⁷:

- операция за защита на суверенитета и териториалната цялост на държавата;
- участие в съзна отбранителна операция по член 5 от Вашингтонския договор на територията на страната;
- участие в съзна отбранителна операция по член 5 от Вашингтонския договор извън територията на страната;
- наблюдение, контрол и защита на въздушно-космическото пространство в рамките на интегрираната система за ПВО и ПРО на НАТО;
- наблюдение и защита на морските пространства;
- ранно предупреждение и управление;
- други включени в тях операции от по-малък мащаб.

От заповяданата мисия и прилежащите за изпълнение операции произтичат **основните задачи** на националните съвместни сили, както следва:

- изпълнение на задълженията като страна домакин и провеждане на съзна съвместна операция за защита суверенитета и териториалната цялост на държавата в регионален военен конфликт с висока интензивност;
- провеждане на национална съвместна операция за прикритие и отбрана на застрашен участък от държавната граница, въздушното и морските пространства на страната и създаване на условия за развърщане на съюзни сили за защита на суверенитета и териториалната цялост на страната в регионален военен конфликт със средна интензивност;
- провеждане на национална съвместна операция за защита суверенитета и териториалната цялост на страната в ограничен регионален военен конфликт с ниска интензивност;
- провеждане на бойни и небойни операции и действия от резервите и формированията на пряко подчинение на министъра на отбраната за защита суверенитета и териториалната цялост на страната в регионален военен конфликт;
- създаване на стратегически резерви за усилване на националните и съюзните съвместни сили;
- участие в провеждането на национални или съюзни информационни операции, с цел недопускане завоюването на превъзходство в управлението от противостоящите сили.
- участие в провеждане на национални и международни учения с цел да се демонстрира сила и решителност за възпиране и недопускане прерастването на кризата във военен конфликт.

В контекста на описаните мисия и задачи, които въоръжените сили са в състояние да изпълняват по отношение на отбраната на страната, се формират два периода в подготовката на страната за отбрана: **Стратегическо развърщане на въоръжените сили** и **Използване на въоръжените сили за отбрана на страната**.

Стратегическото развърщане на въоръжените сили за отбрана се извършва с цел създаване на необходимите условия за организираното им развърщане и последващото им участие в разрешаването на военнополитическа криза и/или военен конфликт. Възможните сценарии за стратегическо развърщане на националните въоръжени сили се определят преди всичко от мащабите на военния конфликт.

В съответствие с изискванията за изграждане на възпиращ и отбранителен ефект въоръжените сили се състоят от **Сили за съдържане** и **Сили за отбрана**, съответстващи и на приетата категоризация на военните формирования, съгласно системата на НАТО.

Силите за съдържане⁹ са военни формирования от въоръжените сили с висока степен на готовност и с висока мобилност, които са способни да участват в пълния спектър от операции по мисиите на въоръжените сили. Част от силите за съдържане формират сили за незабавно действие, които са с много висока степен на готовност. Предназначението на силите за незабавно действие е да осигурят първоначален бърз военен отговор в кризисна ситуация.

Силите за отбрана⁹ са военни формирования, необходими за допълване на въоръжените сили във военно време с ограничена мобилност, с висока и по-ниска степен на готовност, способни да участват в операции по мисия „Отбрана“ за защита на териториалната цялост на страната, както и за поддръжка на съюзни сили.

Съобразно етапите на националната съвместна операция за изпълнението на основните задачи по отбраната на страната развърщането и използването на националните въоръжени сили се обособява в провеждането на комплекс от мероприятия¹⁰, както следва:

- привеждане на националните въоръжени сили от мирно на военно положение (отнася се към ЕТАП 1);

- прегрупиране на националните въоръжени сили за създаване на групировки за отбрана на страната и формиране на стратегически и оперативен резерв (отнася се към ЕТАП 2);

- прегрупиране и създаване на групировки за провеждане на национални и съюзни военни действия за отбрана на страната (отнася се към ЕТАП 3).

Привеждането на националните въоръжени сили от мирно във военно положение е заключителният етап в подготовката за участие в национални и съюзни военни действия за защита на териториалната цялост на държавата. С привеждането на националните въоръжени сили в по-висока степен на бойна готовност се цели да се осигури последователност и гъвкавост на системата за подготовка на войските и силите за водене на военни действия за отразяване на агресията на противника.

Прегрупирането на националните въоръжени сили за създаване на групировките за отбрана на страната включва прегрупиране на силите и създаване на:

- групировката на войските и силите, участващи в провеждането на националната съвместна отбранителна операция за прикритие и отбрана на застрашен участък от държавната граница и осигуряване на развърщането на съвместните сили на НАТО;

- групировката на войските и силите, участващи в провеждането на съюзната съвместна отбранителна операция;

- групировката на резервите и формированията от националните въоръжени сили на пряко подчинение на министъра на отбраната;

- групировката на силите и средствата за провеждане на националната и съюзната информационна операция.

Прегрупирането на войските и силите за създаване на групировката на националните съвместни оперативни сили, формирани за провеждането на национална съвместна операция, включва прегрупиране на сухопътния, военновъздушния и военноморския компонент, компонента сили за специални операции и формированията за единна комуникация и логистика. Редът за създаване на групировката на националните съвместни оперативни сили се определя от поставените им задачи за прикритие и отбрана на застрашената държавна граница и осигуряване на развърщането на съюзните сили за отбрана на страната.

Участващите в операцията компоненти се подготвят за развърщане, като се съчетава повишаване на степента на бойната готовност на формированията с готовността на транспортните средства, необходими за осъществяване на прегрупирането. Тяхното придвижване от районите за съсредоточаване към зоните за операции изисква способности по защитата на силите за осигуряване на придвижване, включително и вътре в зоната на съвместните операции.

Развърщането в зоната на съвместни операции е отговорност на командващия на съвместните сили. То може да бъде подпомагано с техника и транспорт предоставени от стратегическото ниво.

Прегрупирането на националните въоръжени сили за създаване на групировката на многонационалните съвместни оперативни сили, формирани за провеждането на съюзната съвместна операция, включва провеждането на комплекс от мероприятия и практически действия по прегрупиране на компонентите на видовете въоръжени сили в зоната на съвместните операции и създаването на групировките и оперативното им построение за участие в съюзната съвместна операция.

Националните съвместни сили провеждат задържащи бойни действия с цел създаване на изгодни условия за формирането и развърщането на съвместните сили на НАТО за провеждане на съюзна съвместна операция за разрешаване на военния конфликт.

Прегрупирането и създаването на групировката на резервите и формированията от националните въоръжени сили на пряко подчинение на министъра на отбраната се извършва в съответствие с плана за техните действия и с цел заемане на определените им райони и осигуряване на условия за организирано изпълнение на поставените им задачи.

Формированията от въоръжените сили на пряко подчинение на Министъра на отбраната могат да бъдат обособени като сили за отбрана, които провеждат бойни и небойни операции и действия от резервите, и за разрешаване на регионален военен конфликт с различна интензивност се подготвят и провеждат с цел изпълнение на поставените им задачи в интерес на основните съвместни сили. Провеждането на бойни и небойни операции от резервите и формированията от въоръжените сили на пряко подчинение на министъра на отбраната по своята същност са съвкупност от съгласувани и взаимосвързани подчинени бойни и небойни действия, провеждани от тях по единни концепция и план на техните командири, за изпълнение на определени военни мисии в интерес на силите за сдържане.

Провеждането на бойни и небойни операции от силите за отбрана може да включва действия за:

- охрана и отбрана на обекти с особена важност на територията на страната;
- охрана на държавните граници с неучастващите във военния конфликт съседни държави;
- организиране на военнопленнически лагери;
- създаване на стратегически резерви за усилване на националните и съюзните съвместни сили;
- осигуряване и поддръжка на действията на националните съюзни и съвместни сили за отбрана на страната и други.

Провеждането на национални и съюзни информационни операции е успешен метод за въздействие и снижаване волята и единството на бойна мощ на противостоящите сили. По своята същност те представляват *координирано и синхронизирано въздействие спрямо информационните системи на противостоящите сили, защита на собствените, както и оказване на влияние в социалната среда*. Целта е създаване както на физически, така и на нематериални ефекти, влияещи върху волята и способностите на противостоящите сили за водене на въоръжена борба. Информационният инструмент се използва с цел легитимиране на собствените действия и получаване на подкрепа от широката общественост за тях, възпиране на опонента или привеждането му в заблуждение относно собствените намерения.¹⁰

Информационното въздействие в операциите може да бъде пряко и косвено, като съдържанието му се определя от съставните операции и действия, както следва: психологически операции; присъствие, развърщане и демонстрация на сила; защита на операциите; сигурност на информацията; дезинформация; електронна война; физическо унищожение на комуникационни средства, възли и пунктове за управление и операции в компютърните мрежи, съчетани с ефективно разузнаване, комуникации и управление, с цел недопускане завоюването на превъзходство над противника.¹¹

В контекста на колективната отбранителна политика на НАТО и страните членки българските въоръжени сили трябва да са в състояние: да проведат национална съвместна отбранителна операция за прикритие на застрашен участък от държавната граница, защита на въздушното и морските пространства на страната; да създадат условия за развърщане на съюзните сили на НАТО; да са в състояние своевременно и синхронизирано с намеренията на съюзния командир да заемат зоната на операцията; да сформират компоненти, осигуряващи бързото им последващо интегриране в съюзните сили; да осигурят свободното придвижване на войските и силите в зоната на операция; да са в състояние да участват в съюзна съвместна отбранителна операция както на територията на страната, така и извън нея.

ЛИТЕРАТУРА

1. Програма за развитие на отбранителните способности на въоръжените сили на Република България 2032. *Държавен вестник*, бр. 13 от 16.02.2021.
2. *Доктрина на въоръжените сили на Република България (НП-01, издание А)*. София: Министерство на отбраната, 2017, стр. 14.
3. Пак там, стр. 6.
4. *Северноатлантически договор*. 39 НС, 2004.

5. *Allied Joint Doctrine (AJP-01, Edition E, Version 1)*. NATO, 2017.
6. Структура и състав на Националните съвместни сили. *Формиране и използването им в мисия „Отбрана“*. София: Съвместно командване на силите, 2015.
7. Доктрина за провеждане на операции (НП-3, издание А). София: Министерство на отбраната, 2018 г., стр.23
8. План за развитие на въоръжените сили на Република България 2026. Министерски съвет, 2021, стр. 9
9. Пак там, стр.9
10. Доктрина на въоръжените сили на Република България (НП-01, издание А). София: Министерство на отбраната, 2017, стр. 13.
11. *Allied Joint Doctrine For The Conduct Of Operations (AJP-3, Edition C, Version 1)*. NATO, 2019.

REFERENCES

1. Programa za razvitie na otbranitelните sposobnosti na vaorazhenite sili no Republika Bulgaria 2032. *Darzhaven vestnik*, br. 13 ot 16.02.2021.
2. *Doktrina na vaorazhenite sili na Republika Bulgaria (NP-01, izdanie A)*. Sofia: Ministerstvo na otbranata, 2017, str. 14.
3. *ibidem*, p. 6.
4. *Severnoatlanticheski dogovor*. 39 NS, 2004.
5. *Allied Joint Doctrine (AJP-01, Edition E, Version 1)*. NATO, 2017.
6. *Struktura i sastav na Natsionalnite savmestni sili. Formirane i izpolzvaneto im v misia „Otbrana“*. Sofia: Savmestno komandvane na silite, 2015.
7. *Doktrina za provezhane na operatsii (NP-3, izdanie A)*. Sofia: Ministerstvo na otbranata, 2018 g., str.23
8. *Plan za razvitie na vaorazhenite sili na Republika Bulgaria 2026*. Ministerski savet, 2021, str. 9
9. *ibidem*, p. 9
10. *Doktrina na vaorazhenite sili na Republika Bulgaria (NP-01, izdanie A)*. Sofia: Ministerstvo na otbranata, 2017, str. 13.
11. *Allied Joint Doctrine For The Conduct Of Operations (AJP-3, Edition C, Version 1)*. NATO, 2019.

ИЗПОЛЗВАНЕ НА ГЛАДКОЦЕВНО ОГНЕСТРЕЛНО ОРЪЖИЕ ОТ ПОЛИЦЕЙСКИТЕ СЛУЖИТЕЛИ ПРИ ПРОВЕЖДАНЕ НА ВИСОКОРИСКОВИ ОПЕРАЦИИ – СПЕЦИФИКИ И ТАКТИЧЕСКО ПРИЛОЖЕНИЕ

Марин Григоров, докторант

Военна академия „Г. С. Раковски“, grigorov_marin@abv.bg

Резюме: В наши дни достиженията на научно-техническия прогрес заемат челни места в сферата на оръжейната индустрия. Появяват се и биват рекламирани все по-нови и атрактивни системи оръжия, аксесоари и прибори. Все по-често новите поколения полицейски служители в специализираните тактически звена се съсредоточават върху използването на автоматичните оръжия и карабините, а гладкоцевните оръжия се възприемат като анахронизъм. Като ги считат ги за изживели своето време системи, много служители пренебрегват гладкоцевните оръжия, без да си дават сметка за неоспоримите им достойнства.

Ключови думи: *гладкоцевно оръжие; високорискови операции; тактически звена; помощни средства*

USE OF SMOOTHBORE FIREARMS BY POLICE OFFICERS IN CONDUCTING HIGH-RISK OPERATIONS – SPECIFICS AND TACTICAL APPLICATION

Marin Grigorov, PhD Student

Rakovski National Defence College

Sofia, Bulgaria

E-mail: grigorov_marin@abv.bg

Abstract: Nowadays the achievements of scientific and technical progress occupy a leading place in the sphere of weapons industry. They appear and advertise more and more new and attractive weapon systems, accessories and devices. Increasingly, new generations of police officers in specialized tactical units are turning to the use of automatic weapons and carbines, while smoothbore weapons are perceived as an anachronism. Believing them to be systems that have outlived their time, many officers disregard smoothbore weapons without realizing their undeniable merits.

Keywords: *smoothbore weapons; high-risk operations; tactical units; supporting resources*

Преимущества при използването на гладкоцевно оръжие от полицейските служители, участващи във високорискови операции, често са пренебрегвани или недооценявани. Обикновено служителите от тактическите звена го използват по необходимост като основно оръжие поради липса на дългоцевно нарезно оръжие, зачислено по щат. Причините за такива липси са основно икономически и организационни – някои дирекции на МВР не разполагат със средства за закупуване на ново и необходимо въоръжение, а в самото министерство все още няма изградена визия по отношение на унификацията на оборудването на служителите от тактическите звена. В други случаи гладкоцевното оръжие се използва единствено като помощно средство – за преодоляване на врати (използват се боеприпаси с цинково-магнезиев или медно-калаен прах) или за въздействие чрез несмъртоносна сила (използват се боеприпаси с каучукови сачми или каучукови куршуми).

В световен мащаб обаче използването на гладкоцевно огнестрелно оръжие от силите за специални операции е широко застъпено поради неговите специфични функционалности, превъзхождащи в редица случаи възможностите на късоцевните или дългоцевните нарезни оръжия.

Дистанцията за работа

На първо място може да се отбележи голямата степен на универсалност при гладкоцевните оръжия по отношение на дистанцията за работа. Условно дистанциите за работа с огнестрелно оръжие се определят от неговата далекобойност по следния начин:

– тактически действия в затворени пространства, обозначавани с термина CQB (англ.) – характерно за тях е, че средата за работа е основно в сгради и помещения, поради което дистанцията за използване на оръжие е от 0 до около 20 м. Основно приложение тук имат пистолетите (полуавтоматични и картечни), револверите и автоматичните оръжия;

– тактически действия в градска среда – особеностите на този тип обстановка произтичат от наличието на много зони за отговорност с различна големина и на различна дистанция. Отново приложение тук имат пистолетите, револверите и автоматичните оръжия. Последните могат да бъдат заменени с карабини с цел намаляване риска от косвени жертви;

– тактически действия на средни дистанции – в тези ситуации разстоянието за използване на оръжие се приема за дистанция до около 100 м. В такъв тип среда е целесъобразно използването предимно на автоматични оръжия и карабини;

– тактически действия в отворени пространства – такива могат да бъдат всякакъв тип обширни равнинни територии (полета, пустини и др.). В подобна среда предимство имат карабините и на следващо място – автоматичните оръжия.

При първите три варианта на обстановка може да бъде използвано гладкоцевно оръжие. Това е възможно благодарение на голямото разнообразие при боеприпасите, както и поради особеностите на самите системи гладкоцевни огнестрелни оръжия.

Специфики при боеприпасите

Сачми (buckshot). Най-разпространените патрони за гладкоцевно оръжие както в България, така и по-света, са в калибър 12 и дължина на гилзата 70 мм. (2 и 3/4 инча). Според това дали целта на стрелбата е поразяващ/стопиращ ефект на голяма площ или се търси ефективен изстрел на далечна дистанция, патроните са снабдени със сачми или с куршуми.

Основно употребата на гладкоцевно оръжие се свързва със стрелбата със сачми. Тяхното използване повишава вероятността от попадение на близки дистанции, особено при намалена видимост или движещи се цели. Сачмите представляват оловни сфери с различен диаметър, които заместват куршума в гилзата. В някои боеприпаси сачмите могат да са обвити в медни ризници или да е добавен антимоном в оловото. Това се прави с цел увеличаване на твърдостта им и запазване на сферичната им форма при изстрел¹.

По света за нуждите на правоохранителните органи, за военни цели, както и за самоотбрана, най-разпространени са патроните в калибър 12, дължина 70 мм със сачми 13/0 (англ. 00 buckshot). Размерът на всяка сачма е 8,65 мм. или около 0,33 инча². Броят на сачмите обикновено е 9. Всяка от тях може да носи до около 338 джаула дулна енергия³. Според направени изследвания, ако всички сачми попаднат в целта, ефектът върху нея ще бъде идентичен с този на 15 изстрела на картечен режим с боеприпаси .380 ACP⁴.

Ограничаващ фактор при стрелбата със сачми е дистанцията. При тях ефективното разстояние за поразяване/стопиране на целта значително намалява до около 40 – 50 м⁵. Снопът сачми има способността да преминава през определени материали и да поразява зад тях – например автомобилни ламарини и стъкла⁶.

Използването на сачми не се ограничава само до поразяване на живи цели. В редица държави правоохранителните органи използват подобни боеприпаси за поразяване на безпилотни летателни апарати (дронове) или при обезвреждане на взривни вещества от сапъорските екипи.

Куршум (slug). Както беше посочено, необходимостта от ефективен изстрел на далечна дистанция изисква патроните да са снабдени с куршуми, вместо със сачми. Според направени изследвания куршум от гладкоцевна пушка може да измине максимално разстояние от около 1125 м, измерени на морското равнище, и разстояние от около 1600 м при приблизително 3650 м надморска височина⁷. Установено е също така, че при далечни дистанции (над 100 м) куршумите за гладкоцевно оръжие имат относително малко отклонение до около 180 м. Някои образци на куршуми, изстрелвани от определени системи оръжия 12 калибър, позволяват точност от 1,5 MOA на 100 м. Въпреки че не позволява изстрел с прецизността на карабина, използването на гладкоцевно оръжие далеч надминава възможностите на пистолетите и картечните пистолети на дистанции до 200 м.

От значение за поразяване на целта е не само далекобойността, но и предаваната кинетична енергия. Тя трябва да бъде в необходимото количество, за да се постигне търсеният поразяващ/стопиращ

ефект. Според лабораториите на ФБР на проектилът са необходими около 220 джаула, за да проникне през кожата и около 290 джаула, за да счупи кост в тялото. При така поставените критерии куршум калибър 12 може да отдаде около 1355 джаула енергия на дистанция от около 100 м. Видно е, че това количество надвишава 4 – 5 пъти необходимата енергия за нанасяне на поражение върху костите. В същото време някои образци куршуми могат да достигнат стойности на дулна кинетична енергия от порядъка на над 4070 джаула⁸, което превишава дулната енергия на най-разпространените боеприпаси за дългоцевно оръжие, както следва: на патрон 5,56 NATO – над 2 пъти; на патрон 5,45 M74 – 3 пъти; на патрон 7,62 M43 – 2 пъти; на патрон .308 Win – с около 1000 джаула. Посочената стойност на дулна енергия на куршума за гладкоцевна пушка се доближава до тази на патрони 7,62 M1908/30 (2930 – 4466 джаула) и .30-06 Springfield (3261 – 3793 джаула)⁹.

Посочените характеристики на куршума са причина той да отдава голямо количество кинетична енергия дори след преминаване през относително тънки прегради (дървени плоскости, 3 – 4 мм ламарина, автомобилни стъкла и др.)¹⁰. Благодарение на балистичните си характеристики, при стрелба през предното автомобилно стъкло отклонението на куршумите за гладкоцевно оръжие е много по-малко, отколкото при изстрел от пистолети, картечни пистолети или карабини. Тази особеност е от изключителна важност при необходимост от неутрализиране на нападател в случаи на масови убийства или терористични актове, извършвани чрез превозни средства. Пример за това може да бъде нападението с тежкотоварен автомобил в Ница през 2016 г., при което загинаха над 80 души. Установено е, че полицейските служители са направили опит да спрат превозното средство чрез стрелба по предното стъкло, но използването на пистолетни куршуми препятства бързото постигане на целта¹¹. Най-високоэффективни за принудително спиране на автомобили са патроните с бронебойни куршуми¹². Достатъчната кинетична енергия позволява на куршума да пробие радиатора или блока на двигателя. Изстрел в гумите на автомобила ги спада мигновено за разлика от попадения от калибри 9 мм или 5,56 мм, при които спадането в някои случаи продължава и до около 30 – 40 сек. Бронебойен куршум е способен да пробива и джантата. Този ефект може да предотврати или да намали значително настъпването на неблагоприятните последици от извършването на нападения с превозни средства.

Боеприпаси за специфични дейности. При изпълнение на служебните си задължения служителите на правоохранителните органи са длъжни да пазят живота и здравето на лицата, включително на правонарушителите. В тази връзка и поради някои други специфични съображения органите на реда могат да използват определени видове боеприпаси, дефинирани по националното ни законодателство като „помощни средства“. Съгласно разпоредбите на чл. 15 от Наредба № 8121з-418 от 14 март 2017 г. за реда за употреба на физическа сила и помощни средства от служителите на Министерството на вътрешните работи „при изпълнение на служебните си задължения в случаите по чл. 85, ал. 1 ЗМВР полицейските органи могат да бъдат снабдени с халосни патрони, патрони с гумени, пластмасови и шокови куршуми“. В тази наредба е регламентирано също така, че „халосните патрони и патроните с гумени, пластмасови и шокови куршуми са предназначени за оказване на физическо и психологическо въздействие върху правонарушители и се използват в случаите по чл. 85, ал. 1 ЗМВР. (чл. 16, ал. 1) В случаите по ал. 1 минимално допустимото разстояние до лицето, срещу което се използват халосни патрони и патрони с гумени, пластмасови и шокови куршуми, се определя от тактико-техническата характеристика на всеки отделен вид боеприпас (чл. 16, ал. 2)“. Минималното допустимо разстояние е дистанция, под която използването на боеприпаси, предназначени за помощни средства, може да предизвика риск за живота и здравето на лицата, срещу които са използвани. Поради тази причина по света посочените категории боеприпаси се класифицират като less-lethal (англ.), тъй като при неправилна употреба могат да доведат до фатални последици.

Широко разпространени, но с разновидности основно в броя гумени сфери, са патроните със сачми. В зависимост от диаметъра на всяка сфера в един патрон калибър 12 могат да бъдат снабдени между 3 и 24 и повече броя каучукови сачми. Ефективното им разстояние за употреба е около 15 – 16 метра¹³. Използваните в Република България патрони калибър ПКС-12 отговарят по тактикотехническите си данни на световните стандарти. Установените норми при използването са минимално разстояние 7 м и ефективно разстояние 15 м.¹⁴

В световен мащаб са разработени различни разновидности на несмъртоносни куршуми – каучукови цилиндрични, каучукови със стабилизатори, звездовидни, балистични (кинетични) торбички и др. Широко разпространени са цилиндричните куршуми¹⁵, чийто аналог в Република България са ПКК-12. При тях минималното допустимо разстояние за използване е 20 м, а ефективното разстояние – 25 м.¹⁶

За подобряване на балистичните характеристики някои производители въвеждат подобрения върху тези боеприпаси. Широко разпространение имат гумените куршуми със стабилизатори, които способстват за увеличено ефективно разстояние на използване до около 40 – 50 м.¹⁷

Звездовидните куршуми са вариант, при който площта на отдаваната кинетична енергия се увеличава значително в сравнение със стандартни гумени куршуми. Въпреки това безопасното използване на този боеприпас е обвързано с правилната преценка на дистанцията, облеклото и състоянието на лицето.¹⁸

Балистичните (наричани още кинетични, „бобови“ и др.) торбички са междинен вариант, близък едновременно до куршум и сачми. Те представляват торбичка, най-често от памучна тъкан, в която са събрани няколко каучукови или желатинови сачми. Ефективното разстояние за използване на такъв боеприпас е около 7 м.¹⁹ При някои образци тъканта на боеприпаса оцветява мястото на попадение в целта²⁰.

Освен регламентираните в указанията случаи, в редица държави правоохранителните органи са изградили процедури за използването на несмъртоносни боеприпаси при различни ситуации – например за защита от агресивни животни или при невъзможност да бъде използвано друго помощно средство. Такъв случай представлява например ситуация с лице, заплашващо със самозапалване или самовзривяване. Използването на TASER в такава ситуация е забранено, тъй като може да предизвика възпламеняване или взрив. Ефективно средство за обезвреждане на правонарушители в такива случаи е използването на несмъртоносни боеприпаси. Такава е практиката на френските полицейски специални сили RAID.

Друг вид помощни средства са боеприпасите, съдържащи химически вещества за обгазяване. Съгласно националното законодателство използваните вещества, утвърдени от министъра на здравеопазването, са две: ортохлорбензиденмалонитрил (CS) и хлорацетофенон (CN). Те имат рефлекторно действие и въздействат върху лигавиците на очите и горните дихателни пътища, като предизвикват сълзотворен и кихавичен ефект. Газовите патрони калибър 12 се използват на разстояние от 20 до 250 м както на открито, така и в затворени пространства. Един патрон е в състояние да задими до непоносимост помещение с обем между 20 и 25 кубични метра²¹. Стандартът за използването на веществата CS и CN е световно признат. В последните години обаче посочените химически съединения биват изместени от веществото „олеорезин капсикум“ (OC), което се съдържа в лютите чушки. Редица производители на боеприпаси го използват като активно вещество в своите продукти. Към настоящия момент съществуват различни разновидности газови патрони. Някои са с мигновено действие и са ефективни на дистанция до 10 м.²² Други комбинират действието на гумени куршуми и химическо вещество (OC или CS). Куршумът е със стабилизатори, като в предната му част е разположена капсулата с активното вещество. Използването на такъв вид боеприпас предизвиква двоен ефект – болка, чрез отдаване на кинетичната енергия и разпръскване на химическото вещество. Ефективната дистанция на посочения вид боеприпас е около 50 м.²³

Специфична разновидност на този вид боеприпас са куршумите за преодоляване на прегради, съчетани с химическо вещество (OC или CS). Патроните се използват за пробиване на прегради като стъкла (на автомобили или помещения) и кухи интериорни врати, като след проникването разпръскват активното вещество в помещението или купето на автомобила. Ефективното им разстояние е около 30 – 45 м.²⁴ Посочените боеприпаси имат приложение основно при високорискови операции за противодействие на барикадирали се лица с цел намаляване на риска за участващите полицейски служители.

В редица случаи при провеждането на специални операции възниква необходимост от осигуряване на точка за проникване чрез извършване на пробив (англ. breaching, фр. effraction). В тези случаи един от вариантите за преодоляване на заключени прегради се явява използването на специфичен вид боеприпаси за разбиване на врати. Те най-често са в следните разновидности – оловен куршум в полимерна обвивка²⁵ или пресован метален прах (например медно-калаен)²⁶. Посочените боеприпаси се използват за разрушаване на ключалки и панти на врати, тъй като при съприкосновението си с целта те се фрагментират и не преминават преградата. За разбиване на ключалки могат да се използват и стандартни оловни куршуми, но не е препоръчително поради високия риск от увреждане на лицата зад преградата.

Не съвсем познати у нас са патроните калибър 12 със светлинно-звуков ефект. По света се използват предимно при масови нарушения на обществения ред за контрол на тълпата. Различните видове боеприпаси могат да произведат шок ефект на разстояние от 1 до 100 м.²⁷

В съвременната обстановка на достъп и разпространение на неограничено количество информация изключително популярно средство за видео заснемане са безпилотните летателни апарати (БЛА), наречени на разговорен език „дронове“. Нерядко полицейските действия биват заснемани нерегламентирано от лица с цел разпространяване на информацията. Тези действия в редица случаи водят до не-

благоприятни последици по отношение на тактическите или оперативните способности, използвани от полицейските служители. В този ред на мисли интересна разработка представляват и боеприпасите калибър 12, предназначени за неутрализиране на безпилотните летателни апарати. При изстрел специално изработеният куршум се фрагментира и образува 5-лъчева мрежа, покриваща площ с диаметър около 1,5 м. Ефективното разстояние на този вид патрон е до около 90 м.²⁸

Специфики при по-разпространените образци пушки. Главно значение при стрелбата с гладкоцевно оръжие имат не само боеприпасите, но и оръжейната система, която ги изстрелва. Служителите от правоохранителните органи, както и тези от въоръжените сили на различните държави, са възприели на въоръжение различни видове гладкоцевно оръжие. Тук ще бъдат разгледани най-популярните системи, като акцентът ще е върху уникалните особености на всяка система и преимуществата, които произтичат от тях.

Най-често срещаната система гладкоцевни пушки сред правоприлагащите органи и въоръжените сили по света е може би тази на Mossberg. Вариантът Mossberg 590 е обявен за единствената пушка тип „помпа“, покриваща военния стандарт MilSpec 3443E на САЩ. Това, както и дългата ѝ история, датираща от 1960 г., я прави категоричен избор в службите за сигурност и военните формирования. Признание за надеждността и ефективността на Mossberg 590 се явява и фактът, че пушката е обявена за най-продавана пушка тип „помпа“ в САЩ за 2019 г.²⁹ От тогава и досега тя не слиза от призовата позиция³⁰. В Република България Mossberg и Mossberg Maverick са сред приетите на въоръжение в някои тактически звена в структурите на МВР.

Benelli M1014 е образец, използван от военнослужещите в Морската пехота на САЩ. При използване на всички видове 70 мм патрони, отговарящи на стандартите на U.S. Department of Defense, оръжието има поразяващ ефект на 40 м при стрелба със сачми 13/0 и до около 100 м при стрелба с куршуми. Посоченият модел се използва единствено от въоръжените сили. За употреба от правоприлагащите органи или от цивилни лица е предназначен моделът M4. Разликите са основно при броя патрони в магазина (7+1 за M1014 и 5+1 за M4) и при аксесоарите. Основното предимство на двата модела е подобрената система за газово презареждане. Недостатък в случая се явява наличието на повече части и механизми, които се нуждаят от регулярно почистване, в сравнение със системите за инерционно презареждане. Друг недостатък е, че автоматичното действие не сработва при употреба на патрони с гумени сачми или куршуми, поради което е необходимо ръчно презареждане³¹. Посоченият проблем е „решен“ чрез Benelli M3. При нея презареждането може да става автоматично или ръчно (тип „помпа“). За целта е създаден малък превключвател в предната част на ложата. Моделът M3 е предпочитан сред правоприлагащите органи точно поради тези свои особености. Използването му дава възможност на служителите да променят степента на прилаганата сила от оръжие към помощно средство и обратно съобразно обстановката.

Beretta 1301 Tactical е обявена за „най-бързо презареждаща“ пушка. Според данните от производителите газовата система позволява презареждане с 36% по-бързо в сравнение с останалите полуватоматични гладкоцевни пушки. Това позволява на системата да възпроизведе 4 изстрела в рамките на една секунда. От значение за служителите на правоохранителните органи са, освен всичко друго, и дължината и теглото на оръжието. Те могат да окажат значителен ефект при ситуации на продължителни тактически действия в сгради например. По тези показатели Beretta 1301 Tactical със своите 96 см дължина и 2,9 кг тегло превъзхожда повечето модели на Mossberg 590, както и Benelli M3 и M4. Ето защо пушката се явява предпочитано гладкоцевно оръжие сред служителите от правоохранителните органи³².

С появата си през 2011 година пушката тип помпа Kel-Tek (KSG) Tactical изцяло запълва обема на понятието „тактическа пушка“, както гласят някои статии. Моделът е предназначен и разрешен само за употреба от въоръжените сили и правоохранителните органи, поради което неговите преимущества по отношение на тактиката в затворени пространства за неопровержими. На първо място, по своите размери 54,6 см и 2,3 кг, (незаредена) пушката няма конкуренция. Дори стандартният модел KSG, разрешен за употреба от цивилни, е по-къс от всички дотук разгледани образци оръжия с над 30 см (общата му дължина е 66,3 см). Намалените размери са благодарение на системата bullpup. В същото време двата туболяра на пушката позволяват зареждането ѝ с 5+5+1 патрона калибър 12/70 мм (при KSG Tactical) или респектиращите 7+7+1 (при стандартна KSG). В същото време всеки от туболярите може да бъде пълнен с различни боеприпаси: в единия – бойни патрони, а в другия – патрони с гумени куршуми, с гумени сачми, за разбиване на врати и т.н. Превключването между двата туболяра позволява бърза адаптация на тактическите действия спрямо обстановката и нуждите на екипа – от смъртоносна сила към помощно средство и обратно³³.

Интересен факт е, че в своя каталог от оръжия, американската компания Smith & Wesson предлага модел, значително идентичен с KSG – това е M&P 12. Моделът представлява пушка „тип помпа“ в калибър 12 с двоен туболяр (за 7+7+1 70 милиметрови патрони), базирана на bullpup-система³⁴.

Руската оръжейна индустрия също не изостава от световните стандарти за гладкоцевни оръжия. Полуавтоматичната пушка „Вепрь-12“ на руския производител „Молот-Оружие“ се нарежда сред най-надеждните полуавтоматични пушки в света. Базирана на системата на РПК-74, пушката има среден настрел около 15000 изстрела според някои източници³⁵. Боровенето с нея не се отличава от това с АК, а възможността да бъдат използвани пълнители с до 25 патрона калибър 12 я нарежда сред първите места в редиците на полуавтоматичните пушки. Неслучайно служителите от френското антитерористично звено RAID са приели на въоръжение именно „Вепрь-12“ (по отношение на пушките тип „помпа“ пък изборът им пада върху KSG Tactical).

Другият типичен руски представител, признат сред западните държави, е „Сайга-12“, произвежда на от „Калашников Концерн“ в Руската федерация. Пушката отново е полуавтоматична и е базирана на системата на АК, което гарантира нейната надеждност. Конструирена през 90-те години на XX в. за нуждите на специалните подразделения на МВД в Русия, към момента интерес към нея има от цял свят. За нуждите специално на правоприлагащите органи „Калашников Концерн“ е разработил модела „Карабин специальный 18,5 КС-К“, базиран върху системата на „Сайга-12“. По своите характеристики е превъзхожда единствено от „Вепрь-12“³⁶.

В заключение може да бъде направено обобщението, че гладкоцевните пушки във вариантите полуавтоматична и тип „помпа“, заедно с голямото разнообразие от боеприпаси, осигуряват един богат инструментариум в ръцете на служителите от правоохранителните органи и въоръжените сили. Широкият набор от приложения на гладкоцевното оръжие предполага подобряване на ефективността и ефикасността на специалните тактически звена при изпълнение на техните задачи, а това е от ключово значение за постигане на успех в защитата на националната сигурност.

ЛИТЕРАТУРА

1. Brass, Fletcher. *Ballistic Testing: Maximum Effective Range of Buckshot*. [online] <https://brassfletcher.com/Shotguns/Maximum%20Effective%20Range/Buckshot.html>
2. Обретенков, А., Русев, Д., Янакиев, П. *Право на лов. Теоретичен курс*. София: Нова звезда, 2020, с. 355.
3. Johnston, J. The Maximum Practical Range of Slugs & Buckshot. *NRA Shooting Illustrated*. 15.02.2019. [online] <https://www.shootingillustrated.com/content/the-maximum-practical-range-of-slugs-buckshot/>
4. Brass, Fletcher. *Ballistic Testing: 12 Gauge Shotgun*. [online] <https://brassfletcher.com/Shotguns/12%20Gauge%20Shotgun/12%20Gauge%20Shotgun.html>
5. Brass, Fletcher. *Ballistic Testing: Shotguns*. [online] <https://brassfletcher.com/Shotguns/Shotguns.html>
6. Brass, Fletcher. *Ballistic Testing: 12 Gauge Shotgun*. [online] <https://brassfletcher.com/Shotguns/12%20Gauge%20Shotgun/12%20Gauge%20Shotgun.html>
7. *Aiming Expert Blog: 12 Gauge Slug Ballistics – How Far Do They Shoot?* [online] <https://aimingexpert.com/12-gauge-slug-ballistics-how-far-do-they-shoot/>
8. Johnston, J. The Maximum Practical Range of Slugs & Buckshot. *NRA Shooting Illustrated*. 15.02.2019 [online] <https://www.shootingillustrated.com/content/the-maximum-practical-range-of-slugs-buckshot/>
9. Вълков, Н., Давидов, К., Цонев, Ц., Ганев, В. *Основи и правила за стрелба с огнестрелни оръжия. Материална част на стрелковото оръжие*. Варна: ИК Стено, 2009, с. 135-136.
10. *Aiming Expert Blog: 12 Gauge Slug Ballistics – How Far Do They Shoot?* [online] <https://aimingexpert.com/12-gauge-slug-ballistics-how-far-do-they-shoot/>
11. *Nice attack: What we know about the Bastille Day killings*. [online] <https://www.bbc.com/news/world-europe-36801671>
12. AP-20: Solid, Hardened Armour Piercing Steel Slug. [online] <https://www.dduplex-defence.com/ap-20>
13. ALS1204HV: Hornets Nest .32 Cal. Rubber Balls (24 Count) High Velocity. [online] <https://www.lesslethal.com/products/12-gauge/als1204hv-detail>
14. *Методически указания за използването на различните видове техники за използване на физическа сила и помощни средства, технически характеристики и правила за безопасност при употребата и съхранението им*. София: МВР, 2018, с. 39.
15. Lightfield Home Defender Less Lethal Ammunition 12 Gauge 2-3/4" 130 Grain Rubber Slug. [online] <https://www.midwayusa.com/product/1002100435?pid=859089>
16. *Методически указания за използването на различните видове техники за използване на физическа сила и помощни средства, технически характеристики и правила за безопасност при употребата и съхранението им*. София: МВР, 2018, с. 39.
17. ALS1202HV: Rubber Fin Rocket (Direct Fire) High Velocity. [online] <https://www.lesslethal.com/products/12-gauge/als1202hv-detail>
18. Lightfield Home Defender Less Lethal Ammunition 12 Gauge 2-3/4" 75 Grain High Velocity Rubber Star Slug. [online] <https://www.midwayusa.com/product/1002099885?pid=123158>

19. ALS1200: Hydro-Kinetic Impact Bag, Short Range. [online] <https://www.lesslethal.com/products/12-gauge/als1200-detail>
20. 12 Gauge Ballistic Bean Bag. [online] <https://www.nonlethaltechnologies.com/12-BB.htm>
21. Методически указания за използването на различните видове техники за използване на физическа сила и помощи средства, технически характеристики и правила за безопасност при употребата и съхранението им. София: MBP, 2018, с. 28-29.
22. ALS120C: Muzzle Blast Powder, OC. [online] <https://www.lesslethal.com/products/12-gauge/als120c-detail>
23. ALS1216CS: Rubber Fin Rocket (Direct Fire) With CS Powder. [online] <https://www.lesslethal.com/products/12-gauge/als1216cs-detail>
24. ALS1216BPOC: Powder Rocket Barricade Penetrator, OC. [online] <https://www.lesslethal.com/products/12-gauge/als1216bpoc-detail>; 12 Gauge Barricade Penetrator. [online] <https://www.nonlethaltechnologies.com/12-BP.htm>
25. Flocchi Special Application Breaching Ammunition 12 Gauge 2-3/4" 540 Grain Polymer Encapsulated Lead Shot. [online] <https://www.midwayusa.com/product/1019391860>
26. ALS1210S: Door Breaching Cartridge (375 Grain Frangible Copper-Tin Slug). [online] <https://www.lesslethal.com/products/12-gauge/als1210s-detail>
27. 12 Gauge Flash Bang / Muzzle Bang. [online] <https://www.nonlethaltechnologies.com/12-FB.htm>
28. SKYNET Mi-5: SkyNet Drone Defense [online] <https://www.lesslethal.com/products/12-gauge/als12skymi-5-detail>
29. Sagi, G. Mossberg 590: Top-Selling Pump Shotgun of 2019. *NRA American Rifleman*. 08.04.2020. [online] <https://www.americanrifleman.org/content/mossberg-590-top-selling-pump-shotgun-of-2019/>
30. Top 10 Shotguns of 2021. [online] <https://www.gunengenius.com/top-selling/guns/top-10-shotguns-of-2021/>
31. Poole, E. *Military Peculiarities: The Benelli M1014*. 30.06.2016. [online] <https://www.gunsandammo.com/editorial/military-peculiarities-the-benelli-m1014/248448>
32. Sadowski, R. *Don't Blink! Beretta 1301 Tactical Shotgun Review*. 07.01.2016. [online] <https://gundigest.com/gun-reviews/dont-blink-beretta-1301-tactical-shotgun-review>
33. Suci, P. *Why the Kel-Tec KSG Tactical is a True Tactical Shotgun*. 21.01.2021. [online] <https://nationalinterest.org/blog/buzz/why-kel-tec-ksg-tactical-true-tactical-shotgun-176801>
34. *The All New M&P 12 Bullpup Shotgun*. [online] https://www.smith-wesson.com/mp12?utm_source=Athlon&utm_campaign=MP12Bullpup&utm_medium=display&utm_content=BallisticTacticalLife&utm_term=native
35. Розин, И. *Какво прави руската „Вепрь“ една от най-добрите пушки в света?* 17.03.2019. [online] <https://bg.rbth.com/science/329881-ruski-vepr-sred-naj-dobrite-pushki-v-sveta>
36. *Карбин специальный 18,5 КС-К: Специальное гладкоствольное оружие ближнего боя для сил охраны правопорядка*. [online] https://ak.kalashnikovgroup.ru/card/karabin_spetsialnyy_18-5_ks-k

REFERENCES

1. Brass, Fletcher. *Ballistic Testing: Maximum Effective Range of Buckshot*. [online] <https://brassfetcher.com/Shotguns/Maximum%20Effective%20Range/Buckshot.html>
2. Obretenov, A., Rusev, D., Yanakiev, P. *Pravo na lov. Teoretichen kurs*. Sofia: Nova zvezda, 2020, s. 355.
3. Johnston, J. The Maximum Practical Range of Slugs & Buckshot. *NRA Shooting Illustrated*. 15.02.2019. [online] <https://www.shootingillustrated.com/content/the-maximum-practical-range-of-slugs-buckshot/>
4. Brass, Fletcher. *Ballistic Testing: 12 Gauge Shotgun*. [online] <https://brassfetcher.com/Shotguns/12%20Gauge%20Shotgun/12%20Gauge%20Shotgun.html>
5. Brass, Fletcher. *Ballistic Testing: Shotguns*. [online] <https://brassfetcher.com/Shotguns/Shotguns.html>
6. Brass, Fletcher. *Ballistic Testing: 12 Gauge Shotgun*. [online] <https://brassfetcher.com/Shotguns/12%20Gauge%20Shotgun/12%20Gauge%20Shotgun.html>
7. *Aiming Expert Blog: 12 Gauge Slug Ballistics – How Far Do They Shoot?* [online] <https://aimingexpert.com/12-gauge-slug-ballistics-how-far-do-they-shoot/>
8. Johnston, J. The Maximum Practical Range of Slugs & Buckshot. *NRA Shooting Illustrated*. 15.02.2019 [online] <https://www.shootingillustrated.com/content/the-maximum-practical-range-of-slugs-buckshot/>
9. Valkov, N., Davidov, K., Tsonev, Ts., Ganey, V. *Osnovi i pravila za strelba s ognestrelni orazhia. Materialna chast na strelkovoto orazhie*. Varna: IK Steno, 2009, s. 135-136.
10. *Aiming Expert Blog: 12 Gauge Slug Ballistics – How Far Do They Shoot?* [online] <https://aimingexpert.com/12-gauge-slug-ballistics-how-far-do-they-shoot/>
11. *Nice attack: What we know about the Bastille Day killings*. [online] <https://www.bbc.com/news/world-europe-36801671>
12. AP-20: Solid, Hardened Armour Piercing Steel Slug. [online] <https://www.ddupleks-defence.com/ap-20>
13. ALS1204HV: Hornets Nest .32 Cal. Rubber Balls (24 Count) High Velocity. [online] <https://www.lesslethal.com/products/12-gauge/als1204hv-detail>
14. *Metodicheski ukazania za izpolzvaneto na razlichnite vidove tehniki za izpolzvaneto na fizicheska sila i pomoshni sredstva, tehnichestki harakteristiki i pravila za bezopasnost pri upotrebatata i sahraneniето im*. Sofia: MVR, 2018, s. 39.
15. *Lightfield Home Defender Less Lethal Ammunition 12 Gauge 2-3/4" 130 Grain Rubber Slug*. [online] <https://www.midwayusa.com/product/1002100435?pid=859089>
16. *Metodicheski ukazania za izpolzvaneto na razlichnite vidove tehniki za izpolzvaneto na fizicheska sila i pomoshni sredstva, tehnichestki harakteristiki i pravila za bezopasnost pri upotrebatata i sahraneniето im*. Sofia: MVR, 2018, s. 39.

17. ALS1202HV: Rubber Fin Rocket (Direct Fire) High Velocity. [online] <https://www.lesslethal.com/products/12-gauge/als1202hv-detail>
18. Lightfield Home Defender Less Lethal Ammunition 12 Gauge 2-3/4" 75 Grain High Velocity Rubber Star Slug. [online] <https://www.midwayusa.com/product/1002099885?pid=123158>
19. ALS1200: Hydro-Kinetic Impact Bag, Short Range. [online] <https://www.lesslethal.com/products/12-gauge/als1200-detail>
20. 12 Gauge Ballistic Bean Bag. [online] <https://www.nonlethaltechnologies.com/12-BB.htm>
21. Metodicheski ukazania za izpolzvaneto na razlichnite vidove tehniki za izpolzване na fizicheska sila i pomoshтни sredstva, tehicheski harakteristiki i pravila za bezopasnost pri upotreбата i sahranениeto im. Sofia: MVR, 2018, s. 28-29.
22. ALS120C: Muzzle Blast Powder, OC. [online] <https://www.lesslethal.com/products/12-gauge/als120c-detail>
23. ALS1216CS: Rubber Fin Rocket (Direct Fire) With CS Powder. [online] <https://www.lesslethal.com/products/12-gauge/als1216cs-detail>
24. ALS1216BPOC: Powder Rocket Barricade Penetrator, OC. [online] <https://www.lesslethal.com/products/12-gauge/als1216bpoc-detail>; 12 Gauge Barricade Penetrator. [online] <https://www.nonlethaltechnologies.com/12-BP.htm>
25. Flocchi Special Application Breaching Ammunition 12 Gauge 2-3/4" 540 Grain Polymer Encapsulated Lead Shot. [online] <https://www.midwayusa.com/product/1019391860>
26. ALS1210S: Door Breaching Cartridge (375 Grain Frangible Copper-Tin Slug). [online] <https://www.lesslethal.com/products/12-gauge/als1210s-detail>
27. 12 Gauge Flash Bang / Muzzle Bang. [online] <https://www.nonlethaltechnologies.com/12-FB.htm>
28. SKYNET Mi-5: SkyNet Drone Defense [online] <https://www.lesslethal.com/products/12-gauge/als12skymi-5-detail>
29. Sagi, G. Mossberg 590: Top-Selling Pump Shotgun of 2019. *NRA American Rifleman*. 08.04.2020. [online] <https://www.americanrifleman.org/content/mossberg-590-top-selling-pump-shotgun-of-2019/>
30. Top 10 Shotguns of 2021. [online] <https://www.gungenius.com/top-selling/guns/top-10-shotguns-of-2021/>
31. Poole, E. *Military Peculiarities: The Benelli M1014*. 30.06.2016. [online] <https://www.gunsandammo.com/editorial/military-peculiarities-the-benelli-m1014/248448>
32. Sadowski, R. *Don't Blink! Beretta 1301 Tactical Shotgun Review*. 07.01.2016. [online] <https://gundigest.com/gun-reviews/dont-blink-beretta-1301-tactical-shotgun-review>
33. Suci, P. *Why the Kel-Tec KSG Tactical is a True Tactical Shotgun*. 21.01.2021. [online] <https://nationalinterest.org/blog/buzz/why-kel-tec-ksg-tactical-true-tactical-shotgun-176801>
34. *The All New M&P 12 Bullpup Shotgun*. [online] https://www.smith-wesson.com/mp12?utm_source=Athlon&utm_campaign=MP12Bullpup&utm_medium=display&utm_content=BallisticTacticalLife&utm_term=native
35. Rozin, I. *Kakvo pravi ruskata „Vepr“ edna ot nay-dobrite pushki v sveta?* 17.03.2019. [online] <https://bg.rbth.com/science/329881-ruski-vepr-sred-naj-dobrite-pushki-v-sveta>
36. *Karabin spetsialnii 18,5 KS-K: Spetsialnoe gladkostvolynoe oruzhie blizhnego boya dlya sil ohrani pravoporyadka*. [online] https://ak.kalashnikovgroup.ru/card/karabin_spetsialnyy_18-5_ks-k

ВЪЗНИКВАНЕ И РАЗВИТИЕ НА МОРСКИЯ „СПЕЦНАЗ“ НА РУСИЯ

капитан III ранг Георги Калинов

Военна академия „Г. С. Раковски“, g.k.kalinov@rmdc.bg

Резюме: За водата с право се смята, че предоставя едни от най-тежките условия за действие на командоси. За разлика от сухопътните, операциите във водна среда трябва да бъдат сериозно осигурени от уникални ССО и средства. Специалните операции на море обикновено са много сложни и изискват много висока степен на оперативна готовност. Уменията на морските ССО на Русия са строго специфични и без постоянни и реалистични тренировки и учения се стига до отслабването им, което крие голям риск за хората и операциите. Проникването и действието по въздух, вода и суша на бойните пливци ги прави уникална и ценна бойна единица за флота на всяка една държава. Руската федерация притежава изключително голям брой такива формирования както с нападателни, така и с отбранителни функции.

Ключови думи: *водолази-разузнавачи; бойни пливци; Сили за специални операции; ПДСС; МРП; ВМФ; СПЕЦНАЗ; СССР; Русия*

ORIGINE AND EVOLUTION OF RUSSIAN NAVAL “SPECNAZ”

Lieutenant-commander Georgi Kalinov

Rakovski National Defence College

Sofia, Bulgaria

E-mail: g.k.kalinov@rmdc.bg

Abstract: It is for sure that water is the most severe military environment for Special Forces. In comparison with the land operations, the waterborne operations must be ensured with unique SOF units and assets. The waterborne special operations are usually very complex and require high level of operational readiness. The Russian naval SOFs' skills are quite specific, and lack of constant and realistic training end exercises could lead to reduce power, which could endanger the people and operations. Infiltration and operating in air, sea and land, make combat swimmers unique and valuable combat unit for each countries' NAVY. Russian Federation have a large number of that kind of military detachments, which ensure offensive and defensive operations.

Keywords: *combat diver; combat swimmer; Special Operation Forces; PDSS; MRP; NAVY; SPECNAZ; USSR; Russia*

Бойните действия под вода имат корени още от древността. С развитието на водолазното дело паралелно се явява и нуждата от бойни подразделения с такива способности. За първи път, от гледна точка на съвременното разбиране за тези подразделения, бойни пливци са използвани през Първата световна война на 31 октомври 1918 г. от ВМС на Италия, които потапят флагмана на австро-унгарския флот. През Втората световна война също са регистрирани редица успешни случаи на използване на бойни пливци за разузнаване на военноморски бази и крайбрежия, миниране на обекти и потапяне на кораби. Поради въвеждането на тези тактики в морския бой и техния голям успех, се доказва, че има бъдеще за подобен тип подразделения и редица държави започват да проучват възможности за тяхното създаване².

Информацията за произхода и развитието на морски командоси винаги е била чувствителна и оскъдна в световен мащаб, особено за страна като Русия, която е с една от най-големите и боеспособни армии в света. В началото на 30-те години на миналия век с изобретяването на леководлазното снаряжение на основа кислородни дихателни апарати се създават предпоставки за използване в разузнавателно-диверсионните части, способни скрито да преодоляват водни прегради. Първа възможност за оценка на способностите се прави от инженерните войски на СССР, които правят и първите опити в подобна дейност, тъй като са компетентни по минно-поддривната подготовка. Въпреки това предшественици на

бойните водолази от ВМФ на СССР са сухопътните диверсанти, които са участвали в учения на Тихоокеанския флот през 20 – 22 октомври 1938 г., където изпълняват десант от подводница Щ-112.

На 11 август 1941 г. в разгара на Великата отечествена война под Ленинград се създава рота с особено назначение (от тук идва и терминът „ОСНАЗ“) – **първото съветско подразделение бойни пливци** с щат 146 човека, с 3 катера и 4 автомобиля и мотоциклети. По време на войната подводните диверсанти извършвали подривна дейност, разминирание, разузнаване и наблюдение на конвои. През 1942 г. е проведен налет* на катерна база в Стрелна (Ленинград), както и разрушаване на пристана в Нижний парк в Петергоф. Това е първата в историята на ВМФ на СССР диверсионна операция, осъществена под вода.

През август 1944 г. водолазите-разузнавачи провели специфична операция по вдигането на потънала немска подводница U-250 във Виборгския залив, която събудила интереса на съветското командване, тъй като немската авиация се е опитвала да я унищожи на няколко пъти. Работата на пределни дълбочини за онова време не попречила за успешното издигане на подводницата, в чиито торпедни апарати били намерени важни документи и най-новите немски торпеда Т-5, неизвестни за СССР и съюзниците. Въпреки доказаната роля, ротата е разформирована на 20 октомври 1945 г., като част от личният състав преминава в аварийно-спасителната служба на флота, а друга – в запаса⁶.

След известно прекъсване, на 20 май 1953 г. са създадени отново части със специално предназначение на флота – морски разузнавателен пункт (МРП). Същата година в Черноморския флот (ЧФ) е сформирани първият МРП със специално назначение, дислоциран в залив под Севастопол с щат 72 души. И така в 1967 г., по заповед главнокомандващия ВМФ, е създаден и учебно-тренировъчен отряд леководолази на Краснознамения Черноморски флот. Опитът от ученията през 60-те години потвърждава необходимостта от създаване на подобни подразделения във всички флотове. Така били сформирани седем МРП-та и 315-и учебен отряд леководолази (в.ф. 20884) в Киев⁷.

През 1969 г. се създават и отрядите за защита от подводни диверсионни сили и средства (ПДСС) във всеки флот. Тук е добре да направим разлика във видовете подразделения и понятия в Руския ВМФ. **Водолази-разузнавачи** са специално обучени военнослужещи за изпълнение на офанзивни бойни задачи под и над вода в пристанища, акватории и бреговете на противника, които са обособени в подразделения със специално назначение (СПН), откъдето идва и терминът **СПЕЦНАЗ**. **Бойни пливци** са водолази, използвани за изпълнение на дефанзивни задачи по защита на собствените кораби и брегови съоръжения от ПДСС на противника, които са обособени обикновено във формирования към военноморските бази. Под термина **ПДСС** се има предвид диверсионно-разузнавателни подразделения, техническите им средства за доставка (движители), тяхното снаряжение (навигационни прибори, разузнавателна и свързочна апаратура), въоръжение (специални мини и заряди, както и автомати и пистолети за подводна стрелба) за изпълнение на задачи по морски и брегови обекти от критичната инфраструктура⁸.

Следват години на подготовка и усъвършенстване в периода на Студената война, където бойците изпълняват различни задачи по охрана и разузнаване на брегови обекти. Ежегодно се провеждат различни учения по разузнаване, проникване и учебно минирание на различни обекти на територията на Калининградския район, а също и в Лиена, Талин, Балтийск и на други места. Спецназът на ВМФ изпълнява задачи там, където са и другите военни съветници от СССР – Ангола, Виетнам, Египет, Мозамбик, Никарагуа, Етиопия и др. страни, често по молба на техните правителства. В Ангола и Никарагуа бойните пливци охраняват съветските кораби и обучават местните въоръжени сили. През 1978 г. в Хавана, Куба, обезпечават съвместно с Група „А“ охраната на подводната част на корабите „Грузия“ и „Леонид Собинов“, задържани за размяна на делегати на борда⁹.

От 24 февруари до 27 април 1982 г. група за първи път изпълнява бойно дежурство на кораб от ТОФ. В периода 1988 – 1989 г. в течение 130 денонощия се намира в бойно дежурство група, снабдена с подводен двигател „Сирена“ и пълен боекомплект. След разпадането на Съветския съюз някои от частите остават към Република Украйна.

Спецназът на ВМФ не взема участие във войната в Афганистан, но взема активно участие в Първата чеченска война под прикритие в морската пехота през 1994 – 1996 г., където във военните действия загиват двама военнослужещи. През лятото на 1997 г. се изпълняват специални задачи и в Република Дагестан.

*Налет – скрито придвижване и внезапно нападение от усилена група, върху предварително избран и добре изучен обект с цел унищожаване, залавяне на пленници, образци въоръжение, снаряжение и др., възстановяване контрола върху чувствителни въоръжения, техника или материали. [НП 3.5, с. 71]

През 2008 г. морската пехота и Спецназът на ЧФ участват в първия след 1944 г. съвременен военен конфликт в Черно море, когато в период от 8 до 13 август се провеждат бойни действия в Грузия (Петдневната война). След превземането на гр. Потий бойните пливци от ЧФ провеждат операция съвместно с подразделения на въздушно-десантни войски (ВДВ) по затопяване на намиращите се там кораби на ВМС на Грузия, като освобождават екипажите преди десанта на морската пехота и ударите на авиацията.

През май 2010 г. в източната част на Аденския залив сомалийски пирати пленяват танкера „Московский университет“, изцяло с руски екипаж. Екипажът на танкера успял да съобщи за нападението, като спира хода на кораба и се барикадира. Големият руски противолодвоен кораб „Маршал Шапошников“, намиращ се в Арабско море, се насочва към района на сигнала, на борда на който има група със специално назначение от ВМФ. След планирана кратка атака заложниците са освободени за 22 минути без загуби от руска страна.

Есента на 2014 г. 431-ви МРП взема активно участие в събитията известни като „Кримска есен“. В периода от 22 февруари до 15 март 2014 г. се провежда операция по блокиране, а после – завземане на обекти на Министерство на отбраната и МВР на Украйна на територията на п-в Крим.

Командването на Силите за специални операции (ССО) на въоръжените сили на Руската Федерация е новосъздадена структура в рамките на руските въоръжени сили. Официално е формирано през 2009 г. и по план трябва да придобие окончателната си форма към 2018 – 2020 г. Командването е на директно подчинение на началника на Генералния щаб, докато бригадите, полковете и отделните отряди са на двойно подчинение, от една страна, на Главно разузнавателно управление (ГРУ) на Генералния щаб и, от друга, на военните окръзи, отделните армии и флотове. Морските ССО на ГРУ са еквивалентът на бригадите „СПЕЦНАЗ“. Докато бригадите са компонентът за наземни СО в поддръжка на СВ, то морските разузнавателни пунктове са компонентът за СО по море в интерес на военните флотове.

Мирновременният щат на един МРП включва около 124 души. От тях 56 са командоси, а останалите са команден и логистичен персонал. Състав – щаб, две роти СпН (разузнаване и диверсии), рота за подводно миниране, свързочна рота, взводове за МТО и охрана. В ротите има групи разделени по 14 човека. В тях има по-малки групи със специално назначение по 6 човека за по-голяма автономност – 1 офицер, 1 мичман и 4 матроса. По-голямо подразделение от МРП се явява бригада със специално назначение (брспн). Такава бригада е имало в периода на Студентата война в гр. Севастопол на Черно море. Малко преди разпада на СССР 17-а отделна брспн ВМФ СССР се трансформира в 1464-и МРП, който по-късно преминава към Република Украйна. За определен период съществува и 801-и отделен отряд за борба с ПДСС в гр. Севастопол. В състава му влизат отделения за борба с бойни пливци, група СпН и осигуряващи подразделения⁹. След анексирането на полуостров Крим от Руската Федерация през 2014 г. пунктът и отрядът престават да съществуват, а личният състав е прехвърлен в различни формирования на ВМС на Украйна, предимно в ССО.

В подчинение на всеки флот на Русия има по един пункт:

- 561 МРП СпН (в.ф. 10617) – Парусное, Калининградска област, Балтийски флот;
- 388 МРП СпН (в.ф. 43071), предишни 137-ми и 431-ви – Севастопол. Туапсе, Черноморски флот;
- 420 МРП СпН (в.ф. 40145) – Зверосовхоз, Мурманска област, Северен флот;
- 42 МРП СпН (в.ф. 59190) – о. Русский, Владивостокски окръг, Тихоокеански флот.

За разлика от ССО на ГРУ, спецназът на ВМФ е подчинен единствено на конкретния военен флот. Изпълняват задачи по прикритие на собствените сили, а също и надводните и подводните средства от диверсионни действия на противника. Във всяка военноморска база има по един отряд за борба с подводните диверсионни сили и средства (ОБ с ПДСС). Мирновременният щат е от около 60 души, като включва щаб, взвод минно-подривници, взвод бойни пливци и осигуряващи подразделения.

Балтийският флот включва:

- 313 ОБ с ПДСС (в.ф. 10742 – Балтийск);
- 473 ОБ с ПДСС (в.ф. 39080 – Кронщат, до Санкт Петербург).

Северният флот включва:

- 140 ОБ с ПДСС (в.ф. 69068 – Видяево, Мурманска област);
- 152 ОБ с ПДСС (в.ф. 13106 – Полярни, Мурманска област);
- 160 ОБ с ПДСС (в.ф. 09619 – Заозьорск, Мурманска област);

- 269 ОБ с ПДСС (в.ф. 30853 – Гаджиево, Мурманска област);

- 153 ОБ с ПДСС (в.ф. 34242 – Гремиха).

Тихоокеанският флот включва:

- 159 ОБ с ПДСС (в.ф. 87200 – Павловск, залив Разбойник, Приморски край);

- 311 ОБ с ПДСС (в.ф. 59048 – Петропавловск, Камчатски край).

Каспийска флотилия включва:

- 137 ОБ с ПДСС (в.ф. 72969 – Махачкала, Република Дагестан).

Черноморски флот включва:

- 102 ОБ с ПДСС (в.ф. 27203 – Севастопол, Град с федерално значение Севастопол);

- 136 ОБ с ПДСС (в.ф. 75976 – Новоросийск, Краснодарски край).

В 2012 г. за осигуряване безопасността на Зимните олимпийски игри в Сочи (7 – 23 февруари 2014 г.) в гр. Туапсе се създава временно военно формирование 777-и ОБ за ПДСС. В него се носят предимно дежурства на вода и под вода, като личният състав е формиран от останалите отряди⁸.

Водолазите-разузнавачи разполагат с голям арсенал от въоръжение и снаряжение, което включва различни оръжия за стрелба под („АПС“, „СПП-1“) и над вода („АДС“), магнитни мини, водолазни апарати с открита и затворена схема на дишане, системи за разузнаване и свързка, както и подводни движители от ново поколение. Изпълняват се и парашутни скокове на вода с ВиС с парашути Д-6, ПО-9, СВП-1 с ПВ-3 и др. През годините са разполагали и с мини-подводници тип „Тритон“.

Отрядите за ПДСС също са въоръжени с подобни оръжия, макар и не с най-новите водолазни апарати, и различни модификации на подводни движители („Сирена“, „Протон“, „Протей“). Разполагат също с ръчен противодиверсионен гранатомет ДП-61, ДП-64. На въоръжение са и съвременните противодиверсионни катери пр. 21980 „Грачонок“, бързоходен брониран катер пр. 03160 „Раптор“ (който се използва и от ССО), автономен подводен необитаем апарат „Гавия“ за разузнаване на подводната обстановка, както и Противодиверсионен брегови самоходен реактивен комплекс ДП-62 „Дамба“⁶.

Процесът на подбор и подготовка за морския СПЕЦНАЗ се провежда непрекъснато. Програмата включва в себе си следните подготовки: водолазна, парашутно-десантна, топографска, алпийска, морска, физическа, огнева (в т.ч. и с чуждестранни оръжия), минно-поддривна, специализиран ръкопашен бой, оцеляване, знания за въоръжените сили на вероятния противник, свързочна и др. Значително време се отделя на действия под вода – проникване на територията на противника и евакуация по вода, ориентирание под вода, наблюдение в условия на лоша видимост, преследване на противника и откъсване от преследвания, маскировка на дъното. Някои от нормативите, които трябва да се покрият от водолазите-разузнавачи, включват бягане и плуване на дълги разстояния с въоръжение и снаряжение. Медицинските изисквания за водолази и парашутисти са завишени, като се правят непрекъснати специализирани изследвания.

Безспорно най-подготвеният специално морско формирование е отряд „Делфин“ към ГРУ. Създаден през 1970 г., той е специално разузнавателно-диверсионно формирование, предназначено за тайни операции срещу военноморски бази, командни пунктове за управление и брегови обекти на вероятния противник. Подборът и подготовката са изключително сурови и се провеждат в дълбока секретност. Служителите са само офицери, които преминават 26-седмично обучение в различни бази, разделено на 3 етапа. В подготовката се включват теми, които не са залегнали в плановите на другите подразделения с морски командоси, включително боравене с чуждестранно оръжие и изучаване на чужд език, тъй като бойците се подготвят за задачи извън СССР и се разпределят по региони. Набляга се на способности за неутрализиране на противник, както и оцеляване и избягване от плен. С падането на режима на управление в СССР отрядът е разформирован през 1990 г., като личният състав преминава предимно в отрядите за борба с ПДСС и МРП¹.

В наши дни към морския СПЕЦНАЗ се причисляват и отделни водолазни подразделения от Група „А“ и „В“ на Федералната служба за безопасност (ФСБ) на Русия. Група „А“ изпълнява предимно антитерористични задачи на собствена територия, докато група „В“ – зад граница (подобно на разформирования отряд „Делфин“). В тези подразделения служат само офицери и са въоръжени с най-съвременното оръжие и екипировка.

Други водолазни подразделения има в Морската пехота, които изпълняват предимно разузнавателни задачи, предхождащи десант, както и във Федерална служба „Войски“ на националната гвардия на

Русия (бившите Вътрешни войски), имащи полицейски функции, и изпълняват задачи по защита на обекти от критичната инфраструктура на море и във вътрешността на страната.

В съвременната политически нестабилна среда се доказва необходимостта от поддържане и развитие на морски ССО не само в Русия, но и във всички държави с излаз на море, защото са един изключително ефективен инструмент за провеждане на специални операции в приморско направление и осигуряване на действията на ВМС в пълния спектър от мисии и задачи, както и за гарантиране на сигурността в регионите.

ЛИТЕРАТУРА

1. Митева, Р., Григоров, П. *Морските дяволи*. София: Распер, 2000.
2. Чонев, Ч. *Подводните диверсанти*. София: Еър Груп 2000, 2000.
3. Зарембовский, В., Колесников, Ю. *Морской спецназ. История 1938-1968 гг.*, Санкт-Петербург: Галейя Принт, 2001.
4. Колесников, Ю. *Морской спецназ*. Яуза: Эксмо, 2004.
5. Колонтаев, К. *История сил специального назначения Черноморского флота*, 2017.
6. Миллер, Д. *Подводный спецназ – история, операции, снаряжение, вооружение, подготовка боевых пловцов*. Минск: Харвест, 1998.
7. Министерство Обороны СССР. *Военно-морской словарь*. Москва: Военное издательство, 1990.
8. Пашиц, В. *Подводный спецназ России*. Яуза: Эксмо, 2006.
9. Тарас, А., Бешанов, В. *Люди лягушки. История подводных диверсионных средств и сил*. Минск: Харвест, 2000.

REFERENCES

1. Miteva, R., Grigorov, P. *Morskite dyavoli*. Sofia: Rasper, 2000.
2. Chonev, Ch. *Podvodnite diversanti*. Sofia: Ear Grup 2000, 2000.
3. Zarembovskiy, V., Kolesnikov, Yu. *Morskoy spetsnaz. Istoriya 1938-1968 gg.*, Sankt-Peterburg: Galeya Print, 2001.
4. Kolesnikov, Yu. *Morskoy spetsnaz*. Yauza: Eksmo, 2004.
5. Kolontaev, K. *Istoriya sil spetsialnogo naznacheniya Chernomorskogo flota*, 2017.
6. Miller, D. *Podvodnyy spetsnaz – istoriya, operatsii, snaryazhenie, vooruzhenie, podgotovka boevayh plovtsov*. Minsk: Harvest, 1998.
7. Ministerstvo Oboronay SSSR. *Voenno-morskoy slovar*. Moskva: Voennoe izdatelystvo, 1990.
8. Pashits, V. *Podvodnyy spetsnaz Rossii*. Yauza: Eksmo, 2006.
9. Taras, A., Beshanov, V. *Lyudi lyagushki. Istoriya podvodnykh diversionnykh sredstv i sil*. Minsk: Harvest, 2000.

ФАКТОРИ ВОДЕЩИ ДО ТРАНСФОРМАЦИЯ НА ОПЕРАЦИИТЕ В ОТГОВОР НА КРИЗИ

гл. ас. д-р инж. Данко Фаразов

Военна академия „Г. С. Раковски“, *d.farazov@rmdc.bg*

Резюме: С бурното развитие на компютърните технологии и широката им комерсиализация и достъпност създадоха нова среда за информационните процеси. Тези процеси постепенно обхващаха широки категории потребители във всички сфери на приложение. За съжаление, обаче това създаде и един нов източник на заплахи. Това ново „бойно“ поле, макар и виртуално има възможността да създава реални заплахи, които нанасят дори и значително по-големи разрушения и щети от използването на конвенционални военни средства.

Ключови думи: *кибер сигурност; кибер отбрана; квантови компютри; НАТО; ЕС*

FACTORS LEADING TO TRANSFORMATION OF CRISIS RESPONSE OPERATIONS

Assist. Prof. Danko Farazov, PhD

Rakovski National Defence College

Sofia, Bulgaria

E-mail: *d.farazov@rmdc.bg*

Abstract: Rapid development of computer technology and its widespread commercialism and accessibility, they have created a new environment for information processes. These processes have gradually reached broad categories of users in all areas of application. Unfortunately, this has also created a new source of threats. This new “battlefield”, even virtually, has the potential to create real threats that cause even greater destruction and damage than conventional military means.

Keywords: *cyber security; cyber protection; quantum computers; NATO; EU*

Съвременните военни операции, на които ставаме свидетели през последните две десетилетия са продиктувани най-вече от специфичните условия на средата, които определят и техния характер, параметри, интензивност, цели, средства и методи на провеждане. Избраното до тук, показва, че когато говорим за тясно военните аспекти, можем да го фокусираме от широкия контекст на политическите, икономическите и социални аспекти към чисто военната дейност в оперативните измерения на даден конфликт. Оперативните измерения от своя страна се обуславят от оперативните фактори на средата. Тяхната промяна е пряко свързана с постоянната трансформация при използване на военни способности в редица съвременни операции.

Един от факторите на оперативната среда, който през последните три десетилетия достига изключително развитие, е информационният фактор. Той се обуславя от три направления – изкуствения интелект, квантовите компютри и все по-голямата цифрова свързаност.

Процеси, обуславящи трансформацията на оперативната среда

В контекста на все по-широките и дълбоки процеси на глобализма, като че ли се пропускат други процеси, които са свързани с редица трансформации. На първо място, тава е развитието на високите технологии, за които вече научаваме само от рекламите, без да си даваме сметка за промените, които те предизвикват около нас.

Бурното развитие на информационните технологии дава силен тласък на оперативния фактор информация, като го превърна реално в основен. Разбира се, тук говорим основно за тези кризи и конфликти, които не са в категорията на класическа междудържавна война, въпреки че днес наблюдаваме точно този процес дори и във войната между Русия и Украйна, където руската пропаганда е почти буквално блокирана в цял свят. Не е новост на изключителното значение на информацията по време на война, независимо дали става въпрос за гражданска, междудържавна и по-голяма регионална война.

Информацията винаги е била и ще бъде ключът към успеха, основно в две направления – за въздействие върху противника и в областта на разузнаването. Целта на доклада обаче е значително по-различна от този смисъл. Идеята е да се представи физическата среда, в която съществува информацията, която е тясно свързана с главоломното развитие на цифровите технологии в наши дни и предизвиква качествено ново изменение на военните операции.

От гореизложеното трябва да се отбележи, че качествените промени не само изискват, но и налагат доктринални и концептуални промени в глобалната среда, националната и най-вече във военната област. Независимо че разглеждаме информационния фактор като част от факторите на средата, трябва да се има предвид, че киберпространството вече е съвсем различна среда, в която се провеждат „бойни действия“ и в която съществуват други и различни процеси, характеристики и физични закони от тези на класическата бойна среда. Новите закономерности и процеси от своя страна поражда не само нови предизвикателства и възможности, но и нови рискове и заплахи. Един от факторите, които ги обуславя е изключително бързото развитие на информационните технологии, което не позволява, дори и относително за кратко време, да бъдат запазени постоянни отношения и процеси в новото пространство. В този смисъл е и доклада за „Китайската заплаха по време на квантовата ера“. В него експерти на компанията Booz Allen Hamilton предупреждават, че Китай възнамерява да похищава огромни обеми данни, които след това да декриптира с помощта на квантови компютри и да използва информацията за свои собствени цели. Най-голям интерес представляват промишлените данни и по-конкретно, данните от сферата на икономиката и информационната безопасност.

Експертите изразяват безпокойство, че само след две-три години е напълно възможно да стане лидер в разработването и разгръщането на първите практически сценарии с използване на квантови компютри.

Китайските хакери са в състояние да откраднат криптирани и шифрирани данни, които остават ценни в дългосрочна перспектива – биометрични маркери, секретен данни на служители на разузнаването, номера на социалното осигуряване, чертежи на нови оръжия и т.н. Въпреки че тази информация е добре криптирана, Китай може да използва квантови компютри, с помощта на които лесно да я декриптира.

В доклада се казва още, че Китай няма как да не се заинтересува от използването на квантови технологии за създаването на изкуствен интелект от съвсем ново поколение. Това може да се окаже опасно за националната сигурност на САЩ и на другите държави.¹

Този доклад, колкото и да е спорен, недвусмислено показва размера и реалната опасност на заплахата, независимо откъде ще дойде тя. Като се има предвид характерът на съвременните военни кризи, където буквално състоянието на война и мир е размито до степен, която не позволява да се постави ясна граница между чисто военната и гражданската (цивилната) сфера, технологиите и рисковете, които те поражда, задължават да бъдат вземани мерки от най-широкия смисъл – на националното и наднационалното равнище, до най-тесния военен аспект. Именно това налага да се разглежда и киберсигурността в България на базата на регулаторните инструменти, политики и стратегии на НАТО и ЕС, които влияят на кибер сигурността.

Политика за киберотбрана в НАТО

Преди повече от 10 години, през 2007 и 2008 г., НАТО за първи път разработва и приема два документа в областта на киберотбраната (NATO Cyber Defense Policy, 20 December 2007 и NATO Cyber Defense Concept, 13 March 2008).

Три години по-късно, на срещата на върха в Лисабон през 2010 г. е взето решение Северноатлантическият съвет да разработи цялостна политика на НАТО в областта на киберотбраната и да подготви План за действие за нейното прилагане. В изпълнение на взетото решение, през 2011 г. министрите на отбраната на НАТО одобряват Политика на НАТО за киберотбрана, която определя визия и план за действие с цел гарантиране на координирани действия на Алианса в контекста на бързо развиващата се стратегическа среда за сигурност².

Същността на политиката на НАТО за кибер отбрана включва:

- интегриране на киберзащитата в процесите на планиране на Алианса, за да се изпълняват пълноценно основните задачи на НАТО за колективна отбрана и управление при кризи;
- съсредоточаване върху превенцията, гарантиране на устойчивостта и защитата на критичните киберинфраструктури на НАТО и на съюзниците;

- създаване и поддържане на стабилни способности за киберотбрана и централизирана защитата на мрежите на НАТО;
- разработване на минимални изисквания за киберзащита на националните мрежи, които са от критично значение за изпълнението на основните задачи на НАТО;
- осигуряване на съдействие на съюзниците за постигане на минимално ниво на киберзащита и намаляване на уязвимостта на националните критични инфраструктури;
- ангажиране с партньори, международни организации, структури в частния сектор и с академичните среди³.

На срещата на върха в Чикаго през май 2012 г. лидерите на страните, членки на Алианса отново потвърждават своя ангажимент за подобряване на киберотбраната, като включват всички мрежи на НАТО под централизирана защита и осъществяват поредица от действия за развитие на способностите на НАТО в отговор на компютърни инциденти (NATO Computer Incident Response Capability – NCIRC)⁴. В изпълнение на приетите решения, през същата година киберотбраната става неотменна част от процеса на отбранително планиране в НАТО.

През февруари 2014 г. министрите на отбраната на НАТО вземат решение да се разработи нова, подобрена политика в областта на киберотбраната, която по-късно е одобрена на срещата на високо равнище в Уелс през 2014 г. Освен това по време на срещата на върха на НАТО в Уелс, съюзниците приемат, че международното право се прилага в киберпространството и, че въздействието на кибератаките може да бъде толкова опасно за нашите общества, колкото една конвенционална атака. Поради тази причина те могат да предизвикат реакция съгласно чл. 5 от Северноатлантическия договор. В резултат на това киберотбраната е призната като част от основната задача на НАТО за колективна отбрана. Решение за задействане на чл. 5 ще се взема за всеки отделен случай от Северноатлантическия Съвет. Основен акцент е поставен и на изграждането на капацитет и способности за киберотбрана на страните, членки на Алианса, интегрирането на киберотбраната в операциите на НАТО и в процеса на отбранително планиране, както и на необходимостта от повишаване на обмена на информация и постигане на подобрена ситуационна осведоменост между съюзниците. Вземат се важни решения също и по отношение на засилване на партньорствата с Европейския съюз и отделни страни партньори, както и с индустрията. Не на последно място е посочена потребността от подобряване на образованието и обучението в областта на киберотбраната в Алианса⁵.

На срещата на върха във Варшава през 2016 г. са взети важни решения, които по-нататък развиват и усъвършенстват политиката на НАТО в областта на киберотбраната. На първо място, държавните и правителствените ръководители потвърждават, че киберотбраната е част от основната задача на НАТО за колективна отбрана и, че съюзниците могат да разчитат на колективна отбрана в отговор на значителна кибератака, еквивалентна на въоръжено нападение. Освен това, киберпространството е дефинирано като домейн на бойното пространство, наред с въздуха, морето и сушата⁶.

В приета по време на срещата Cyber Defence Pledge се посочва, че съюзниците потвърждават поетите национални отговорности съгласно чл. 3 от Вашингтонския договор и в областта на киберотбраната. Те заявяват готовност да работят за изпълнение на приетата по време на срещата на високо равнище в Уелс подобрена политика в областта на киберотбраната. Наред с това се потвърждава ролята на сътрудничеството между НАТО и ЕС за гарантиране сигурността в киберпространството. Изграждането и развитието на националните способности за киберотбрана се определят като приоритет. Друг основен акцент в документа е подобряване на капацитета и осведомеността на всички заинтересовани страни, както и засилване на сътрудничеството и обмена на информация между тях. Не на последно място се отделя специално внимание на ролята на образователните институции в Алианса за подобряване на образованието и обучението в областта на киберотбраната⁷.

На срещата на върха в Брюксел през 2018 г. държавните и правителствените лидери на държавите в Алианса потвърждават, че НАТО ще продължи да се адаптира към развиващия се спектър от киберзаплахи, които се осъществяват от държавни и недържавни участници. Препотвърждава се разбирането, че киберотбраната е част от основната задача на НАТО за колективна отбрана. Затова НАТО трябва да може да работи така ефективно в киберпространството, както във въздуха, на сушата и в морето за укрепване цялостната възпираща и защитна сила на Алианса. Киберпространството се разглежда като домейн на операциите. За първи път се посочва, че за да изпълни отбранителната си задача, НАТО ще прилага и използва пълната гама от способности, включително в киберпространството, за да възпира, защитава и

противодействия на целия спектър от киберзаплахи, включително тези, провеждани като част от хибридна кампания.

Друг важен момент, който се посочва за първи път в подобен документ е, че за установяването и противодействието на злонамерени действия в киберпространството, ще се търси координиран отговор, за да се повиши себестойността на една кибер атака и така да се засили възпиращия потенциал на Алианса. На следващо място, ръководителите на държавите и правителствата решават да се създаде нов Център за операции в киберпространството (Cyber Operations Centre) като част от командната структура на НАТО. Центърът трябва да осигурява ситуационна осведоменост и координация на операциите на НАТО в киберпространството. Съюзниците приемат, че НАТО може да използва националните способности на отделните държави членки в киберпространство за своите мисии и операции.

Политика за киберсигурност в ЕС

Цялостната дейност по формиране и реализиране на политиките в областта на киберсигурността и киберотбраната в рамките на Европейския съюз (ЕС) и съответните действия за тяхното изпълнение следва да се разглеждат в контекста на Стратегията на Европейския съюз за киберсигурност от 2013 г. и Заключенията на Съвета. Това са двата ключови документа, които дефинират основните принципи, стратегически приоритети, цели на Съюза и средствата за тяхното постигане в контекста на Общата политика за сигурност и отбрана (ОПСО) и отношенията с НАТО.

В Стратегията категорично е посочено, че основните ценности на ЕС се прилагат с еднаква сила както във физическия, така и в цифровия свят. Същите закони и норми, които се прилагат в други области от ежедневието, се прилагат и в киберпространството. Освен това, всяко споделяне на информация за целите на кибер сигурността, когато могат да бъдат застрашени личните данни, следва да съответства на законодателството на ЕС за защита на данните и да отчита изцяло правата на физическите лица в тази област.

Стратегията дефинира следните три основни принципа на сигурността в кибер пространството:

Първо, осигуряване на свободен и равен достъп на всички до интернет. Ограниченият или липсващият достъп до интернет и „цифровата неграмотност“ се разглеждат като неравнопоставеност за гражданите, като се има предвид в каква степен дигитализацията обхваща обществото. В този смисъл всеки човек трябва да има свободен достъп до интернет.

Второ, гарантиране на демократично и ефикасно управление на множество заинтересовани страни в настоящия модел на управление на интернет, като фактор за киберсигурността.

Трето, съвместна споделена отговорност за гарантиране на сигурността в киберпространството на всички заинтересовани страни, независимо дали са публични органи, представители на частния сектор или отделни граждани. Всички те трябва да приемат тази отговорност и, ако е необходимо, да осигурят координиран отговор за гарантиране на киберсигурността.

Основните стратегически приоритети и действия са следите:

На *първо място* е поддържането на киберустойчивост на национално ниво. В това отношение Стратегията е придружена от предложение за законодателни промени (Директива за мрежова и информационна сигурност) с цел да се установят общи минимални изисквания за мрежова и информационна сигурност (МИС) на национално равнище. Тези изисквания следва да задължат държавите членки:

- да определят национални компетентни органи за МИС;
- да създадат добре функциониращ Национален център за действие при инциденти в информационната сигурност (CERT);
- да приемат национална стратегия за киберсигурност и национален план за сътрудничество в областта на МИС.

Изграждането на капацитет и координацията в областта на киберсигурността се отнасят и до институциите на ЕС. През 2011 г. е създаден екип за реагиране срещу киберинциденти с трансгранично измерение, отговарящ за сигурността на информационните системи на институциите, агенциите и органите на ЕС (CERT-EU), който започва да работи постоянно през 2012 година.

Важни инструменти за поддържане на киберустойчивост са European Public-Private Partnership for Resilience (EP3R), Connecting Europe Facility (CEF) и многонационалните учения на ниво ЕС като Cyber Europe 2018. Важна задача, която Стратегията поставя, е повишаване на ситуационната осведоменост на крайните потребители, което е от изключителна важност за защита на информационните системи и

мрежи и е обща отговорност на всички заинтересовани страни. Не на последно място в Стратегията се поставя акцент на повишаване на националните усилия в областта на образованието и обучението по киберсигурност, чрез въвеждане на обучение в училищата със срок до 2014 г., обучение на студенти по компютърни науки и основно обучение на персонала, работещ в публичната администрация.

Вторият стратегически приоритет е драстично намаляване на киберпрестъпността. Акцентът в тази област е върху създаване и прилагане на силно и ефективно законодателство за борба с киберпрестъпността. В това отношение се препоръчва да бъдат подкрепени държавите членки да идентифицират слабите места и пропуските и да засилят способността си да разследват и да се борят с киберпрестъпността. Основната цел е да се постигне подобрена оперативна способност за борба с нея. Разчита се на Европейския център за киберпрестъпления към Европол, като ключова институция, като и на Евроюст и на Европейския полицейски колеж.

Третият стратегически приоритет е свързан с разработване на политика и способности за киберотбрана в контекста на Общата политика за сигурност и отбрана на ЕС. Стратегията предвижда да се направи оценка на оперативните изисквания на ЕС в областта на киберсигурността и да се насърчи развитието на способности, които да обхващат всички им аспекти, включително доктрината, ръководството, организацията, персонала, обучението, технологиите, инфраструктурата, логистиката и оперативната съвместимост. Освен това се планира разработване на Рамка на ЕС за политика в областта на киберотбраната за защита на мрежите и информационните системи в мисиите и операциите по линия на ОПСО. На следващо място, в Стратегията е предвидено насърчаване на диалога и координацията между гражданските и военните участници в рамките на ЕС – със специален акцент върху обмена на добри практики, обмена на информация и ранното предупреждение, реакцията при инциденти, оценката на риска, повишаването на осведомеността и установяването на киберсигурността като приоритет. Не на последно място се предвижда осигуряване на диалог с международни партньори, включително с НАТО, с други международни организации и многонационални центрове за върхови постижения, за да се осигурят ефективни отбранителни способности, да се определят областите на сътрудничество и да се избегне дублирането на усилия.

Четвъртият приоритет в Стратегията е свързан с осигуряване на промишлени и технологични ресурси за киберсигурност. Тук акцентът е поставен върху насърчаване на единния пазар на ЕС за продуктите, свързани с киберсигурността, стимулиране на разработването и приемането на единни стандарти за сигурност, технически норми и принципи на сигурност. Освен това се обръща специално внимание за насърчаване на инвестициите в научноизследователска и развойна дейност и на иновациите. В това отношение полезен инструмент е Програмата на ЕС „Хоризонт 2020“ за насърчаване на ранното включване на промишлеността и на академичните среди в разработването и предлагането на координирани решения, както и Програмата „Хоризонт Европа“ – следващата рамкова програма на ЕС за научни изследвания и иновации, която също поставя киберсигурността сред своите приоритети.

Петият приоритет в Стратегията е свързан със създаване и прилагане на съгласувана международна политика на Европейския съюз в киберпространството, за да се насърчават основни ценности на ЕС като достойнство, свобода, демокрация, равенство, върховенство на закона и зачитане на основните права на човека. Приоритет е включването на въпросите на сигурността в киберпространството във външните отношения на ЕС и в Общата външна политика и политиката на сигурност.

В заключение, в Стратегията се подчертава, че централизираният подход на ниво ЕС не е най-доброто решение за гарантиране на киберсигурността. Дейностите трябва да се организират и координират между три основни стълба:

- 1) националните органи за мрежова и информационна сигурност;
- 2) правоприлагащите институции;
- 3) министерствата на отбраната.

Проблем е, че те действат в различни нормативни рамки.

Представените по-горе политики на ЕС в сферата кибер сигурността са съгласно изследване на БАН на тема: „Киберсигурност и възможности за приложение на иновативни технологии в работата на държавната администрация в България“⁴⁸

От гореизложеното напълно логично трябва да се представи и Националната стратегия за киберсигурност⁴⁹. В нея са представени основните направления и елементи за развитие на киберсигурността

на България в съвременното киберпростанство, което е свързано основно с дигиталната зависимост, заплахите и киберсигурността, като е фокусирано тяхното въздействие и значение върху предизвикателствата, рисковете и възможностите за развитие и превенция.

Визията за киберустойчива среда очертава стратегическите цели, основните фази на изследване и начините и подходите, където трябва да се насочат усилията и какви резултати трябва да се очакват. Това налага дефиниране на принципи, области на действие, цели и мерки. За установяване и развитие на националната система за киберсигурност и устойчивост е необходимо създаването на политики, стратегии и планове. Организирането на надеждна система за оперативна координация, която да се базира на национален координатор по киберсигурност, формиране на национална система за управление при киберкризи, като това трябва да доведе до повишаване на ролята и отговорностите на държавните структури. Фундамент на киберустойчивостта е мрежовата и информационна сигурност. Тя трябва да доведе до закономерен преход от киберсигурност към киберустойчивост.

Главна цел на мерките в Националната стратегия са фокусирани към киберотбраната и защита на националната сигурност. Това се постига чрез киберразузнаване, противодействие на хибридни заплахи базирани на кибертероризма и киберотбрана, интегрирана във командната структура на въоръжените сили. В Стратегията ясно се казва, че Министерството на отбраната има водеща роля за осъществяване на киберотбраната на страната. За ефективното ѝ реализиране е необходимо да се поддържат и развиват съществуващите и да се изграждат нови високотехнологични способности за киберотбрана, съвместими с тези на НАТО и ЕС, както и адекватни структурни и организационни реформи и развитие на съответните способности.

На тази основа през 2021 г. във въоръжените сили е създадено *Командване за комуникационно-информационна поддръжка и киберотбрана*. Неговата мисия включва осигуряване на устойчива комуникационно-информационна поддръжка и киберотбрана на системата за командване и управление при изпълнение на пълния спектър от мисии и задачи на въоръжените сили (ВС) на Република България.

Функциите, които трябва да изпълнява включват:

- Изграждане, поддръжка и експлоатация на мрежовата комуникационна и информационна инфраструктура, и системата за киберотбрана на въоръжените сили;

- Събиране, съхраняване, обработка, изобразяване, разпространение и обмен на информация за нуждите на системата за командване и управление на въоръжените сили, в ежедневната дейност и при кризи от военен и невоенен характер;

- Изграждане на шлюзове към комуникационно-информационни системи на съюзни, държавни, ведомствени и други организации, при провеждане на операции за защита на суверенитета и териториалната цялост на страната в национален и коалиционен формат, оказване на помощ на централната, областна, местна администрация и населението при бедствия.

На основата на изброените функции, е необходимо формулиране на няколко логично свързани задачи:

- Изгражда, менажира, експлоатира и поддържа комуникационно-информационната среда на системата за командване и управление, като предоставя комуникационно-информационни услуги и осигурява комуникационна свързаност и защитен информационен обмен;

- Изгражда и поддържа оперативен център за киберотбрана (MilCERT) за осигуряването на непрекъснат мониторинг, анализ и реакция при инциденти и атаки в киберпространството;

- Формира и участва в екипи за бързо реагиране при киберинциденти в критичната инфраструктура на страната;

- Осигурява привързване на стационарните пунктове за управление към Интегрираната комуникационно-информационна система за управление на страната;

- Осъществява непрекъснат мониторинг, анализ и реакция при инциденти и кибератаки свързани с функционирането на комуникационноинформационните мрежи и системи с контингентите от Българската армия, участващи в операции и мисии извън територията на страната;

- Възстановява ресурсите на стационарните комуникационноинформационни мрежи и системи.

В подкрепа на изложеното до тук, мога да посоча за пример кибер защитата на САЩ, която е отговорност на киберкомандването, като в момента американската армия разполага със сили, предназначени да се използват непосредствено в зоната на операцията за осигуряване на защита на комуникацията на

силите в съпрекосновение с противника в целия електромагнитен спектър. 915-ти батальон за кибер-война има отговорността за обучението и оборудването на 12 кибер екипа от по 45 войници, които ще се ситурат в рамките на дивизия за осигуряване на устойчивостта и защита на електромагнитния спектър за запазване на цялостта на системата за командване и управление¹⁰.

Сериозното отношение към този проблем на големите държави и съюзи ясно изразява не само важността, но и голямата тревога, която имат в тази посока. Важно е да се подчертае, че проблематиката се усложнява много поради постоянното развитие на тези технологии, борбата между технологичните гиганти в лицето на мултинационалните корпорации от една страна и националните държави от друга. Това създава изключително голяма степен на неопределеност, което пък допълнително способства за значителна несигурност и в резултат на това се стига често пъти до неадекватни мерки, свързани основно с недооценяване на заплахите, ненавременност на действията и грешни подходи при вземане на решение в критични моменти. Допуснатите слабости винаги водят след себе си до верижни реакции от крайно негативни последици.

ЛИТЕРАТУРА

1. Десподов, Даниел. Излезе докладът „Китайската заплаха по време на квантовата ера“. KALDATA, 30.11.2021. [онлайн], достъпно на: <https://www.kaldata.com/it-новини/излезе-докладът-китайската-заплаха-п-373862.html>
2. Lisbon Summit Declaration, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Lisbon. *Press Release 155*, Issued 20 November 2010, p. 11.
3. NATO. *Defending the Networks: The NATO Policy on Cyber Defence*. Brussels: NATO, 2011.
4. Chicago Summit Declaration, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Chicago, *Press Release 062*, Issued on 20 May 2012, pp. 12-13.
5. Wales Summit Declaration, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, *Press Release 120*, Issued on 05 September 2014, pp. 15-16; NATO Policy on Cyber Defence, endorsed by Allied Defence Ministers in June 2014.
6. Warsaw Summit Communiqué, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw, *Press Release 100*, Issued on 09 July 2016, pp. 15-16.
7. Cyber Defence Pledge, *Press Release 124*, Issued on 08 July 2016.
8. *Киберсигурност и възможности за приложение на иновативни технологии в работата на държавната администрация в България*. София: НЛКВ – БАН, 2018, с. 46 – 58.
9. *Национална стратегия за киберсигурност, „Киберустойчива България 2020“*. София: Министерски съвет, 2016.
10. <https://www.meta-defense.fr/bg/2019/05/09/lus-army-подсилва-киберзащитата-от-полевите-единици/>

REFERENCES

1. Despodov, Daniel. Izleze dokladat „Kitayskata zaplaha po vreme na kvantovata era“. KALDATA, 30.11.2021. [onlayn], dostapno na: <https://www.kaldata.com/it-novini/izleze-dokladat-kitayskata-zaplaha-p-373862.html>
2. Lisbon Summit Declaration, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Lisbon. *Press Release 155*, Issued 20 November 2010, p. 11.
3. NATO. *Defending the Networks: The NATO Policy on Cyber Defence*. Brussels: NATO, 2011.
4. Chicago Summit Declaration, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Chicago, *Press Release 062*, Issued on 20 May 2012, pp. 12-13.
5. Wales Summit Declaration, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, *Press Release 120*, Issued on 05 September 2014, pp. 15-16; NATO Policy on Cyber Defence, endorsed by Allied Defence Ministers in June 2014.
6. Warsaw Summit Communiqué, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw, *Press Release 100*, Issued on 09 July 2016, pp. 15-16.
7. Cyber Defence Pledge, *Press Release 124*, Issued on 08 July 2016.
8. *Kibersigurnost i vazmozhnosti za prilozhenie na inovativni tehnologii v rabotata na darzhavnata administratsia v Bulgaria*. Sofia: NLKV – BAN, 2018, s. 46 – 58.
9. *Natsionalna strategia za kibersigurnost, „Kiberustoychiva Bulgaria 2020“*. Sofia: Ministerski savet, 2016.
10. <https://www.meta-defense.fr/bg/2019/05/09/lus-army-подсилва-киберзащитата-от-полевите-единици/>

ОПЕРАТИВНА СЪВМЕСТИМОСТ – СЪЩНОСТ И ПРЕДИЗВИКАТЕЛСТВА ЗА ПОСТИГАНЕ ПРЕД СИСТЕМАТА ЗА КОМАНДВАНЕ И УПРАВЛЕНИЕ

майор Кръстьо Парасков

Военна академия „Г. С. Раковски“, *k.paraskov@rndc.bg*

Резюме: Страните членки на НАТО трябва да могат да извършват военни действия съгласувано помежду си в напълно координиран и максимално интегриран начин. Това се нарича оперативна съвместимост, дефинирана като „способността на системите, силите и средствата да осигуряват обмен на услуги между системи, сили и средства и да използват обменяните услуги, така че това да им позволи да работят ефективно заедно“.

Ключови думи: *оперативна съвместимост; система за командване и управление*

INTEROPERABILITY – NATURE AND CHALLENGES TO ACHIEVE BY THE COMMAND AND CONTROL SYSTEM

Major Krastyo Paraskov

Rakovski National Defence College

Sofia, Bulgaria

E-mail: *k.paraskov@rndc.bg*

Abstract: NATO members must be able to carry out military action in a coherent manner in a fully coordinated and fully integrated way. This is called interoperability, defined as “the ability of systems, forces and means to exchange services between them and to use exchanged services so as to enable them to work effectively together”.

Keywords: *interoperability; command and control system*

Коалиция от 30 държави може да работи ефективно заедно в съвместни операции, само ако е осигурено необходимото взаимодействие. От основаването на Алианса през 1949 г. основна цел на НАТО е да гарантира свободата и сигурността на своите държави членки чрез политически и военни средства. Оперативната съвместимост става още по-важна, откакто Алиансът извършва операции извън пределите на страните членки от началото на 90-те години.

Оперативна съвместимост е възможността да се действа съвместно при изпълнение на поставени задачи¹. Тя често е споменавана като център на тежестта на Алианса и е в основата на успеха на НАТО. Осигуряването на оперативна съвместимост е способността на държавите членки да действат съвместно и да генерират военни способности за изпълнението на поставените задачи и провеждането на оперативни мисии.

Политиката на НАТО за оперативна съвместимост определя термина като способност на съюзниците да действат заедно съгласувано, ефективно и ефикасно за постигане на тактически, оперативни и стратегически цели. По-конкретно, тя дава възможност на силите и средствата и/или системите да работят заедно и позволява споделянето на общи доктрини и процедури, инфраструктура и бази, както и да могат да комуникират свободно. Оперативната съвместимост намалява дублирането, дава възможност за обединяване на ресурси и създава взаимодействие между всички съюзници и когато е необходимо със страни партньори².

Оперативната съвместимост не изисква непременно стандартно военно оборудване. Важното е, оборудването да може да споделя общи съоръжения и е в състояние да взаимодейства, да се свързва и комуникира, да обменя данни и услуги с друго оборудване.

Чрез своите технически (хардуер, оборудване, въоръжение и системи), процедурни (доктрини и процедури) и човешки (терминология и обучение) измерения, допълнени от информацията като критичен

елемент, оперативната съвместимост подпомага изпълнението на инициативи на НАТО като интелигентна отбрана и свързани сили.

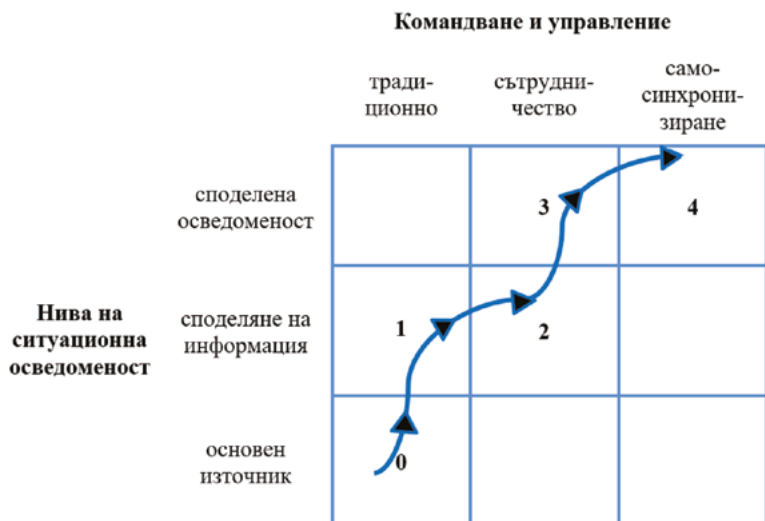
Оперативна съвместимост може да бъде постигната само чрез ефективно прилагане на стандартизация, обучение, тренировки, поуки от практиката, демонстрации, тестове и изпитания.

НАТО е организация, която е постигнала високо ниво на оперативна съвместимост на силите и средствата си чрез десетилетия съвместно планиране, обучение и тренировки. Съвсем отскоро членовете на Алианса прилагат своята оперативна съвместимост на практика и я доразвиват по време на съвместни операции и мисии на Балканите, в Средиземноморието, Афганистан, Либия, Ирак и на други места. Тези операции позволяват и на страните партньори на НАТО да подобрят оперативната съвместимост с Алианса³.

За да направят това успешно, страните членки трябва да могат да извършват военни действия съгласувано помежду си, по напълно координиран и максимално интегриран начин. Това се нарича оперативна съвместимост, дефинирана като „способността на системите, силите и средствата да осигуряват обмен на услуги между системи, сили и средства и да използват така обменните услуги, така че това да им позволи да работят ефективно заедно“.

Това определение предполага, че има няколко нива на оперативна съвместимост, които трябва да бъдат разгледани, за да се гарантира, че силите и средствата са в състояние да действат заедно във военен контекст. Те включват технически характеристики, позволяващи на системите физически да се свързват помежду си и да обменят информация, но и стандартизиране на процедурите и процесите, които да позволят на собствените/приятелските сили и средства да функционират в едно и също пространство и да постигат заложените цели без допускане на приятелски огън. Предполага се, че това се случва на всички нива – от тактическо до стратегическо. С оглед на нуждата от управление на огромното количество информация и за осигуряване на обмен между отделните елементи се изгражда комуникационно-информационна система.

Оперативната съвместимост може да се разбира като спектър от взаимосвързаност, който варира от несвързани, изолирани обекти до напълно интерактивни, споделящи обекти. Разбира се, има различна степен на оперативна съвместимост. Нивата на мрежово-центрични способности, определени в модела за развитие на мрежово-центрични операции (МЦО), пряко съответстват на степента, до която е постигната оперативна съвместимост (фиг. 1).



Фиг. 1. Нива на постигане на оперативна съвместимост

Ниво „0“ изисква ограничена оперативна съвместимост и споделяне на информация. Съществуващата оперативна съвместимост се основава на стандартизирани изисквания за обмен на информация, разработени и използвани от организации, процеси и системи.

Ниво „1“ изисква повече обекти да могат да споделят информация.

Ниво „2“ изисква достатъчна оперативна съвместимост, за да могат обектите да участват в съвместни среди и процеси.

Ниво „3“ изисква субектите да бъдат оперативно съвместими не само в информационната област, но и в когнитивната област, така че да може да се постигне споделена осведоменост.

Ниво „4“ изисква оперативна съвместимост в социалната област, така че действията да могат да бъдат динамично самосинхронизирани.

По този начин преминаването от едно ниво на друго изисква повече оперативна съвместимост във всичките три компонента на информационното пространство (информационна инфраструктура, информационни ресурси и потребители), както и оперативна съвместимост в повече области (не само в информационната, но и в когнитивната и социална области).

Технологиите са от решаващо значение, но сами по себе си не са достатъчни, ако не бъдат интегрирани в организациите, работните потоци и процеси. Напредъкът в технологиите, все по-широкото разпространение на стандартизирани компютърни и комуникационни системи, улесняват процеса по постигане на оперативна съвместимост⁴.

В никакъв случай не е гарантирано, че новите елементи от СКУ, които подлежат на въвеждане в експлоатация, ще взаимодействат с другите елементи без проблем. Това поражда необходимостта от среда за тестване на оперативната съвместимост, така че проблемите да могат да бъдат разпознати и решени, преди да станат критични по време на изпълнението на реални операции⁵.

Различават се три нива на оперативна съвместимост на СКУ (фиг. 2). Оперативното ниво е основно и включва системно и техническо ниво на оперативна съвместимост.

Водещо е техническото ниво: системите трябва да бъдат свързани помежду си коректно, преди да могат да започнат да комуникират. След това е системното ниво на оперативна съвместимост: системите трябва да комуникират, използвайки общи протоколи и стандарти за съобщения. И накрая, на оперативното ниво съвместимостта се заключава в това, че всяка система трябва да разбира напълно съдържанието на съобщенията на други елементи от СКУ и да корелира тези данни със собствената информация⁶.

Валидирането на техническото ниво може да бъде осъществено посредством симулация. Валидирането на оперативната съвместимост на системно ниво може да бъде ограничено до симулационни тестове, включващи елементи от СКУ в затворен цикъл. Валидирането на оперативната съвместимост на оперативното ниво изисква учения и тренировки с личния състав.

Техническото ниво изисква използване на реални комуникации на интерфейсите на СКУ (обмен на данни в реално време и канали за обмен на информация). Необходимо е предварително валидиране на оперативната съвместимост на системата. Системното ниво изисква обмен на информация между елементите на СКУ и проверка за правилната ѝ обработка от нейните елементи. Симулации се използват за генериране на синтетична среда (т.е. заплаха, повреда или унищожаване на елемент от системата). Платформа със софтуер на СКУ и симулации, свързани чрез локална мрежа, са достатъчни, за да демонстрират оперативната съвместимост на системата при различни сценарии.

Национални, мултинационални и коалиционни учения, базирани на симулационни платформи и платформи на СКУ, ще бъдат използвани в подкрепа на валидацията на оперативната съвместимост. Факт е, че оперативната съвместимост на СКУ е необходимост и че тя е подложена на непрекъснати подобрения.

Настоящите предизвикателства пред СКУ, свързани с взаимосвързаност (техническо ниво на оперативна съвместимост), са:

- въвеждане в експлоатация на тактическите линкове (различни версии и ограничения в обработваните съобщения);
- въвеждане и тестване на нов хардуер/софтуер (висок риск и цена);
- липса на универсални стандарти за информация в реално време;
- липса на инфраструктура за тестове за взаимосвързаност.

Настоящите предизвикателства пред СКУ, свързани с последователна обработка (системно ниво на оперативна съвместимост), са:

- функционални несъответствия на национални и НАТО СКУ;



Фиг. 2. Нива на оперативна съвместимост

- обща съвместна база данни (за заплахи и др.);
- липса на инфраструктура за системни тестове;
- описание на сценариите на съвместни и компонентни мисии.

Настоящите предизвикателства пред СКУ, свързани с подходящи тактики, техники, процедури и планове (оперативно ниво на оперативна съвместимост), са:

- липса на стандартни процедури и методология за развитие на ПВО и ПРО;
- цената и ограниченията на ученията и тренировките.

Един от най-важните въпроси, които стоят пред интегрираната система за ПВО и ПРО на НАТО, е оперативната съвместимост между всички елементи и по-специално: елементите за командване и управление; тактическа и процедурна координация между силите и средствата за ПВО и ПРО; внедряване и използване на иновативни елементи (например БЛС, лазери и др.).

НАТО и коалиционните партньори могат да подобрят командването и управлението, като превърнат отделните оръжейни системи в отбранителна система. Ефективен начин да се разбере какво трябва да се направи на национално и коалиционно ниво, е да се използват симулации (и при правилно анализирани, изучаване и използване на симулираните елементи в течение на времето те могат да се заменят с реални). Симулационната среда може да бъде основна рамка за обучение⁷.

СКУ на НАТО се очаква да реши много от въпросите за оперативната съвместимост, свързани с тактическия контрол и управлението на мисиите на силите и средствата за ПВО и ПРО, поради това, че е единна интегрирана система. Все пак се изисква взаимодействие и с външни системи и следователно ще продължи да се обръща сериозно внимание на оперативната съвместимост. Трите основни области, които представляват предизвикателство за оперативна съвместимост за ИСПВПРО на НАТО, са:

- оперативна съвместимост между командванията от по-високото ниво (стратегическо, регионално и компонентно) и изпълнителното ниво (центрове за управление и докладване със съответните софтуерни продукти);

- оперативна съвместимост между изпълнителното ниво (центрове за управление и докладване) и оръжейни и сензорни системи;

- оперативна съвместимост между командната структура на НАТО и тези на други държави, действащи заедно в коалиционна среда.

Първите две области могат да бъдат описани като предизвикателства за вертикална оперативна съвместимост (оперативна съвместимост между различните нива на командване), докато последната област е случай на хоризонтална оперативна съвместимост, тъй като се занимава с въпроси в рамките на едно и също ниво на командване и управление.

За ешелони над обединен център за въздушни операции (ОЦВО) (англ. Combined Air Operational Center, CAOC) НАТО разработва стратегическа автоматизирана информационна система за командване и управление. Оперативната съвместимост между двете системи включва преди всичко планиране и свеждане на директиви за задачи от горе на долу, и информация в реално време за ситуацията от сензорите, постъпваща от долу на горе, така че да може да се формира обобщена оперативна картина (англ. Common Operational Picture, COP).

За оперативна съвместимост с национални оръжейни и сензорни системи, които са под контрола на НАТО, СКУ комуникира чрез съществуващите тактически линкове на НАТО за обмен на информация, които тези системи вече използват. СКУ използва стандартизиран протокол за обмен на информация между автоматизирани системи (AWCIES – ACCS WIDE COMMON INFORMATION EXCHANGE STANDARDS) за комуникация с елементи в рамките на СКУ, включително комуникации към и от сензори на НАТО. Данните, свързани с оперативната съвместимост с оръжейни и сензорни системи, се обменят в реално време.

Тактическите линкове са механизми, чрез които системите могат да обменят съобщения в електронен формат и се използват от години за улесняване на комуникацията между системите. Те обикновено се състоят от набор от предварително дефинирани съобщения, които са стандартизирани. Основните тактически линкове, които се използват понастоящем от НАТО, са Link 1, Link 11A, Link 11B, ATDL-1 (Army Tactical Data Link), Link 16, Link 22 и протоколи за обмен на радиолокационна информация като ASTERIX (All-purpose Structured Euro Control Radar Information Exchange).

Текущите предизвикателства за оперативната съвместимост на СКУ са това, че тя е постоянно развиваща се сложна система от свързани системи, която трябва да се управлява⁸. Тя е комбинацията от дейности, извършвани в реално и близко до реалното време, които съответстват на фазите на планиране и изпълнение. Цялостната СКУ включва много елементи, свързани хоризонтално и вертикално. Огромният брой елементи и различията в технологиите през годините на придобиване означава, че съществуват значителни предпоставки за достатъчни нива на оперативна съвместимост.

ЛИТЕРАТУРА

1. Речник на термините и дефинициите, използвани в НАТО, AAP-6. 2020.
2. NATO Interoperability Standards and Profiles, Volume 1, Introduction, Edition N, Version 1, 2021.
3. Interoperability of U.S. and NATO Allied Air Forces: Supporting Data and Case Studies. RAND, 2003.
4. Изследване на цикъла на планиране и поставяне на задачите във ВВК чрез прилагане на Теорията на ограниченията. Long-Term Security Environment Challenges And Armed Forces Capabilities Development. В: Сборник доклади от Международна научна конференция на Военна академия „Г. С. Раковски“, 12 – 14.11.2019 г., част II. София: ВА „Г. С. Раковски“, 2019, с. 166 – 172. ISBN 978-619-7478-35-8.
5. M&S Support to Assessment of Extended Air Defence C2 Interoperability, RTO TECHNICAL REPORT, TR-MSG-006, May 2004.
6. Пак там
7. Interpreting the interoperability of the NATO's communication and information systems, 2019.
8. Кокудева, П. Подходи при изграждането на система от системи в отбраната. В: Международна научна конференция 10 – 11 ноември 2020. София: ВА „Г. С. Раковски“, 2020, с. 48 – 52. ISBN 978-619-7478-58-7.

REFERENCES

1. Rечник на термините и дефинициите, използвани в НАТО, AAP-6. 2020.
2. NATO Interoperability Standards and Profiles, Volume 1, Introduction, Edition N, Version 1, 2021.
3. Interoperability of U.S. and NATO Allied Air Forces: Supporting Data and Case Studies. RAND, 2003.

4. Izsledvane na tsikala na planirane i postavyane na zadachite vav VVK chrez prilagane na Teoriyata na ogranicheniyata. Long-Term Security Environment Challenges And Armed Forces Capabilities Development. In: *Sbornik dokladi ot Mezhdunarodna nauchna konferentsia na Voenna akademia „G. S. Rakovski“*, 12 – 14.11.2019 g., chast II. Sofia: VA „G. S. Rakovski“, 2019, s. 166 – 172. ISBN 978-619-7478-35-8.
5. M&S Support to Assessment of Extended Air Defence C2 Interoperability, *RTO TECHNICAL REPORT, TR-MSG-006*, May 2004.
6. ibidem
7. *Interpreting the interoperability of the NATO's communication and information systems*, 2019.
8. Kokudeva, P. Podhodi pri izgrazhdaneto na sistema ot sistemi v otbranata. In: *Mezhdunarodna nauchna konferentsia 10 – 11 noemvri 2020*. Sofia: VA „G. S. Rakovski“, 2020, s. 48 – 52. ISBN 978-619-7478-58-7.

ВЪЗМОЖНОСТИ ЗА ПРЕДСТАВЯНЕ НА ВОЕННИЯ КОРАБ КАТО СЛОЖНА СИСТЕМА ОТ ЙЕРАРХИЧЕН ТИП

старши инструктор Красимир Ангелов
ВВМУ „Н. Й. Вапцаров“, angelov@nvna.eu

Резюме: В доклада са разгледани характерни особености на военните системи. Извършва се анализ на военния кораб, представен като система от военен характер. При декомпозиране на кораба се акцентира върху области от неговата функционалност, анализът на които би разкрил подсистеми, представляващи интерес при осъществяването на други, по-задълбочени изследвания свързани с безопасната експлоатация на военните кораби.

Ключови думи: военен кораб; сложни системи; свойства и характерни особености; система за безопасност

OPPORTUNITIES FOR REPRESENTING THE NAVAL SHIP AS A COMPLEX SYSTEM OF HIERARCHY TYPE

Senior Instructor Krasimir Angelov
Nikola Vaptsarov Naval Academy
Varna, Bulgaria
E-mail: angelov@nvna.eu

Abstract: The report examines the characteristics of military systems. An analysis of the Naval ship as a system of a military nature is performed. The ship's decomposition focuses on areas of its functionality, the analysis of which would reveal subsystems of interest in conducting other, more in-depth research related to safety operation of naval ships.

Keywords: naval ship; complex systems; properties and characteristics; safety system

1. Общи положения

В наши дни понятието „система“ е широко използвано в различни сфери на живота. Клиланд и Кинг определят системата, като организационно или съставно цяло, набор или комбинация от елементи или части, образуващи отделен комплекс или едно цяло.¹ Според Орлов, системата представлява множество от елементи с определена организация и връзки между тях, т.е. множество, характеризиращо се с единство, цялост, порядък.² Основоположникът на съвременната концепция за системите Берталанфи лаконично, но прецизно формулира системата, като съвкупност от елементи, които взаимодействат помежду си.³ При допълнителното проучване на източници се откриват множество дефиниции на понятието, но в голяма степен те припокриват или надграждат вече използвани формулировки за целите на определено изследване. В настоящото изследване за *система* се приема определението: „Съвкупност от елементи, намиращи се в закономерни отношения и свързани едно с друго, образуващи цялостност и подчинени на определени признаци“. Така дефинирано, понятието дава възможност за определяне на кораба, като сложна система.

Според Величков, *основни свойства* на сложните системи са: негентропийността, системността, отвореността, свързаността, сложността, уникалността и слабата предсказуемост.⁴ За целите на изследването е резонно да се направи съпоставяне на позицията, която заема кораба спрямо посочените свойства. При осъществяването на изследването се допуска, че съществува вероятност тези свойства да бъдат актуални и за кораба.

Корабът като система притежава свойството *негентропийност*, т.е. липса на ентропия. Друг начин по който това свойство може да се използва, е като способността на системата да се самоорганизира. Характеристика, която наблюдаваме, например при извършване на преход по назначен маршрут: Вахтеният офицер на ходовия мостик установява, че основното средство (жирокомпас) за поддържане на курса на кораба е извън строя. След анализиране на ситуацията, той взима решение да продължи плаването, чрез използване на резервно изделие (магнитен компас). С други думи, това означава, че при констатиране на несъответствие в елемент от системата, други елементи се опитват да възстановят този дефицит, като променят функциите си

за действие и едновременно с това осъществяват т.нар. „изключване“ (bypass) на несъответстващия елемент.

Системността е друго основно аксиоматично свойство. Корабът, като система притежава специфични свойства, които не са присъщи за неговите компоненти, те са уникални. За пример може да се посочи способността на кораба да плава, т.е. да осъществява движение по вода от една до друга позиция в двуизмерна пространствена рамка. Средата за осъществяване на тази дейност е водната повърхност на даден басейн (море, река, океан, плавателни канали и фарватери). Субсистемите на кораба също притежават свойства, които не се наблюдават в подсистемите им, т.е. те също притежават свойството системност.

Отвореност – корабът като система съществува в пространството, като въздейства върху него, но от своя страна пространството също осъществява въздействие върху кораба. Могат да бъдат посочени множество примери, като един от тях е наличието на различни хидро-метеорологични условия, които могат да предизвикат промяна в предварително планираните времеви параметри на действието. При наличието на други системи в това пространство, те също оказват въздействие върху него (пространството), както и то оказва влияние върху тях. Различните системи също взаимодействат по между си. Като пример може да се посочат два кораба, които плават на насрещни курсове. Очаквано е, вахтените офицери на мостика да предприемат маневриране по курс и/или скорост за предотвратяване на вероятен инцидент, т.е. всеки от тях изпълнява определени функционални действия чрез които да възстанови равновесието в подсистемите си.

Свързаност – в кораба съществуват множество връзки и взаимоотношения между субсистемите му. Те могат да бъдат от различен характер – от една страна са връзките между човешкия фактор и техническата част на кораба, а от друга – между елементи от човешкия фактор.

Връзките между *човешкия фактор* и *техническата част на кораба* са факт:

– когато при изпълнение на функционалните си задължения човекът експлоатира в голяма част от времето технически средства и съоръжения;

– между едни техническите елементи и други технически елементи, напр. спягането между РЛС и GPS приемник, РЛС и AIS приемо-предавателно устройство, авторулеви и рулева машина и др.

Съществуващите връзки между *елементи от човешкия фактор* са:

– субординиращи връзки между ръководител и подчинен;

– взаимодействие между равнопоставени в йерархичната структура;

– взаимоотношения от междуличностен характер на ниво екипаж и т.н.

Сложност – корабът е определян, като сложно инженерно съоръжение, но сложността в структурата му не го прави автоматично притежател на свойството „сложност“ от гледна точка на системологията. Необходимо е наличието и на т.нар. сложност на функционирането. Без да се търси количествено определяне на тази сложност, може да се потвърди, че до голяма степен това определение може да се приеме за вярно поради множеството функции, които се изпълняват от неговите подсистеми в процеса на експлоатацията му.

Уникалност – всеки кораб няма аналог на своята структура, състав и поведение. Като пример може да се посочи наличието на кораби, които официално принадлежат на един и същ проект. Независимо че при конструирането им се използват едни и същи чертежи и материали, де факто се наблюдава отклонение в основните им размери, което достига до 0,1%*, а това конструктивно се приема за отклонение, но в допустими норми.

Слаба предсказуемост – състоянието в което кораба се намира $S_{1,2}$ в минал период от време $[t_1, t_2]$ не дава с достатъчна достоверност очакването, че в друг период от време $[t_3, t_4]$ корабът ще бъде в аналогично на предходното състояние $S_{3,4}$.

$$S_{1,2} \neq S_{3,4}$$

Това свойство е силно изразено, поради наличието на човешки фактор в системата.

От горепосочените свойства може с висока степен на увереност да се твърди, че корабът в своята същност следва да се разглежда като сложна система. Това от своя страна благоприятства възможността за осъществяване на анализ на военния кораб, като основен вид кораб.

* Бел.авт. Тази величина е представена условно, на база емпиричен анализ на автора за определен проект кораби.

2. Военният кораб, като сложна военна система от йерархичен тип

От дълбока древност човекът е предявявал претенции за осъществяване на плавателна дейност в рамките на реки, езера и морета. С известни условности средствата за осъществяване на тази дейност могат да бъдат наречени кораби. Прието е, че корабът (от гр. *καραβος*) е инженерно-техническо съоръжение, което плава по вода и е предназначено за превоз на хора и товари или за изпълнение на други дейности (риболов, удълбочаване на дъното на водни басейни, прокарване на кабели, изследване на морските пространства и т.н.)⁵ От гледна точка на системологията той може да бъде класифициран, като изкуствено създадена сложна система.⁶

Според Василев сложните системи се характеризират с голям брой елементи и вътрешносистемни връзки, а компонентите на сложните системи могат да се разглеждат като подсистеми, всяка от които може да бъде детайлирана на още по-прости подсистеми.⁷ Интерес би представлявала възможността от разкриване на същностните особености на военния кораб.

Съгласно общоприета дефиниция в международното морско право *военен кораб е всеки кораб, който принадлежи към въоръжените сили на някоя държава, има външни знаци за различаване на неговата националност, намира се под командването на офицер на военна служба, името на когото е вписано в списъка на офицерите от военноморските сили на държавата или в друг подобен документ, и има екипаж, подчинен на военна дисциплина*.^{8,9} Така дефинирано понятието „военен кораб“ дава възможност за извеждане на две подсистеми, които го отличават от т.нар. конвенционални кораби – система за защита на кораба от въздействието на противникови сили и система за въздействие на кораба срещу противникови сили. Възможно е тези две системи да бъдат разглеждани като една обща система за въздействие и противодействие върху други военни системи. Такава възможност е продиктувана от наличието на общи компоненти за управление на посочените системи и общ ресурс за въздействие и противодействие на противниковата система. Компонентът за управление е човекът и/или група от хора в единство с автоматизиран електронен компонент.

За декомпозирането на кораба-система може да се използва функционалният подход. При първо ниво на декомпозиране на военния кораб, който е сложна система от отворен тип, като негови подсистеми или функционални модули можем да определим три основни системи:

– *системата за управление на кораба* – представлява съвкупност от човешки, машинни и информационни ресурси, връзките между тях и процедури, позволяваща на командването на кораба да осъществява управлението му. Основната цел на системата за управление е осигуряване на равновесно състояние на системата-кораб спрямо други системи в пространството и самото пространство, чрез:

- формиране на достоверна обща картина на системата-кораб, други системи, които взаимодействат или биха взаимодействали с нашата система и пространството, в което се намират тези системи, за отминал, настоящ или вероятен бъдещ момент от времето;

- подпомагане вземането на решение от командването на кораба чрез редуциране на времето и нарастване на точността;

- подготовката и дистрибуцията на адекватни към настоящ или бъдещ момент управленски сигнали към субсистеми от кораба.

Системата за управление на кораба осъществява дейности по наблюдение и предупреждение за възможни въздействия на противодействащи системи. Текущото ѝ състояние е в постоянна готовност за осигуряване на възможности за въздействие и противодействие на тези системи;

– *системата, осигуряваща общокорабната дейност* – често в практиката за специфичните дейности, извършвани на и над главната (основната) палуба на кораба и нямащи пряко отношение със системата за управление на кораба и инженерните дейности на кораба, се използва обобщеното понятие „общокорабни дейности“. При тези условия под система за осигуряване на общокорабната дейност, за целите на това изследване, ще разбираме „свкупност от елементи намиращи се в закономерни отношения и свързани едно с друго, осигуряващи общокорабната дейност на системата-кораб“;

– *система, свързана с инженерната дейност на кораба* – традиционно дейности, осъществявани на кораба под ръководството на механика на кораба (за военните кораби – от командира на електромеханичната бойна част/инженерната секция) под обща рамка. Това са т.нар. „инженерни дейности“. За целите на изследването е възможно да се допусне съществуването на субсистема, която да обединява целия спектър от дейности, подвластни на гореспоменатото лице и това да бъде система, свързана с инженерната дейност на кораба.

При декомпозирането на кораба по функционални модули анализиращият има възможност да приведе в рамки целия спектър от дейности, които човекът осъществява в качеството си на човешки фактор. Според някои учени човекът представлява един от изграждащите елементи на *интелекта*, съвместно с електронни системи с възможности на ниво изкуствен интелект.¹⁰

При прилагане на декомпозиране от втора степен чрез функционалния подход на вече дефинираните подсистеми, към системата за управление на кораба се определят следните подсистеми (функции):

- *система за наблюдение* – с основна функция осъществяване на наблюдение на клъстери от пространството (подводен, надводен, въздушен) и своевременно откриване на обекти с цел добиване на пълна морска картина. Получената от нея и обобщена информация преминава по съответните канали към системата за опознаване на целите.

- *система за опознаване на целите* – специфична система, която съществува като субсистема в системата „военен кораб“. Основната ѝ функция се основава на възможността за определяне на държавната принадлежност (т.нар. „свой-чужд“) на наблюдавания обект.

- *система за комуникационно-информационна поддръжка* – съществува в тясна връзка със системата за наблюдение, като функция на всеки тип кораб и съчетава възможностите на техническите средства със способностите на човека (множество от хора). Функцията на системата е да осигурява надеждна свръзка в кораба-система (вътрешнокорабна свръзка) и на кораба-система със съществуващи надсистеми, системи и субсистеми в пространството.

- *система за морска навигация* – осигурява управлението на кораба-система посредством определяне на мястото му спрямо заобикалящата го среда и избора на движението му (курс и скорост) към желано крайно място. Системата трябва да осигури безопасен маршрут, необходимата скорост за осъществяване на прехода, а в много случаи – и други специфични изисквания.

- *система за въздействие и противодействие върху противникови военни системи* – специфична на системата, съществуваща като подсистема на военните кораби. Задължителното надеждно функциониране на системата изисква свързаност с целия спектър от субсистеми на кораба-система. Тя функционира в тясно взаимодействие с вече посочената система за опознаване на целите, от чийто алгоритъм зависи.

- *система за безопасност на кораба* – при военните кораби, тази система често (ако такава съществува, като отделна система) бива negliжирана за сметка на системата за сигурност, която дефинираме като субсистема на системата за действие и противодействие на въздействието на противодействащи системи. При въздействие върху безопасността на системата се установяват малфункции на подсистемно ниво – грешки на човешкия фактор; технически несъвършенства; несъответствия във взаимодействието на машинни и енергийно-суровинни ресурси; липса на правилните информационни ресурси и др.

Общокорабна система може да се декомпозира на следните функционални модули:

- подсистема за осигуряване на заемането и поддържането на позиция в пространството: като елементи на системата могат да бъдат изведени котвеното и швартовото устройства;

- подсистема за буксиране и отбуксиране – осигурява възможността на кораба-система да извършва движение в пространството посредством използване на енергийно-суровинни ресурси на друга система от същия порядък. В реципрочност собственият кораб-система е възможно да осигури преодоляването на фактори, въздействащи върху липсата на движение на друг кораб-система в пространството.

- подсистема, осигуряваща кораба-система с машинни и енергийно-суровинни ресурси. Включва в себе си пълния набор от средства и съоръжения като: кран-балки, стрели, лод-балки, виюшки, лебедки, устройства за приемане на борда на кораба на горива и смазочни материали по различни методи, устройства за приемане и предаване на леки и тежки товари по траверзен и вертикален способ и др. Подсистемата не може да осигури планираните функционалности при отсъствието на човешкия фактор.

Специфичните процеси на субсистемите в инженерната система също са невъзможни да бъдат осъществени в пълен обем без наличието на човешкия фактор. Инженерната система се декомпозира на подсистеми, като се използва функционален подход, на:

- подсистема, осигуряваща системата-кораб в пожаробезопасно отношение – съдържа елементи, свързани с пожаробезопасността на кораба като: пожарни помпи; пожарни магистрали; системи за водна защита и/или универсална водна защита; пожарни кранове; пожарни шлангове и струйници; пожарогасители; датчици, следящи за отклонение на температурата в отсеци, помещения или палуби; системи за звуково и/или светлинно известяване и др.

– подсистема, осигуряваща нормалната работата на трюмните съоръжения на кораба – включва елементи, свързани със: съхраняването, прехвърлянето или подаването на ГСМ, сладка, солена и отходна вода; сепариращи устройства; водопреснителни устройства и др. Машинни ресурси към системата са: цистерни; тръбопроводни трасета; помпи; шпигати; дънно-задбордна апаратура, датчици осигуряващи информация за нивото на определен флуид; звуково и/или светлинно известяващи устройства.

– подсистема, осигуряваща изменението на позицията на кораба-система в пространството – системата, която осигурява основната функционалност на кораба да извършва придвижване по водната повърхност, с което осигурява превоза на хора, стоки и товари от една точка в друга. Подсистемата може да бъде опростена, като съдържа единствено движител и рул, но може да бъде надградена посредством винтове с регулируема крачка, подрулващи устройства, азимутно подрулващо устройство, динамично позиционираща система и др.

– филтърно-вентилационна система на кораба – подсистема, осигуряваща преноса и филтрирането на атмосферен въздух в определени за това помещения и отсеци. Към нея принадлежи и подсистемата за кондициониране на кораба, която е предназначена за осигуряване на оптимално състояние на функциониране на човешките, машинните и енергийно-суровинните ресурси на кораба-система. Освен за управление на температурните режими на въздуха в зададените помещения, подсистемата осигурява и режим на влажност в помещения със специални изисквания.

На фиг. 1 е представена схематично функционална йерархичната структура на подсистемите на кораба-система.



Фиг. 1. Функционална йерархична структура на кораба-система

За целите на изследването са разгледани две функционални поднива. По такъв начин системата за управление се реализира като водеща субсистема от първо функционално подсистемно ниво спрямо системата-кораб и останалите две подсистеми от първо ниво. На второто функционално подсистемно ниво са представени субсистемите на трите подсистеми (Система за управление, Система за общокорабна дейност и Система за инженерна дейност). Независимо, че съществуват различни по сложност и многообразие връзки, на фигурата са представени основните връзки между старшите системи и техните подсистеми.

При така извършения анализ интерес за допълнително изследване се наблюдава при подсистемата за безопасност на кораба. Като подсистема на системата-кораб, тя отговаря на определени изисквания и притежава специфични характерни свойства. При negliжиране на нейното съществуване е възможно пораждаването на малфункции на надсистемно ниво в система-кораб, което от своя страна да доведе до понижаване на нейната способност за реакция срещу противодействащи системи от подобен порядък.

ЛИТЕРАТУРА

1. Клиланд, Дэйвид и Вильям Кинг. *Системный анализ и целевое управление*. Москва: Советское радио, 1974, с. 32.
2. Орлов, Никола. *Синтез и анализ на сложни системи*. Русе: Ивона, 2003. с. 29.
3. Warbletoncouncil. *The General Theory of Systems, by Ludwig von Bertalanffy – Psychology* [Online]. available at: warbletoncouncil.org (accessed 02 March 2021)
4. Величков, Владимир. *Целева устойчивост на военните системи*. София: ВА „Г. С. Раковски“, 2003. с. 41 – 47.
5. Михайлов, Михаил. *Морски илюстриран пъловен речник*. Варна: Стено, 2011. с. 150.
6. Колев, Кирил. *Управление на безопасността на морския транспорт*. Варна: Стено, 2012, с. 28.
7. Василев, Валентин. Системен подход в помощ на командирите при организиране на експлоатацията на корабното въоръжение. В: *Сборник доклади от Годишна университетска научна конференция на Национален военен университет „Васил Левски“* – 14 – 15 юни 2018 г. Велико Търново, 2018, с. 537 [онлайн] достъпно на: <https://www.ceeol.com/search/chapter-detail?id=673126> (посетено 7 май 2020 г.)
8. Конвенция на Организацията на обединените нации по морско право, чл. 29. *Държавен вестник*, № 73, 1996.
9. Закон за морските пространства, вътрешните водни пътища и пристанищата на Република България (§2, т.1 от Допълнителни разпоредби). *Държавен вестник*, № 12, 2000.
10. Величков, Владимир. *Целева устойчивост на военните системи*. София: ВА „Г. С. Раковски“, 2003, с. 99.

REFERENCES

1. Kliland, David & William King. *Sistemnyi analiz i tselevoe upravlenie*. Moskva: Sovetskoe radio, 1974, s. 32.
2. Orlov, Nikola. *Sintez i analiz na slozhni sistemi*. Ruse: Ivona, 2003. s. 29.
3. Warbletoncouncil. *The General Theory of Systems, by Ludwig von Bertalanffy – Psychology* [Online]. available at: warbletoncouncil.org (accessed 02 March 2021)
4. Velichkov, Vladimir. *Tseleva ustoychivost na voennite sistemi*. Sofia: VA „G. S. Rakovski“, 2003. s. 41 – 47.
5. Mihaylov, Mihail. *Morski ilustrovan talkoven rechnik*. Varna: Steno, 2011. s. 150.
6. Kolev, Kiril. *Upravlenie na bezopasnostta na morskia transport*. Varna: Steno, 2012, s. 28.
7. Vasilev, Valentin. Sistemen podhod v pomosht na komandirite pri organizirane na eksploatatsiyata na korabnoto vaorazhenie. In: *Sbornik dokladi ot Godishna universitetska nauchna konferentsia na Natsionalen voenen universitet „Vasil Levski“* – 14 – 15 yuni 2018 g. Veliko Tarnovo, 2018, s. 537 [online] dostapno na: <https://www.ceeol.com/search/chapter-detail?id=673126> (poseteno 7 may 2020 g.)
8. Konventsia na Organizatsiyata na obединените natsii po morsko pravo, chl. 29. *Darzhaven vestnik*, № 73, 1996.
9. Zakon za morskite prostranstva, vatreshnite vodni patishta i pristanishtata na Republika Bulgaria (§2, t.1 ot Dopalnitelni razporredbi). *Darzhaven vestnik*, № 12, 2000.
10. Velichkov, Vladimir. *Tseleva ustoychivost na voennite sistemi*. Sofia: VA „G. S. Rakovski“, 2003, s. 99.

ПОУКИТЕ ОТ ОПЕРАЦИИТЕ И УЧЕНИЯТА КАТО НЕОБХОДИМИ ЗНАНИЯ ЗА ПОВИШАВАНЕ НА ОТБРАНИТЕЛНИТЕ СПОСОБНОСТИ

подполковник д-р Пламен Петков
Военна академия „Г. С. Раковски“, papetkov@rndc.bg

Резюме: Докладът разглежда трансформирането на военна организация в обучаваща се организация, за да отговори на изискванията на текущата оперативна среда. Няма съмнение, че поуки/научените уроци допринасят за разработването на нови способности и подобряването на съществуващите. Те също така обогатяват знанията на въоръжените сили и усъвършенстват доктриналната мисъл.

Ключови думи: *способности; знание; поуки*

LESSONS LEARNED FROM OPERATIONS AND TRAININGS AS A NECESSARY KNOWLEDGE FOR IMPROVEMENT OF DEFENSE CAPABILITIES

Lieutenant Colonel Plamen Petkov, PhD
Rakovski National Defence College
Sofia, Bulgaria
E-mail: papetkov@rndc.bg

Abstract: This report deliberates on transform to a learning organization in order to answer the demands of current operating environment. There is no doubt that lesson learned contribute to developing new capabilities and enhancing the existing ones. They also contribute to enriching Armed Forces' knowledge and refining doctrinal thought.

Keywords: *capability; knowledge; lessons learned*

Увод

Съвременната среда се променя с толкова бързи темпове и драматично по същество, че човек трябва да бъде много пъргав и добре организиран, за да се адаптира към тази нея. В днешния свят най-постоянната парадигма е промяната.

Наблюдаваме глобализация, невъобразим технологичен напредък в почти всички области на живота, увеличено промишлено производство, което води до нарастване на потреблението и изчерпване на природните ресурси. Виждаме и компресия на икономическите цикли, която все по-често причинява кризи. Свидетели сме на ужасно влошаване на условията на живот в някои части на света, което принуждава големи маси от хора да мигрират в различни страни, а също така и на действащ въоръжен конфликт недалеч от нас.

На фона на тази мрачна картина ние преживяваме широко разпространена финансова криза, която влошава начина на живот и предизвиква социални въннения.

За да отговорят на изискванията на глобалната геополитическа среда, въоръжените сили трансформират своите знания и опит в обучаващи се организации. По този начин те ще останат привлекателни като работни места, където уникалните и пълноценни възможности за обучение представляват стимули за хората да останат отдадени на военната професия. Особено ценни и важни за военните организации са поуки (уроците) от операции и ученията.

1. Система за извличане и използване на научените уроци

Във войсковата практика научените уроци не са нищо друго, а естествен продукт от дейността на формираната по време на операции, ученията и подготовката, т.е., знанията, придобити от рутинната дейност на армейските организации. По време на тези дейности командирите и щабовете

обикновено осъзнават по-добри, по-лесни и по-ефективни начини за извършването на една или друга дейност, както и проблемите и грешките, с чието избягване ще се предотвратят загуби, трудности, разходи и време от следващите формирования, които ще извършват същата дейност. Процесът за извличането и използването на научените уроци са доказан процес за използване и приложение на най-добрите практики и избягване на грешките на другите. Следователно, уроците са знания, които се придобиват и утвърждават в непосредствената практическа дейност на войските и силите и, за да бъдат „научени“ трябва да се въведат в последващата практика за промяна на поведението на войсковите формирования и опосредствено да допринесат за по-висока ефективност в практиката.

За диференциране на понятията *поука* и *урок* е необходимо да се изяснят някои термини в лексиката на НАТО по отношение на процеса на извличане и използване на знанията от научените уроци. В доклада се приема, че *поука* е синоним на *научен урок*.

С цел постигане на единно разбиране и съвместимост със системите на НАТО и Българската армия по отношение на процеса на извличане и използване на знанията от научените уроци, се възприемат и следните основни понятия:

Наблюденията са необработена информация от различни източници. Те разясняват събитията, които са се случили на войсковите формирования в хода на операцията (учението, подготовката), проблемите, които са възникнали при изпълнението на задачите и възможните им решения. Могат да бъдат както негативни, така и позитивни. Документирани примери на наблюдения, мнения и констатирани уроци са оперативните доклади за изпълнение на задачите, интервюта с участници в мисиите, бойни донесения, анализи и разбори от ученията и подготовката, и др.

Анализът е изучаване на даден обект чрез цялостно изследване на неговите съставни части и взаимодействие между тях с цел постигане на подобрение или усъвършенстване. Анализът се различава от оценяването по това, че при него се преследва пълно разбиране на дадени процеси, явления или обстоятелства и придобиване на конкретни знания за обекта на изследването. Анализът на наблюденията, поуките и чуждия опит е основната и най-важна дейност в системата за извличане и използване на научените уроци.

Коригиращи действия – действия, които се извършват с цел въвеждане на корекции в определени тактики, техники и процедури за отстраняване на неправилни действия или отучване на стари практики. Те могат да бъдат и дейности за въвеждане на най-добрите практики на съюзниците от НАТО, или утвърдени поуки от практиката – продукт на процеса за извличане и използване на поуки.

Идентифицирана поука – констатиран, но не утвърден урок, който е установен от анализаторите, но все още не е утвърден от компетентния командир и за него не са въведени коригиращи действия.

Поука от практиката – научен урок при който коригиращото действие е експериментирано, одобрено и притежава практическа ефективност. Крайният резултат води до промяна на човешкото поведение и, респективно – до по-добри постижения и способности.¹

1.1. Компоненти на системата

Организирането и използването на научените уроци (НУ) е на базата на *Система за извличане и използване на научените уроци* (фиг. 1). Системата минимално трябва да съдържа следните основни компоненти:

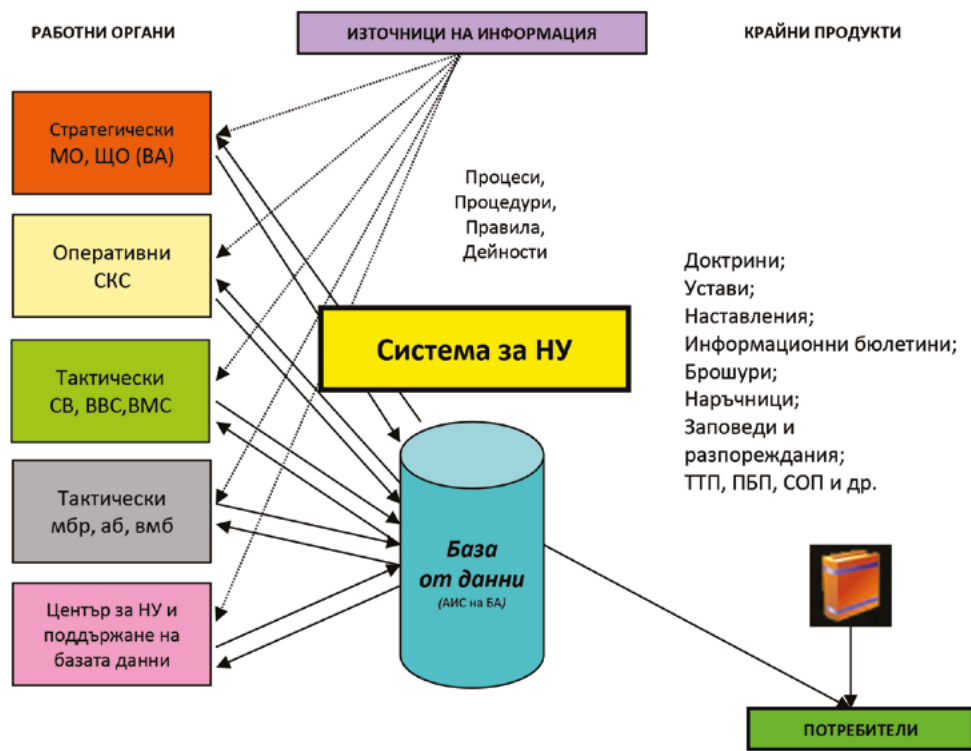
- Работни органи;
- Работни процедури;
- Инфраструктура с изградена комуникационно-информационна платформа;
- Електронна база от данни;
- Изходни продукти.

Работни органи на системата

НАТО – Съвместен център за анализ и поуки от практиката (JALLC) в САЩ, Канада и други страни са развърнали и осигурили в щатно и ресурсно отношение добре развити структури за изучаване и приложение на опита на стратегическо, оперативное и тактическо ниво.

Работни процедури на системата

Теорията за управление на знанията най-често разглежда процеса като съвкупност от системни и взаимосвързани дейности: създаване, придобиване, съхраняване, обмен, разпространяване, приложение и обновяване на знанията. Тези дейности, след специфична модификация, са валидни и при формулирането и използването на научените уроци от операциите и ученията.



Фиг. 1. Система за извличане и използване на научените уроци

Следователно, процесите за обобщаване на НУ са целенасочени дейности за събиране и анализиране на бойна информация, разпространение, интегриране и архивиране на наблюдения, мнения и уроци, добити от бойните операции или ученията. Тези процеси са дейности-процедури, както и всички останали щабни дейности, които се извършват в интерес на изпълнение на бойните и други задачи. Те осигуряват обратната връзка и установяват последващи дейности за осигуряване на постоянно обучение, коригиране на грешките и приложение в практиката на войските и силите на това, което се е доказало като правилно и ефективно.

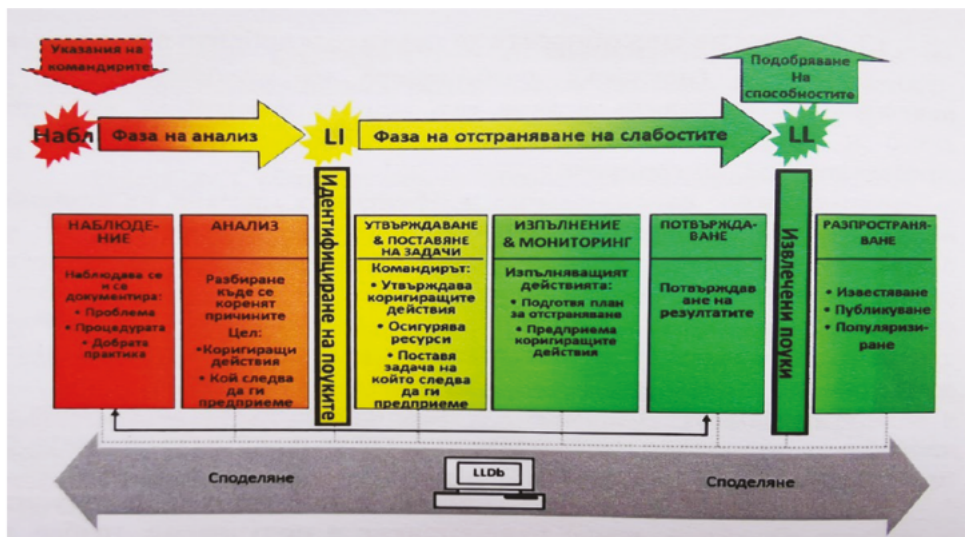
Основната идея в целия комплекс от дейности е, че процесът за обобщаване на научените уроци задължително трябва да води със себе си промяна в поведението на войсковите формирования при подготовката и провеждането на операции и ученията.

В съответствие с теорията за управление на знанията, за да бъде едно ново знание приложено отново в практиката, трябва да премине през определени процедури-фази (етапи). Във военните среди тези етапи се преосмислят. Като задължителни елементи за обработването на новите знания във вид на научени от практиката уроци се очертават осем процедури:

- събиране на информацията;
- анализ на наблюденията, мненията и уроците;
- формулиране на идентифицираните уроци и валидиране на обобщените изводи;
- утвърждаване на уроците;
- класифициране, сортиране и съхраняване;
- разработване на краен продукт с научените уроци;
- разпространяване и приложение в практиката;
- мониторинг (контрол) за изпълнението.

Комплексът от дейности протича в определен ред Алгоритъм (фиг. 2)² от работни процедури, които се подчиняват на определена последователност. Да допуснем, че в определен район за провеждане на

операция по поддържане на международния мир и сигурност се е случило Събитие X, и е предизвикало необходимост от провеждане на специализирано наблюдение. В следствие на тази необходимост командирът, от чието поделение е контингентът, е направил заявка за наблюдение в театъра на операциите, сформирал е екип за наблюдение и го е командирова на мястото на събитието. Екипът е провел наблюдението, съгласувал е всички детайли с командира на контингента, подготвил е доклад от наблюдението и, след завръщането си в постоянния гарнизон, го е предоставил на командира. На основата на доклада на екипа за наблюдение и заявката на командира започва поредица от дейности от системата за научените уроци.



Фиг. 2. Процес за поуки и добри практики

А1. Събиране на информацията

Екипът, натоварен със събирането на информацията пристъпва към колекцията на данни и информация от всички налични източници. Като най-достоверен и пълен източник се счита докладът на екипа, провел наблюдението. Опитът показва, че този източник съвсем не е достатъчен за извършване на пълен и задълбочен анализ. Ето защо, екипите за събиране на информацията използват и допълнителни източници като:

- резултати от проведени наблюдения и изследвания на други подобни събития в електронната база от данни и базите данни на съюзниците и партньорите;
- резултати от проверки на изпълнението на задачите в районите на операциите или ученията;
- бойни и други донесения за събитието или подобни такива;
- отчетната документация на контингенти и подразделения след завръщането им от изпълнение на задачи;
- провеждане на беседи и интервюта с участници в мисии и учения;
- ежедневни доклади на подчинените щабове, отговорни за подготовката и окомплектоването на контингентите;
- справки, изготвени от старшите на групи, извършващи контролни проверки по окомплектоването и хода на подготовката;
- доклади на председателите на комисии при оценка готовността и сертифициране на контингентите;
- отчетна документация по подготовката и провеждането на учения и участието в мисии извън страната;
- доклади от индивидуално или колективно участие в международни учения и реални операции, курсове, инспекции, семинари, конференции и др.

Цялата информация, която анализаторите считат, че може да бъде полезна за изследването на събитието, се сортира по тематика и се подготвя за анализа.

A2. Анализ на наблюдението

Има различни методи, форми и начини на анализ. Специалистите от НАТО са възприели схема за анализи за формулиране на научени уроци от операции или учения, която включва организиране, изследване, интерпретиране и формулиране.

Организирането на анализа се състои в събирането и сортирането на наличната за анализа информация. То подпомага експертите да извършат първичен анализ и да се подготвят за неговата последващата съществена част. То ги подпомага и да преценят необходимостта от друга информация и къде, евентуално, да бъде търсена. За удобство и системност информацията може да се подреди в списък, т.е. да се индексира. Това подпомага експертите да уловят съществуващи аномалии, тенденции и прилики. Организирането и подготовката следва да са съобразени с целите и задачите на анализа. В повечето случаи се проверява по тематика и наличие на подобни случаи в базата данни. Често се налага съществуващи експлицитни знания от практиката на войските и силите да се доразвиват и обогатяват.

Изследването на информацията е мисловен процес по нейното изучаване и сравняване. В процеса на изследване е възможно да се наложи различните носители на информация да бъдат сортирани по теми, съдържание, статистически данни или по други показатели. При стартиране на изследването анализаторът обикновено изгражда няколко хипотези по изследвания проблем и на базата на тях подхожда и към наличната информация. Например, преценява, че материалите в Папка „А“ и Папка „С“ съдържат основната информация за изследването, а материалите в Папки „В“ и „Д“ могат да се използват за допълнителна информация.

Изследването е процес, при който се търсят причинно-следствените връзки в анализираните явления, процеси или обстоятелства. Основен момент е да бъдат открити приликите, разликите и тенденциите в изследвания проблем, които се проверяват за коректност, повтаряемост, съдържателност и релевантност. Този процес специалистите по научени уроци наричат *валидиране*. Опитът на напредналите в тази област армии показва, че в много случаи за валидирането и изясняването на основните проблеми от наблюдението е необходимо да се извършат допълни изследвания на подобна информация в базата от данни, опита на съюзниците, а в някои случаи да се проведат и доуточняващи интервюта с участници в събитието.

При формулирането на изводи от изследването и определянето на правилната хипотеза за трансформирането ѝ в теза анализаторите трябва да бъдат сигурни, че тя (тезата) е валидна и в нея не са включени елементи, които са плод на предубеждение.

В края на изследването резултатите се сумират и се пристъпва към следващия етап.

Тълкуването (интерпретирането) на *резултатите* е процес на формулиране на заключенията на базата на изследване на информацията по конкретния проблем. Заключения могат да се формулират тогава и само тогава, когато анализаторът е придобил пълно разбиране на проблема и ясно осъзнава към какви изводи водят заключенията – както в контекста на изследвания проблем за конкретно войсково формирование, така и отражението му като цяло за дейността на войските и силите.

Заключенията не са препоръки. Те са кратко и обективно изложение на резултатите от изследването.

Формулирането на изводи е крайната фаза на анализа. На базата на заключенията от анализа се формулират кратки и ясни изводи от анализа на изследваното явление, събитие или обстоятелство и се очертават препоръки как да се използват резултатите от анализа за последващата дейност на войските и силите.

A3. Формулиране на поука

На основата на анализа и изводите от него се формулира поуката от конкретното наблюдение. На този етап това все още е констатирана поука. Анализаторите сглобяват цялото изследване, което съдържа:

- резултатите на екипа за наблюдение;

- допълнителната справочна литература, която е използвана за анализа;
- проведени интервюта с участници в събитието или експерти, чиято помощ е била необходима за правилното формулиране на проблемите и хипотезите на изследването;
- статистическа информация в подкрепа на изследването;
- изводи от анализа и препоръки за предприемане на конкретни коригиращи дейности за отстраняване на проблема;
- кой трябва да регламентира и кой да изпълни препоръките;
- идентифицираните (констатираните) уроци от наблюдението;
- очакван ефект от приложението на уроците в практиката;
- срок и форма за разпространяване на уроците сред изпълнителите – незабавно, бързо или нормално.

A4. Валидиране на поуката

Резултатите от анализа се преглеждат и валидират от външни експерти и командири, с цел да не се допуснат аномалии и неверни заключения, което може да доведе и до неправилно формулиране, разпространяване и приложение на уроците от събитието. Нормално е идентифицираните уроци и препоръките с коригиращи действия, да бъдат предоставени приоритетно на командира, извършил заявката за изследването. Те могат да бъдат предоставени и на други командири на подразделения със същата специфика на дейност. След получаването на отзивите за валидността на заключенията на екипа, отговорният за изследването командир дава указания за изготвяне на план за въвеждане на коригиращите дейности в практиката.

На този етап идентифицираната поука вече е формално одобрена и може да се заложи в базата от данни, а другите крайни продукти, ако се разработват, да се дават за предпечатна подготовка.

A5. Разработване на план за приложение на уроците

За въвеждането на коригиращи дейности, произтичащи от идентифицираните уроци, се изготвя план за изпълнение. Планът се разработва от организацията, в чийто ресор е извлечената поука. Ако въпросът, който следва да се коригира е оперативен – планът се изготвя от оперативното звено, ако е логистичен – от логистичното звено, ако е конкретен военно-технически – от ресорното щабно звено.

Съдържанието на плана се определя от ръководителя на организацията, която го изготвя. В него задължително трябва да присъстват елементите: кратко описание на наблюдението и цел на плана; констатирани уроци; коригиращи дейности; изпълнители, ресурси и срокове за реализиране на коригиращите дейности; при необходимост – предложения за доктринални промени и др. В разработването на плана участват и експерти от аналитичното звено, формулирало поука, както и експерти от звеното по подготовка на подразделенията.

A6. Утвърждаване на плана

Планът се утвърждава от най-старшия командир, който е упълномощен да ръководи съответната военна организация. Ако коригиращите дейности се отнасят за цялата армия и са общовалидни, планът се утвърждава от Началника на отбраната, ако коригиращите дейности се отнасят за отделен вид въоръжени сили – утвърждава се от началника на вида ВС, ако е за конкретен род войска – от началника на рода войска.

След утвърждаването на плана за въвеждане на коригиращите дейности, за официално утвърдени се считат и идентифицираните уроци, които могат да бъдат разпространявани и съхранявани без корекции.

Планът се обвързва по време, дейности и финансови и материални ресурси. За изпълнението на конкретните дейности се назначават отговорници. С утвърждаването му, планът се превръща в решение на командира за внедряване в практиката на уроците с цел изменение поведението на войските и силите.

A7. Осигуряване на решението

Изпълнението на решението на старшия командир се осъществява от назначените за това отговорници. За въвеждане на коригиращите дейности в изпълнение могат да се разработят конкретни

тактики, техники и процедури, правила за поведение или други правила. Те се разпространяват със заповед или разпореждане, в което се указват новите правила и се отменят, ако е необходимо, стари регламенти.

В много случаи, когато въвеждането на коригиращите дейности налага модификации по техниката и въоръжението, изграждане на нови съоръжения за изпълнение на задачите или за подготовка на формированията, са необходими значителни финансови ресурси. Осигуряването им се осъществява от старшия командир, утвърдил плана.

A8. Изпълнение и разпространение

Разпространяването и приложението в практиката на научените уроци е най-важната дейност на целия процес. Изпълнението на коригиращите дейности се извършва в съответствие със заложените в плана срокове от съответните отговорници. При възможност уроците се разпространяват в печатни издания – информационни бюлетени, паметки и др.

A9. Промяна на поведението на войсковите формирования

Промяната на поведението на войсковите формирования с въвеждането в изпълнение на новите уроци, ги утвърждава окончателно като *научени уроци*. Това е крайната цел на цялостния процес. След като е верифицирано, че новите знания, умения и навици са усвоени от изпълнителите и се използват в практиката на войските и силите, процесът приключва.

A10. Научените уроци окончателно се класифицират, подреждат по тематика и се съхраняват в базата от данни.

Процесът за извеждане на поуки и въвеждане на добри практики е постоянен и всеобхватен. Във Военна академия от 2019 година функционира научна секция „Доктрини, концепции и поуки от практиката“ в институт „Перспективни изследвания за отбраната“. Част от задачите ѝ са да провежда наблюдение, да извършва анализ, да идентифицира поуки, да предлага коригиращи действия, валидиране и утвърждаване на поуките и на добри практики, и да ги въвежда в дейността на Академията.

Със заповед на началника на Военна академия е назначена постоянно действаща работна група за събиране и анализиране на информация, разпространяване, интегриране и архивиране на наблюдения, мнения и поуки, добити от практиката във Военна академия „Г. С. Раковски“. Нейният фокус е насочен към ежеднезната, учебната и научноизследователската дейност, командно-щабните тренировки и учения и контрола на качеството на учебния процес.

Съгласно т. 3.2. от Ръководство за поуки от практиката във въоръжените сили научната секция изготвя и изпраща до дирекция „Операции и подготовка“-МО шестмесечни доклади за идентифицирани поуки, въведени коригиращи действия, установени добри практики в Академията.

Заклучение

Процесът за поуките от операциите и ученията, като система за извличане и използване на научените уроци, е започнат. Той трябва да продължава да се разширява и усъвършенства. Основно предизвикателство е формирането на така необходимата организационна култура за участие на военнослужещите в тези процеси. Тяхната активна позиция е жизнено важна за обмена на знания и обогатяване на базата данни на въоръжените сили на Република България с безценния опит от операции и учения. Това, от своя страна, ще допринесе и в бъдеще за повишаване на ефективността на формированията, за предотвратяване на загуби, икономия на средства и предаване на опита на следващите поколения.

ЛИТЕРАТУРА

1. Тактическа публикация на въоръжените сили на Република България ТП 7-6. *Ръководство за поуки от практиката във въоръжените сили, Приложение 1*, 2020, с. 32.
2. Пак там, с. 12.
3. *Joint Analysis Handbook, 4th Edition*, February 2016, p. 19.
4. *ibidem*, p. 22.

REFERENCES

1. Takticheska publikatsia na vaorazhenite sili na Republika Bulgaria TP 7-6, *Rakovodstvo za pouki ot praktikata vav vaorazhenite sili, Prilozhenie 1*, 2020, s. 32.
2. ibidem, p.12.
3. *Joint Analysis Handbook, 4th Edition*, February 2016, r. 19.
4. ibidem, p. 22.

СЪВРЕМЕННИТЕ ТЕХНОЛОГИИ ЗА РАЗУЗНАВАНЕ НА РУСИЯ И ТЯХНОТО ИЗПОЛЗВАНЕ В УКРАИНСКИЯ КОНФЛИКТ

майор гл. ас. д-р Кръстю Кръстев
НВУ „Васил Левски“, kikrastev@nvu.bg

Резюме: Целта на настоящия доклад е, на базата на анализа на национални и чуждестранни публикации и въз основа на съществуващите литературни източници, да се изследват съвременните технологии за разузнаване, използвани от въоръжените сили на Русия в конфликта в Украйна.

Ключови думи: технологии за разузнаване; военен конфликт; Русия; Украйна

MODERN RUSSIAN INTELLIGENCE TECHNOLOGIES AND THEIR USE IN THE UKRAINIAN CONFLICT

Major Assist. Prof. Krastyu Krastev, PhD
Vasil Levski National Military University
Veliko Tarnovo, Bulgaria
E-mail: kikrastev@nvu.bg

Abstract: The purpose of this report is to study modern intelligence technologies used by the Russian armed forces in the conflict in Ukraine, based on the analysis of national and foreign publications and existing literature.

Keywords: intelligence technologies; military conflict; Russia; Ukraine

Въведение

През последното десетилетие сигурността на европейските държави е изправена пред редица предизвикателства. Както посочват съвременните специалисти^{4, 12}, основните проблеми пред сигурността на ЕС и НАТО са регионалната нестабилност, неустойчивото развитие, появата и изострянето на конфликти на етническа и религиозна основа и свързаните с тях форми на тероризъм и честите природни бедствия [14], съдържащи в себе си потенциал на антропогенни катастрофи^{5, 12, 14, 15}. Затова управлението на кризи от невоенен характер се превръща в един от основните подходи за гарантиране на международната и националната сигурност и стабилност. ООН, НАТО, ЕС и ОССЕ концентрират усилията за разширяване на сътрудничеството и взаимопомощта както по проблемите на сигурността, така и по въпросите за предотвратяване и ликвидиране на последствията от бедствия, промишлени аварии и кризи от невоенен характер³. С подкрепата на ООН в НАТО е създаден Евроатлантически съвет за партньорство и постоянно действащ Евроатлантически център за координиране на действията при бедствия с цел съсредоточаване на усилията и координиране на действията за оказване на навременна и ефективна помощ на населението¹⁴, чрез формиране на адаптивни екипи^{1, 2}.

Нападението над Украйна се определя като най-сериозната военна обстановка в Европа след края на Втората световна война²¹ и е осъдено остро и категорично от българския президент^{22, 23}, Народното събрание²⁴ и правителството на РБ²⁵, от страните от Европейския съюз, включително от канцлера на Германия Олаф Шолц²⁵ и френския президент Еманоел Макрон²⁶, от председателката на Европейската комисия Урсула фон дер Лайен²⁷, министър-председателя на Великобритания Борис Джонсън²⁸, президента на САЩ Джо Байдън²⁹, генералния секретар на НАТО Йенс Столтенберг³⁰, както и от Канада, Япония, Израел, Грузия, Турция и много други държави и международни институции^{31, 32, 33, 34, 35, 36}. В частност, действията на руските въоръжени сили се определят като „варварска атака“, оправдавана с „цинични аргументи“³⁷ и „най-голямата атака на стабилността и Европа от десетилетия“³⁸.

Извън политическите дебати и изявления, в интерес на военната наука е необходимо специалистите по сигурността да се абстрахират от субективните гледни точки и обективно да насочат усилията си към детайлен анализ на случващото се в зоната на конфликта с цел установяване на тенден-

циите и за развитието на военното изкуство при действията на противостоящите сили в Украинския конфликт.

Имайки предвид широкия спектър от области и сфери на приложение на технологиите за разузнаване, ще огранича предмета на изследване за целите на настоящия доклад в направление новоприети на въоръжение във въоръжените сили на Русия разузнавателни и разузнавателно-ударни технологии.

Същността на разузнаването във военните операции е добиване, обработване и разпространение на информация, която осигурява изпълнението на целите на операцията при минимален риск за участващите в нея военни формирования. Както отбелязват специалистите^{9, 11, 13}, този процес е неразделна част от самите операции и е елемент от особена важност при тяхната предварителна подготовка.

Целта на настоящия доклад е на базата на анализа на национални и чуждестранни публикации и съществуващите литературни източници, да се изследват съвременните технологии за разузнаване, използвани в конфликта в Украйна.

За постигането на тази цел са поставени за решаване следните научно-изследователски задачи:

1. Да се извърши анализ на съвременните разузнавателни технологии, приети на въоръжение в армията на Русия.
2. Да се изследват наличните открити източници на информация, относно средствата за разузнаване, използвани от Въоръжените сили на Русия в конфликта в Украйна.
3. Формулиране на основни насоки за подобряване и усъвършенстване на съвременните технологии за разузнаване в съвременните конфликти.

В хода на изследването са използвани основно методите на системния анализ, синтез, сравнение, изследване на опита, експертни мнения, анализи и изследвания вследствие на натрупаният опит от участие на формированията от БА за защита на населението при бедствия, аварии и катастрофи.

1. Съвременни разузнавателни технологии за наблюдение

Според В. Мураховски в западните страни съществува мит, че Русия изостава в роботиката. Всъщност едва ли друга армия в света притежава такова разнообразие от безпилотни летателни средства и системи, както Русия. Не е за подценяване факта, че днешната руска армия е наследник на Червената армия, която създава дистанционно управляемите танкове през 30-те години. След войната в СССР са разработени и безпилотните летателни системи. В тези области има огромен прогрес. Ако Русия изостава някъде в технологиите за БЛС, по отношение на наземните и морски роботи тя има най-обширната програма в света.

Оптико-електронен комплекс „Око“ е система от космически спътници от първо поколение, които засичат изстрелване на балистични и крилати ракети. Комплексът осигурява пълно и денонощно наблюдение на всички военни обекти на САЩ, и частично наблюдение на военни обекти на други държави.

Системата денонощно следи ядрените обекти на САЩ и в случай на война може да засече изстрелване на ракета от всяка точка на страната. В орбита са общо 85 спътника, 4 от които са изстреляни с ракетата „Протон“, а останалите 81 – с „Мълния-М“. Последният такъв спътник е изстрелян на 23 октомври 2007 г. Програмата е стартирана с изстрелването на един прототипен спътник през 1975 г. и 4 оперативни спътника през 1979 г. „Око“ е приведена в бойна готовност през 1982 г. С оглед на разпространението на ракетни технологии и ядрени оръжия е създадена и СРПН-2 „Прогноз“ (второ поколение), която може да наблюдава ракетите на Израел, Иран, Северна Корея, Китай, Индия и Пакистан. Русия разполага и с нова, свръхмодерна система за ранно предупреждение, първият сателит от която е изстрелян през 2009 г.

СРПН-2 „Прогноз“ служи като допълнение на системата „Око“ и, освен ракети, може да следи движението на самолети, вертоleti, бойни кораби и подводници. Постоянно активни са само 2 спътника, а други 14 осигуряват частично наблюдение. Системата е в процес на разширяване. Целта на програмата е да засича изстрелвания на ядрени ракети и детонации на техни заряди. Програмата е започната като част от мащабния проект за противоракетна отбрана на СССР в началото на 80-те години. Първият спътник е изстрелян на 29 март 1984 г., а цялата система е активирана през 1996 г. Изстрелването на още спътници е в ход, като последното е на 26 юни 2008 г. (успешен). Сателитите следват геосинхронна орбита на около 35 750 км над земния екватор. Към август 2021 г. в орбита има 16 спътника, от които два наблюдават денонощно земната повърхност, а останалите 14 са позиционирани над други части на земята и не осъществяват денонощно наблюдение. СРПН-2 „Прогноз“ (както и „Око“) е разработвана от бюро „НПО Лавочкин“.

Освен наблюдение на ракетните установки по цялата територия на САЩ и други страни с ядрени оръжия, системата се използва и за наблюдаване на полети на бойни самолети.

„Окно“ е оптико-електронен комплекс за космическо наблюдение на територията на Таджикистан, близо до град Нурек. Може да наблюдава космическото пространство най-малко 300 дни в годината, и да следи обекти, отдалечени на разстояние до 40 000 км от Земята. Комплексът е под командването на ВКС и е предназначен за автоматично откриване и следене на обекти на височина до 40 000 км над земната повърхност по оптико-електронен способ, чрез регистриране на отразената от тях слънчева светлина.



Сн. 1. Оптико-електронен комплекс за космическо наблюдение „Окно“

Източник: mil.ru

Проектът „Окно“ започва още през 80-те, но поради редица причини изграждането му се забавя. Окончателно е въведен в експлоатация през 2003 – 2004 година. Комплексът е труднодостъпен и се намира на 2200 м надморска височина, но е оборудван с хеликоптерна площадка и до него има път. Персоналът се превозва от военното градче в предградията на Нурек с автобуси. Освен за наблюдение, комплексът може да се употребява и за граждански цели и навигация на спътници.

2. Безпилотни летателни системи на въоръжените сили на Русия

В Руската армия действат 36 части и подразделения на безпилотната авиация, в които на въоръжение са около 2000 съвременни безпилотни апарата.

Един от първите, дори съветски, модели се счита за безпилотен самолет „Вее-1Т“. Първият му полет е през 1990 г. със задача да извърши корекция на стрелба от артилерийските реактивни системи „Смерч“ и „Ураган“. Използван е от руската армия по време на чеченския конфликт, но и понастоящем този модел е на въоръжение. БЛА „Вее-1Т“ е проектиран за обхват до 60 хил. метра. Теглото на устройството е 138 кг. За стартирането на дрона са предвидени специални инсталации и ракетни бустери. Кацането става с помощта на парашут. Друг стар руски разузнавателен дрон е моделът Dozor-85. След успешно преминаване на теста през 2007 г., военните поръчват първата партида от 12 БЛА. Предназначен е да удовлетворява нуждите на Гранични войски. Масата на устройството е 85 кг и може да остане във въздуха до 8 часа.

БЛС „Скат“ е на въоръжение в разузнавателните формирования в Русия от 2007 г. Той е проектиран в експерименталното проектантско бюро на Микоян и Гуревич и АД Климов.

През 2010 г. се подписва договор за производство на безпилотни летателни апарати между руските военни и израелската компания IAI. В основата е на проекта е израелският UAV Searcher. В Русия, е подобрен и преименуван на Outpost. Масата на излитане на дрона е 400 кг, обхватът на полета не надвишава 250 км. За устройството са предвидени сателитна навигационна система и термовизионни камери.

От 2007 г. дейностите по разузнаването се извършват от самолетите на Тихак БЛА. Началното тегло на самолета е 50 кг. Продължителността на полета на дрона не надвишава два часа. Може да бъде оборудван с конвенционални и инфрачервени камери.

През 2009 г. руската компания „Трансас“ пуска в производство БЛА за Dozor-600. Самолетът е многофункционален безпилотен апарат. За първи път е представен на изложението МАКС-2009. Експертите смятат, че този дрон е аналог на MQ-1B Predator. Въпреки това, няма надеждна информация за точните характеристики на американския UAV. Бъдещите планове на руските авиационни дизайнери са, да оборудват радарната система с видеокамера и термовизионна камера. Също така за дрона е разработена система за насочване. С „Дозор-600“ се провежда разузнаване и наблюдение в прифронтовите зони.

В началото на 2014 г. в руската армия БЛС наброяват около 500 единици. Това неоглямо количество закупени в Израел безпилотни летателни апарати е от вида IAI Searcher Mk II и IAI Bird Eye 400, както и руски апарати от частни компании, събрани с широкото използване на чуждестранни производители. Към 2015 г. на въоръжение във ВС са постъпили 5 типа безпилотни летателни апарати, национално производство. Това са безпилотните летателни апарати „Груша“, „Гранат“ (на „Ижмаш“ – Безпилотни системи“), „Орлан-10“ („Специален технологичен център“), както и „Елерон“ и „Тахион“ (ЗАО „Еникс“).

Във военната авиация на Русия се използват моделите БЛА за „Орлан-3М“ и „Орлан-10“. Малките разлики са в тяхната полетна маса и обхват. За стартиране и двата дрона използват специален катапулт. Кацането на БЛА се извършва с парашут.

За нуждите на военния производител на самолети от типа Zala, Aero Group създава нов модел безпилотен летателен апарат, който е известен като БЛС „Zala 421-08“. Основната задача на БЛС е да води наблюдение и да коригира огъня от артилерийски РСЗО. Според експерти, отличителната черта на този самолет е възможността за извършване на видео и фото наблюдение от малко разстояние.

През 2017 г. дизайнерите на самолетите на компаниите „Сухой“ и „Микоян и Гуревич“ извършват проектантска работа по производството на модерен руски БЛА. В документацията дронът е посочен като „Хънтър-Б“.

През 2021 г. на МТУБС „Запад 2021“ са демонстрирани три типа БЛС – „Форпост“, „Ласточка“ и „Иноходец“.

Към 2022 г. сред ударните безпилотни летателни апарати (БПЛА) са програмите „Алтиус“, „Охотник“, „Сириус“, „Карнивора“, вертолетните дроне „Платформа“, комплексите за групово използване „Молния“ и други.

3. Дистанционно управляеми разузнавателно-ударни технологии

През месец септември 2021 г. Русия и нейният стратегически съюзник Беларус проведеха мащабното учение „Запад 2021“, на което демонстрират технически и тактически иновации. Представени са пехотната машина Б-19 с боен модул „Епоха“ и военният дрон „Ласточка“.



Сн. 2. Пехотна машина Б-19 с боен модул „Епоха“

Източник: ran.bg

Б-19 е въоръжена с 57-мм голямокалибрена картечница, ПТУР „Хорнет“ и нов управляем ракетен комплекс „Булат“ за поражение на противникова жива сила и малоразмерни обекти на бойното поле. Особеност на бойният модул „Епоха“ са системите за автоматично откриване, съпровождане на противникови цели, подготовка на данни за стрелба и подпомагане на действията на екипажа при изпълнение на задачи по огнево поразяване – поотделно, последователно или едновременно по два огневи канала.

Обозначението Б-19 има вариант на бойната машина на пехотата БМП-3, оборудван с разработеното от АД „Конструкторско бюро за приборостроене „Академик А. Г. Шипунов“ (КБП, Тула) нов безекипажен боен модул ТКБ-973 „Епоха“ (32Б01). Моделът БМП-3 с боен модул „Епоха“ е демонстриран на Международния военно-технически форум „Армия-2017“ във версията, оборудвана с 57-мм автоматично оръдие с ниска балистика ЛШО-57 и пускови установки ПТУР „Корнет-Д“, както и разработеният от КБП нов управляем ракетен комплекс „Булат“ с малогабаритни ракети за поразяване на огневи точки, лекобронирани и небронирани военна техника.

През август 2017 г. Министерството на отбраната на Руската федерация подписва договор с холдинга „Високоточни комплекси“ и влизащото в състава му Конструкторско бюро по приборостроене (КБП) за доставка на експериментална партида БМП-3 (Б-19) с безекипажен боен модул „Епоха“. Според известните данни, поръчката е за експериментална партида бойни машини на пехотата Б-19 (12 единици) и е доставена на Министерството на отбраната през 2020 г.

4. Роботизирани дистанционно управляеми разузнавателно-ударни технологии

Руската армия има на въоръжение различни видове наземни, въздушни и подводни бойни роботи в различна степен на готовност. Много от тях вече участват в тестове и учения. Съвременните авиационни и наземни роботизирани системи, представени в рамките на МТУБС „Запад 2021“ заслужават особено внимание. По време на основната фаза на ученията са използвани и два типа бойни роботи – „Уран-9“ и „Нерехта“.



Сн. 3. Боен робот „Уран 9“

Източник: mil.ru

В момента „Уран-9“ е най-големият робот на Русия. Комплекс от среден клас, той има характерен външен вид поради установките, разположени отстрани. Бойната машина е въоръжена с 30-мм автоматично оръдие, противотанкови управляеми ракети „Атака“ и огнемети „Шмел“. Тежи до 12 т, малко по-лек от БМП-2.

Необходимо е да отбележим, че ученията в рамките на МТУБС „Запад 2021“ е проведен първият експеримент в използването на наземните роботи в познати формации на боен ред на военни формирования. В координация с механизирани формирования, БЛС „Уран-9“ и „Нерехта“ атакуват и унищожават различни цели, включително и бронирани (с НУРС). Роботите са осигурили прикриващ огън за маневъра на силите на бойното поле.

В другите дни пък умения демонстрираха роботите „Платформа-М“, въоръжени с картечници и гранатомети. В тренировката на бойните действия участваха няколко вида наземни бойни робота – „Платформа-М“, „Нерехта“ и „Уран-9“. Руската армия смята да използва машините основно за разузнаване, патрулиране около стратегически обекти и подкрепа на пехотата в бойни действия.

Разработват се и много други руски дронаве и роботи. Към въоръжените наземни роботи в бъдеще ще се присъединят тежките „Штурм“ и средните системи „Соратник“, роботите „Маркер“ и, вероятно, дори безпилотния танк „Амата“.

Според Денис Федудинов, руски експерт в областта на безпилотната авиация, ученията „Запад 2021“ са забележителни с широката употреба на различни безпилотни и роботизирани системи, някои от които – развърнати за първи път. Нещо повече, той казва, че това не е цялата гама от дронаве, създадена в Русия: например „Форпост“ и „Иноходец“ се очаква да бъдат допълнени от тежките „Алтиус“ и разработки по технологията стелт – „Охотник“.



Сн. 4. Боен робот „Нерехта“

Източник: irossiya.ru

„Желанието за наваксване в тази област, което доведе до създаване на голяма линия базови БЛА системи, имаше значителна финансова и времева цена, което бе урок за Русия, така че сега тя отдава голям приоритет на безпилотните разработки“, отбелязва Федудинов.

Междувременно Мураховски отбелязва, че руските технологии днес покриват широк спектър наземни роботи: от разузнавателни, разминиращи и поддържащи машини, до бойни дронаве. „По отношение на обсега, Русия има всичко – от миниатюрни сферични роботи, които могат да бъдат пуснати ръчно

от земята, до тежки комплекси на танкова платформа като „Штурм“. А по отношение на полезния товар, руските роботи, независимо бойни или разузнавателни, са сред авангарда“, добавя той.

Русия работи и над автоматизирането на конвенционалните управляеми оръжия и боеприпаси. Изкуственият интелект на борда, или т.нар. виртуален пилот, на Су-57 му позволява да изпълнява повечето мисии без пилот в кабината. Дори старомодните буксирни гаубици ще бъдат автоматизирани и дистанционно контролирани (чрез инсталиране на комуникационни устройства и електрически мотори на лостове, с които оперира разчетът).

За сравнение, армията на САЩ днес използват усъвършенствана система от дронаве, но имат пропуски по отношение на безпилотните наземни машини. По-рано армията на САЩ пушна програмата „Бойни системи на бъдещето“, която трябва да развива щурмовите роботехнически машини с маса до 10 т и въоръжение, сходно с това на руския „Уран“ – с 25-мм оръдие, картечница и управляеми противотанкови ракети, но проектът е спрян. В момента сухопътните войски на САЩ използват само мини-роботи, въоръжени с картечници, които тежат не повече от 45 килограма.

Заедно с роботизацията, руската армия развива и идеята за унифицирана разузнавателно-ударна система – нещо като програмата „Мрежово-ориентирани военни операции“ на САЩ. И двата подхода предвиждат всички елементи от активното бойно оборудване – било то самолети или дронаве във въздуха, бойни машини, войници и роботи на земята или сателити в космоса – да се комбинират в единна комуникационна система. Още повече, че обменът на данни трябва да се случва в реално време, за постигане на информационно превъзходство над противника.

Специфичните системи за прехвърляне и обработка на данни вече са инсталирани на въоръжение във всички видове въоръжени сили, включително на танкове, гаубици и щурмови самолети. Свързването на военните дронаве и бойни роботи в унифицирано информационно пространство с повишено използване на изкуствен интелект, вероятно ще формира бъдещия етап на тази програма.

Както отбелязва Мураховски, в бъдеще някои области от военните операции могат да бъдат напълно роботизирани. Руската армия вижда роботите като разработка за защита на фланговете, охрана на тила и изпълнение на други задачи, като щурмуване на вражеските позиции. Това ще бъде своеобразен независим авангарден ешелон, който изпълнява задачи автономно, без човешка намеса. Например в градски условия, където битките могат да вземат много човешки жертви. Според експертната оценка на Мураховски, Русия вече е демонстрирала независимо опериране на безпилотни бойни системи. Противокорабните крилати ракети „Оникс“ работят в „ято“ с *водещи* и *водими* ракети. Алгоритъмът на опериране осигурява разнообразни опции. „Оникс“ определя главната цел сред групата вражески кораби, разпределя други цели в ято и определя траекториите.

Заклучение

Вследствие на извършените анализи и проучвания по темата е възможно да се формулират следните изводи:

1. В условията на ескалирания в Украйна конфликт е възможно да определим, че съществуват предпоставки за широко използване на съвременните разузнавателни и разузнавателно-ударни технологии на Русия.

2. В рамките на отделните фази на провеждащите се бойни действия осигуряването на разузнавателна информация за руските военни формирования ще се организира в съответствие с необходимостта от разузнавателни данни за всеки от районите и участъците на бойни действия, за което въоръжените сили на Русия разполагат със съвременни разузнавателни технологии, платформи и системи.

3. В определен момент на развитие на конфликта е възможно провеждане на бойни действия от ново поколение – смесен роботизиран и човешки боен ред, което изправя военните експерти и специалисти пред предизвикателството за търсене на решения и способности за противодействие на роботизираните разузнавателно-ударни системи и комплекси.

4. В съответствие с разработените планове за действие на руските военни формирования можем да предположим, че използването на роботизираните системи ще се наблюдава във фазата на преминаване от блокадни към действия по систематично прочистване на населените пунктове.

ЛИТЕРАТУРА

1. Атанасова-Кръстева, Невена. Необходимостта от адаптивни екипи за действие в екстремални ситуации. В: *Сборник научни доклади – Пети национален конгрес по психология*, бр. 1-4. София: Изток-Запад, 2008, с. 700 – 707. ISSN 0861-7813.
2. Атанасова-Кръстева, Невена. *Психология на кризиса*. Велико Търново: ИК на НВУ „Васил Левски“, 2019, с. 330. ISBN 978-954-753-290-8.
3. Георгиев, Георги. Взаимодействие между областната и общинската администрация с Българската армия в управлението при бедствия и аварии. В: *Годишник на Факултет „Командно-щабен“*. София: ВА „Г. С. Раковски“, 2018, с. 400 – 408. ISSN 1312-2991.
4. Георгиев, Георги. *Взривни технологии в аварийно спасителни работи*. София: ВА „Г. С. Раковски“, 2016, с. 216.
5. Георгиев, Георги. Защита на обекти от критичната инфраструктура от терористични заплахи. В: *Сборник доклади от Международна научна конференция „Сигурност – образование, наука, индустрия“ – втора част*. София: ВА „Г. С. Раковски“, 2020, с. 154 – 159. ISBN 978-619-7478-58-7.
6. Георгиев, Георги. Перспективи за използване на формирования от Българската армия за овладяване и/или преодоляване на последствията от бедствия. В: *Сборник материали от военна научна конференция на факултет „Командно-щабен“*. София: ВА „Г. С. Раковски“ 2/2014, с. 81 – 89. ISSN 1312-2991.
7. Филипов, Христо, Кирил Петров, Георги Георгиев. *Организиране и провеждане на операции по търсене и спасяване*. София: ВА „Г. С. Раковски“, 2012, с. 123.
8. Георгиев, Христо. Участие и специфични задачи на ССО в операции по преодоляването на кризи в мирно време. В: *Сборник с материали от конференция на факултет „Артилерия, ПВО и КИС“*. Шумен, 2019, с. 118 – 124. ISSN 2367-7902.
9. Градев, Калин. Подход за разработване на вариант за действие при планиране на операциите. В: *Сборник доклади от международна научна конференция „Сигурност – образование, наука, индустрия“, Втора част*, София: Военна академия „Г. С. Раковски“, с. 26 – 29. ISBN 978-619-7478-58-7.
10. Кокудева, Петрана. Теорията на системите в епохата на платформите. В: *Сборник доклади от Международна годишна научна конференция на НВУ „Васил Левски“*, 27-28 май 2021 г. Велико Търново: ИК на НВУ „Васил Левски“, 2021, с. 1084 – 1090. ISSN 2367-7481.
11. Кръстев, Кръстю. *Тактическо разузнаване във военните формирования*. Велико Търново: ИК на НВУ „Васил Левски“, 2021, с. 161. ISBN 978-954-753-326-4.
12. Маринов, Петър. *Тероризмът – абстракции и реалности*. София: Изток – Запад, 2016, с. 295. ISBN 619-152-866-3.
13. Петков, Йордан. Основни насоки за повишаване на уменията на личния състав на разузнавателните формирования. В: *Сборник с материали от конференция на факултет „Артилерия, ПВО и КИС“* – Шумен, 2019, с. 106 – 111. ISSN 2367-7902
14. Радева, Николина. *Актуални аспекти на защитата на населението при бедствени ситуации*. Варна: Стено, 2019, с. 141. ISBN 978-619-241-046-9.
15. Романова, Христиана. *Потенциални антропогенни екокатастрофи във Варненски регион. Стратегия за защита на населението и запазване на биоразнообразието*. Варна: БВМУ „Н. Й. Вапцаров“, 2014.
16. Watts, William. *Here's the technology being used to watch Russian troops as Ukraine invasion fears linger*. February 16, 2022 [online] available at: <https://www.marketwatch.com/story/how-fears-of-russian-invasion-of-ukraine-put-open-source-intelligence-in-spotlight-11645033603?mod=home-page>
17. Vardhan Harsh. *Canada's Space Company To Provide Intelligence To Ukraine Via Satellites To Resist Russia*. 11 March, 2022. [online] available at: <https://www.republicworld.com/world-news/russia-ukraine-crisis/canadas-space-company-to-provide-intelligence-to-ukraine-via-satellites-to-resist-russia-articleshow.html>
18. Borrell, Josep. *EU to help Ukraine with intelligence from own satellite centre-EU's Borrell*. Reuters, 28-02-2022 20:30 IST. [online] available at: <https://www.devdiscourse.com/article/technology/1941820-eu-to-help-ukraine-with-intelligence-from-own-satellite-centre-eus-borrell>
19. Thomson, Reuters. *Ukraine Receives Shipment of Machine Guns and Surveillance Gear From Canada*. Reporting by Natalia Zinets, Edit. Mark Potter, Feb. 19, 2022. [online] available at: www.usnews.com/news/world/articles/2022-02-19/ukraine-receives-shipment-of-machine-guns-and-surveillance-gear-from-canada
20. Radio Free Europe. *UN Approves Resolution Deploring Russia's Invasion Of Ukraine*. 2022-03-02. [online] available at: RadioFreeEurope/RadioLiberty (Посетен на 02.03.2022)
21. *Световните лидери: Путин е отговорен за най-сериозната военна обстановка след ВОВ*. Vgonair [онлайн] (посетен на 25.02.2022).
22. *„Абсолютно недопустимо“: Румен Радев остро осъди нападението на Русия над Украйна*. Deutsche Welle [онлайн] достъпно на: www.dw.com (посетен на 25.02.2022)
23. *България осъжда военните действия в Украйна, няма пряка заплаха за страната*. Българско национално радио [онлайн] достъпно на: bnr.bg. (посетен на 25.02.2022)
24. Недкова, Ванина. *НС категорично осъди военната интервенция срещу Украйна*. Нова телевизия [онлайн] достъпно на: NOVA. 24.02.2022. (посетен на 26.02.2022)

25. Германският канцлер Олаф Шолц осъди нападението на Русия срещу Украйна. 24 часа [онлайн] достъпно на: www.24chasa.bg. (посетен на 25.02.2022)
26. Макрон: Руската агресия срещу Украйна е най-сериозната атака срещу мира в Европа – Свят. Радио „Дарик“ [онлайн] достъпно на: dariknews.bg. (посетен на 25.02.2022)
27. Лидерите на ЕС осъдиха остро решението на Путин. [онлайн] достъпно на: www.trt.net.tr. (посетен на 25.02.2022)
28. Джонсън: Това варварско начинание на Путин трябва да завърши с провал – Свят. Радио „Дарик“ [онлайн] достъпно на: dariknews.bg. (посетен на 25.02.2022)
29. Байдън осъжда „необоснованата атака на Русия срещу Украйна“. [онлайн] достъпно на: www.actualno.com. (посетен на 25.02.2022)
30. Столтенберг: Това е умишлено, хладнокръвно и дълго планирано нападение. Труд (видео). [онлайн] достъпно на: trud.bg. 2022-02-24. (посетен на 26.02.2022)
31. Светът осъди нападението на Русия срещу Украйна. Свободна Европа [онлайн] (посетен на 25.02.2022)
32. Путин избра проливането на кръв: реакция след руското нападение срещу Украйна. Deutsche Welle [онлайн] достъпно на: www.dw.com (посетен на 25.02.2022)
33. Израел осъди руското нападение срещу Украйна. БТА [онлайн] достъпно на: bta.bg. (посетен на 25.02.2022)
34. Изявление на лидерите на Европейския парламент относно Украйна. Европейски парламент [онлайн] достъпно на: www.europarl.europa.eu. (посетен на 25.02.2022)
35. Западът осъди нахлуването в Украйна. Българско национално радио [онлайн] достъпно на: bnr.bg. (посетен на 25.02.2022)
36. Светът остро осъди нападението срещу Украйна (обзор) – Войната в Украйна. Радио „Дарик“ [онлайн], достъпно на: dariknews.bg. (посетен на 25.02.2022)
37. Владимир Путин в санкционен списък на ЕС. Българско национално радио [онлайн] достъпно на: bnr.bg. (посетен на 25.02.2022)
38. Макрон: Руската агресия срещу Украйна е най-сериозната атака срещу мира в Европа. Радио „Дарик“ [онлайн], достъпно на: dariknews.bg. (посетен на 25.02.2022)

REFERENCES

1. Atanasova-Krasteva, Nevena. Neobhodimostta ot adaptivni ekipi za deystvie v ekstremalni situatsii. In: *Sbornik nauchni dokladi – Peti natsionalen kongres po psihologia*, br. 1-4. Sofia: Iztok-Zapad, 2008, s. 700 – 707. ISSN 0861-7813.
2. Atanasova-Krasteva, Nevena. *Psihologia na krizisa*. Veliko Tarnovo: IK na NVU „Vasil Levski“, 2019, s. 330. ISBN 978-954-753-290-8.
3. Georgiev, Georgi. Vzaimodeystvie mezhdu oblastnata i obshtinskata administratsia s Balgarskata armia v upravlenieto pri bedstvia i avarii. In: *Godishnik na Fakultet „Komandno-shtaben“*. Sofia: VA „G. S. Rakovski“, 2018, s. 400 – 408. ISSN 1312-2991.
4. Georgiev, Georgi. *Vzrvin tehnologii v avariyno spasitelni raboti*. Sofia: VA „G. S. Rakovski“, 2016, s. 216.
5. Georgiev, Georgi. Zashita na obekti ot kritichnata infrastruktura ot teroristichni zaplahi. In: *Sbornik dokladi ot Mezhdunarodna nauchna konferentsia „Sigurnost – obrazovanie, nauka, industriia“ – vtora chast*. Sofia: VA „G. S. Rakovski“, 2020, s. 154 – 159. ISBN 978-619-7478-58-7.
6. Georgiev, Georgi. Perspektivi za izpolzvanie na formirovania ot Balgarskata armia za ovladyavane i/ili preodolyavane na posledstviyata ot bedstvia. In: *Sbornik materiali ot voennonauchna konferentsia na fakultet „Komandno-shtaben“*. Sofia: VA „G. S. Rakovski“ 2/2014, s. 81 – 89. ISSN 1312-2991.
7. Filipov, Hristo, Kiril Petrov, Georgi Georgiev. *Organizirane i provezhdane na operatsii po tarsene i spasyavane*. Sofia: VA „G. S. Rakovski“, 2012, s. 123.
8. Georgiev, Hristo. Uchastie i spetsifichni zadachi na SSO v operatsii po preodolyavaneto na krizi v mirno vreme. In: *Sbornik s materialy ot konferentsia na fakultet „Artileria, PVO i KIS“*. Shumen, 2019, s. 118 – 124. ISSN 2367-7902.
9. Gradev, Kalin. Podhod za razrabotvane na variant za deystvie pri planirane na operatsiite. In: *Sbornik dokladi ot mezhdunarodna nauchna konferentsia „Sigurnost – obrazovanie, nauka, industriia“, Vtora chast*. Sofia: Voenna akademia „G. S. Rakovski“, s. 26 – 29. ISBN 978-619-7478-58-7.
10. Kokudeva, Petrana. Teoriyata na sistemite v epohata na platformite. In: *Sbornik dokladi ot Mezhdunarodna godishna nauchna konferentsia na NVU „Vasil Levski“*, 27-28 may 2021 g. Veliko Tarnovo: IK na NVU „Vasil Levski“, 2021, s. 1084 – 1090. ISSN 2367-7481.
11. Krastev, Krastyu. *Takticheskoto razuznavane vav voennite formirovania*. Veliko Tarnovo: IK na NVU „Vasil Levski“, 2021. s. 161. ISBN 978-954-753-326-4.
12. Marinov, Petar. *Terorizmat – abstraktsii i realnosti*. Sofia: Iztok – Zapad, 2016, s. 295, ISBN 619-152-866-3.
13. Petkov, Yordan. Osnovni nasoki za povishavane na umeniyata na lichnia sastav na razuznavatelните formirovania. In: *Sbornik s materialy ot konferentsia na fakultet „Artileria, PVO i KIS“* – Shumen, 2019, s. 106 – 111. ISSN 2367-7902
14. Radeva, Nikolina. *Aktualni aspekti na zashitata na naselenieto pri bedstveni situatsii*. Varna: Steno, 2019, s. 141. ISBN 978-619-241-046-9.

15. Romanova, Hristiana. *Potentsialni antropogeni ekokatastrofi vav Varmenski region. Strategia za zashtita na naselenieto i zapazvane na bioraznoobrazieto*. Varna: VVMU „N. Y. Vaptsarov“, 2014.
16. Watts, William. *Here's the technology being used to watch Russian troops as Ukraine invasion fears linger*. February 16, 2022 [online] available at: <https://www.marketwatch.com/story/how-fears-of-russian-invasion-of-ukraine-put-open-source-intelligence-in-spotlight-11645033603?mod=home-page>
17. Vardhan Harsh. *Canada's Space Company To Provide Intelligence To Ukraine Via Satellites To Resist Russia*. 11 March, 2022. [online] available at: <https://www.republicworld.com/world-news/russia-ukraine-crisis/canadas-space-company-to-provide-intelligence-to-ukraine-via-satellites-to-resist-russia-articleshow.html>
18. Borrell, Josep. *EU to help Ukraine with intelligence from own satellite centre-EU's Borrell*. Reuters, 28-02-2022 20:30 IST. [online] available at: <https://www.devdiscourse.com/article/technology/1941820-eu-to-help-ukraine-with-intelligence-from-own-satellite-centre-eus-borrell>

АНАЛИЗ НА СЪЩЕСТВУВАЩА СИСТЕМА ЗА УПРАВЛЕНИЕ НА ИНФОРМАЦИЯТА В ЩАБА НА СУХОПЪТНИ ВОЙСКИ

майор ас. Мартин Христов

Военна академия „Г. С. Раковски“, *m.hristov@rndc.bg*

Резюме: Информацията е основен и най-важен ресурс на командването и щаба за изграждане на качествено управленско решение. Управлението на информацията е съвкупност от дейности, отговорност на щаба, за доставяне на правилната информация, на правилното място в точното време. На базата на изградения модел на системата в щаба на Сухопътните войски е извършен анализ за разкриване на положителните и проблемните аспекти при прилагане на тези дейности.

Ключови думи: сухопътни войски; статистически анализ; мрежов анализ; управление на информацията

ANALYSIS OF AN EXISTING INFORMATION MANAGEMENT SYSTEM AT THE LAND FORCES HEADQUARTERS

Major Assist. Prof. Martin Hristov

Rakovski National Defence College

Sofia, Bulgaria

E-mail: *m.hristov@rndc.bg*

Abstract: The information is the main and most important resource for the command and headquarters for quality decision-making. Information management is a set of activities, responsibility of the headquarters, to deliver the right information to the right place at the right time. Based on the established model of the system at the headquarters of the Land Forces, an analysis is performed to reveal the positive and problematic aspects of implementation of these activities.

Keywords: land forces; statistical analysis; network analysis; information management

В подхода към изграждане на познание за съществуващата система за управление на информацията в командването и щаба на Сухопътните войски е необходимо да се добие информация за мнението на служителите в тази система чрез анкетиране на служителите. Анкетата, се използва като инструмент за определяне на състоянието на системата за командването и щаба на КСВ по отношение на употреба на термина и прилагане на политиките и процесите за управление на информацията при *планиране на операцията*.

Анкетата е представена и разпространена сред служителите на щаба със съдействието на командването на Сухопътните войски на принципа на стратифицирания случаен подбор.

В *центъра на вниманието* на предложената анкета е да отчете участието на респондентите в процеса на планиране на операцията, както личното, така и на лицата от екипите.

Изборът на този вид подбор е продиктуван от желанието да се получи представителна извадка за мнението на щаба, която да бъде достатъчно детайлна според нивата и категориите служители в него. Третото условие е да бъде осигурен достатъчно голям брой единици в извадката.

Настоящият въпросник не цели получаване на информация за попълнили го лица, а търси проблемите в системата и мястото на всяка длъжност в прилагане на политиките и процесите по управление на информацията. Дискретността на данните е приоритет за анкетиращия. Въпросите, на които залага анкетата, изследват становището на респондентите за тяхното отношение, мнение и оценка към управлението на информацията, към проблематиката и процесите, свързани с управлението на информацията в щаба на сухопътните войски и др.

Чрез анкетата, поради включения стратифициран подбор, се обособяват различни категории и групи, чието мнение трябва да бъде анализирано поотделно. От друга страна въпросите са групирани около няколко смислови центъра.

I. Познанията на респондентите за системата за командване и управление като цяло и в частност – за управлението на информацията като същност и съдържание.

II. Търсене на подходящ превод на термина *information management*, който да носи достатъчно разбиране за същността и съдържанието на съвкупността от дейности и процеси.

III. Как е изградена системата за управление на информацията и познава ли се от отделните лица в щаба.

IV. Участието на отделните лица, в частност, и на звената като цяло в процесите по управление на информацията, категоризирани в отделни потоци.

V. В какво се състои изградената система за подготовка на личния състав от щаба по отношение на управлението на информацията.

VI. Качество на предоставяната/получаваната информация и факторите от които зависи то.

Много от въпросите в различните части отчитат конкретното състояние на индивидуалната подготовка на служителите за изпълнение на дейностите по управление на информацията, както и участието им в тези дейности и обособени процеси. С цел постигане качество на модела на щаба и на колективно ниво, отговорите са стратифицирани и по други критерии по хоризонтала и вертикала (длъжностни нива и звена в щаба).

Чрез резултатите от анкетното проучване, авторът си поставя още една задача – да анализира общото разбиране и прилагане на теорията и нормативните документи, свързани конкретно с управлението на информацията в щаба на Сухопътните войски. Търсят се отговори на въпросите за познаване на процесите за управление на информацията, за прилагане на процесите и, не на последно място, за недостатъците в цялостния процес по управлението на информацията и най-вече от какво са породени тези недостатъци, което от своя страна може да послужи като стабилна основа за намиране на решения и за предлагане на подходящи мерки за подобряване на управлението на информацията като част от системата за командване и управление на Сухопътните войски.

Проведената анкета се основава върху следните стратифицирани показатели: звено и експертно ниво в йерархията.

Стратифицирани показатели за сегментиране на респондентите намират широко приложение в теорията и практиката. Популярността им се дължи на факта, че от тях в значителна степен става ясно отношението на отделните колективи към въпросите, участието на отделните колективи и експертни нива в изследваните процеси и дейности. Наред с това, така структурирани резултатите са лесно измерими и достъпни, което би могло да повиши интереса към тяхното използване за цели извън обхвата на настоящия доклад.

Според автора разделението на показателите има своите формално-логически основания. В изследването звеното и подзвеното са необходими показатели по отношение на определяне на участието на отделните групи в процесите по управление на информацията като цяло, както и по отделните потоци. Друго основание за това решение е необходимостта да се определят по-точно връзките и зависимостите между звената и качеството на получената/предадена информация.

Експертното ниво е показател, необходим да се представят резултатите спрямо равнището на познание. Логично е различните експерти да не бъдат поставяни под общ знаменател и техните отговори да носят различна тежест. Този подход произтича от различията в знанията между експертните нива.

Знанието може да бъде емпирично и теоретично, псевдо научно и научно, технологично, житейско, явно (кодифицирано) и неявно (тацитно). Знанието може да се определи и като способност на човека за вземане на решения и пораждане на действие. Предполага се, че експертите на по-високите нива имат повече теоретични и житейски познания, придобити от по-дългото им престояване в структурата. Друг аргумент в подкрепа на този показател е разпределението на дейностите, свързани с управлението на информацията по различните нива в йерархията на организацията.

В анализа на анкетните резултати се търси отговор на определени въпроси:

– Какви са по актуалност и задълбоченост познанията на анкетираните по отношение на елемента „управление на информацията;

– Колко задълбочени са познанията в тази област и какъв е произходът на дефицита, ако има такъв;

– Има ли в щаба разработени процедури, или отдадени заповеди, разпореждания, указания, свър-

зани с управлението на информацията, знаят ли служителите за тяхното съществуване и как оценяват отделни елементи от тяхното съдържание;

- Запознати ли са служителите от щаба с нещата дължности, служителите и групите (нешатни, функционални, пулсиращи или постоянни), свързани с управлението на информацията;

- Какво е участието на всеки служител и звено в процесите по управление на информацията и има ли открояващи се важни елементи (служители, или звена) в цялата съвкупност;

- Кои са характерните за щаба комуникационни канали и кои са основните процеси, прилагани в щаба;

- Каква е подготовката на служителите в щаба за управление на информацията и изградена ли е система за подготовка;

- Каква е степента на удовлетвореност на служителите от качеството на предоставяната в щаба информация;

- Кои са основните фактори, влияещи на качеството на информацията.

I. Познанията на респондентите за системата за командване и управление както цяло и в частност – за управлението на информацията като същност и съдържание

В тази част фокусът е върху знанията и разбиранията на анкетираните, недостига или липсата на познания и най-вече за причините и факторите, които са довели до тези недостатъци. Изследва се смисълът, който влагат анкетираните в основни понятия и термини, свързани със системата за командване и управление като цяло и отделните й елементи, касаещи „управлението на информацията“. Както вече стана ясно, съществува сериозно разминаване между терминологията и съдържанието на отделни елементи на командването и управлението и на поддръжката на системата за командване и управление. Разминаването между националните доктринални документи, съюзните такива и теоретичните постановки по темата може да доведе до объркване, неразбиране и липса на определени познания. От друга страна анкетата предизвиква респондентите да споделят собственото си виждане за определени елементи, според това как най-добре биха съвпаднали и имат най-добра приложимост в средата, в която работят. На следващо място, съществен е въпросът за липсата на определени познания в областта и за произхода на недостатъците. Това би разкрило проблемни области както извън структурата (доктринални, теоретични, индивидуалната подготовка извън структурата), така и вътрешни (колективна подготовка, процедури и организационни дефицити).

Резултати от анализа и изводи за смислов център I:

- Като цяло експертите работят с отменени вече концепции, като малка част от тях възприемат и/или познават новите постановки в националните нормативни документи. Очаквано, младите са носители на промяната като по-голяма част от тях възприемат настоящите схващания за по-правилни.

- Мнението на анкетираните е нееднозначно при определянето на *управлението на информацията* като елемент от системата за командване и управление или като елемент на поддръжката на командването и управлението.

- Колективното ниво на познание за елемента *управление на информацията* е приемливо, но има слоеве, в които нивото е осезаемо по-ниско от общото.

- Личното мнение за познанията са на средно ниво, като ниските експертни нива смятат, че познанията им са по-ниски от средните за колектива, което създава предпоставки за неувереност при прилагане на елемента *управление на информацията* на колективно ниво

- Според респондентите основният проблем, водещ до ниски познания за елемента *управление на информацията* е външен за щаба на СВ и се корени в липсата на терминология и описанието й в националните доктринални документи.

II. Търсене на подходящ превод на термина *information management*, който да носи достатъчно разбиране за същността и съдържанието на съвкупността от дейности и процеси

Фокусът е в търсенето на интуитивност и удобство при използване на термина, като се прилага подходът за допитване до специалистите, от които се очаква да боравят с него и да се търси разпознаваемост на термина в средата, в която ще се използва.

Изследва се смисловата асоциация на термини, представени на български с оригиналния термин на английски език. Очакванията асоциацията да е най-силна в средите, боравещи с термина.

Търси се припознаване на определен термин на български език, който да предостави достатъчно интуитивен превод на термина *information management* без необходимост от разсъждение и доказване, а идващ наум бързо.

Въпросът цели да се проучи нагласата на аудиторията за интуитивността на превода на термина в съюзните публикации.

Резултати от анализа и изводи за смислов център II:

- Голяма част от служителите припознават термина *управление на информацията* като добър и интуитивен превод на *information management* в сравнение с другите възможни алтернативи на превод.
- Не може да се пренебрегне и фактът, че като цяло аудиторията е разделена в мнението си за различните термини (което задължително налага уеднаквяване на терминологията в нормативните и доктринални документи).

III. Как е изградена системата за управление на информацията и познава ли се от отделните лица в щаба

В тази част фокусът е върху елементите, изграждащи системата за управление на информацията в щаба на СВ. Тези елементи са: разработените документи в щаба на СВ, свързани с управлението на информацията – концептуални (политики, процедури) и/или нормативни (заповеди, указания, разпореждания); описанието на схващанията, процесите и дейностите за управление на информацията; описанието на групите и ролите на тези групи и лицата в тях.

Изследва се присъствието или отсъствието на определените елементи в организирането на системата за управление на информацията.

Търси се информация за наличието или липсата на конкретни документи – процедури, указания, заповеди, разпореждания, свързани с управлението на информацията, информираността за съществуването на тези документи от анкетираните, както и тяхната оценка на конкретни елементи от тяхното съдържание.

На следващо място, се търсят нещата дължности, служителите и групите (нешатни, функционални, пулсиращи или постоянни), свързани с управлението на информацията и в каква степен ги познават останалите служители от щаба.

Резултати от анализа и изводи за смислов център III:

- Голяма част от състава знае, че процедури, както и нормативни документи за управление на информацията са разработени, но не посочват по категоричен начин кои са те.
- Всички посочени елементи от съдържанието на документите са разработени и оценени между средно и високо ниво.
- Може да се предположи, че документите създават основа за добра организация, която логически трябва да е продължена в анализа на резултатите от следващия смислов център.
- В щаба има назначен „инфомениджър“, но повечето служители не знаят за наличието на такива или други нешатни служители.
- Не се назовават еднозначно групите, занимаващи се с менажиране на процесите по управление на информацията, като е по-вероятно такива групи да не съществуват или най-малкото служителите само да са чували за тях, но не знаят за тяхното съществуване.
- Уж има документи, които регламентират, на ниво над средното, процесите, ролите и задълженията, а всъщност почти никой от анкетираните не е такъв, не познава служители и най-вече – не могат да ги назоват.

IV. Участието на отделните лица и на звената в процесите по управление на информацията, категоризирани в отделни потоци

В тази част фокусът е върху създаване на обща представа за участието на отделните служители в процесите, свързани с управлението на информацията, както и върху придобиване на представа за организацията и важноста на отделните процеси.

Изследва се характерът и същността на информационните канали (връзки) между участниците в комуникацията по време на планиране на операцията, между служителите, звената, и различните структури (подчинени формирования, старши, съседни, външни).

Анализ на количествените параметри на свързаността на звената в щаба и в експертните нива по типове връзки – общо и по процеси.

Общият извод, който би могъл да се направи в това направление е, че комуникацията протича в доста нехарактерни за процеса на планиране посоки. Основна роля играе комуникацията с подчинените. Различните звена не участват в характерни процеси както в рамките на щаба, така и с подчинените. Експертните нива участват в процесите хаотично.

Чрез прилагане на мрежов анализ на служителите и връзките се търси открояване на „важни“ ключови длъжности, звена и структури, оказващи най-голямо влияние върху изградената система за пренос на информация в щаба.

Мрежов анализ на специалистите и звената в щаба – едни спрямо други – в търсене на „важните“ за протичане на информацията.

Подходът, необходим за анализ на щаба и служителите, цели открояване на отделните елементи, опознаването им от гледна точка на тяхното място в общата картина, както по отношение на свързаността им с другите елементи. Мрежовият анализ е подход, изцяло базиран на математически инструменти, който използва теорията на графите. За нуждите на мрежовия анализ средата се представя чрез два компонента:

- служителите в щаба се представят като „възли“ или „участници“;
- линиите, свързващи елементите са наречени „дъги“ и представят взаимодействието между възлите.

Взети заедно, графите изобразяват отделните участници в мрежата и релациите между тях¹.

Анализът на елементите на мрежите цели да предостави познанието и да представи характеристики на елементите, свързани с местоположението им в мрежата. Този тип представяне дава възможност да се открият възлите, действащи като мостове и по този начин свързват различни групи области, допринасяйки за сближаването на мрежата. Анализът на мрежата изследва преноса на информация и възможностите или невъзможността за предаване на информация между източници и потребители в определена мрежа (щаб, старши и подчинени структури и др.). Както посочва Енев, „Основните направления, в които може да се прилага той са идентифициране на пропуски, модели, определяне на точки на въздействие, определяне на критични линии.“²

Тези приложения далеч не изчерпват възможностите, които дава подходът. Важно е да се отбележи как използването на този подход подпомага изброените дейности – както директно, така и индиректно – чрез подпомагащи анализи. Подходът може да е бъде прилаган при изготвяне на диаграми на влиянието за определяне на елементите, от които системата черпи своята устойчивост и стабилност. От друга страна, докато теорията на информацията се занимава с ентропията, кодирането, търсенето на най-икономичните методи за кодиране и пропускателната възможност на каналите, анализът на комуникационната мрежа може да покаже най-натоварения елемент, важния свързващ елемент или възела, който най-бързо би предал определена информация до всички точки от мрежата.

Важно условие при използването на този инструментариум е, преди началото на анализа, анализаторът ясно и конкретно да определи „каква е целта“ по отношение на тази мрежа или „каква е важната дефиниция“. Вероятността в този случай да бъдат дефинирани различни понятия за „важно“, според всеки анализатор, се покрива и от няколко характеристики. Основните, които биха могли да дадат яснота за „важността“ на елементите, са степен на централност, междинност, както и ключов елемент за сплътеност и ключов елемент за вграденост.

Степен на централност е броят на директните (преките) връзки, които има дадена единица в мрежата или с други думи – броят на възлите, с които той е в пряк контакт.

Степента се разглежда като важен показател за комуникационния потенциал на възела. В мрежа на връзките на служителите в щаба степента може да посочи най-натоварения в информационно отношение елемент, т.е. – служителя, който е най-добър проводник и разпространител на информация – формална (данни) или неформална (слухове).

Степента на централност не измерва косвени връзки или връзките на един възел с други възли.

Друг показател за измерване на централността е да се измери честотата на възел, лежащ на пътя между други възли, дефиниран като *междинност*.

В реалния свят участниците се опитват да сведат до минимум трети страни, участващи в комуникацията им с техните кореспонденти. Мярката за междинност е обвързана с допускането, че потокът

(информационен или материален) между два възела ще следва най-краткия физически път между тях. От тук произтича и определението: междинност на един възел е броят на най-късите пътища, които преминават през възела.

Елементите с висока междинност са съхранители на сила и знания, поради централното място, което заемат по отношение на потоците, протичащи между два възела и високата степен на контрол на пропускливост в мрежата. От друга страна, те са важната връзка между различните разклонения на мрежата и проводник на материалния или информационен поток между тези разклонения. В социалните структури (от щабли елементи до терористични групировки) тези елементи са най-запознати с дейността на мрежата и са потенциалните информатори.

Следващият подход, свързан с местоположението на елементите в мрежата, е търсенето на ключови играчи по два възможни критерия: доколко елементът спомага за сплотеността на мрежата и доколко елементът е вграден в мрежата.

В първия случай елементите с най-висока *степен на сплотеност* показват връзката, която е най-силно обвързваща и чието премахване разкъсва най-много мрежата. Поразяването на тези елементи в комуникационната система прекъсват управлението на формированията, което играе пагубно влияние при военни системи, които не използват подхода на мисийно командване. Спира се информационният поток и се нарушава информационната осведоменост на участниците в процеса на планиране.

Мрежи с множество елементи с максимална стойност са по-устойчиви на разкъсване от мрежи с един или два елемента с изразена висока стойност.

Ключов елемент за вграденост е показател, свързан със степента, в която ключовите играчи са вградени в мрежата около тях, защото измерва предимно разпространението на информацията. Това са елементите, които най-ефективно могат да бъдат използвани за пренос на информация в рамките на мрежата. Това най-често са неформалните лидери или личностите, които оказват най-силно влияние на групата. В комуникационните системи обикновено те са елементите, източник (генератор) на информация (заповеди, сводки, данни).

Ключовите участници в този контекст, когато се използват като семена за дифузия, могат да допринесат за разпространение на информация по-бързо и по-ефективно от други възли. Например, може да помогне да се определят неформални лидери, които да насърчават определено желано поведение или практики.

Резултати от анализа и изводи за смислов център IV:

От казаното дотук се открояват няколко важни съждения:

Основни процеси за щаба и за отделните звена, с много слабо предимство, са процесите събиране, обработване, съхраняване, предоставяне и разпространение на информация.

Най-интензивна е комуникацията с подчинените формирования – основно с прилагане на процесите разпространяване, обработване и предоставяне, а вътрешната комуникация е на второ място – основно с прилагане на процесите събиране, обработване, разпространяване и предоставяне.

При комуникацията с подчинените формирования във всички процеси основна роля играе L-1. Що се касае до останалите звена, характерно е прилагането на всички процеси без определена структурираност и признаци на нелогичност (L-5 – защита и разпространяване).

При комуникацията с подчинените формирования високите експертни нива също представят нехарактерност и дезорганизираност на процесите (НО – разпространяване и защита; НС – събиране), докато главен експерт и старши експерт са по-добре структурирани в процесите събиране, разпространяване и обработване.

При комуникацията в щаба отново основна роля във всички процеси играе L-1, а звената с основна роля за анализа и вземането на решение (L-2, L-3 и L-5) прилагат процесите разпространяване, предоставяне, съхраняване и защита.

При комуникацията в щаба високите експертни нива очаквано участват в процеси обработване и предоставяне и, нехарактерно – в защитата. Главните експерти също са най-активни в обработването, а за старшите експерти основни процеси са разпространяване, предоставяне и събиране.

Съществени длъжности, носители на определени важни характеристики са:

- най-добри разпространители на информация – гл. експерти в L-3 и НС в L-5;
- най-добър генератор на знания и най-силен проводник на информацията – командирът.

Централно място в разпространението на информацията в щаба заемат L-3, L-5 и L-2, а L-3 и L-5 са и подходящи проводници на информация и генератори на знания.

В щаба е изградена стабилна мрежа за разпространение на информацията между служителите.

Най-влиятелни в разпространението на информацията в щаба са началникът на сектор в L-5 и служителят, главен експерт в L-3, а по отношение на звената – L-3 и L-5.

V. Същност на изградената система за подготовка на личния състав от щаба по отношение на управлението на информацията

В тази част фокусът е върху подготовката на личния състав. Целта е да се подпомогне изследването на останалите смислови центрове с детайлизиране на резултатите. Евентуалният недостатък на познания за управлението на информацията и изпълнението на дейностите биха могли да са свързани с подготовката – индивидуална и/или колективна. Подготовката може да се раздели и на подготовка в частта или специализирана подготовка извън формирането, в специализирани центрове за квалификация и обучение. Логично е да се смята, че повече подготовка е необходима на по-младите служители. Изследва се създадената система за подготовка и резултатите от нея по звена и по експертни нива.

Резултати от анализа и изводи за смислов център V:

Представените резултати водят до противоречив извод за подготовката на служителите. Не става категоричен ясно дали е изградена система за подготовка на служителите, но както служителите, така и звената са подготвени за управление на информацията на ниво над средното.

VI. Качество на предоставяната/получаваната информация и факторите, от които зависи това качество

В тази част фокусът е върху качествените характеристики на информацията като ресурс за вземане на управленско решение. Всички опити да бъде организиран и структуриран процесът по управление на информацията, трябва да водят до качествена промяна, най-вече на предоставяната. Целият щаб трябва да разбира правилно контекста на информацията, която обработва, за да я управлява ефективно. Удовлетвореността на служителите от получената информация е стабилен критерий за оценяване на качеството на доставяната информация.

Изследва се удовлетвореността на служителите от доставяната информация и факторите, които оказват влияние на липсата на информационна осведоменост и рефлектиращи върху качеството на информацията в щаба.

Всеки потребител има присъщи отговорности за придобиване, оценяване, аргументиране, поставяне под въпрос, корелация и разпространение на качествена информация за други потребители. Всички служители на щаба, като потребители на информация, също са информационни мениджъри.

Резултати от анализа и изводи за смислов център V:

Качеството на предоставяната в щаба информация е на ниво над средното, като с по-високо качество се отличава текстуалната информация, докато заниженото качество на графичната се обуславя от липсата на еднаквост на използваните символи за изобразяване.

Основни фактори, влияещи на качеството на информацията, са свързани със споделянето между служителите и звената.

Изводите на отделните смислови центрове, както и общият им анализ дават възможност за обширни и изчерпателни отговори на въпросите, поставени при проведената анкета, които биха могли да се обобщат в следващите редове.

Познанията на основна част от анкетираните за управлението на информацията са неактуални, но изключения правят младшите експертни нива, което е породено от съвременната им подготовка преди постъпване във формирането. Служителите оценяват задълбочеността на познанията си на средно ниво, но високите експертни нива се чувстват по-неуверени в познанията си, което си проличава и във всички аспекти на прилагането на тези знания (изготвяне на качествени процедури и структурирано прилагане на процесите за УИ). Що се касае до причината за липсата на познания, анкетираните считат, че проблема идва от неясната терминология и от липсата на описание на тази дейност в доктриналните документи. Запитани за най-подходящия превод на термина *information management*, аудиторията колебливо посочва „управление на информацията“, което отново е породено от нееднаквостта на терминологията в доктриналните документи. Не е категоричен и отговорът на въпроса за вътрешните документи за

УИ – процедури и/или заповеди, тъй като голяма част знаят, че такива има, но не са запознати със съдържанието им. В продължение на това съждение идва и колебливата оценка на съдържанието им, като анкетираните смятат, че документите не описват достатъчно детайлно дейностите по УИ. Това твърдение е подкрепено и от липсата на еднозначност при описването на отговорностите и процесите в щаба.

Инфомениджър е назначен, но той не е известен на всички служители, а групи и звена, управляващи процесите и дейностите по УИ, изглежда, че има, но по-скоро са с фиктивни функции, тъй като не могат да бъдат еднозначно посочени от анкетираните, а и управление на процесите не се прилага на практика.

Прави впечатление, че комуникацията с подчинените формирания заема основна част от общата комуникация по време на планирането. Вътрешната комуникация се отличава с не структурираност, която се изразява в участие на всички звена и специалисти в почти всички процеси и още повече – звена, които обичайно нямат водеща роля в планирането, имат водеща в комуникацията.

Анализът на изградената мрежа за комуникация в щаба показва възможност за устойчива комуникация и отличава водещите звена в процеса на планиране като подходящи проводници на информация и генератори на знания. Мрежовият анализ също посочва експертите, които са най-добри разпространители на информация (началник на сектор в L-5 и главен експерт в L-3), както и най-добрият генератор на знания и най-силен проводник на информацията (командирът).

Като основни за вътрешната комуникация в щаба се разпознават процесите разпространяване, предоставяне, съхраняване и защита, но като цяло е трудно да се определи участието на конкретни звена или длъжности в определени процеси, което допълва извода, че процесите не се управляват правилно.

ЛИТЕРАТУРА

1. West, D. B. *Introduction to Graph Theory, 2nd Edition*. Prentice-Hall, Inc., Upper Saddle River, 2001, p. 82-83.
2. Енев, Е. *Разбиране на оперативната среда и определяне на центъра на тежестта посредством мрежов анализ и анализ на социалните мрежи*. София: Българска наука, 2020, с 8 – 16.

REFERENCES

1. West, D. B. *Introduction to Graph Theory, 2nd Edition*. Prentice-Hall, Inc., Upper Saddle River, 2001, p. 82-83.
2. Enev, E. *Razbirane na operativnata sreda i opredelyane na tsentara na tezhestta posredstvom mrezhov analiz i analiz na sotsialnite mrezi*. Sofia: Balgarska nauka, 2020, pp. 8 – 16.

КОМПЛЕКС ВЪЗДУШНА ОБСТАНОВКА ПЕРСПЕКТИВИ ЗА РАЗВИТИЕ

полковник проф. д-р Петър Христов
Военна академия „Г. С. Раковски“, pshtbg@abv.bg

Резюме: В доклада са разгледани възможности за развитие на „Комплекс въздушна обстановка“, чрез прилагане на иновативни решения в подготовката на формированията на Въоръжените сили базирани на верифицирани постижения на родната индустрия.

Ключови думи: въздушна обстановка; формирования от ПВО; подготовка; родна индустрия; експериментални полети

AIR SPACE SITUATION COMPLEX

Colonel Prof. Petar Hristov, PhD
Rakovski National Defence College
Sofia, Bulgaria
E-mail: pshtbg@abv.bg

Abstract: The development of technology creates opportunities for the implementation of innovative solutions in the preparation of armed forces units based on the achievements of the home industry and the research potential of automation and remotely controlled systems.

Keywords: air space; air defence units; preparation; home industry

Провеждането на постоянна и максимално близка до реалната обстановка подготовка на формированията е една от основните задачи за изграждането, поддържането и усъвършенстването на отбранителните способности на въоръжените сили на Република България. Успешното провеждане в процеса на непрекъснато адаптиране относно променящата се среда за водене на бойни действия през XXI век налага използването на нови подходи.

През настоящата година за успех в една операция се утвърждава като ключов фактор господството над въздушното пространство. Господството над въздушното пространство гарантирано намалява рисковете за успешното провеждане на многокомпонентни операции и минимизира загубите на личен състав, материални и финансови ресурси. Създава се бойно пространство за развързване и използване на пълните възможности на формированията от родовете войски.

Постигането на господство над въздушното пространство чрез провеждане само на въздушна операция или само на настъпателна противовъздушна операция срещу добре организирана система за противовъздушна и противоракетна отбрана (ПВ и ПРО) се доказва, като непостижима мисия в досегашните бойни действия в продължаващия военен конфликт в Украйна. Провеждането на успешни противовъздушни боеве чрез активно участие в построението на формирования на ПВ и ПРО (наземно и въздушно базирани) в Украйна дава възможност за развързване на отбранителните сили и съхранение на логистичните способности на украинските формирования. В рамките на наложеното превъзходство над въздушното пространство в строго определени зони е създадена възможност за нанасяне на удари от въздуха по незащитени от формирования на ПВО логистични колони, снабдяващи руските формирования с гориво и боеприпаси – предимно с дистанционно управляеми въздухоплавателни средства. Наличието и тактически правилното използване на мобилни и преносими противовъздушни и противоракетни комплекси от различен тип, разпределени по цели, височини, разстояние, направления и скорости, не допуска завоюване на господство над въздушното пространство на Украйна и нанася значителни загуби на авиационни средства – пилотируеми и безпилотни – на руските формирования, което е и един от факторите за промяна на темпа на бойните действия. Спечелено е време за формиране на формални и неформални позиции спрямо конфликта в световен мащаб и за разширяване на санкциите спрямо Русия.

Подготовката на формированията от ПВ и ПРО в голяма степен е решаващ фактор при защита на силите в зоната на операцията. Изграждането и поддържането на устойчива ПВ и ПРО за действия при всякакви метеорологически условия и на способност за провеждане на успешни противовъздушни и въздушни боеве, независимо от широкия тип на използваните средства за нанасяне на удари от въздуха по прикриваните обекти и войски, налага използване на нови подходи при провеждането на подготовката във формированията. През настоящия военен конфликт се забелязва разширяване на използваните средства за нанасяне на удари от въздуха и от двете страни.

Голямото разнообразие в използваните средства за нанасяне на удари от въздуха създава възможност да се атакуват слабите страни на изградената система за ПВ и ПРО в зоната на операцията. Тя трябва да е способна да отразява удари от въздуха както с пилотируеми, така и с все по-масово използване на дистанционно управляеми въздухоплателни средства.

Ограничените материални и най-вече финансови ресурси налага въвеждането на подходи за подготовка и търсене на нови възможности при провеждане на индивидуалната и колективната подготовка на формированията от ПВ и ПРО.

Във Военна академия „Г. С. Раковски“ е разработена на концептуално ниво и са проведени серия от летателни изпитания на прототип на „Комплекс въздушна обстановка“, като се използват потенциалът и постиженията в информационните технологии, симулационни системи и програмни продукти на родната индустрия, както и научният потенциал на катедра „ВВС и ПВО“ от факултет „Командно-щабен“.

Гарантираната защита на войски и критична инфраструктура в зоната на операцията до голяма степен зависи от устойчиво структурирана система за ПВ и ПРО и от подготовката на формированията за откриване, съпровождане и унищожаване на обекти, атакуващи от въздуха във всякакви условия на водене на въздушни и противовъздушни боеве. Високата степен на подготовка изисква, освен формирането на определени теоретични знания, и практически опит чрез използване на симулационни системи в тренажорни комплекси и най-вече с провеждане на практически тренировки с реално обозначаване на въздушните цели. Поради традиционно ограничения финансов ресурс този решаващ етап на подготовка протича с недопустими за днешната реалност условности и намалена интензивност, което не способства за поддържане на необходимото ниво на ПВ и ПРО за гарантиране на защитата на войски и критична инфраструктура, както в мирно време, така и в конфликт от военен характер на територията и в акваторията на страната.

Пълноценната практическа натренираност и формирането на устойчиви умения в разчетите и екипажите от ПВО налага изразходване на значителен ресурс от самолеточасове на разнотипни летателни средства от състава на ВВС. За формирането на авиационен въздушен удар по прикриваните войски и инфраструктурни критични обекти от подразделенията за ПВО в рамките на тактическо учение (ТУ) са необходими не по-малко 8 – 10 самолеточаса, разпределени по определен модел на удара в зависимост от огневите възможности на формирането за постигане на пълно съответствие за действията на ударната авиация по прикриваните обекти. Методически правилно е провеждане на не по-малко от едно тактическо учение (ТУ) с всяко отделно подразделение от ПВО в годината. В периода на груповата подготовка се провеждат тренировки и проверки за допускане до тактически учения с бойни стрелби (ТУБС) на формированията от ПВО и се проверяват способностите за бойно управление на оперативните центрове, които също изискват определен авиационен ресурс. Общо за година, за провеждане на системна и пълноценна подготовка на формированията от ПВО, са необходими минимум 110 до 150 летателни часа. Ограничените възможности за целево заделяне на самолетоизлитания в етапа на груповата подготовка на формированията от ПВО води до несистемност в подготовката им и до дефицит на способности.

Повишаването на изискванията към обхвата на практическата подготовка на разчетите и екипажите от ПВО за откриване, съпровождане и унищожаване на широк спектър от средства за нанасяне на удари от въздуха, са в остър конфликт с ограничения ресурс от самолетоизлитания за провеждане на тренировки с реално обозначаване на целите.

Разрешаването на създадала се конфликтна ситуация налага въвеждането в различните етапи на подготовка на екипажите и разчетите от ПВО на „Комплекс въздушна обстановка“. Самият комплекс може да се разгледа и като практическа реализация на теоретичния принцип на системата от системи, допринасящ за онагледяване на теоретичната концепция, приспособена към конкретните изследвания за дадена структура или система¹.

Създаването на концепция за използване на „Комплекс въздушна обстановка“, разработването и провеждането на серия от летателни изпитания на ниво прототип са осъществени за период от две години на основание на договор за съвместна дейност от екип в състав катедра „BBC и ПВО“ и фирма „Фрага Х“ ЕООД.

При проведените летателни изпитания на КВО за времето от 07.09 до 12.09.1922 г., като неразделна част от съвместни експериментални и бойни стрелби „Шабла 2021-2“ е констатирана пълна функционалност на комплекса и са разкрити възможности за перспективно развитие и в други функционални области.

Проведените експериментални полети потвърждават ефективността от внедряването във формирования от ПВО на комплекс за въздушна обстановка (КВО) в състав: наземна станция, дистанционно управляеми летателни апарати (до 3 бр.) и дистанционно управляващи пилоти (един/два).

С придобиване на КВО във формирования от ПВО ще се компенсира дефицитът на авиационен ресурс за провеждане на пълноценни тренировки с реално обозначаване на целите от формированията за ПВО. Въвеждането на комплекса с цел повишаване на практическия опит от една страна ще даде възможност за пестене на авиационен ресурс на пилотируемата ни авиация, а от друга – ще се повиши и разшири натренираността на екипажите и разчетите по откриване, съпровождане и унищожаване на дистанционно управляеми летателни системи от различен клас.

При проведените функционални изпитания на КВО в ТУБС е доказано, че създаването, експлоатацията и поддръжката му е напълно възможна мисия на базата на натрупания опит и разполагаемия потенциал на родната авиационна индустрия („Фрага-Х“) и научния потенциал на катедра „BBC и ПВО“ на факултет „Командно-щабен“ от Военна академия „Г. С. Раковски“.

По време на проведените летателни изпитания на КВО са разкрити възможност за последващо усъвършенстване на дистанционно управляемите системи за постигане на други функционалности, като комплекс за въздушно наблюдение (обективен контрол, разузнаване, целеуказване), ударен комплекс (платформи за нанасяне на удари от въздуха, управляеми високоточни поразяващи боеприпаси), комплекс за логистични услуги, комплекс за радиоелектронно противодействие, комплекс за ретрансляция на бази данни. КВО доказва, че може да се използва като основа за изследвания и изпитания на дистанционно управляема летателна система (ДУЛС) за нуждите както на формированията от въоръжените сили, така и на бизнеса.

Разработената, експериментирана и верифицирана система за управление в КВО може да се прилага като концептуална база за развитие на национална система за контрол на безпилотни въздухоплавателни средства и като техническа основа за създаване на национална система за опознаване на Въоръжените сили.

Развитието на дистанционно управляеми системи за опериране в бойното пространство (въздушно, морско и по суша) с по следващо внедряване във формированията на въоръжените сили на Република България, базирани на високотехнологични продукти на родната индустрия е единствената алтернатива за формиране на национални отбранителни способности, отговарящи на съвременните предизвикателства пред системите за гарантиране на суверенитета и териториалната цялост на страната ни.

Проверката на функционалността е проведена при следният състав на КВО:

- наземната станция (мобилна);
- наземната станция допълнителна;
- БЛА „Таласъм – Х“ (D6 – по спецификация на „Фрага – Х“);
- БЛА „Скорпион – Х“ (D1);
- БЛА „Делта – Х“ (D2);
- БЛА „Асистент – Х“ (D3);
- спомагателно оборудване;
- дистанционно управляващи инструктори пилоти (двама).

Унифицираната наземна станция е мобилен тип с възможност за работа 9 – 12 часа на автономно захранване, както и на захранване от външен 12V източник. В станцията се въвеждат полетните планове на БЛА, изобразяват се видеоданни от бордовата камера, приемат се и се изобразяват на дисплей основните параметри на полет на БЛА и местоположението му върху цифрова подложка на района за изпълнение на задачата. Чрез нея могат да се управляват всичките БЛА от състава на КВО. Станцията е способна да



Сн. 1. Унифицирана наземна станция в развърнато положение

Допълнителната станция е със същите възможности както основната. По време на експерименталните полети чрез нея се осигурява безопасност на полетите и обективен контрол от командния пункт. Във всеки момент, по разпореждане на ръководителя на стрелбите, дистанционно управляващият пилот може чрез нея да променя полетните планове на БЛА. Развързването ѝ в командния пункт създава възможност за обективен контрол на действията на разчетите на зенитноракетните и радиотехническите комплекси.

БЛА „Таласъм – X“ (D6) изпълнява полетен план със заходи от двадесетия до десетия километър от стартовите позиции на комплексите в сектора за стрелба на височини от 2500 до 5100 м, за полетно време от 1 час и 4 минути. Пролетените километри в сектора за стрелба са 235 със средна скорост от 218 км/ч при скорост на вятъра 17 м/с. Постигнатата от „Таласъм – X“ (D6) височина на полета са рекорд за български БЛА.

БЛА „Скорпион – X“ (D1) изпълнява полетни планове (два) със заход от седми до втори километър от стартовите позиции на комплексите в сектора за стрелба, на височина 800 м, за общо полетно време от 50 минути. Пролетени километри в сектора за стрелба – 94, със средна скорост от 115 км/ч, при скорост на вятъра 17м/с.

На 08.09.2021 г. за времето от 10.58 до 12.20 часа чрез КВО, с трите разнотипни по клас БЛА, е създадена сложна въздушна обстановка за тренировка на разчетите на зенитноракетните и радиотехническите формирования в сектора за стрелба на полигон „ШАБЛА“, като едновременно трите БЛА (за първи път три БЛА едновременно оперират в сектора за стрелба на полигон „ШАБЛА“) изпълняват полетните си планове на височини от 800 до 5100 м, по разстояние от 2 до 20 км от стартовите позиции, в условия на умерен североизточен вятър със скорост 17 м/с. По време на функционалните изпитания на КВО сумарно за трите БЛА полетното време е 2 часа и 51 минути. Общо пролетените километри са 396.

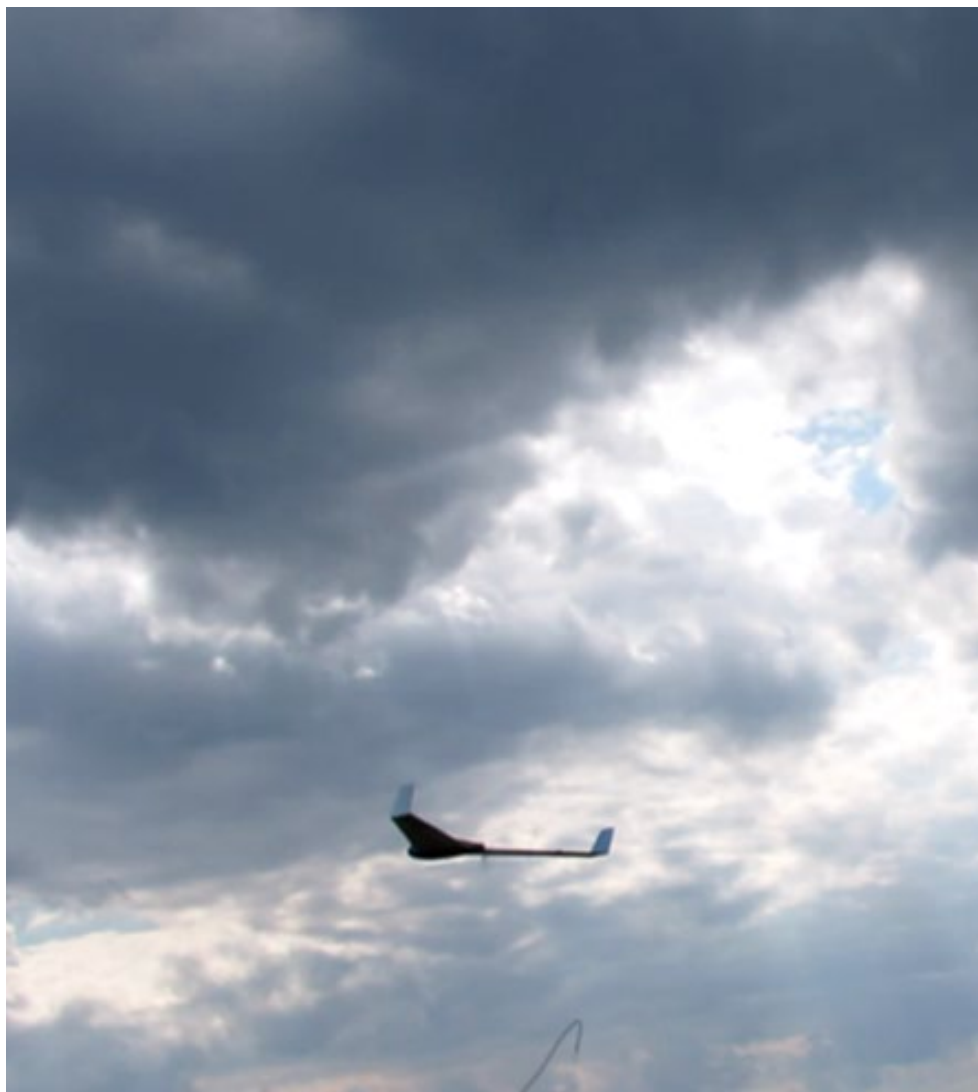


Сн. 2. „Таласъм – Х“ (D6) в полет



Сн. 3. БЛА „Скорпион – Х“ (D1)

БЛА „Делта – Х“ (D2) изпълнява полетен план със заходи от десетия до петия километър от стартовите позиции на комплексите в сектора за стрелба, на височини от 1000 м , за полетно време от 57 минути. Пролетени километри в сектора за стрелба – 67, със средна скорост 71 км/ч, при скорост на вятъра 17 м/с.



Сн. 4. БЛА „Делта-Х“ (D2) в полет

БЛА „Асистент – Х“ (D3) е функционално пригоден за обучение на дистанционно управляващи пилоти и се използва като резервен БЛА в полетните изпитания.

В рамките на съвместни експериментални и бойни стрелби „Шабла 2021-2“ на 10.09.2022 г. са проведени летателни изпитания с КВО с един БЛА за определяне на способностите за откриване, определяне на координатите на стрелящи пускови установки от състава на ЗРВ и РВ. Проведените летателни изпитания потвърждават перспективата за развитието на КВО в комплекс за наблюдение, координиране на огневото поразяване, целеуказване и развитието му в ударен комплекс чрез безпилотни летателни апарати за еднократно използване (камикадзе). В зависимост от комплектуването с различните прототипи БЛА (D1, D2, D3, D6, D7) могат да се постигнат и пространства за опериране в широки граници. Пространството за опериране с изброените прототипи БЛА, произведени от фирма „Фрага – Х“ ЕООД, варират по радиус и горна граница по височина – от 30 км и 2500 м, до 500 км и 5500 м.



Сн. 5. БЛА „Асистент – X“ (D3) в полет

Анализът на проверените по време на летателните изпитания тактико-технически характеристики на тестваните БЛА и унифицираната наземна станция сочи, че получените резултати дават основания да се твърди за високия потенциал на КВО за развитие в многофункционален комплекс чрез по-нататъшно усъвършенстване на БЛА и специализация на състава му.

При проведените летателни изпитания за проверка на способностите на КВО и експерименталното му използване по време на проверка на подготовката на разчетите от ЗРВ за допускане до бойни стрелби на ТУБС „Шабла-2021“ са разкрити алтернативите за развитие на комплекса и е потвърдена ефективността му за създаване на реална въздушна обстановка с цел компенсиране на дефицита при подготовка на формированията от ПВО (ЗРВ, РТВ и ИА) за откриване, съпровождане и огнево въздействие по реални обекти във въздушното пространство, както и за създаване на напрегната мишенна обстановка при провеждане на бойни стрелби със зенитноартилерийски, зенитноракетни и изстребително-авиационни формирования.

По време на проведените изпитания КВО показва пълно съответствие с концептуалната разработка по отношение неговото използване в подготовката на формированията за бойна работа в реална въздушна обстановка и за проверка състоянието на подготовка на екипажите и разчетите. Комплексът изпълнява предназначението си при проверка състоянието на техниката и въоръжение в РТВ, ЗРВ, ИА и ЗА, а също и за установяване способностите на оперативните центрове, пунктовете за бойно управление и командните пунктове от ПВО за осъществяване на централизирано бойно управление на подчинените формирования в зоната на операцията чрез създаване на сложна въздушна обстановка в рамките на провежданите тренировки и учения по управление на огъня с реално обозначаване на целите.

Използването на КВО ще намали чувствително изразходването на авиационен ресурс за нуждите на подготовка на формированията за ПВО, като в същото време ще съдейства за повишаване уменията на екипажите и разчетите при бойна работа по откриване, съпровождане и въздействие по БЛА от различен клас и способностите за неутрализиране на удари от въздуха с подобни средства.

Придобиването и използването от формированията на въоръжените сили на произведени от родната индустрия, различни по функционалност дистанционно управлявани комплекси, ще намали усилия-

та и ресурсите, свързани с гаранционното обслужване, експлоатацията, осигуряването с резервни части и консумативи през периода на експлоатация. Осъществяването на тясно сътрудничество между родния индустриален потенциал, висшите учебни институции, изследователските звена и формированията от въоръжените сили би допринесло за придобиване, поддържане и развитие на дистанционно управляеми системи за формиране на устойчиви национални бойни способности.

ЛИТЕРАТУРА

1. Кокудева, П. Сложните системи и системата от системи в сигурността. В: *Въздушният суверенитет и единно европейско въздушно пространство, сборник доклади от научна конференция*. София: ВА „Г. С. Раковски“, 2019, с. 143 – 152. ISBN 978-619-7478-36-5.

REFERENCES

1. Kokudeva, P. Slozhnite sistemi i sistemata ot sistemi v sigurnostta. In: *Vazdushniyat suverenitet i edinno evropeysko vazdushno prostranstvo, sbornik dokladi ot nauchna konferentsia*. Sofia: VA „G. S. Rakovski“, 2019, s. 143 – 152. ISBN 978-619-7478-36-5.

Панел

**ТРАНСФОРМАЦИЯ,
ПРЕВЪОРЪЖАВАНЕ,
СПОСОБНОСТИ**

Panel

**TRANSFORMATION,
REARMAMENT,
CAPABILITIES**

ОБРАЗЪТ НА ТЕРОРИЗМА ПРЕЗ ХХІ ВЕК

доц. д-р Мирослав Мирчев

Военна академия „Г. С. Раковски“, *mirchevm1958@gmail.com*

Резюме: В доклада е направен анализ за схващанията на едни от най-активно действащите терористични групировки в лицето на „Ал Кайда“ и Ислямска държава, за водене на съпротива. На базата на натрупания през последните 20 години опит е обоснован изводът, че самоубийствените атентати са се превърнали в тяхна „запазена марка“ и са оформили новия облик на терориста през ХХІ век. Разгледани са доктриналните постановки за „джихада“ и „фард айн“ (индивидуалното задължение) в Корана и тяхното тълкуване, с цел оправдаване акта на самоубийство и създаването на културата на мъченичеството.

Ключови думи: *Ал Кайда; Ислямска държава; Ислямски халифат; атентатор-самоубиец; джихад; шахида и фард айн*

THE IMAGE OF TERRORISM IN THE XXI CENTURY

Assoc. Prof. Miroslav Mirchev, PhD

Rakovski National Defence College

Sofia, Bulgaria

E-mail: *mirchevm1958@gmail.com*

Abstract: The report has analyzes the perceptions of some of the most active terrorist groups in the face of Al Qaeda and Islamic State for resistance. Based on the experience gained over the last 20 years, there has been concluded that suicide bombings have become their "trademark" and have shaped the new image of the terrorist in the XXI century. The doctrinal statements of "jihad" and "fard ain" (individual obligation) in the Qur'an and their interpretation in order to justify the act of suicide and the creation of a culture of martyrdom have been discussed.

Keywords: *Al Qaeda; Islamic State; Islamic Caliphate; suicide bomber; jihad; martyrdom and fard ain*

Отличителна черта на съвременния тероризъм са самоубийствените атентати. Тази своеобразна „епидемия“ започва бързо да се разпространява в началото на ХХІ век от Ню Йорк до Бали, когато „Ал Кайда“ включва „шахида“ (мъченичеството) в своята стратегия за световно господство. Основите са положени през 2003 г. в Ирак, където тази терористична организация превръща самоубийствените атентати в ежедневие и основен механизъм за съпротива срещу коалиционните сили и законно избраното правителство на страната.

Самоубийството е акт, при който човек умишлено причинява смъртта си, а философията на самоубийствения атентат е стара колкото света. Най-често тя се определя като хладнокръвна сметка, направена от фанатици за това, че убийствата на невинни хора или заплахата за тях може да служи като брутално и ефективно средство за пропагандиране на определена кауза. Той показва липса на каквато и да било връзка на терористите с реалността и фундаменталните ценности, върху които е изградена цивилизацията. Този вид атентати третират човека като обикновено средство за постигане на целта, придавайки му роля на инструмент, а не като истинска стойност на човешко същество.

В исторически аспект корените на самоубийствения акт могат да бъдат търсени в древността. Като първи опит за това в човешката цивилизация се посочва саможертвата на Самсон, който бута една от колоните в храма на Дагон и загива заедно с пленилите го филистимци, отправяйки призов към Бог „Нека умра заедно с филистимците“. Три от най-известните секти от древността, свързани с използването на тероризма като средство за постигане на политически и религиозни цели – зилоти, асасини и туги, също са извършвали самоубийствени атентати.

Американският политолог Робърт Пейп в книгата си „Dying to win: The strategic Logic of Suicide Terrorism“ прави извода, че „атентаторите-самоубийци не са психически болни или объркани хора“. Той смята, че „те знаят какво правят, но се нуждаят от ритуални обреди, за да се подготвят психически“. Друг политолог – Йозеф Кройтоп счита, че „...атентаторът-самоубиец, в повечето случаи мюсюлманин, е едновременно жертва и извършител. Той е инструмент в ръцете на безскрупулни терористични лидери, които го вербуват и индоктринират на млада възраст, за да се прославят на негов гръб. Индоктринирането става още по-лесно, когато една група или едно общество се чувства безпомощно, застрашено или несправедливо потискано“. Това обяснява донякъде и огромния брой самоубийствени атентати в миналото от палестинци в Израел и понастоящем в Афганистан, Ирак, Пакистан, Сирия и Ливан.

Според редица международни анализатори това е „другото направление“ на тероризма, имащо за цел да ерозира вътрешната сигурност на държавата и неговият „различен характер“ – извършването на особено опасни престъпления с политическа цел (вместо военни действия). В този смисъл всяка невъзможност за водене на политическа борба на паритетна основа може да е косвен генератор на тероризъм, защото стимулира асиметричност в действията на по-слабия. Както посочва генерал Карл Стайнър (бивш началник на американското Съвместно командване за специални операции – Joint Special Operations Command, JSOC в периода 1990 – 1993 г.), „това е просто нападение срещу слабите ни места, вместо срещу силните“. Счита се, че тероризмът винаги е бил и си остава асиметрична реакция спрямо военната защита на сигурността и невоенно средство за постигане на политически цели и въздействие. Той може да бъде използван като тактическо средство в хода на войната, но не е война или нейна форма и затова е безсмислено борбата срещу него да се води единствено с военни средства.

В резултат на успешно водената от САЩ и техните съюзници война срещу тероризма, възможностите на „Ал Кайда“ да провежда самоубийствени атентати, основно с чуждестранни бойци, в района на Ирак и Близкия Изток са силно ограничени. Това вероятно налага Осама бин Ладен и Айман ал-Зауахири да пренесат синдрома на атентатора-самоубиец в районите на Афганистан и Пакистан, където той успешно мутира като средство за съпротива в „световния ислямски джихад срещу евреите и кръстоносците“. На практика тези действия правят от шахида (мъченика) най-ефективното оръжие в ръцете не само на „Ал Кайда“, но и на другите терористични организации. От основен инструмент за водене на война той се превръща и в оптимален метод за пропаганда, базиращ се на религиозен и културен дълг за фанатичите, изповядващи исляма. По този начин се формира един вид култура, свързана с мъченичеството на терористите-самоубийци, която става еталон за много други терористични организации.

Другият важен въпрос при разглеждането и анализирането на самоубийствените атентати, извършвани от терористични организации е свързан с доктриналната постановка за воденето на джихад от мюсюлманите, залегнала в Корана. Същата се използва много активно от пропагандната машина на терористите за „промиване“ на мозъците на бъдещите атентатори. Редица автори разглеждат джихада и като шестия „стълб“ на Исляма – след шахида (засвидетелстване на вярата), намаз (молитва), сиам (пост), зекат (милостиня) и хадж (поклонничество).

Джихадът като елемент от религиозните вярвания на мюсюлманите не е посочен изрично от Пророка Мохаммад като основополагаща верска категория. Съществуват различни тълкувания и множество интерпретации на джихада. Самият арабски термин „**джихад**“ е свързан с глагола *джахада* – „полагам усилия“, „старая се“, „боря се в името на благородна кауза“, но неговият автентичен смисъл се разкрива в словосъчетанието *Джихад фи сабил Аллах* („върховно усилие“, „борба по пътя на Аллах“). В Корана думата джихад е спомената повече от сто пъти в най-различен контекст. Това определя и възникването, още през VIII – IX в., на теоретичния и тълковен дебат относно смисъла и значението на джихада, който и до днес не е приключил с даване на еднозначно обяснение.

През първия период на формирането на Исляма (между 610 г. и 622 г.) джихад означава най-вече мирно, ненасилствено разпространение на ислямската религия. Тогава елементът на насилие се съдържа единствено в действията за самозащита, ако такива се налагат. Този подход е формулиран в кораническия стих: „*Бийте се в името на Аллах и отвърнете на удара на онези, които ви нападат, но вие не нападайте, тъй като Аллах не обича тези които нападат*“ (Коран, сура „Хадж“, стих 39).

От 622 г., след преселването на Мухаммад от Мека в Медина под натиска на мразещите го езичници, джихадът приема вече насилническа интерпретация. Тогава се появяват двата стиха – „Ако не е свещен месецът, убивайте езичниците, *където ги намерите*“ и „*Убивайте тези, които не вярват в Аллах, в Страшния съд, не почитат Аллах и неговия пратеник и не вярват в правата вяра.*“ (Коран, сура „Покаянието“, стихове 9 и 29). След този период и до смъртта на Мухаммад през 632 г. джихадът придобива откровено настъпателен и войнствен характер. Осъществяват се нападения върху племена, които са наказвани за съпротивата си срещу Исляма или са приобщавани насилствено към тази религия. Именно през този период на разрастване на мюсюлманската умма и създаването на арабската държавност изкрystalизира съвременното значение на джихада – свещена война в името на Исляма. Така в Корана се формулират различни постановки на джихада, които се утвърждават, приемат и в съвременното тълкуване на този елемент от ислямската религия, че основна и дългосрочна цел на джихада е ислямизирането на целия свят, като се толерира използване на военна сила при разпространението му. Предвижда се задължителен военен разгром на неверниците, налагане на данък върху последователите на християнската и еврейската религии, вземане на плячка и използването ѝ за засилване на ислямската мощ.

С течение на времето джихадът се превръща в едно от най-полемичните и нееднозначни понятия в Исляма, свързани както с идеята за духовно самоусъвършенстване, така и с тази за воденето на „свещена война“ срещу неверниците. Под една или друга форма, той е определен като задължение. При това тълкуване джихадът може да се счита за задължителна военна повинност, което автоматично го включва като шести стълб на Исляма, но може да се разглежда и като задължение само за една строго определена група, ангажирана с отбраната и завоеванията на ислямската държава.

Първообразът на сунитския шахид е създаден от палестинските съпротивителни организации в средата на 90-те години на миналия век. „Ал Кайда“ започва да използва атентатори-самоубийци през август 1998 г. за извършване на атентатите срещу посолствата на САЩ в Кения и Танзания.

Медийното отразяване на самоубийствените атентати, което според американския журналист и политически анализатор Уолтър Зеев Лакюер е най-добрият приятел на терориста, прави още по-популярна тяхната идеология и превръща „шахида“ в един вид герой и пример за подражание. Често СМИ изпълняват ролята и на инструмент за възможно най-добрата пропаганда, бързо разпространение на техните идеи и цели, за създаване на престиж и повишен интерес сред контингентите от евентуални бъдещи последователи.

Тази стратегия, използвана основно от „Ал Кайда“, за безмилостен самоубийствен тероризъм легитимира самоубийствените атентати като акт на мъченичество в сунитското течение на исляма и стимулира получаването на по-широка подкрепа от страна на радикално настроените мюсюлмани.

На второ място, превръщайки акта на самоубийство в оръжие на терора, „Ал Кайда“ демонстрира стратегическо предимство при атаките, извършвани в миналото срещу военни обекти, заменяйки ги с т. нар. „меки цели“. Това предизвиква одобрение в ислямския свят като цяло и по-специално в Саудитска Арабия, където водещи духовници започват да издават фетви (становище по точка от ислямското право), оправдаващи използването на самоубийствени атентати срещу цивилно население и граждански обекти.

Ако до 11 септември 2001 г. основната цел на „Ал Кайда“ е да набира, финансира и обучава терористи, които да провеждат световен джихад, то след тази дата Осама бин Ладен и Айман ал-Завахири се стремят, в рамките на световната ислямска общност, да мотивират и вербуват възможно повече последователи за участие в „акта на мъченичеството“. Част от анализаторите определят това като средство за „въдъхновяване и привличане вниманието на широки слоеве от мюсюлманското население, както и на други радикални ислямистки движения към целите, които си е поставила тази терористична организация“.

Вероятно това е и една от причините, изповядващите исляма днес да са изправени пред необходимостта да си формулират ясен и аргументиран отговор на въпроса какъв следва да бъде джихадът – общ или индивидуален, насилствен или духовен, градивен или разрушителен. Преданието за „малкия (войната) и големия (битката на вярващите с техните страсти и суета) джихад“, формулирано от Мухаммад и тълкувано по-късно от ислямските богослови, дава основание да се търси и получи отговор, че Ислямът определя джихада като усилие за неговото силово налагане. Това са постановки, залегнали в

стратегията на Осама бин Ладен и Айман ал-Зауахири за Глобалния джихад или войната с „вътрешния и външния (далечния) враг“.

При създаването на новия образ на терориста на XXI век, съвременната идеология и стратегията на „Ал Кайда“ се фокусира приоритетно върху отделния индивид и боец. Джихадът вече се представя и като възобновяване на един от чисто идеологическите принципи, залегнали в исляма – „фард айн“ (индивидуално задължение), който свързва идеята за умишлено убийство чрез самоубийство като „мъченичество“ и предлага прилагането на това лично задължение на всеки мюсюлманин като призив за джихад. Двама анализатори на дейността на тази терористична организация – Йорам Швайцер и Сари Фербер, определят тези идеологически схващания като концепция за жертване в името на Аллах, целяща да се превърне във върховен организационен идеал в рамките на „Ал Кайда“ и след това да се *разпространява до нейните бойци, поддръжници и структури в различни краища на света*, докато се превърне постепенно във възпроизвеждащ се и саморазпространяващ се вирус. Развивайки тази стратегия Айман ал-Зауахири се стреми да не бъде пасивен наблюдател на случващото се, а търпеливо и систематично да води война със САЩ и техните съюзници, противопоставяйки им волята и мечтата на отделния мюсюлманин за налагане на идеята за ислямски халифат, която да се ръководи от законите на шериата. Чрез едно доста спекулативно тълкуване на отделни сури от Корана той се стреми да получи подкрепа за водене на джихад, пропагандирайки позицията, че това е „отбранителен джихад“, който изисква от вярващия мюсюлманин, физически или финансов „фард айн“. Тази си позиция ал-Зауахири аргументира с думите на основателя на „Ал Кайда“ Абдала Азам, че „фард айн“ *има основна роля в борбата за освобождаване на „окупираните“ ислямски земи и*, че джихадът ще остане индивидуално задължение на всеки мюсюлманин за връщането на Палестина, Бухара, Ливан, Еритрея, Сомалия, Филипините, Южен Йемен, Ташкент и Андалусия в царството на исляма.

Продължавайки идеите за повсеместно извършване на самоубийствени атентати Айман ал-Зауахири прави опити да обедини и координира действията на различни социални слоеве на мюсюлманското общество на основата на ислямското културно наследство. Той подчертава, че самоубийственият тероризъм е спираловиден процес на обратна връзка между ръководството на организацията и мюсюлманската общност, населяваща даден географски район. За да се поддържа тази връзка е необходимо да бъдат разяснени и насадени в съзнанието на членовете на общността идеите за значението на мъченичеството чрез използване на религиозни, културни, индивидуални и други средства. Счита се, че точно тази симбиоза между културните особености и социалното адаптиране на мотивите за шахида може да допринесе за възприемане на самоубийствения акт.

Един от изследователите на съвременния тероризъм, професорът от Центъра за борба с тероризма в Уест Пойнт Асаф Могхадам, развива теорията, че същността на самоубийствения терористичен атентат се гради от три компонента – създаване на враг, легитимно убиване на врага и готовността за собствената смърт. Според него, при обличаване на първите два компонента се появява и осъзнатото желание за саможертва. По този начин, според Асаф Могхадам, се създава култура на мъченичеството, която мотивира готовността на отделния индивид да се жертва в процеса на ликвидиране на „злия враг“.

Този вид култура, определяна от някои анализатори като джихадистко-салафитска, през последните години масово се разпространява посредством Интернет и СМИ и добива облик на сателитна или виртуална култура на мъченичеството, при която всеки последовател или поддръжник на определена терористична организация може да влезе в нейния сайт и подробно да се запознае с нужната му информация.

Феноменът, свързан с новия образ на терориста, е повлиян пряко от социалните мрежи. Бъдещият самоубиец, който попада в сайта на терористична организация, се потапя в джихадисткия начин на живот, научава неговите убеждения, ценности, нагласи, цели, реторика, аргументация и влиза в контакт с оператора на сайта. Първоначално бъдещият терорист е привлечен от религиозни, политически и социални проблеми, основани на идентичността на индивида, но с течение на времето приема и идеологическите рамки, решенията и предписанията на създателите или ръководителите на терористичната организация. По този начин, отделните доброволци и бъдещи самоубийци приемат мъченичество. Културата на мъченичеството, често в рамките на социалната мрежа, успява да събуди задължението на индивида да вземе нещата в свои ръце.

Счита се, че философията на самоубийствения тероризъм се крепи на три стълба – стратегическа необходимост, мотивирани индивиди и култура на мъченичество. В този контекст мотивирането на готовността за самоубийство води до определяне на това кой е врагът и дава обяснение защо тези или този, който го организира трябва да умре и в името на какво. Отговорите на тези въпроси трасират политическата стойност на самоубийствения атентат и го правят катализатор за бъдещото мотивиране на терористите за извършване на такива актове. Подобен *modus operandi* изисква непрекъснато и гъвкаво формулиране на „социални злини“ или „противници“, които да са цели на съответната терористична организация.

„Ал Кайда“, както и повечето активно действащи терористични организации, представят пред своите последователи света в рамката на борбата между исляма и „ционистко-кръстоносен съюз“, определян като световно зло. В тази реторика се насажда и мнението, че мюсюлманите трябва да водят джихад, за да защитят своята религия.

През 1998 г. Световният ислямски фронт за джихад срещу евреи и кръстоносци, финансиран от „Ал Кайда“ разпространява идеите, че убиването на американците и техните съюзници – цивилни и военни – е задължение на всеки мюсюлманин, което той може да направи навсякъде по света, докато джамията Ал Акса в Ерусалим и Светата джамия в Мека не бъдат освободени от тяхната хватка и докато армиите им не се оттеглят от всички земи на исляма, победени, разбити и неспособни да заплашат нито един мюсюлманин“. По този начин „Ал Кайда“ се стреми да насочи основните усилия в своя джихад срещу християните, евреите и другите немюсюлмански народи, спекулирайки с тезата, че те „контролират земи, населени от правоверни“ и са заплаха за исляма. Това прави САЩ, Израел, Испания, Русия, Индия, Филипините и други национални държави, в които живеят големи мюсюлмански общности, реални мишени за терористите. В този смисъл ислямистите разглеждат всички проблеми на мюсюлманския свят в контекста на „еврейската конспирация“, в която САЩ заемат ключова позиция.

По подобен начин „Ал Кайда“ разглежда и своя подход за привличане и вербуване на нови членове, противопоставяйки пороците на западното общество, като корумпирано и неморално, на идеализираната ислямска общност. На тази база се прокарват мотивите, че мюсюлманите трябва да защитават исляма дори ако това означава, че ще заплатят със собствения си живот, т.е. самоубийство в името на религията.

В началото на новия век сме свидетели на завръщането на политическия ислям в глобалния свят, при това с нови концепции, включително такива като джихад и фард айн. Те водят до появата на явления като самоубийствени атентати, отвлечения, обезглавявания и др. Културата на мъченичеството вероятно ще продължава да играе значима роля в поведението на повечето терористични организации и в бъдеще, оправдавайки действията на атентатора-самоубиец за постигане на крайната цел – създаване на Ислямски халифат.

REFERENCES

1. Biblia. *Star zavet, Kniga na Sadiite, Glava 16*. [in Bulgarian]
2. Knip, Kersten. *Verigata na smartta: da umresh, za da ubivash*. DW [onlayn] 26.02.2016. dostapno na: <https://p.dw.com/p/112kP> [in Bulgarian]
3. Klansi, Tom i Karl Staynar. *Voyni v syanka*. Sofia: Prozorets, 2003. [in Bulgarian]
4. Vasilev, Milko. *Za islyama, terorizma i samoubiystvenite atentati*. Ekspertna kragla masa tema „Terorizmat sled Madrid-2004. Novi predizvikelstva i protivodeystvie“. 01.07.2004. [in Bulgarian]
5. Laqueur, Walter quoted in Assaf Moghadam "The Roots of Suicide Terrorism: A Multi-Causal Approach. – In: *Root Causes of Suicide Terrorism: The Globalization of Martyrdom*, ed. Ami Pedahzur. New York: Routledge, 2005, p. 95.
6. Baer, Robert in *The Cult of the Suicide Bomber*, prod. and dir. David Betty and Kevin Toolis, 1 hr. 35 min., Many Rivers Films, 2006.
7. Sheikh Yousef al-Qaradhwai. Al-Jazeera TV on 16 July 2007, trans. in MEMRI, Special Dispatch Series No. 1672, 2007.
8. Rohan K. Gunaratna. The New al-Qaida: Developments in the Post-9/11 Evolution of al-Qaida. – In: *Post-Modern Terrorism: Trends, Scenarios and Future Threats*, ed. Boaz Ganor, Herzliya, Israel: Publishing House, 2005.
9. Mira, Mayer. Globalniyat dzihad e neprekasnata vojna sreshu zapadnata tsivilizatsia. – V: *Frognews* [online, last visited on 20.09.2020]. Available at: <https://frognews.bg/obshtestvo/misterii/globalniat-djihad-neprekasnata-vojna-sreshu-zapadnata-tsvilizatsia.html> [in Bulgarian]
10. Ferber, Schweitzer and Goldstein. *Jihad: The Trail of Political Islam*. Cambridge, Mass.: Harvard University Press, 2002, 147. – In: Marc Sageman, *Understanding Terror Networks*. Philadelphia: University of Pennsylvania Press, 2004. p. 3.

11. Hafez, Mohammed M. *Manufacturing Human Bombs: The Making of Palestinian Suicide Bombers*. Washington D.C.: United States Institute for Peace Press, 2006, p. 36.
12. Pedahzur, Ami. *Suicide Terrorism*. Malden, Mass.: Polity Press, 2005, p. 163.
13. Moghadam, Assaf. Palestinian Suicide Terrorism in the Second Intifada: Motivations and Organizational Aspects. *Studies in Conflict & Terrorism*. Vol. 26, Issue 2, 2003, pp. 68-69.
14. Pedahzur, Ami and Arie Perliger. The Changing Nature of Suicide Attacks: A Social Network Perspective. *Social Forces* 84, no. 4, 2006.
15. The World Islamic Front's Declaration to Wage Jihad against the Jews and Crusaders. – In: *Raymond Ibrahim, ed. and trans. The Al-Qaeda Reader*. New York: Broadway Books, 2007, p. 13.
16. *Usama bin Laden. Sermon for the Feast of the Sacrifice*. Al-Jazeera TV on 16 February 2003, trans. in MEMRI, Special Dispatch Series No. 476 (6 March 2003), available at: <http://www.memri.org>
17. *Sheikh Yousef al-Qaradawi*, Qatar TV [online] 25 February 2006, trans. in MEMRI, Special Dispatch Series No. 1102, 2006. available at: <http://www.memri.org>

СПЕЦИАЛНИ СПОСОБИ ВЪВ ВЪОРЪЖЕНИТЕ СИЛИ НА САЩ ЗА СЪБИРАНЕ НА РАЗУЗНАВАТЕЛНА ИНФОРМАЦИЯ

д-р Антон Михайлов

Военна академия „Г. С. Раковски“, *a.mihaylov@rncd.bg*

Резюме: Разузнавателната дейност на военното разузнаване на САЩ чрез специални разузнавателни способности се извършва съобразно регулация AR 381-10 US Army Intelligence Activities от 2007 г., уреждаща отговорността, възможностите и ограниченията при провеждането на специални мероприятия по събиране на информация от американски и неамерикански граждани, във и извън територията на САЩ. В доклада са разгледани основните оперативни способности като електронно наблюдение, прихващане на комуникацията със съгласие на страна по нея, скрито наблюдение, секретно проникване и претърсване, проверка и изземване на кореспонденция, физическо наблюдение, неразкрито участие в организации. Изведени са забранени способности за добиване на разузнавателна информация и незаконосъобразно поведение при обработване на разузнавателни данни.

Ключови думи: *разузнаване; САЩ; методи; разузнавателна информация; наблюдение; претърсване; проникване*

SPECIAL METHODS IN THE US ARMED FORCES FOR COLLECTING INTELLIGENCE

Anton Mihaylov, PhD

Rakovski National Defence College

Sofia, Bulgaria

E-mail: *a.mihaylov@rncd.bg*

Abstract: The intelligence activities of the US military intelligence through special intelligence methods are carried out in accordance with the regulation AR 381-10 US Army Intelligence Activities 2007, governing the responsibility, capabilities and limitations of special actions to collect information from American and non-American citizens, inside and outside the United States. The report discusses the main operational methods such as electronic surveillance, interception of communication with the consent of a party, covert surveillance, secret penetration and search, verification and seizure of correspondence, physical surveillance, undisclosed participation in organizations. Prohibited means of obtaining intelligence and illegal conduct in the processing of intelligence data have been introduced.

Keywords: *intelligence; USA; methods; surveillance; search; penetration*

Разузнавателната дейност на военното разузнаване на САЩ чрез специални разузнавателни способности се извършва съобразно регулация AR 381-10 US Army Intelligence Activities на Щаба на американската армия от май 2007 г., уреждаща отговорността, възможностите и ограниченията при провеждането на специални мероприятия по събиране на информация от американски и неамерикански граждани, във и извън територията на САЩ. Тази инструкция допълва Изпълнителна заповед на Президента на САЩ 12 333 и в по-големи детайли разглежда провеждането на електронно наблюдение, скрито наблюдение, физическо претърсване, проверка на кореспонденция и другите уредени специални способности. Тъй като използването на цитираните способности има голямо значение в работата на Агенцията за военно разузнаване (DIA) на САЩ като цяло, а и противодействието на терористични групи в частност, с голяма практическа насоченост е анализирането им в детайли и извеждането на оценка на приложението им.

Основните специални способности за събиране на разузнавателна информация съгласно AR 381-10 са следните:

Електронно наблюдение на територията на САЩ (оперативен способ) – може да се извършва от армейските разузнавателни и контраразузнавателни органи въз основа на Закона за наблюдение на

чужди разузнавания от 1978 г. спрямо лица, намиращи се на територията на САЩ. Одобрението за такова наблюдение се дава от главния прокурор след искане, изготвено от контраразузнавателния орган. Искането съдържа следните данни:

а) кой или какво е обект на наблюдението (имейл адрес, IP адрес, URL адрес или име на отделен човек или организация);

б) местоположение на обекта на наблюдението;

в) устройството/средата, към която се насочва наблюдението (мобилен телефон, сателитен телефон, електронна поща, интернет чат, сървър на доставчик на интернет услуги, факс машини);

г) как ще бъде насочено средството за наблюдение;

д) откъде ще се извършва наблюдението (територия, държава, област, град, къща, автомобил);

е) ако е приложимо – физическият и/или електронният адрес. Идентификация на доставчика на услуги, предупредителни известия, потребителски споразумения, командни комуникационни политики и политики и практики за сигурност, прилагани от лицето/обекта; телефонен номер; номер на стая; независимо дали става въпрос за обществена или частна собственост; и всяка друга подходяща информация.

ж) обобщение на фактите, показващи каква е вероятната причина да се смята, че обектът попада в поне една от следните категории: лица ангажирани в конспиративни разузнавателни дейности (включително тайни действия, предназначени да засегнат политическия или правителствен процес), саботаж, международни терористични действия, подготовката на международни терористични дейности или участие в конспирация или съзнателно съдействие и съучастие на лице, участващо в описаните действия, за или от името на чуждестранна власт; служител на чужда държавна власт; съзнателно приема инструкции от или действа съзнателно в съзвучие с чуждестранна власт; дружество или друг правен субект, който е притежаван или контролиран пряко или непряко от чуждестранна власт; намира се в контакт с или в сътрудничество с чуждестранно разузнаване или служба за сигурност, за да предостави достъп до информация или материали, класифицирани от САЩ и до които субектът е получил достъп.

Електронно наблюдение на лица и обекти, намиращи се извън територията на САЩ. Изразява се в придобиване на непублична комуникация по електронен път без съгласието на страните по комуникацията или в случай на неелектронна комуникация, без съгласието на лице, което присъства на мястото на комуникацията. Електронното наблюдение е извън САЩ, ако обектът е физически извън територията на САЩ, независимо от местоположението, от което се извършва наблюдението.

Когато наблюдението касае неамерикански граждани, одобрението му е много улеснено и се извършва не от Главния прокурор на САЩ, а от който и да е компонент, свързан с американското разузнаване. Искането на одобрението следва да съдържа: а) достатъчно информация, показваща обосновано предположение, че чрез наблюдението ще се събере ценна разузнавателна информация; б) описание на естеството и съдържанието на комуникациите, които трябва да бъдат прихванати; в) посочване на всички американски лица, чиито комуникации може разумно да се очаква да бъдат прихванати; г) описание на начините, по които ще се извършва електронното наблюдение, включително оборудването, устройството за записване и средствата за инсталиране. *Първоначалните искания за одобрение и подновяване могат да бъдат предоставени за срок до 120 дни. Молбите за подновяване на електронно наблюдение за продължително прилагане при наличие на дългосрочен интерес могат да бъдат одобрени за срок до 1 година.*

Одобряващите органи по отношение на електронно наблюдение на чужда територия са: командващите на отделните американски армии, командващия Специалните сили, командващия Командването за разузнаване и сигурност на САЩ, както и всеки друг служител (офицер) на задгранично командване, отговорен за наблюдение на набелязани цели. Посочените в предното изречение длъжностни лица могат да делегират писмено одобрението на електронно наблюдение на своите заместник-командири, старши офицери по разузнаване, командири на корпус или дивизия или командир на разузнавателна бригада или разузнавателна група. Не се разрешава допълнително делегиране.

Видно от нивата на делегиране вземането на решение и одобрението на електронно наблюдение на неамерикански граждани извън границите на САЩ е сравнително лесно и може да продължи дълго време, а одобряващият орган да не е на толкова високо йерархично ниво. Това обстоятелство улеснява прилагането на електронното наблюдение, ускорява процеса на разрешаването му и запазва информацията за прилаганите средства в разузнавателните звена.

Прихващане на комуникациите със съгласието на страна (оперативен способ). Това е електронно наблюдение, при което една, но не всички от страните по комуникацията, е съгласна с провеждане

на електронното наблюдение. Съдържанието на искането за прихващането и органите, които го одобряват, са по същество същите, както при електронното наблюдение, с особеността, че трябва да се представи и изричното съгласие на една от страните по комуникацията тя да бъде прихваната.

Скрито наблюдение (оперативен способ) – наблюдение на конкретно лице или група без тяхното съгласие, по скрит и непрекъснат начин чрез електронни, оптични или механични устройства, при което се фиксира движението или дейността на лицето или групата. Наблюдението е скрито, когато се провежда по начин, който не позволява на обекта/тите да знаят за наблюдението и е продължаващо, ако се провежда без прекъсване за определен период от време. Наблюдението се провежда на открито, т.е. на места на които обектът не се намира в лично пространство. Особеността в случая касае наблюдение на обекта на публични места, например поставяне на маяк или транспондер на автомобил, паркиран на публичен паркинг. Когато се касае за американски граждани няма да се изисква заповед от Главния прокурор, но ако американският гражданин се намира в дома си, наблюдението няма да е скрито, а ще се третира като електронно наблюдение с прилагане на съответните процедури за разрешение. Ако се касае за неамерикански гражданин, извън територията на САЩ, няма изисквания за уведомяване на Главния прокурор и наблюдението се разрешава по опростен ред. На практика тук се включва използването на GPS локатори и електронни предавателни устройства за следене движението на набелязаните обекти. Друга важна характеристика на скритото наблюдение извън територията на САЩ, извършвано от DIA, е изискването да се координира с представител на ЦРУ.

Секретно физическо претърсване (проникване), което представлява:

а) Всяко навлизане в имущество/имот или лице, за да се получи дадена вещь или информация. То не включва навлизане в области, които са на общ показ и се виждат с невъоръжено око, ако не е налице физическо проникване, изоставени имущества, оставени на обществено място, или каквото и да е проникване, разрешено за извършване на законно електронно наблюдение;

б) Всяко физическо навлизане в помещения или имущество/имот на територията на САЩ (включително проверка на интериора с технически средства), което има за цел да доведе до изземване, възпроизвеждане, проверка или промяна на информация, материал или имущество при обстоятелства, при които човек има разумно очакване за неприкосновеност на личния живот и когато за целите на правоприлагането е необходима заповед).

Особено внимание заслужава правото да се извърши физическо претърсване извън територията на САЩ спрямо лица, които не са американски граждани. Искането за извършването му следва да съдържа: достатъчно информация, за да се покаже разумно убеждение, че претърсването ще доведе до придобиване на значителна разузнавателна информация; описание на имота (помещението), който ще се претърси, както и местоположението му и начина, по който ще се извърши претърсването. Одобрението се дава от заместник-началник на щабовете за разузнаване.

Проверка и изземване на кореспонденция. Службата за военно разузнаване на САЩ няма право да проверява и изземва кореспонденция на територията на САЩ без разрешението на Пощенската служба на САЩ. След получаването на такова разрешение няма правна пречка кореспонденцията да бъде иззета. *DIA има право да иземе, отвори и провери кореспонденцията на неамерикански гражданин извън територията на САЩ.* В този случай получателят и изпращачът не трябва да са американски граждани. Одобрението за такова действие зад граница се извършва от същите субекти, които предоставят одобрение при електронно наблюдение извън САЩ.

Физическо наблюдение – систематично и преднамерено наблюдение на лице, извършвано по всякакъв начин на постоянна основа, включващо придобиване на непублична комуникация от лице, което не е страна по нея или не е видимо присъстващо, по начин, *който не включва* електронно наблюдение (т.е. не прихваща и/или записва комуникацията). Когато се касае за американски граждани на територията на САЩ разузнавателната служба може да извършва физическо наблюдение на военнослужещи, настоящи и бивши служители на разузнавателни служби на САЩ, кандидати за служители, лица в контакт с посочените категории. Когато обаче наблюдението се провежда извън военни обекти, то задължително се съгласува с ФБР.

Както при вече посочените случаи, физическо наблюдение може да се провежда и извън територията на САЩ на неамерикански граждани. Одобрение се дава от органите, които допускат и електронно наблюдение, но само ако чрез наблюдението може да се придобие значима разузнавателна информация, което не е възможно по друг начин. Наблюдение се провежда и ако ЦРУ търси съдействие за провежда-

нето му от военноразузнавателния орган.

Участие в организации под прикритие. Такова участие се разглежда в няколко аспекта, съгласно AR 381-10, а именно: а) служител на разузнавателния орган участва в организация на територията на САЩ; б) американски гражданин участва в организация извън територията на САЩ; в) служител е помолен от разузнавателния орган да предприеме действия в дадена организация, но в интерес на DIA, при което служителят вече е член на организацията; г) дадено лице е помолено от DIA да стане член на организацията.

Общото в действията при неразкрито участие, е че те се извършват в полза на разузнавателната служба, не се разкрива принадлежността към DIA или работата на трето лице за DIA и включват: събиране на информация, идентифициране на потенциални източници на информация или оперативни контакти, както и други действия отнасящи се към чуждестранни разузнавателни или контраразузнавателни структури. Тук не се включват случаите, в които сътруднически източници доброволно предоставят информация от участието си в дадена организация, без да са били инструктирани за това от разузнавателната служба.

В раздел II „Термини“ на AR 381-10 се разяснява понятието „сътруднически източник“ (cooperating source). Това са лица или организации, които съзнателно и доброволно предоставят информация или достъп до информация на военното разузнаване при поискване или по собствена инициатива. Източниците включват правителствени агенции, правоприлагащи органи, кредитни агенции, академични институции, работодатели и представители на чуждестранни правителства и организации. Сътрудническите източници трябва да знаят, че работят с разузнавателен компонент.

Служител на разузнаването служба може да участва под прикритие в дадена организация с цел придобиване на разузнавателна информация или – ако участието е извън САЩ – да събере информация за американски гражданин, който може да е потенциален източник на чужда разузнавателна служба. Работата под прикритие не може да продължава повече от 12 месеца.

Участието бива два основни вида: а) общо – участие на открити срещи, симпозиуми, конференции, участие на професионални семинари, търговски панаири и други, за които може да се изисква или да не се изисква специална покана; б) специално участие – включващо срещи извън територията на САЩ за придобиване на значима разузнавателна информация, както и срещи с чуждестранни граждани на територията на САЩ, контакти, които са част от контраразузнавателни операции на територията на САЩ по искане на ФБР, срещи с лица, които са потенциални източници на разузнавателна информация извън територията на САЩ, действия по разработване и поддържане на легенда (официално прикритие, authorized cover).

Договаряне на стоки и услуги без разкриване на принадлежност към разузнавателна служба. Служители на разузнавателната служба могат да встъпват в договорни отношения с американски граждани за получаване на стоки и услуги. Насрещни страни по договора може да бъдат и частни институции, търговски организации и физически лица, пред които не се разкрива принадлежността на служителя към военноразузнавателната служба. Запазването в тайна на принадлежността към специалната служба обаче може да стане при определени обстоятелства: а) договорът е за придобиване на публикувани материали, достъпни за широката общественост; б) договорът е за придобиване на рутинни стоки или услуги, необходими за поддържане на одобрени дейности, като например кредитни карти, коли под наем, пътуване, подслон, храна, наем на офиси или апартаменти и други принадлежности, както и търговски услуги за онлайн достъп (с доставчик на интернет услуги); в) секретарят на армията или негов заместник е подписал писмено решение, че сключването на договора трябва да бъде прикрито, за да се защити разузнавателната дейност.

Регулация AR 381-10 включва и други способности, които няма да бъдат разгледани в настоящия доклад, предвид по-ограниченото им използване и ограничения обем на материала. От съществено значение обаче е да се споменат *забранените способности* за събиране на информация и какво се разбира под *неправомерно поведение* при обработването на разузнавателни данни, като:

- неправилно събиране, запазване и разпространение на информация за американски гражданин;
- неправомерно и заблуждаващо използване на принадлежност към разузнавателна служба за събиране на информация, която не е за целите и в полза на DIA;
- кражба на пари за заплащане на лица, източници на информация;

- използване на секретни фондове на разузнаването за лично облагодетелстване;
- фалшифициране на разузнавателни доклади;
- кражба на ценни вещи, установени в хода на претърсвания;
- обучаване и тренировка на лице, източник на информация преди да е преминал проверка с поли-физиограф с цел да премине успешно такава проверка.

Предвид изложената уредба на специалните (оперативни) способности за събиране на разузнавателна информация може да се направят следните изводи:

Налице е улеснен ред при получаване на разрешение за прилагане на специални способности и средства извън САЩ.

Приложима е широка гама от способности, които могат да бъдат използвани в много държави, без да са въведени каквито и да е ограничения към субекти и географски региони, принадлежност или не към съюзи или алианси, стига да може да се придобие значима разузнавателна информация.

Прилагането на специалните способности по отношение на неамерикански граждани е улеснено, а електронното наблюдение може да се използва за дълъг период от време. Налице е сериозно финансово и организационно обезпечаване на прилагането на специалните способности и средства. Допуска се съдействие и възможности за коопериране с ЦРУ и ФБР.

Изискванията към информацията, която следва да се предостави преди провеждане на електронно наблюдение предполагат сериозна предварителна подготовка, а това означава, че за прилагането му е необходим екип за обезпечаване, както и лица от чуждестранната държава, подпомагащи прилагането на специални разузнавателни средства зад граница. Макар и подобни действия да са скъпи и трудни за организиране, те са нормативно напълно допустими за DIA.

От гледна точка на защита от злоупотреби с разгледаните специални средства, регулацията вмениява определено поведение на оперативни служители като недопустимо и го квалифицира като престъпление (кражби, злоупотреби, неправомерно обучение на източници).

В заключение, от уредбата и видовете специални разузнавателни средства, прилагани за събиране на информация, може обосновано да се посочи, че те са ефективни и ограниченията в прилагането им са сравнително по-малки.

REFERENCES

1. AR 381-10 *US Army Intelligence Activities, Military Intelligence*. Headquarters Department of the Army Washington, DC, 03.05.2007.
2. *ADP 2-0 Intelligence*. Headquarters Department of the Army Washington, DC, 31.07.2019.
3. *DoD Dictionary of Military and Associated Terms*. US Department of Defense, November 2021.
4. *Executive Order 12333*, United States intelligence activities, as amended by Executive Orders 13284 (2003), 13355 (2004) and 13470 (2008).
5. *MCTP 2-10A MAGTF Intelligence Collection*. Department of the NAVY Headquarters United States Marine Corps, 2016.

ТРАКИЙСКИЯТ ПОХОД НА СЦИПИОНИТЕ ПРЕЗ 190 Г. ПРЕДИ ХРИСТА

д-р Йордан Илиев

Научен център за история и археология на войната, *jordan_iliev@hotmail.com*

Резюме: В предлагания доклад са събрани преведени на български език и анализирани наличните антични свидетелства за първия документиран поход на римски войски през тракийските земи. Обърнато е внимание на активното съдействие, което Филип V Македонски оказал на римляните, като то е обяснено със завзетите от Антиох III през предходните години тракийски владения на македонския цар. Разгледана е запазената информация за военни сблъсъци по време на похода и проблемите на неговата хронология.

Ключови думи: Древна Тракия; Рим; военни походи

THE THRACIAN MARCH OF THE SCIPIOS IN 190 BEFORE CHRIST

Jordan Iliev, PhD

Research Centre for History and Archaeology of War
Plovdiv, Bulgaria

E-mail: *jordan_iliev@hotmail.com*

Abstract: In the paper are collected translated in Bulgarian and analyzed all of the available ancient sources about the first documented march of Roman troops through the Thracian lands. A special attention is paid to the support that Philip V of Macedon gave to the Romans; it is explained with the seized by Antiochus III in previous years Thracian possessions of the Macedonian king. The available information about military clashes through the march is considered and also the problems about its chronology.

Keywords: Ancient Thrace; Rome; military campaigns

Въведение

През 196 г. пр. Хр. Антиох III Велики (223 – 187 г. пр. Хр.) се прехвърлил от Азия в Европа начело на значителни сухопътни и военноморски сили, като завлаждал Тракийския Херсонес и няколко години воювал в Тракия.¹ Римляните следили с тревога неговите операции, още повече заради присъствието на Ханибал в сирийския царски двор²; твърди се дори, че картагенският пълководец предложил план за война срещу Рим³, в който имало и препоръка как да се неутрализира Македония чрез нападение от Тракия с важното съобщение за пребиваването на Селевк, сина на Антиох III, в Лизимахия, където разполагал със собствена армия с неизвестна численост (Liv., 36.7.15; App., Syr., 3.14).⁴ Планът, ако наистина е съществувал, не бил възприет от сирийския монарх.⁵

Постепенно се стигнало до директен военен сблъсък между Рим и Антиох III, обикновено наричан Сирийска война (192 – 188 г. пр. Хр.).⁶ Местото на Тракия и траките в тази война не е обект на достатъчно задълбочени изследвания. В историографията често е обръщано внимание на завръщането на римските войски през 188 г. пр. Хр., предвождани от Гней Манлий Вулзон, когато те претърпяват сериозни загуби от нападение на траките⁷, но преминаването на същите войски през тракийските земи по същия път към Мала Азия две години по-рано не е обект на детайлни изследвания; в научните публикации това събитие се споменава бегло, без всякакви опити за систематизиране на наличната – макар и сравнително ограничена – информация.⁸ Настоящата работа представлява опит за запълване на тази съществена празнина в научните изследвания, като събира и анализира наличните свидетелства на античните писатели.

Антиох III Велики в Европа, Филип V и римляните

Известно е, че за разлика от предишните години, когато воювал в Европа срещу траките⁹, в Гърция сирийският цар се прехвърлил по море с не особено значителни сили. Още античните писатели посочили редица организационни и тактически грешки в цялостното провеждане на военните действия от сирий-

ската страна. Закономерно Антиох III бил победен в Битката при Термопилите през 191 г. пр. Хр., след което панически напуснал Балканите. Римляните решили да се прехвърлят в Азия, за да се справят окончателно със сирийската заплаха. Предпочели обаче да преминат по суша през Македония и Тракия, за което много разчитали на съдействието на Филип V Македонски (221 – 179 г. пр. Хр.), който след загубата на Втората македонска война (200 – 197 г. пр. Хр.) бил причислен сред римските съюзници и вече имало случаи да им оказва подкрепа, включително с военни сили.¹⁰

В античната литература са посочени различни причини за усърдието, с което Филип V съдействал на римляните през Сирийската война. Като че ли по-разпространено е емоционалното обяснение, представено от Апиан, според което македонският цар не бил взел решение на чия страна да се присъедини в сблъсъка между Рим и Сирия, докато Антиох III не се погрижил за погребването на загиналите Филипови войници в Битката при Киноскефале¹¹; това действие било интерпретирано като насочено лично срещу него и затова избрал да воюва на страната на римляните (App., Syr., 3.16). Несъмнено трябва да е имало и други причини, като много убедително изглежда гледището на Дион Касий, според когото Филип V напълно съдействал на римляните: „διὰ τε ἄλλα καὶ ὅτι ὁ Ἀντίοχος χωρὶς αὐτοῦ ἐν τῇ Ὀράκῃ τινὰ ἐπεσπίασато / преди всичко заради това, че Антиох анексирал някои места в Тракия, които принадлежали на него“ (Cass. Dio, 19.1 – Zon. 9.19).

Не е известно кои конкретно били въпросните места (χωρὶς). Може би Филип V се стремел към градовете по тракийското егейско крайбрежие, защото самият той по-късно (при дипломатически разговори за съдбата на тези градове) разкрил пред римски пратеници, че имал изгодно предложение от Антиох III да воюва на неговата страна: била му обещана сериозна парична сума и всички градове в Гърция (Liv. 39.28.6-9). Въпреки това, той предпочел да остане лоялен към Рим.

Идеята за преминаването на римските войски през Тракия се приписва на Луций Корнелий Сципион, консул през 190 г. пр. Хр. или на неговия прочут брат Публий Корнелий Сципион Африкански, който го придружавал като военен съветник.¹² Началото на експедицията било предшествано от сключването на 6-месечно примирие в Гърция¹³.

Мисията на Тиберий Семпроний Грах и преминаването на римските войски през Тракия

Преминаването на римските войски през Македония и Тракия било предхождано от специална разузнавателна мисия при македонския цар, предадена с достатъчно подробности от Ливий¹⁴: „[...] et consul ab Amphissa Thessaliam repetit, ut per Macedoniam Thraeciamque duceret in Asiam. Tum Africanus fratri: iter, quod insistis, L. Scipio, ego quoque approbo; sed totum id vertitur in voluntate Philippi, qui si imperio nostro fidus est, et iter et commeatus et omnia, quae in longo itinere exercitus alunt iuvantque, nobis suppeditabit; si is destituit, nihil per Thraeciam satis tutum habebis; itaque prius regis animum explorari placet. Optime explorabitur, si nihil ex praeparato agentem opprimeret qui inittetur.' Ti. Sempronius Gracchus, longe tum acerrimus iuvenum, ad id delectus per dispositos equos prope incredibili celeritate ab Amphissa – inde enim est dimissus – die tertio Pellam pervenit. In convivio rex erat et in multum vini processerat; ea ipsa remissio animi suspicionem dempsit novare eum quicquam velle. Et tum quidem comiter acceptus hospes, postero die commeatus exercitui paratos benigne, pontes in fluminibus factos, vias, ubi transitus difficiles erant, munitas vidit. haec referens eadem, qua ierat, celeritate Thaumacis occurrit consuli. Inde certiore et maiore spe laetus exercitus ad praeparata omnia in Macedoniam pervenit. Venientis regio apparatu et accepit et prosecutus est rex. Multa in eo et dexteritas et humanitas visa, quae commendabilia apud Africanum erant, virum sicut ad cetera egregium, ita a comitate, quae sine luxuria esset, non aversum. Inde non per Macedoniam modo sed etiam Thraeciam prosequente et praeparante omnia Philippo ad Hellespontum perventum est / [след като получил предводителството на армията] консулт се завърнал от Амфиса в Тесалия, с намерението да поведе своите войски през Македония и Тракия. Тук Африкански казал на своя брат, Луций Сципион: „Аз също, Луций Сципионе, одобрявам избора от теб път. Но цялото дело зависи от предразположението на Филип. Ако той остане лоялен към нас, ще ни осигури преминаване, провизии и всички неща, необходими за подпомагане и издръжка на една армия в дълъг поход. Но ако той не остане [лоялен], няма да намериш безопасност в никоя част на Тракия. Затова, по мое мнение, на първо място трябва да се разбере разположението на царя. Той ще бъде проверен най-добре, ако лицето, което бъде изпратено, пристигне внезапно при него, без да прави нищо по предварително съгласуван план“. Тиберий Семпроний Грах, един младеж, най-активен от всички на неговата възраст по това време, бил избран за изпълнението на тази задача. Сменяйки шафетно конете и придвижвайки се с изключи-

телна скорост, той тръгнал от Амфиса, откъдето бил изпратен, и достигнал до Пела на третия ден. Царят пирувал и бил напреднал с чашите: това отпускане на ума премахнало всяко подозрение за евентуално намерение да заблуди с поведението си. Гостът бил приет любезно и на следващия ден видял провизии в изобилие, вече приготовени за армията, мостове над реките и пътища, укрепени на местата, където преходът бил труден. Връщайки се от тази разузнавателна мисия със същата скорост, с която пристигнал, той срещнал консула в Таумахия. От всичко това армията се зарадва, отправи се с по-сигурни и по-големи надежди към Македония, където всичко необходимо било приготовено. При тяхното пристигане царят ги приел с царствено великопепие, и ги придружил по време на похода. Той демонстрирал много желание и добро настроение, което много се понарявало на Африкански, който, макар да бил несравним в други отношения, не оставал безразличен към добрите обноски, стига да не били прекомерни. Филип ги придружил не само докато преминали през Македония, но също така и през Тракия, като се погрижил за всичко необходимо и по този начин те достигнали до Хелеспонта“ (Liv. 37.7.8-16).

Така през 190 г. пр. Хр. за пръв път римски войски преминали през Тракия, предвождани от двамата Сципиони. В разказа не са представени много детайли. Числеността на преминаващите войски не е известна със сигурност, но определено ставало въпрос за значителни сили, доколкото Сципионите разполагали в навечерието на Битката при Магнезия (вероятно през декември 190 г. пр. Хр.) с армия, наброяваща до около 50 хил. души.¹⁵ Прави впечатление добрата информираност за ситуацията в Тракия, демонстрирана от Публий Корнелий Сципион Африкански. Пролитчат и силните позиции на Филип V в тракийските земи, познати от предходните събития¹⁶, включително и от Сирийската война: у Ливий е запазено кратко съобщение за ескортиране от македонски части на дезорганизирані войници на Антиох III от Навпакт през Тракия до Лизимахия (Liv. 36.33.6).

Предоставената от Апиан информация за преминаването през Тракия е по-ограничена: „Πότλιος δὲ Σκιπίων ἀφίκόμενος ἐς Αἰτωλίαν μετὰ τοῦ ὑπάτου, καὶ Μανίου στρατὸν παραλαβὼν, τὰς μὲν ἐν Αἰτωλίᾳ πολιορκίας ὑπερεῖδεν ὡς μικρὸν ἔργον, καὶ τοῖς Αἰτωλοῖς δεομένοις ἐπέτρεψεν αὐτοῖς ἐς Ῥώμην πρεσβεῦσαι περὶ σφῶν, ἐπὶ δὲ τὸν Ἀντίοχον ἡπείλετο πρὶν ἐκβῆναι τῷ ἀδελφῷ τὴν στρατηγίαν. διὰ δὲ Μακεδόνων ὥδευε καὶ Θρακῶν ἐπὶ τὸν Ἑλλησπόντον, δυσχερὴ καὶ χαλεπὴν ὁδὸν αὐτῷ γενομένην ἄν, εἰ μὴ Φίλιππος ὁ Μακεδὼν ὠδοποίει καὶ ὑπεδέχετο καὶ παρέπεμπεν ἐξευγμένοις τε ποταμοῖς ἐκ πολλοῦ καὶ ἀγοραῖς ἐτοίμοις / Междувременно Публий Сципион пристигнал в Етолия с консула и получил командването на армията от Маний. Веднага се отказал от обсадата на етолийските градове като незначителна работа, и позволил на жителите им да изпратят ново пратеничество в Рим, докато той самият побързал да се изправи срещу Антиох, преди командването на брат му да изтече. Придвигнал се по суша през Македония и Тракия до Хелеспонта, а това щяло да бъде много труден преход за него, ако Филип Македонски не поправил пътищата, забавлявал го, ескортирал го, направил мостове през потоците известно време преди това и му предоставил провизии“ (App., Syr., 5.23).

Не е възможно да се проследи в най-пълни детайли откъде точно през Тракия преминали римляните, но посоката им на придвижване от запад на изток до Тракийския Херсонес напомним за трасето на бъдещия римски път Via Egnatia. У Ливий е запазена по-късна реч на Филип V, в която самият той изброявал услугите, които направил за римляните: „et insequenti consuli L. Scipioni, cum terra statuisset ducere exercitum ad Hellespontum, non iter tantum per regnum nostrum dedi, sed vias etiam munivi, pontes feci, commeatus praebui; nec per Macedoniam tantum, sed per Thraciam etiam, ubi inter cetera pax quoque praestanda a barbaris erat / и на следващия консул, Луций Сципион, когато реши да поведе армията си към Хелеспонта по суша, аз не само му дадох право на преминаване през моето царство, но и направих пътища, построих мостове, осигурих провизии; направих това не само през Македония, но и през Тракия, където наред с всичко останало трябваше да поддържам мира с варварите“ (Liv. 39.28.8-9).

Нова информация в това сведение е изрично посочената необходимост македонският цар да поддържа „мира с варварите“, което следва да се интерпретира в смисъл, че неговият авторитет в тракийските земи не бил неограничен.

Римските военноморски сили в подкрепа на Сципионите

Успоредно с придвижването на сухопътната армия, към Хелеспонта по море се отправила и по-голямата част от римската флота, налична по това време в Източното Средиземноморие: „Λίσιος δ' ὁ ναύαρχος ἐπεὶ τῆς ὀδοπορίας τῶν Σκιπίωνων ἐπύθετο, Πανσίμαχον μὲν τὸν Ῥόδιον μετὰ τῶν Ῥοδίων νεῶν ἐν τῇ Αἰολίδι κατέλιπε, καὶ μέρος τι τοῦ ἰδίου στόλου, ταῖς δὲ πλείοσιν ἐς τὸν Ἑλλησπόντον ἐπλεῖ τὸν στρατὸν ὑποδεξόμενος. καὶ Σητὸς μὲν αὐτῷ καὶ Ροίγειον καὶ ὁ Ἀχαιῶν λιμὴν καὶ τινα ἄλλα προσέθετο, Ἀβυδὸν δὲ

ἀπειθοῦσαν ἐπολιόρκει / Ливий, командирът на флотата, когато научил, че Сципионите били на поход, оставил Павсимах, родосеца, с родоските и с част от неговите кораби в Еолида, а самият той отплавал с по-голямата част [от флотата] към Хелеспонта, за да пресрещне армията. Сестос, Роетум, Пристанището на ахейците и някои други места се предали. Абидос отказал [да се предаде] и бил подложен на обсада“ (App., Syr., 5.23).

Нищо не е запазено за реакция на Селевкидите срещу римските военноморски операции. Съобщено е само, че по същото време Селевк, синът на Антиох III, опустошавал земите на пергамския цар Евмен и подложил на обсада Пергам (App., Syr., 5.26).

Сблъсък с траките

В историографията се приема, че римската войска преминала безпроблемно през Тракия¹⁷, макар че в отклонение при по-късния разказ за засадата, в която попаднал Вулзон, Ливий съобщил за инцидент по пътя на Сципионите през тракийските земи. Първоизточникът на информацията бил римският анализист Квинт Клавдий Квадригарий: „[...] quamquam tunc quoque Claudius auctor est ad quindecim milia Thraecum praecedenti ad exploranda loca agmen Mutini Numidae occurrisset. Quadringentos equites fuisse Numidas, paucos elephantos; Mutinis filium per medios hostes cum centum quinquaginta delectis equitibus perripisse; eundem mox, cum iam Mutines in medio elephantis locatis, in cornua equitibus dispositis manum cum hoste conseruisset, terrorem ab tergo praeuisse, atque inde turbatos equestri velut procella hostis ad peditum agmen non accessisset / около 15 хил. траки застанали на пътя на нумидиеца Мутин, който бил изпратен напред, за да разузнае местността, като разполагал с 400 нумидийски конници и няколко слона. Синът на Мутин тогава си пробил път през неприятелите с командваните от него 150 конници и веднага, след като Мутин с разположените в центъра [на строя] слонове и с разпределените по крилата конници завързал сражение с неприятелите, нападнал траките за техен ужас откъм тила. В резултат на тази кавалерийска атака неприятелите били така дезорганизирани, че не смеели след това да се доближат до римската пехотна колона... [В този случай] траките се оказали по-миролюбиви не по някаква друга причина, а защото тогава [войската] носела със себе си по-малко плячка, отколкото желаели“ (Cl. Quadrig., Ann., 7, fr. 65 = Liv. 38.41.12-14).

Ако се вярва на цифровите данни, броят на траките при този инцидент е бил с 50% по-голям от тези, които нападнали Вулзон две години по-късно. Нищо не е съобщено за тяхната племенна принадлежност и за мястото на сблъсъка; предвид разположението на разказа в труда на Ливий е допустимо да се предположи, че участниците и географската позиция на двете събития били сравнително близки.¹⁸ Идентичност между траките от 190 и 188 г. пр. Хр. може да се допусне въз основа на текста на Апиан: „περὺντάς τε ἐπὶ Ἀντίοχον ἐς τὴν Ἀσίαν διὰ Θράκης καὶ Μακεδονίας ὁδὸν οὐκ εὐμαρῇ παρῆλτεπτεν οἰκεῖσι τέλεσι καὶ τροφαῖς, ὁδοποῶν καὶ ποταμούςς δισπόρους ζευγὺς καὶ τοὺς ἐπικειμένους Θράκας διακόπτων, ἕως ἐπὶ τὸν Ἑλλήσποντον ἦγαγεν [...] οἱ δὲ Θράκες οἶδε Ῥωμαίους ἀπὸ τῆς ἐπ’ Ἀντιόχῳ νίκης, ἐπανιόντας, οὐκέτι Φιλίππου παρόντος, τὴν τε λείαν ἀφείλοντο καὶ πολλοὺς διέφθειραν, ὧ καὶ μάλιστα ἐπεδείχθη ὅσον αὐτοὺς ἀνιόντας ὅσον ὤνησεν ὁ Φίλιππος / [...] когато [римляните] се придвижвали срещу Антиох в Азия, преминавайки през Тракия и Македония по труден път, той [Филип V] ги ескортира със собствените си войски, снабди ги с храна и пари, поправи пътищата, направи мостове по непроходимите потоци и разпръсна враждебно настроените траки, докато не ги преведе до Хелеспонта [...] Но траките се нахвърлиха върху римляните при завръщането им след победата над Антиох, когато Филип вече не беше с тях, отнеха плячката им и убиха мнозина. Така станало ясно колко голяма услуга им оказал Филип на отиване“ (App., Mac., 5).

Това свидетелство се причислява към редките документираните през елинистическата епоха примери за взаимодействие на различни тракийски племена.¹⁹

Установяване на римски контрол върху Тракийския Херсонес

Ливий разказал накратко последните етапи от прехода през Тракия: „per idem fere tempus consuli, transgresso Aeniorum Maronitarumque finis, nuntiatur victam regiam classem ad Myonnesum relictamque a praesidio Lysimachiam esse. Id multo quam de navali victoria laetius fuit, utique postquam eo venerunt, refertaque urbs omnium rerum commeatibus velut in adventum exercitus praeparatis eos excepit, ubi inopiam ultimam laboremque in obsidenda urbe proposuerant sibi. paucos dies stativa habuere, impedimenta aegrique ut consequerentur, qui passim per omnia Thraciae castella, fessi morbis ac longitudine viae, relictis erant. Receptis omnibus ingressi rursus iter per Chersonesum Hellespontum perveniunt / Междувременно консулт, който пре-

минавал през областите на Енос и Маронея, получил сведения за поражението на царския флот при Мионесос и евакуирането на Лизимахия. Последното предизвикало у него по-голямо удовлетворение от първото, изобщо от всички неща, които се случили при тяхното пристигане там, защото те намерили града пълен с припаси от всякакъв вид, все едно приготвени за пристигането на армията, защото те очаквали да бъдат в крайна нужда и трудности при обсадата на града. За няколко дни те останали там, за да изчакат пристигането на багажа и на болните, които, изтощени от болест и от дължината на похода били оставени във всички укрепления на Тракия. Когато всичко било готово, те подновили похода си през Херсонес и пристигнали при Хелеспонта“ (Liv. 37.33.1-4).

Прави впечатление, че римляните подминали Енос и Маронея, където – според друго съобщение на Ливий – имало гарнизони на Антиох III (Liv. 37.60.7).

Апиан представил повече подробности за установяването на римски контрол върху Тракийския Херсонес: „οὐτω δ' αὐτῆς ὁ Ἀντίοχος αἰσθόμενος Χερρόνησόν τε καὶ Λυσιμάχειαν ἐπιμελῶς ὠχύρου, μέγα, ὥσπερ ἦν, τὸ ἔργον ἡγούμενος ἐπὶ Ῥωμαίοις, ὅπου γε καὶ τὴν ἄλλην Θράκην διελθεῖν στρατοπέδῳ δυσόδευτον αὐτοῖς ἂν ἐγένετο καὶ δύσβατον, εἰ μὴ Φίλιππος διέφερεν. ἀλλ' ὁ Ἀντίοχος ὢν καὶ τὰ ἄλλα κουφόνους αἰεὶ καὶ ταχὺς ἐς μεταβολήν, ἐπεὶ τῆς ἥσσης ἐπύθετο τῆς περὶ Μυόννησον, ἀμπαν ἐξεπλάγη, νομίσας αὐτῷ τὸ δαιμόνιον ἐπιβουλεύειν: παρὰ γὰρ λόγον ἕκαστα χωρεῖν, Ῥωμαίων μὲν ἐν τῇ θαλάσῃ κρατούντων, ἐν ᾗ πολὺ προὔχειν αὐτὸς ἐνόμιζε, Ῥοδίῳ δ' Ἀννίβαν ἐς Παμφυλίαν κατακεκλεικώτων, Φιλίππου δὲ Ῥωμαίους παραπέμποντος ἀβάτους ὁδοῦς, ὃν μάλιστα μνησικακήσειν αὐτοῖς ὢν ἔπαθεν ὑπελάμβανεν. ὑπὸ δὲ τῶνδε πάντων ἔκταρασσόμενος τε, καὶ θεοῦ βλάπτοντος ἤδη τοὺς λογισμοῦς, ὅπερ ἅπασι προσιόντων ἀτυχμάτων ἐπιγίγνεται, Χερρόνησον ἐξέλιπεν ἀλογίστως, πρὶν καὶ ἐς ὅσιν ἐλθεῖν τοῖς πολεμίοις, οὔτε μετενεγκῶν ὅσος ἦν ἐν αὐτῇ σίτος σεσωρευμένος πολὺς ἢ ὅπλα ἢ χρήματα ἢ μηχαναί, οὔτε ἐμπρήσας, ἀλλ' ὑγιεῖς ἀφορμὰς τοσάσδε τοῖς πολεμίοις καταλιπών. Λυσιμαχέας τε αὐτῷ καθάπερ ἐκ πολιορκίας συμφεύγοντας μετ' οἰμωγῆς, ἅμα γυναιξὶ καὶ παιδίῳ, ὑπερεώρα, μόνου τοῦ διάπλου τοῦ περὶ Ἄβυδον εἶρξαι τοὺς πολεμίους ἐπινοῶν, καὶ τὴν λοιπὴν ἐπὶ ἐλπίδα τοῦ πολέμου πᾶσαν ἐν τούτῳ τιθέμενος. οὐ μὴν οὔτε τὸν διάπλου ἐφύλαξεν ὑπὸ θεοβλαβείας, ἀλλ' ἐς τὸ μεσόγειον ἠπειχθῆ ἐπανελθεῖν, φθάνων τοὺς πολεμίους, οὐδὲ τινα φυλακὴν ἐν τῷ διάπλῳ κατέλιπεν. οἱ δὲ Σκιπίωνες ἐπεὶ τῆς ἀναχωρήσεως αὐτοῦ ἐπύθοντο, Λυσιμάχειαν τε δρόμῳ κατέλαβον, καὶ τῶν ἐν Χερρόνησῳ θησαυρῶν τε καὶ ὀπλῶν κρατήσαντες τὸν Ἑλλησπόντον ἔρριπον ὄντα φυλακῆς εὐθὺς [...] / Преди Антиох да чуе за него [за резултата от Битката при Мионесос] той укрепявал Херсонес и Лизимахия с най-голямо внимание, мислейки, както и било наистина, че това е много важно за отбрана срещу римляните, които щели да имат затруднения да преминат през останалата Тракия, ако Филип не ги превел. Но Антиох, който като цяло бил лекомислен и нестабилен, когато чул за загубата при Мионесос бил напълно паникьосан и мислел, че Съдбата му обърнала гръб. Всичко се преобърнало против неговите очаквания. Римляните го победили по море, където той мислел, че има голямо превъзходство; родосците затворили Ханибал в Памфилия; Филип помагал на римляните да преминат през непроходими пътища, докато Антиох предполагал, че той [Филип V] нямало да забрави това, което претърпял от тях. Всичко го изнервяло и божеството започнало да унищожава способностите му за мислене, както се случва винаги, когато нещастията се умножават. Така той изоставил Херсонес без причина, дори преди врагът да се появи, без да се погрижи дори за изгарянето на големите припаси, които събрал там: зърно, оръжия, пари, машини; оставил всички тези военни ресурси в добро състояние за врага. Не обърнал внимание на лизимахийците, които, като след обсада, го придружавали в бягството му с оплаквания, заедно с техните жени и деца. Той имал намерение само да предотврати преминаването на врага при Абидос и уповавал своята надежда за успех изцяло на това. Бил толкова заваян, че дори не защитил мястото за преминаване, а побързал да стигне до вътрешността [на страната си] преди врага, без дори да остави охрана на Проливите. Когато Сципионите узнали за неговото отстъпление, те бързо превзели Лизимахия с първата атака, завзели съкровището и оръжията в Херсонес, преминали оставения без охрана Хелеспонт“ (App., Syr., 6.28-29).

Макар и доста обстоятелствен, представеният разказ е важен за уточняване на последователността на събитията, което не е било обект на достатъчно задълбочени изследвания. От текста става ясно, че до есента на 190 г. пр. Хр., когато се датира решителната морска битка при Мионесос, Антиох III предприемал усилия да задържи владенията си в Тракия.²⁰ След като научил за резултата обаче, той изтеглил силите си от Херсонес.²¹ Още един щрих към събитията се открива във фрагмент на Диодор: „Ὅτι ὁ Ἀντίοχος διὰ τὴν ἥτταν ταπεινωθεὶς ἔκρινε τῆς μὲν Εὐρώπης ἐξίστασθαι, περὶ δὲ τῆς Ἀσίας διαγωνίζεσθαι. Καὶ προσέταξε τοῖς Λυσιμαχεῦσι πανδημεῖ τὴν πόλιν ἐκλιπεῖν, εἰς δὲ τὰς κατὰ τὴν Ἀσίαν πόλεις μετοικῆσαι. Καὶ

ἔδοξε πᾶσιν ἀφρόνως βεβουλευῆσθαι καὶ πόλιν ἐπικαιρότατα κειμένην πρὸς τὸ διακωλύσαι τοὺς πολεμίους ἐκ τῆς Εὐρώπης εἰς τὴν Ἀσίαν περαιοῦν τὰς δυνάμεις ἀκοντὶ προέσθαι τοῖς πολεμίους. Ακολούθως δὲ τῇ διαλήψει ταύτῃ καὶ τὸ τῶν ἀποτελεσμάτων ἔργον ἐπληρώθη. Ὁ γὰρ Σκιπίων τὴν πόλιν καταλαβὼν ἔρῃμον αὐτομάτως εὐήμερῃσε ταύτῃν παραλαβὼν / Примирен със загубата, Антиох решил да се изтегли от Европа и да се концентрира върху отбраната на Азия. Наредил на жителите на Лизимахия да изоставят своя град и да намерят убежище в градовете на Азия. Всеобщото мнение било, че това решение било глупаво и, че той изоставил без борба в ръцете на врага един град, най-удобно разположен, за да попречи на преминаването на вражеските сили от Европа в Азия. Последващият ход на събитията напълно потвърдил тази преценка, защото Сципион, намирайки града изоставен, постигнал голям успех като го завзел“ (Diod., 29.5.1).

Според текста по заповед на сирийския монарх жителите на Лизимахия били евакуирани в Азия. Тук се забелязва противоречие с цитирания по-горе пасаж на Апиан, според който поне част от жителите на града оказали съпротива на римляните. Компромисното и най-логично обяснение е, че Антиох III оттеглил силите си, но някои от лизимахийците решили доброволно да останат в града и да го защитават. Те обаче били победени още с първата атака и градът бързо бил превзет.

Заклучения

Прегледът на античните свидетелства позволява формулирането на няколко по-съществени наблюдения относно първото преминаване на римски войски през тракийските земи.

На първо място, разказите не съдържат достатъчно детайли – включително пространствени и хронологични ориентири – относно преминаването през Тракия. Дискусионно е и авторството на идеята за необичайния преход: Ливий го приписва на Л. Корнелий Сципион, а Апиан – на неговия брат, П. Корнелий Сципион Африкански. Възможно е да се предположи само общото направление на движението на римските сили, които през по-голямата част от пътя вероятно следвали трасето на бъдещия Via Egnatia.

В историографията не е потърсено обяснение за всестранныя помощ, която Филип V Македонски оказал на римляните. Настоящият преглед показва, че усърдието на македонския цар може убедително да се обясни със завземането от Антиох III на принадлежали на него владения в Тракия, както съобщил Дион Касий.

Известни затруднения предизвиква хронологията на придвижването. В историографията е обърнато внимание на необичайно дългия преход през тракийските земи, чиято продължителност се извежда имплицитно от наличните сведения на античните писатели: преминаването на разстоянието от около 400 км между източните граници на Македония край Абдера до Лизимахия трябва да е отнело на римляните четири или пет месеца.²² Убедително обяснение за това изключително бавно движение не е намерено. Предполагано е оказването на съпротива от страна на тракийски и селевкидски сили в страната, допълнено от необходимостта за гарантиране на сигурността на пътя чрез строежи на укрепления.²³ Нито едно от тези предположения не може да намери подкрепа в наличните извори: има данни само за съвсем ограничени и незначителни военни действия, а обезпечаването на строителните дейности по пътните съоръжения се приписва изцяло на Филип V Македонски.

В съобщенията за похода на Сципионите проличават за пореден път силните позиции на Филип V в Тракия. Неговият авторитет сред траките обаче определено не бил неограничен, доколкото изрично е посочена необходимостта да се поддържа мир с тях. В едно от цитираните свидетелства дори е загатнато и за военни действия на Филип V в Тракия във връзка с обезпечаването на римската безопасност: споменато е, че той разпръснал „враждебно настроените траки“ (τοὺς ἐπικειμένους Θρᾷκας διακόπτων). Запазена е информация и за две битки на римската армия: съюзно подразделение се сблъскало с траките, като мястото не е изрично посочено, а военни действия били водени и за превземането на Лизимахия.

Поради недостатъчната информация не може да се предложи еднозначна интерпретация на споменатите от Ливий тракийски укрепления (Thraciae castella), които изглежда били контролирани от римляните и вероятно от македонския цар.

По времето на разглеждания поход се търси сключването на известния от по-късни свидетелства съюзен договор между Рим и тракийското племе сапей²⁴, като присъствието на Сципионите в Южна Тракия може да обясни и наричането на едно тракийско племе корнелии, каквото е родовото име на двамата братя.²⁵ Директни основания за подкрепа на тези две предположения не се откриват в представените антични текстове, но не се намират и основания за тяхното отхвърляне.

Несъмнено римската армия преминала успешно през тракийските земи, доколкото не се съобщава за никакви съществени загуби. Все пак обаче – както ясно показват цитираните антични текстове – на римляните се наложило да воюват в Тракия, макар и в ограничени мащаби.²⁶

ЛИТЕРАТУРА

1. Grainger, J. *The Seleukid Empire of Antiochus III (223 – 187 BC)*. Barnsley, 2015, pp. 151-186.
2. Grainger, J. *The Roman War of Antiochos the Great*. Leiden & Boston, 2002, p. 112.
3. Hammond, N.G.L., F.W. Walbank. *A History of Macedonia, volume III*: pp. 336-167 B.C. Oxford, 2001, p. 450.
4. Walbank, F.W. *Philip V of Macedon*. Cambridge, 2014, p. 200.
5. Срв. J. Rich. „Appian, Polybius and the Romans' war with Antiochus the Great: a study in Appian's sources and methods“. In: K. Welch (ed.). *Appian's Roman History: Empire and Civil War*. Classical Press of Wales, 2015, p. 91.
6. Walbank, F.W. Op. cit., pp. 186-222; Grainger, J. *The Roman War ...*, Pass.; Grainger, J. *The Seleukid Empire ...*, pp. 151-186; Erdkamp, P. *The War against Antiochus III. 191 – 188 BC*. In: *The Encyclopedia of Ancient Battles*. John Wiley & Sons, 2017, pp. 1-9; Dmitriev, S. *Roman-Syrian War (192 – 188 BCE)*. In: *The Encyclopedia of Diplomacy*. John Wiley & Sons, 2018, pp. 1-6.
7. Iliev, J. Gn. Manlius Vulso's March through Thrace in 188 B.C. according to Livy's manuscript tradition. – In: Paola Schirripa (ed.). *Greci e Romani sulle sponde del Mar Nero. Aristonothos – Scritti per il Mediterraneo antico*, 15. Milano, 2019, pp. 209-228.
8. Тачева, М. *История на българските земи в древността през елинистическата и римската епоха*. София, 1997, с. 54; Цветкова, Ю. *История на Тракийския Херсонес (от Троянската война до времето на римското завоевание)*. В. Търново, 2008, с. 232; Петков, Пл. *Военно-политически отношения на тракийските владетели в Европейския Югоизток между 230/229 г. пр. Хр. – 45/46 г. сл. Хр.* В. Търново, 2011, с. 44; Delev, P. *From Koroupedion to the Beginning of the Third Mithridatic War (281 – 73 BCE)*. In: *A Companion to Ancient Thrace*. John Wiley & Sons, 2015, p. 65; Делев, П. *Древна Тракия в края на III и през първата половина на II в. пр. Хр.* В: *Сборник в чест на XX години програми по египтология в Нов български университет*. София, 2017, с. 41.
9. Grainger, J. *The Seleukid Empire ...*, p. 151.
10. Walbank, F.W. Op. cit., p. 189.
11. Hammond, N.G.L., F.W. Walbank. Op. cit., p. 451; Walbank, F.W. Op. cit., p. 200.
12. За забелязаното разминаване в античната традиция по отношение на това кой от двамата Сципиони имал водеща роля във войната срещу Антиох III, виж J. Rich. Op. cit., p. 92.
13. Hammond, N.G.L., F.W. Walbank. Op. cit., p. 453.
14. Мисията на Тиберий Семпроний Гракх била пропусната от Апиан, виж J. Rich. Op. cit., p. 93.
15. Grainger, J. *The Roman War ...*, p. 361.
16. Срв. Iliev, J. *Thracians in the Second Macedonian War (200 – 197 B.C.)*. In: *Hiperboreea*, 7(2), 2020, pp. 109-121.
17. Delev, P. Op. cit., p. 65 – „The Roman army [...] crossed unimpeded through Southern Thrace and passed into Asia“, „римската армия преминала необезпокоявана през Южна Тракия и се прехвърлила в Азия“.
18. Срв. Петков, Пл. *Цит. съч.*, с. 44.
19. Тачева, М. *Цит. съч.*, с. 55.
20. Срв. Цветкова, Ю. *Цит. съч.* с. 232 – „След поражението му при Магнезия в 190 г. пр. Хр. той [Антиох III] панически се оттеглил от полуострова [Тракийския Херсонес] даже без да остави хора за охрана на протока при Хелеспонт, изоставяйки припасите в Лизимахия“. В случая авторката е допуснала фактологична грешка: вместо Магнезия трябва да се чете Мионесос, защото Битката при Магнезия се провежда след като римляните са завладели Тракийския Херсонес и са успели да се прехвърлят в Мала Азия. Интересно е, че такава грешка допуска и Пл. Петков. *Цит. съч.*, 44, твърдейки: „Римската армия успява да се прехвърли в Мала Азия и влиза в Лизимахия“; мястото на двете реални следва да се размени.
21. Rich, J. Op. cit., pp. 94-95.
22. Grainger, J. *The Roman War ...*, p. 308.
23. Grainger, J. *The Roman War ...*, p. 310.
24. Петков, Пл. *Цит. съч.*, с. 70.
25. Iliev, J. Gn. Manlius Vulso's March through Thrace ..., p. 212.
26. Срв. Цветкова, Ю. *Цит. съч.*, с. 232 – 233 – „Настъпващата римска войска завладяла Лизимахия и целия полуостров без съпротива ...“.

REFERENCES

1. Grainger, J. *The Seleukid Empire of Antiochus III (223 – 187 BC)*. Barnsley, 2015, pp. 151-186.
2. Grainger, J. *The Roman War of Antiochos the Great*. Leiden & Boston, 2002, p. 112.
3. Hammond, N.G.L., F.W. Walbank. *A History of Macedonia, volume III*: pp. 336-167 B.C. Oxford, 2001, p. 450.
4. Walbank, F.W. *Philip V of Macedon*. Cambridge, 2014, p. 200.
5. Srv. J. Rich. „Appian, Polybius and the Romans' war with Antiochus the Great: a study in Appian's sources and methods“. In: K. Welch (ed.). *Appian's Roman History: Empire and Civil War*. Classical Press of Wales, 2015, p. 91.
6. Walbank, F.W. Op. cit., pp. 186-222; Grainger, J. *The Roman War ...*, Pass.; Grainger, J. *The Seleukid Empire ...*, pp. 151-186; Erdkamp, P. *The War against Antiochus III. 191 – 188 BC*. In: *The Encyclopedia of Ancient Battles*. John

- Wiley & Sons, 2017, pp. 1-9; Dmitriev, S. Roman-Syrian War (192 – 188 BCE). In: The Encyclopedia of Diplomacy. John Wiley & Sons, 2018, pp. 1-6.
7. Iliev, J. Gn. Manlius Vulso's March through Thrace in 188 B.C. according to Livy's manuscript tradition. – In: Paola Schirripa (ed.). *Greci e Romani sulle sponde del Mar Nero. Aristonothos – Scritti per il Mediterraneo antico*, 15. Milano, 2019, pp. 209-228.
8. Tacheva, M. *Istoria na balgarskite zemi v drevnostta prez elinisticheskata i rimskata epoha*. Sofia, 1997, s. 54; Tsvetkova, Yu. *Istoria na Trakiyskia Hersones (ot Troyanskata vojna do vremeto na rimskoto zaveoevanie)*. V. Tarnovo, 2008, s. 232; Petkov, Pl. *Voенно-politicheski otnoshenia na trakiyskite vladeteli v Evropeyskia Yugoiztok mezhdru 230/229 g. pr. Hr. – 45/46 g. sl. Hr.* V. Tarnovo, 2011, s. 44; Delev, P. From Koroupedion to the Beginning of the Third Mithridatic War (281 – 73 BCE). In: *A Companion to Ancient Thrace*. John Wiley & Sons, 2015, r. 65; Delev, P. *Drevna Trakia v kraya na III i prez parvata polovina na II v. pr. Hr.* V. *Sbornik v chest na HH godini programi po egiptologia v Nov balgarski universitet*. Sofia, 2017, s. 41.
9. Grainger, J. *The Seleukid Empire ...*, p. 151.
10. Walbank, F.W. *Op. cit.*, p. 189.
11. Hammond, N.G.L., F.W. Walbank. *Op. cit.*, p. 451; Walbank, F.W. *Op. cit.*, p. 200.
12. Za zabelyazanoto razminavane v antichnata traditsia po otnoshenie na tova koy ot dvamata Stsipioni imal vodeshta rolya vav voynata sreshtu Antioh III, vizh J. Rich. *Op. cit.*, p. 92.
13. Hammond, N.G.L., F.W. Walbank. *Op. cit.*, p. 453.
14. Misiyata na Tiberiy Semproniy Grakh bila propusnata ot Apian, vizh J. Rich. *Op. cit.*, p. 93.
15. Grainger, J. *The Roman War ...*, p. 361.
16. Srv. Iliev, J. Thracians in the Second Macedonian War (200 – 197 B.C.). In: *Hiperboreea*, 7(2), 2020, pp. 109-121.
17. Delev, P. *Op. cit.*, p. 65 – „The Roman army [...] crossed unimpeded through Southern Thrace and passed into Asia“.
18. Srv. Petkov, Pl. *Tsit. sach.*, c. 44.
19. Tacheva, M. *Tsit. sach.*, c. 55.
20. Srv. Tsvetkova, Yu. *Tsit. sach.* c. 232 – „Sled porazhenieto mu pri Magnezia v 190 g. pr. Hr. toy [Antioh III] panicheski se ottegliil ot poluoostrova [Trakiyskia Hersones] dazhe bez da ostavi hora za ohrana na protoka pri Helespont, izostavyayki pripasite v Lizimahia“. V sluchaya avtorkata e dopusnala faktologichna greshka: vmesto Magnezia tryabva da se chete Mionesos, zashtoto Bitkata pri Magnezia se provezhda sled kato rimlyanite sa zavladeli Trakiyskia Hersones i sa uspeli da se prehvarlyat v Mala Azia. Interesno e, che takava greshka dopuska i Pl. Petkov. *Tsit. sach.*, 44, tvardeyki: „Rimskata armia uspyava da se prehvarli v Mala Azia i vliza v Lizimahia“; myastoto na dvete realii sledva da se razmeni.
21. Rich, J. *Op. cit.*, pp. 94-95.
22. Grainger, J. *The Roman War ...*, p. 308.
23. Grainger, J. *The Roman War ...*, p. 310.
24. Petkov, Pl. *Tsit. sach.*, c. 70.
25. Iliev, J. *Gn. Manlius Vulso's March through Thrace ...*, p. 212.
26. Srv. Tsvetkova, Yu. *Tsit. sach.*, p. 232 – 233 – „Nastapvashtata rimska voyska zavladyala Lizimahia i tselia poluoostrov bez saprotiva ...“.

НОВОТО ЛИЦЕ НА РИСКА В ЕПОХАТА НА ДИГИТАЛНАТА ТРАНСФОРМАЦИЯ

Валентин Мончев, докторант

Военна академия „Г. С. Раковски“, v.v.monchev@rmdc.bg

Резюме: Несъмнено глобалната пандемия от COVID-19 беше катализаторът, нужен за натискане спусъка на тоталната дигитализация. Беше необходимо индустриите бързо да преминат границата, която се страхуваха да пристъпят от години. Страхът от това преминаване е напълно оправдан – дигиталната трансформация отвежда организациите в място, неподвластно на законите на физиката, където пространството е относително и времето не е линейна величина. Това място, наречено в широкия си смисъл „киберпространство“, е колкото плодотворно за разработката на нови продукти и услуги чрез внедряването на инструментариум от сферата на изкуствения интелект (AI), обработката на големи масиви от данни (big data), изчисленията в облак (cloud computing) и т.н., толкова и опасно заради невидимите заплахи, които дебнат в него. Докладът разглежда основните рискове, пред които Индустрия 4.0 е изправена и някои методи за тяхното адекватно управление.

Ключови думи: големи масиви от данни; дигитална трансформация; изкуствен интелект; информационна сигурност; ИТ инфраструктура; кибератака; киберсигурност; облачни услуги; управление на риска

THE NEW FACE OF THE RISK IN THE DIGITAL TRANSFORMATION AGE

Valentin Monchev, MSc, PMP, PhD Candidate

Rakovski National Defense College

Sofia, Bulgaria

E-mail: v.v.monchev@rmdc.bg

Abstract: Undoubtedly, the global COVID-19 pandemic was the trigger of the total digitalization. A border that all the industries were afraid of crossing since years was necessary to be trespassed quite rapidly. The fear of crossing this border is completely understandable – digital transformation leads towards a place beyond the physics laws, a place where the understanding for space is relative and time is no longer a linear dimension. In its broad sense, this place is known under the name “cyberspace”. Cyberspace is at the same time extremely fruitful for development of new products and services with the help of the toolset in the field of Artificial Intelligence, Big Data, Cloud Computing, etc., but is also a dangerous place mainly because of the invisible threats it is surrounded with. This report reviews the main risks that Industry 4.0 is facing and some of the general methods for their adequate treatment.

Keywords: artificial intelligence; big data; cloud computing; cyberattack; cybersecurity; digital transformation; information security; IT infrastructure; risk management

Дигиталната трансформация

Пандемията от COVID-19 далеч не слага началото на дигиталната трансформация (DX). Терминът „дигитална трансформация“ датира от деветдесетте години на XX век. В началото се е считало, че една организация е трансформирана дигитално, когато е внедрила модерна *ИТ инфраструктура*. Впоследствие това схващане се видоизменя до степен, в която няма единно и точно определение. Важно е да се отделят двата основни компонента на дигиталната трансформация – това са цифровизиране (англ. *digitization*)¹ и дигитализация (англ. *digitalization*)². Тези два компонента следват логически и заедно правят цифровата трансформация възможна.

Всеки бизнес, всяка организация има собствено разбиране относно дигитализацията и това, колкото и да е обърквато, не бива да бъде считано за странно или погрешно. Най-общо, от гледна точка на податливостта към цифрова трансформация, съществуват три групи организации:

● **Група А** – дигитални организации. Това са организации, които подлежат на пълна цифровизация. Бизнес процесите на тези организации могат да бъдат дигитализирани на 70% и нагоре. Те могат да съществуват почти изцяло в киберпространството, без това да възпрепятства по някакъв начин техните бизнес операции. Напротив, за тези организации дигитализацията отваря повече врати и възможности. Примери за такива организации могат да бъдат дадени в различни сектори на икономиката като „финтех“ (англ. *financial technology*)³, разработка на софтуер, платформи за онлайн срещи, платформи за електронно обучение и т.н.

● **Група Б** – дигитални хибриди. Този вид организации подлежи на частична дигитализация – между 50 и 70% от бизнес процесите. Това означава, че по-голямата част от бизнес операциите биха могли да бъдат цифровизирани, но друга значителна част (обикновено между 30% и 50%) е наложително да остане физическа. Това са типично продуктовете организации, чиито продукти са извън разработката на софтуерни и кибер-решения. Например, тук влиза хардуерната индустрия, хранително-вкусова промишленост, енергетика, тежка и лека промишленост и т.н.

● **Група В** – конвенционални организации. С под 50% възможност за дигитализация на бизнес операциите си, тези организации остават последни в дигиталната трансформация поради спецификата на своя бизнес. Това са предимно организации, развиващи дейност в сферата на здравеопазването, туризма, спорта, строителството, но тук се нареждат и държавите с всичките си структури и целия държавен апарат. Важно е да се отбележи, че при този тип организации потенциалът за цифровизиране и дигитализация е не по-малък. Ето например в Стратегията за „Цифрова трансформация на България за периода 2020 – 2030 г.“, са записани 17 области на въздействие, между които транспорт, енергетика, селско стопанство, здравеопазване, финанси, култура, образование и обучение и т.н.

Това, което на пръв поглед обединява горните три групи организации, е фактът, че не съществува такава, която да не може да дигитализира нито един свой процес. Логично следва въпросът защо дигиталната трансформация е толкова важна.

Според едно проучване на Международната корпорация за данни (IDC⁴), инвестициите в дигитална трансформация на всички бизнеси и организации в световен мащаб ще достигнат колосалните 2,8 трилиона щатски долара до 2025 г., което е повече от половината, изхарчено за дейности по дигитална трансформация от 90-те години на XX век до 2020 г. От друга страна, глобалният лидер в областта на пазарните проучвания и анализи Гартнер⁵, в свой доклад показва, че дигиталният бизнес представлява средно 36% от общите приходи на бизнеса за 2020 г. Тенденциите са до 2025 г. този процент да достигне 50%.

Дигиталната трансформация обаче не следва да бъде разглеждана единствено отвън навътре. Погледната през призмата на самите организации, дигитализацията означава различни неща за различните групи заинтересовани лица в тях. От гледна точка на изпълнителното ръководство, например, дигиталната трансформация означава дефиниране на дигиталната визия и стратегия. Това, съпроводено с оценка на инициативите, подлежащи на дигитализиране, определя рамката на цифровата трансформация на макро-организационно ниво.

Следващото, оперативнo ниво е това, което реално извършва прехода към дигитализация – тук се трансформира инструментариумът и способностите за доставка на услуги и се идентифицира персоналът от екосистемата – ключов за извършването на дигитализацията.

На тактическо ниво е програмното управление на дигиталната трансформация – то се съсредоточава върху ефикасното внедряване на дигиталната инициатива за съответните бизнес екипи.

На всяко едно от посочените нива цифровата трансформация се задвижва от осезаемата промяна в ролята на технологиите в дадена организация. Технологиите вече не е чисто поддържаща функция, която да прави бизнес процесите възможни. Технологиите вече е способна на много повече. Многонационалната мрежа от професионални услуги Делойт (*Deloitte*) в свой доклад⁶ по темата определя шест основни двигатели на цифровата трансформация. Това са:

- Социални медии (*Social Media*)
- Мобилност (*Enterprise Mobility*)
- Интернет на нещата (*IoT*)
- Киберсигурност (*Cybersecurity*)
- Големи масиви данни (*Big Data*)
- Изчисления в облака (*Cloud Computing*)

Тези шест двигателя, всъщност, се управляват от осем пускови „ръчки“ на цифрова трансформация, които биха могли да бъдат сегрегирани в две основни групи:

Катализатори на растеж, където са процесите по:

- генериране на търсене (*Demand Generation*),
- таргетиране на правилния за организацията пазарен сегмент (*Reach and Selection*);
- управление на клиентските покупки (*Customer Purchase Management*);
- управление на клиентската удовлетвореност (*Customer Experience Management*).

Активатори на непрекъснато подобрене, включващи процесите по:

- ефективност;
- използване на активите;
- бързина на обслужването;
- нови бизнес модели.

Киберсигурност и невидимите заплахи

Това, което прави впечатление е, че киберсигурността някак си не пасва еднозначно в нито една от двете групи, а от друга страна може да бъде причислена към всяка от осемте пускови „ръчки“. Това е така, защото към всяка една от групите могат да бъдат асоциирани много и различни рискове, всички от които по своето същество са рискове, свързани с киберсигурността. Точно киберсигурността определя основните елементи, необходими за защита на техническата инфраструктура, материалните и нематериалните активи, използваната технология и репутацията на организацията в случай на кибератака или теч на данни. Киберсигурността определя и целите на една организация за защита от кражба на данни, която би могла да доведе до сериозни щети. Следователно, благодарение на киберсигурността е възможно да се определят рисковете, свързани с дигиталната трансформация.

Несъмнено дигиталната трансформация е *безпрецедентен феномен* в известната история на човечеството. Тя позволява до голяма степен да се направи видимото невидимо, чрез превръщането му в низ от нули и единици. Това, наред с ползите, които неминуемо са огромни, води и до появата на нови невидими рискове. Ето защо онези, които в друго време ограбваха банки, внедряваха шпиони, за да откраднат търговски или държавни тайни или взривяваха коли-бомби по площадите, сега трябва да влязат в крак с новите тенденции и на свой ред да се трансформират цифрово.

Кибератаките най-общо могат да се разпределят в следните четири категории, според целта, която се опитват да постигнат:

- Пробив в сигурността на данните (*Data breach*). Според анализ на кибератаките през периода 2001 – 2020 г., основната част са насочени към кражба на чувствителни данни, кражба на онлайн идентичност, социален инженеринг, модифициране на данни с цел дългосрочно компрометиране на сигурността и кибершпионаж.

- Финансово облагодетелстване (*Financial Theft*). Друга голяма част от кибератаките са насочени към кражбата на парични средства (в това число влизат и онлайн злоупотребите с банкови карти).

- Прекъсване на услугата (*Service Disruption*). На трето място са кибератаките, насочени към прекъсване на дадена услуга или цялостен бизнес. Прекъсването може да цели пренасочване на потребители към конкурентна услуга или плащане на откуп за възстановяване на услугите (например през 2017 г. с помощта на крипто-вируса WannaCry, над 200 000 компютърни системи в над 150 държави са поразени и това спира бизнес операциите на болници, телекоми, железници и автомобилни компании). Подвариант на тази категория са и т.нар. атаки от тип „отказ от услуги“ (*Denial-of-Service*) и ботнет атаки.

- Политическа дестабилизация (*Political Instability*). На последно място по обем, но не по значение, са кибератаките, целящи политическа дестабилизация. От техническа гледна точка те са смесица от горните три типа, но тъй като са специфични, съществува дори термин за подобни атаки и това е *Cyberwarfare*. Терминът възниква след Стукснет (*Stuxnet*) атаката срещу атомна електроцентрала в Иран през 2010/2011 г.

Въпреки, че всички индустрии са потенциално в риск от кибератаки, някои от тях са по-предпочитани. Тези бизнеси включват здравеопазване, финанси, услуги за крайни потребители и държавни агенции и организации.

Докато здравеопазването традиционно е подложено предимно на т.нар. *фишинг*⁷ атаки, зачестили особено по време на пандемията от COVID-19, с цел кражба на чувствителни пациентски данни, други ин-

дустрии като финансовата са подложени на по-различни атаки – кражба на кодове за платежни средства, разбиване на пароли и компрометиране на клиентски данни с цел облагодетелстване, загуба на репутация и получаване на конкурентно предимство.

Заплахите, свързани с дигиталната трансформация, обхващат всичко онова, което може по някакъв начин да нанесе вреда върху компютърна система, сървър или компютърна мрежа. Киберзаплахите могат да възникнат или не, но те имат потенциал да нанесат сериозна щета на активите на всяка организация.

Възникналите киберзаплахи могат да доведат до кибератаки. Има няколко основни вида киберзаплахи, с които организациите биха могли да се сблъскат. Някои от най-честите от тях за периода 2018 – 2020 г. са представени в таблица 1.

Таблица 1

Статистика на основните киберзаплахи за периода 2018 – 2020 г.

Киберзаплаха	Описание
Фишинг (Phishing)	Над 1,5 милиона нови фишинг сайтове се създават всеки месец
Криптовируси (Ransomware)	Атаките на криптовируси са нараснали с над 350% само през 2018 г.
Откраднати средства за автентикация (Means of authentication theft)	Над 500 хил. пароли и средства за автентикация са продадени в дарк уеб през 2020 г.
Кибер измами (Cyber Fraud)	47% от финансовите институции глобално докладват повишение в измамите с платежни инструменти
Прекъсване на услугата (Service Disruption)	21% ръст на прекъсване на услугите на малки и средни бизнеси вследствие на кибератаки през 2020 г.
Зловреден софтуер (Malware)	25% ръст на ударите на злонамерен софтуер върху финансовите институции глобално през 2020г.

Статистиката в таблицата показва, че киберпрестъпниците прекъсват услуги, изпращат подвеждащи (фишинг) писма, изпълняват зловреден код на чужди компютърни конфигурации, крадат пароли с цел продажба, криптират съдържание срещу подкуп и т.н. Списъкът с престъпни кибердейности е безкраен.

Според проучване на Yahoo Finance от 2021 г.⁸, фишингът е най-често срещаната киберзаплаха. В основата за това е, преди всичко, лесният начин за разпространяване на фишинг мейли. Не е необходима изключително висока компютърна грамотност, за да се направи фишинг сайт и да се разпратят фишинг мейли до определена група от хора. Поради програмите за вътрешнофирмено обучение на служителите в различните организации с цел повишаване знанията и осведомеността по въпросите на киберсигурността, обаче се отбелязва сериозен спад на фишинг атаките.

Въпреки това се отбелязва почти 55% ръст в уникалните киберзаплахи за 2020 г. (общо 389 уникални киберзаплахи са наблюдавани през 2019 г., докато техният брой нараства на 600 през 2020 г.). Същото проучване показва, че финансовата индустрия е най-атакуваната индустрия, която, обаче и най-бързо отговаря на киберзаплахите в глобален мащаб.

Посочените в таблица 1 киберзаплахи са само външни. Това означава, че те възникват извън организациите, а не вътре в тях. Съществуват и достатъчно голям брой вътрешни източници на киберзаплахи. Например, недоволен служител би могъл да откридне, изтрие или модифицира ключова информация и в зависимост от правата му (нивото на достъп), това би могло да засегне изключително сериозно дадена организация. Вътрешните киберзаплахи, свързани с човешките ресурси, са най-общо два вида – умишлени и неволни. И двата вида годишно причиняват значителни щети на организациите в световен мащаб.

Новото лице на риска

Деянието по реализиране на риска от определена киберзаплаха се нарича кибератака. За разлика от киберзаплахите, които биха могли да бъдат неумишлени – вследствие на недостатъчна образованост или квалификация, както и поради ненавременно предприето действие на някой служител или случайна повреда в ключов хардуер, кибератаката винаги е умишлена. Тя е криминално деяние, което има мотив и план как да се извърши.

Кибератаката има по-голям шанс да бъде успешна отколкото реализирането на една киберзаплаха точно защото е умишлена и добре планирана. В таблица 2 са показани най-честите кибератаки за 2020 г.

Таблица 2

Статистика на основните кибератаки за периода 2018 – 2020г⁹

Кибератака	Описание
SQL инжекции (SQL injections)	26% ръст в кражбите от базите данни на малките и средни бизнеси в глобален мащаб
Социално инженерство (Social Engineering)	98% от кибератаките разчитат на социално инженерство
Нарушаване на целостта на данните (Data Breach)	47% от този вид атаки са насочени към банкови институции
Измами с банкови карти (Payment Card Fraud)	212% ръст на компрометираните банкови карти от 2018 до 2020 г.
Отказ на услугата (Denial of Service)	8% ръст на атаките от този тип към финансови институции за 2020 г.
Атаки от типа нулев ден (Zero Day Attacks)	14% ръст на атаките от този тип в рамките на 2020 г.

Често срещани кибератаки са от типа отказ от услуга или дистрибутиран отказ на услугата (Distributed Denial of Service). Разликата между тях е, че при втория атакуващите агенти са много и на различни места. Понякога изпълнението на злонамерен код прави възможно дори даден човек да не знае, че неговият компютър или електронно устройство участва в дистрибутирана атака за отказ на услуга.

Кибератаките могат да бъдат политически и/или финансово мотивирани. Основната им цел е да се открадне ценна информация, да се прекъснат основни бизнес услуги, да се нанесе тежък удар върху репутацията или да се причини финансова загуба на дадена организация.

От статистиката във таблица 2 се вижда огромен ръст в кибератаките, свързани с измами с банкови карти, следвани от атаките с цел нарушаване целостта на данните, които отново са насочени предимно към компании опериращи във финансовия сектор. Финансовите институции са понесли 85 организирани кибератаки за отказ на техни ключови услуги в рамките на 2020 г. Киберпрестъпниците крадат информация и от бази от данни посредством т.нар. SQL инжекции. На свой ред социалното инженерство е важен компонент за набирането на ценна информация за таргетираните човек, компютър и организация. Кибератаките отдавна не са насочени само към компрометиране на компютърни системи – те са насочени към всяко устройство, върху което работи някаква операционна система, включително смартфони, таблети, дори игрови конзоли и IoT устройства като контролери за климатици, осветление, камери за наблюдение у дома и офиса и други.

Освен към финансовия сектор, кибератаки са насочени и към всички останали индустрии като здравеопазване, образование, държавни и общински организации, транспорт и т.н. В глобален мащаб, след финансовия сектор, секторът на здравеопазването е най-потърпевш. Киберпрестъпниците се интересуват от медицински и здравни досиета, номера на социални осигуровки (особено актуални в САЩ) и лични данни. От началото на COVID-19 пандемията до края на 2021 г. е отбелязан 238% ръст на кибератаките в този сектор. От всички тези статистики може да се заключи, че текущата ситуация, свързана с киберсигурността, е изключително сериозна.

Киберсигурността защитава хората и организациите от злонамерени актове на киберагресия по същия начин, по който физическата охрана обезпечава спокойствието и комфорта на тези организации от физически заплахи. Киберсигурността следва да обхваща критичните данни, ресурси, активи и да

гарантира репутацията на една организация. Целта е организацията да бъде сигурна в киберпространството с гаранции за предотвратяване на загуба на критични данни и финансови активи, а вследствие на това – репутацията ѝ да не понася удари.

Инцидентите, свързани с пробиви в киберсигурността, са политически или финансово мотивирани и целят всички критични сектори в икономиката на една държава. Например финансовият сектор, секторът на здравеопазването, образованието, тежката и леката промишленост и т.н. са еднакво критични и важни за една нация. В някои случаи, злонамерени, външни за съответната държава, действия целят спирането на цялата икономика в тази държава.

Освен данните на дадена организация, инцидентите с киберсигурността могат да застрашат нормалното функциониране на комуникационните канали, енергийното осигуряване и критичната инфраструктура – това бързо може да се разрасне до национално ниво или дори ниво на група от държави¹⁰, в зависимост от мащаба на атаката и слабостите в системите, от които атакуващите са се възползвали. Кибератаки към електропреносната мрежа, енергийния сектор и държавните бази данни с критични за населението данни също не са рядкост. Като пример от България може да се посочи пробивът в НАП през 2019 г, при който бяха откраднати личните данни на над пет милиона души.

Нов прочит на традиционната методология за управление на риска

От всичко казано до тук може да се направи еднозначно заключение, че не съществува организация, която да е имунизирана срещу кибератаки и за която не съществуват рискове, свързани с нейната киберсигурност.

Определението за риск, свързан с киберсигурността, не е много по-различно от определението за риск в общия смисъл на думата. От общоприетите дефиниции за киберсигурност и риск може да бъде компилирано определение, което да звучи по следния начин: *това е вероятност от компрометиране на чувствителна информация или теч на данни в резултат на злонамерена дейност*. От гледна точка на организациите, рисковете свързани с киберсигурността са от потенциална загуба или увреждане вследствие на кибератаки на критичната инфраструктура на организацията.

Основните рискове за киберсигурността на организациите са класифицирани от лабораторията по рискове, свързани с киберсигурността на Националния институт по стандарти и технология на САЩ и са представени в таблица 3:

Таблица 3¹¹

Рискове, свързани с киберсигурността, идентифицирани от NIST IT лаборатория

Сериен №:	Риск, свързан с киберсигурността	Организация ¹²	Номер на риска от класификатора на NIST
1	Злонамерен код	DHS	ST18-004
2	Деструктивен злонамерен софтуер	DHS	ST13-003
3	Скрити заплахи: набор от средства за получаване на пълни права на администратор; автоматизиран злонамерен софтуер	DHS	ST06-001
4	Фалшив антивирусен софтуер	DHS	ST10-001
5	Скрити заплахи: повредени файлове	DHS	ST06-006
6	Криптовирус	FTC	-
7	Шпионски софтуер	DHS	ST04-016

8	Атаки по отказ на услуга	DHS	ST04-015
9	Фишинг	FTC	-
10	Фалшиви бизнес email-и	FTC	-
11	Неоторизирани устройства в мрежовата инфраструктура	DHS	ST18-001
12	Фалшиви уебсайтове	DHS	ST18-006
13	Компрометиран безжични мрежи	DHS	ST05-003
14	Компрометиран смартфони и таблети	DHS	ST06-007

Всеки от типовете рискове, индексирани в таблицата, подлежи на специфично третиране от организациите.

От горното определение за киберриск, цикълът на живота на всеки риск, свързан с киберсигурността може да бъде описан с формулата:

$$\text{киберриск} = \text{киберзаплаха} \times \text{киберуязвимост}$$

Според тази формула обаче когато няма уязвимост (уязвимостта е образно казано нула), няма и риск. Това е теоретична постановка, тъй като в реалния живот всичко е уязвимо по един или друг начин. Съществува и напълно реален сценарий, който предполага наличието на една или множество уязвимости в системата, но няма реална заплаха, тъй като те не са известни на атакуващия. Следователно, намаляването на заплахите или уязвимостите директно води и до намаляване на риска.

Най-общо рисковете, свързани с киберсигурността, се управляват по аналогичен начин като всички други рискове. Процесът по управление минава през следните стъпки:

- анализ;
- избор на действие за справяне с риска;
- последващо наблюдение.

Това, по което управлението на киберрисковете се отличава значително от управлението на конвенционалните рискове е не в методологията, а в техниките и инструментите. Например, процесът на риск анализа на киберрисковете е сходен с този при конвенционалните рискове – следва се т.нар. *тристъпкова процедура*¹³, която включва:

- (1) идентификация на критичните ресурси;
- (2) определяне на заплахите, които биха могли да доведат до възползване от уязвимостите в системите, обслужващи критичните ресурси;
- (3) оценка и определяне на рейтинг на съответния риск.

При тази тристъпкова процедура анализът на риска започва с *идентификация на критичните ресурси* – дотук, нищо по-различно от анализа на традиционните рискове. При управлението на киберрисковете обаче критичните ресурси се различават от тези при традиционните рискове. Това са типично мрежови устройства и компоненти, електронни документи, бизнес услуги, процеси и дейности, информация относно мрежовата топология и архитектура, системна информация, лични данни и т.н.

Важно е да се подчертае, че данните, съхранявани на „облак“ също биха могли да представляват критичен ресурс. Това, че се съхраняват по различен начин, не ги прави повече или по-малко критични. Разбира се, кое е по-силно или по-малко критичен ресурс се определя от вида на бизнеса.

При *определянето на заплахите*, които биха могли да доведат до възползване от уязвимостите в системите, обслужващи критичните ресурси се извършва т.нар. *мапинг* между рисковете и ресурсите, от една страна и заплахите и уязвимостите, от друга. Рискът се изразява като отношение между заплахата и уязвимостта, но винаги се асоциира с ресурс (актив). Идентифицираните рискове се анализират с цел тяхното остойностяване и по този начин се постига единна мярка, която служи като критерий за тяхната оценка. За да бъдат идентифицирани уязвимостите и заплахите се използват различни методи и техники, основната част от които са свързани с: разглеждане на доклади от вътрешни одити, документации с извлечени поуки (*lessons learned*) от проекти или инциденти, доклади от тестове на системите и т.н.

Оценката на рисковете и *определянето на риск рейтинг* е третата и последна стъпка от модела. Тя включва няколко дейности, свързани с определянето на въздействието на риска и вероятността той да се случи на практика.

Съществуват два подхода за оценяване на рисковете – единият е количествен, а другият – качествен. Когато се говори за киберрискове, точният количествен подход е изключително труден, тъй като за адекватното му използване е необходимо наличието на много финансово-отчетна информация, на базата на която да се направи анализът. Освен това, не трябва да се подценява субективният фактор в качественния подход. От друга страна е трудно и точното количествено оценяване, когато става въпрос за нематериални активи и тяхната загуба, като информацията или ноу-хау.

Въпреки че количественият подход е предпочитан, защото е много по-лесно да се работи с точни стойности, това е почти невъзможно в областта на информационната сигурност. Затова се използва подходът за трансформиране на качествените показатели в количествени чрез преобразуване и полагане на стойности. Най-често използваният инструмент в този случай е т.нар. *матрица на въздействието и вероятността* (англ. probability and impact matrix), при която по абсциса – от нула до 100%, се оценява въздействието, а по ордината – от нула до 100%, се оценява вероятността. След това съответните рискове се поставят в матрицата, която с цел по-практичното им управление, се разделя на квадранти, които образуват зони.

Най-типично организациите разделят рисковете на три зони – червени, оранжеви (или жълти) и зелени, съответно свързани с висок, среден и нисък риск. Рисковете, които попадат в зелените зони се наблюдават, без да се предприемат действия по тях. Рисковете, които попадат в другите две зони се обработват, като най-приоритетно се третира попадащите в червената зона. Матрицата на въздействието и вероятността е традиционен метод, използван широко не само при киберрисковете, но и при оценката на всякакъв вид рискове. Тя си има своите недостатъци, особено когато става въпрос за голяма организация с множество различни бизнеси и дълъг списък от критични ресурси и активи.

При оценката на киберрисковете се препоръчва използване на т. нар. клъстерни алгоритми. Клъстерните алгоритми спомагат за типизирането на дадени рискове по сходни характеристики и разглеждането им заедно, без значение от степента на въздействие и вероятността даден риск да се случи.

При клъстерните алгоритми водещи са оценките, свързани с финансовите загуби на организацията, а именно:

- кражба на интелектуална собственост;
- директни загуби;
- компрометирани устройства;
- съдебни и извънсъдебни плащания и глоби;
- загуба на репутация.

Изводи

Въпреки краткия обзор на основните рискове, които съпътстват дигиталната трансформация, изложението в този доклад позволява да се направят няколко обобщаващи констатации:

На първо място може да се отбележи стартираният процес по тоталната дигитализация във всички сектори на икономиката, без значение в коя група попада дадената организация – дигитална организация, дигитален хибрид или конвенционална организация. Въпреки че някои организации са по-податливи на цифровизация в сравнение с други, не съществуват такива, които да не могат да дигитализират поне един свой процес.

От горното може да се изведе и *вторият извод*, а той е свързан с невидимите заплахи, съпътстващи дигиталната трансформация. Невидимите заплахи предполагат създаване на нов вид мерки за защита, ранно идентифициране на потенциални уязвимости, които биха могли да доведат до конкретни опасности. Необходимостта от инвестиции в киберсигурност е извън всякакво съмнение. Организацията трябва да изгради процеси, които да могат адекватно да определят заплахите и да създават контрамерки за тяхното неутрализиране или смекчаване до приемливо ниво.

Третият извод, който може да бъде направен е, че при управлението на киберрисковете методологията до голяма степен остава същата, както при традиционните рискове. Това, което се променя, е не самата методология, а техниките и инструментите: въвеждат се клъстерни алгоритми за групиране на рисковете по сходни признаци с цел по-доброто им управление; фокусът се измества от

риска като такъв към активите, които касаят и очаквания негативен резултат от неговата реализация, засягащ предимно финансовите показатели на дадена организация, понасяща директни загуби, кражба на интелектуална собственост, съдебни и извънсъдебни плащания и глоби, компрометирани мрежови устройства, което в съвкупност неминуемо води до загуба на репутация като най-ценния актив на всяка организация.

БЕЛЕЖКИ

1. Digitation – процесът по миграция от традиционните хартиени към цифрови документи.
2. Digitalization – процесът по използване на вече цифровизираната информация за образуване на ефективни и ефикасни бизнес процеси.
3. Financial Technology (финансови технологии) като термин първоначално се използва за описание на програмни интерфейси и услуги, осигуряващи управлението и обработката на информация при работата с масиви от данни от страна на финансовите институции (т.нар. back-ends). От края на първото десетилетие на XXI век, значението му се разширява и с него вече се назовава всяка технологична иновация във финансовата сфера Fintech Definition (Investopedia 2018) <https://www.investopedia.com/terms/f/fintech.asp>.
4. Needham, Mass. *New IDC Spending Guide Shows Continued Growth for Digital Transformation as Organizations Focus on Strategic Priorities*. IDC, November 2021.
5. Gartner. *CIO Agenda, 2020*. <https://www.gartner.com/en/information-technology/insights/cio-agenda>
6. Deloitte. *Managing Risk in Digital Transformation*. January 2018, p. 7.
7. Фишинг (англ. phishing – нарочно променено от fishing – риболов) е злонамерен опит за придобиване на чувствителна информация като потребителско име, парола и детайли на кредитна карта, като извършителят приема чужда самоличност при електронни комуникации. (Handbook of Information and Communication Security).
8. Yahoo Finance [online] available at: <https://finance.yahoo.com/news/2021-gone-phishing-tournament-phishing-110000499.html>
9. Purplesec (Cyber Security Services) [online] available at: <https://purplesec.us/cyber-security-trends-2021/>
10. Слатински, Н. *Петте нива на сигурността*. София: Военно издателство, 2010, с.9.
11. Национален институт по стандартизация и технологии. достъпно на: <https://www.nist.gov/>
12. DHS – Department of Homeland Security; FTC – Federal Trade Commission.
13. Kaur, G., Ziba H. Lashkari, Arash H. Lashkari. *Understanding Cybersecurity Management in FinTech*. Springer, 2021, p. 111.

Европейска декларация относно цифровите права и принципи за цифровото десетилетие. Брюксел, Европейска комисия, 21.06.2022.

Национален стратегически документ „Цифрова трансформация на България за периода 2020 – 2030 г.“. София: Министерски Съвет на Република България, 21.07.2020.

Слатински, Н. *Рускът: новото име на сигурността*. София: Изток-запад, 2019.

Laserfiche. *Digital Transformation Model white paper*. <http://hemingwaysolutions.net/wp-content/uploads/2017/08/digital-transformation-model.pdf>

Stavroulakis, P. M. Stamp. *Handbook of Information and Communication Security*. Berlin: Springer-Verlag, 2010.

REFERENCES

1. Digitation – the process of migrating from traditional paper to digital documents.
2. Digitalization – the process of using already digitised information to form effective and efficient business processes.
3. Financial Technology as a term is originally used to describe programming interfaces and services that provide information management and processing for the handling of data sets by financial institutions (so-called back-ends). Since the end of the first decade of the 21st century, its meaning has expanded to refer to any technological innovation in the financial sphere. Fintech Definition (Investopedia 2018) <https://www.investopedia.com/terms/f/fintech.asp>.
4. Needham, Mass. *New IDC Spending Guide Shows Continued Growth for Digital Transformation as Organizations Focus on Strategic Priorities*. IDC, November 2021.
5. Gartner. *CIO Agenda, 2020*. <https://www.gartner.com/en/information-technology/insights/cio-agenda>
6. Deloitte. *Managing Risk in Digital Transformation*. January 2018, p. 7.
7. Phishing is a malicious attempt to obtain sensitive information such as username, password and credit card details by the perpetrator assuming someone else's identity in electronic communications. (Handbook of Information and Communication Security).
8. Yahoo Finance [online] available at: <https://finance.yahoo.com/news/2021-gone-phishing-tournament-phishing-110000499.html>
9. Purplesec (Cyber Security Services) [online] available at: <https://purplesec.us/cyber-security-trends-2021/>
10. Slatinski, N. *Pette niva na sigurnostta*. Sofia: Voenno izdatelstvo, 2010, p.9.

11. Natsionalen institut po standartizatsiya i tehnologii. dostapno na: <https://www.nist.gov/>
 12. DHS – Department of Homeland Security; FTC – Federal Trade Commission.
 13. Kaur, G., Ziba H. Lashkari, Arash H. Lashkari. *Understanding Cybersecurity Management in FinTech*. Springer, 2021, p. 111.
- ***
- Evropeyska deklaratsia otnosno tsifrovite prava i printsipi za tsifrovoto desetiletie*. Bussels, EC, 21.06.2022.
- Natsionalen strategicheski dokument „Tsifrova transformatsia na Bulgaria za perioda 2020 – 2030 g.“*. Sofia: Ministerski Savet na Republika Bulgaria, 21.07.2020.
- Slatinski, N. *Riskat: novoto ime na sigurnostta*. Sofia: Iztok-zapad, 2019.
- Laserfiche. *Digital Transformation Model white paper*. <http://hemingwaysolutions.net/wp-content/uploads/2017/08/digital-transformation-model.pdf>
- Stavroulakis, P. M. Stamp. *Handbook of Information and Communication Security*. Berlin: Springer-Verlag, 2010.

110 ГОДИНИ ТРАДИЦИЯ, КАЧЕСТВО, ПРЕСТИЖ

Сборник доклади от Годишна научна конференция – Част II
12 – 13 април 2022 г., София

Българска
Първо издание

Отговорен редактор
Николай Кънчев

Редактори
Иван Павлов
Катерина Антонова

Графичен дизайн
Георги Кирилов

Формат 70x100/16

110 YEARS OF TRADITION, QUALITY, PRESTIGE

Proceedings of the Annual Scientific Conference – Part II
12 – 13 April 2022, Sofia

Bulgarian
First edition

Managing editor
Nikolay Kanchev

Editors
Ivan Pavlov
Katerina Antonova

Graphic design
Georgi Kirilov

Format 70x100/16

ISBN (online): 978-619-7478-94-5
ISBN (print): 978-619-7478-97-6