ISSN 2522-9842 (online)

Public organization
Ukrainian Scientific Community

Journal of Scientific Papers

Social Development *and* Security

Volume 14, Issue 5, October, 2024

OPEN ACCESS
https://paperssds.eu/index.php/JSPSDS/

FOUNDERS and PUBLISHER: Public Organization "Ukrainian Scientific Community" (Ukraine)

Executive secretary of the editorial board of the Journal of Scientific Papers "Social Development and Security" Mykola Tkach,
e-mail: tim68@ukr.net; tkachivan9@gmail.com https://paperssds.eu/index.php/JSPSDS/, тел. +38(093) 752-81-56

TABLE OF CONTENTS

ЗМІСТ

The future of warfare. Anticipated changes in military trends

Майбутнє війни. Передбачувані зміни у військових трендах

Arif Hasanov [A]
PhD in National Security and Military Sciences, Assoc. Prof., e-mail: arif.h.hasanov@gmail.com, ORCID: 0000-0002-8814-1590

Rashad Tahirov [A]
PhD in national security and military sciences, e-mail: rashad_tahirov1975@yahoo.com, ORCID: 0000-0003-1936-152X

Khayal Iskandarov [A]
PhD in National Security and Military Sciences, e-mail: xayal1333@gmail.com, ORCID: 0000-0001-8975-6530

[A] National Defence University, Republic of Azerbaijan

Аріф Гасанов [A]
Кандидат наук з національної безпеки та військових наук, доцент, e-mail: arif.h.hasanov@gmail.com, ORCID: 0000-0002-8814-1590

Рашад Тахіров [A]
Кандидат наук з національної безпеки та військових наук, e-mail: rashad_tahirov1975@yahoo.com, ORCID: 0000-0003-1936-152X

Хаял Іскандаров [A]
Кандидат наук з національної безпеки та військових наук, e-mail: xayal1333@gmail.com, ORCID: 0000-0001-8975-6530

[A] Національний університет оборони, Азербайджан

Received: September 6, 2024 | Revised: October 20, 2024 | Accepted: October 31, 2024

DOI: 10.33445/sds.2024.14.5.1

Purpose: to discuss the changes in the scientific and technical field, and examine their impact on military art.

Method: comparative analysis, and synthesis.

Findings: Today's military and political realities require the Armed Forces to be ready for wars that may occur at any time, including in the future, in order to ensure the country's national security. Because, as in the past, the struggle for natural resources, competition between states, aspirations for hegemony, as well as ideological differences and security concerns, which lead to military conflicts, will continue in the future. At the same time, the great progress achieved and expected in the field of technology will significantly change the traditional forms and methods of fighting. The study and skillful application of these forms and methods in the Armed Forces will be one of the main conditions for success in future wars. Scientific and technical progress affects all areas of human activity without exception, and has a noticeable effect on the development of methods and forms of war. In the future, the content and typology of military operations, strategy and tactics, forms and methods of application of armed forces will be formed under the influence of scientific and technical progress, mainly in the fields of artificial intelligence, biotechnology, and nanotechnology. For this reason, in order to study the nature of future wars, to predict the methods and forms of military operations, the article considers the causes of wars, discusses the changes in the scientific and technical field, and examines their impact on military art.

Theoretical implications: The paper enhances our understanding of significant transformations due to advancements in technology, changes in geopolitical dynamics, and evolving societal expectations, against the backdrop of the extensive use of autonomous systems, including drones, unmanned vehicles, and AI-powered decision-making tools.

Practical implications: The paper contibutes to the development of military strategies and operational plans, which consider how technological, social, and geopolitical changes will concretely affect the future warfare.

Value: The study offers significant value in understanding and predicting the nature and character of future warfare and provides multiple lenses through which to analyze the war and devise strategies in line with emerging security threats.

Paper type: theoretical.

Key words: war, politics, peace, conflict, contradiction, strategy, hybrid.

Мета: обговорити зміни в науково-технічній сфері, дослідити їх вплив на військове мистецтво.

Метод дослідження: порівняльний аналіз, синтез.

Результати дослідження: Військово-політичні реалії сьогодення вимагають від Збройних Сил бути готовими до воєн, які можуть виникнути в будь-який час, у тому числі й у майбутньому, задля забезпечення національної безпеки країни. Тому що, як і в минулому, боротьба за природні ресурси, конкуренція між державами, прагнення до гегемонії, а також ідеологічні розбіжності та проблеми безпеки, які призводять до військових конфліктів, триватимуть і в майбутньому. Водночас великий прогрес, досягнутий і очікуваний у галузі техніки, суттєво змінить традиційні форми та методи боротьби. Вивчення і вміле застосування цих форм і методів у Збройних Силах буде однією з головних умов успіху в майбутніх війнах. Науково-технічний прогрес зачіпає всі без винятку сфери людської діяльності, помітно впливає на розвиток методів і форм ведення війни. У майбутньому зміст і типологія військових дій, стратегія і тактика, форми і методи застосування збройних сил будуть формуватися під впливом науково-технічного прогресу, головним чином у сферах штучного інтелекту, біотехнологій і нанотехнологій. Тому з метою вивчення характеру майбутніх воєн, прогнозування методів і форм військових дій у статті розглядаються причини воєн, обговорюються зміни в науково-технічній сфері та їх вплив на військове мистецтво.

Теоретична цінність дослідження: стаття покращує наше розуміння значних трансформацій, спричинених прогресом у технологіях, змінами геополітичної динаміки та еволюцією суспільних очікувань на тлі широкого використання автономних систем, зокрема дронів, безпілотних транспортних засобів та систем прийняття рішень на основі штучного інтелекту. виготовлення інструментів.

Практична цінність дослідження: стаття сприяє розробці військових стратегій та оперативних планів, які розглядають, як технологічні, соціальні та геополітичні зміни конкретно вплинуть на майбутню війну.

Цінність: дослідження пропонує значну цінність у розумінні та прогнозуванні природи та характеру майбутньої війни, а також надає різні позиції, через які можна аналізувати війну та розробляти стратегії відповідно до нових загроз безпеці.

Тип статті: теоретичний.

Ключові слова: війна, політика, мир, конфлікт, протиріччя, стратегія, гібрид.

Introduction

The first record of war dates back to about 5,000 years ago and remains a part of human history to this day. Historical events show that no generation and country is immune from the threat of war, and this threat remains one of the most urgent problems in the world. In general, war is a negative phenomenon that disturbs people's peace, lowers the standard of living and causes radical changes in society. Because wars mean fighting, arms, death, suffering and destruction. However, it is noted by some researchers that wars play a positive role in the development of the country. Thus, wars accelerate the development of new technologies, stimulate economic growth and the creation of new jobs. For example, after World War II, the number of both women and foreign nationals working in heavy industry increased significantly. War unites a country's citizens against a common enemy, leading to national self-awareness and awakening. In addition, the armed forces gain some combat experience in military operations. However, the negative aspects of war, the damage it causes to countries are more and therefore undesirable.

Although wars are undesirable in the modern world, the use of military power still plays an important role in resolving conflicts in the system of international relations. Despite the norms of international law, some states do not hesitate to use force against the territorial integrity and political independence of another state, citing various excuses. In our opinion, this trend will continue in the future. Thus, the country's existence as an independent entity in the present and future world, its ability to protect its territorial integrity and interests from possible threats largely depends on its readiness for armed conflicts. This in turn requires the analysis of both past and current wars and the prediction of the forms and methods of future military operations.

In the analysis and forecasting of wars, it is important to study the experience of developed countries, their successes in military operations, as well as the reasons for their failures. However, the imitation of past experiences without deep analysis results in repetition of the same mistakes or failures. In many cases, the states give preference to the number of personnel, weapons and equipment, and do not pay enough attention to the introduction of new methods and forms of warfare. In the Second World War, France, despite being strong in terms of weapons and technology, was defeated by Germany in a short time because technical innovations were not taken into account in France's military doctrines and it remained attached to the combat forms, methods and rules of the First World War (Beverelli, 2020). A similar mistake was made by the political and military leadership of Armenia during the 44-day Second Karabakh war. There is a number of papers dedicated to the Second Karabakh war and present it as a generation war (Guner, et al., 2022; Iskandarov & Gawliczek, 2021a; Iskandarov & Gawliczek, 2021b; Iskandarov & Gawliczek, 2020c; Iskandarov et al., 2022). For this reason, we believe that the development of forms and methods of war is closely related to scientific and technical progress. Along with the adoption of new weapons and equipment, it is important to study their effective application. If the methods and forms of effective application of new weapons and equipment are not worked out, it is of course difficult or even impossible to achieve great results.

As mentioned, the development of science and technology greatly affects the planning and waging wars. For example, firearms such as cannons, rifles, pistols, and machine guns, created as a result of the invention of gunpowder, revolutionized military affairs and significantly changed the methods and forms of warfare (Walsh, 2023). Similarly, trains, tanks, airplanes, and new types of ships emerged due to the invention of steam engines and internal combustion engines, significantly increased the speed and depth of warfare, as well as expanded its scope. The development of nuclear physics giving impetus to the creation of nuclear energy revealed new laws and principles of war and consequently led to the discovery of nuclear weapons, which had a great destructive force. Fuzzy logic theory has encouraged the development of artificial intelligence capable of making decisions in complex and messy environments, as well as conducting various operations without

human intervention. As a result, semi-autonomous controlled weapon systems were created. In this direction, ongoing researches and tests show that autonomously controlled weapons and equipment will be used in battles in the near future. According to several military analysts, future conflicts will usually not have a front and rear, and the defending side may occasionally launch an attack ahead of the aggressor. Is there truly going to be an aggressor? Ultimately, the challenging encounters of the future will take place in new settings. In addition, armies will fight opponents who are members of unidentified alliances. Strange wars also occur where there are unknown foes. These include confrontations in diplomacy, internal civil conflicts, behavioral, informational, financial, economic, and technological battles, in addition to armed engagements on conventional battlefields (Brychkov et al., 2019).

There is a number of studies dedicated to the nature and character of future warfare. For instance, Brychkov et al. (2019) predict certain features of upcoming wars and armed conflicts based on their examination of the military-political environment globally, the US National Security Strategy, and US military planning documents. According to the authors, asymmetric and indirect activities are becoming more common, armed conflicts are moving into cities and other inhabited areas, and irregular formations are being used more widely. The US officer Amos C. Fox presents the principles for the future of warfare and their roles in the changing landscape (Fox, 2024). The author suggests that army concepts and doctrine need to change as we go from a human-centric to a potentially artificial intelligence-dominated future of warfare that will feature human-machine integrated formations and a myriad of autonomous systems. Therefore, the cooperation among concept developers, doctrine developers, science and technology specialists, and force designers is necessary to provide workable concepts and designs for future forces that incorporate the most important elements of emerging technology while keeping in mind the ongoing difficulties of ground combat. Following the war, which broke out between Russia and Ukraine in early 2022, Tim Sweijs and Jeffrey H. Michaels (2024) have provided the first thorough update and revision of theories regarding the future of warfare. The authors argue that the war has radically changed our understanding of the nature and character of war in the future, but also caution against marginalising many other parallel trends, types of war, and ways of waging them. Mark A. Milley and Eric Schmidt (2024) claim that even the most powerful Army of the World – the US Army is not ready for future wars. Against the backdrop of evolving nature of warfare, Tughral Yamin (2021) presents a radical approach and highlights the necessity of a break from the past and suggests that national leaders and military commanders need to devise new concepts of defense policy that are in line with the emerging threats. However, our study will focus more on the changes in the scientific and technical field and their impact on military art and modern battlefield.

Results

Root causes of wars. Retrospective analysis

Analysis has shown that only eight percent of the current human history has been a period of peace (Hedges, 2003). However, the reasons for the outbreak of war or armed conflict have been different at various times. The situation in Ukraine has brought to light the basic distinctions between two opposing parties, namely Russian and Western conceptions of Euro-Atlantic security, especially with regard to the post-Cold War Euro-Atlantic security framework (Sadiyev & Iskandarov, 2018). Even some scholars suggest that a New Great Game had already begun between the parties. The disintegration of the Soviet Union created a security and influence vacuum, opening up a large amount of “new” territory to potential outside actors and providing the rationale for this New Great Game. There are geographical variances and differences, thus it is important to use caution when using the analogy universally. In addition to troops, European explorers also played a significant role

in the original Great Game, which aimed to conquer and dominate uncharted area. Process was motivated not only by military conquest and territorial expansion but also by a strong desire to establish new trade and markets. Thus, commercial penetration in addition to diplomatic maneuvering. In the New Great Game, trade serves as a tool for both economic reward and coercion, and aid is disguising itself as investment and a way to influence regional politics. In the ancient Great Game, two opposing forces with a parallel but non-contiguous boundary grew closer to one another across an area that was regarded as no-man's land. In the "New Great Game", Russia aims to keep a buffer zone by continuing to exert influence over Western nations. These observations shed light on several important distinctions between the Old and New Great Games, as well as the origins and strategies of the power struggle (Iskandarov & Gawliczek, 2020d). Russia will pull out all the stops in order to exert its influence in its "near abroad" and reassert itself as a dominant power. The only way for the countries (in Russia's so-called "near abroad" is to strike the right balance between the West and Russia, because the latter does not seem to want to give up its political ambitions in the region. But cooperation with NATO has the utmost importance for all three countries in its "near abroad" (Nasirov et al., 2017). Some researchers argue that war is caused by economic, religious and political reasons. Others think that most wars in our time are fought for ideological reasons. In general, the causes of wars are grouped under two approaches: traditional and modern theories (Coccia, 2019). According to the traditional theory, the reason for the outbreak of war is the disruption of the social and economic balance between different nations, states, societies, as well as ethnic and religious groups. The conflict that occurs as a result of the violation of the balance leads the states to use violence. Proponents of this theory believe that war is a manifestation of violence inherent in human nature. According to Thomas Leviathan, a great philosopher who lived in the 17th century, people tend to use violence for the sake of their needs and interests, as well as when those interests are threatened (Finucane, 2013). Since the state and social groups are formed by people who have similar needs and interests in a certain area, they are a means for realizing their wishes. For this reason, a state or a separate social group tends to use violence against other states, political, religious, and ethnic elements, which it considers to be an obstacle or a threat to the fulfillment of its needs or the realization of its interests. This violence involves taking preventive and violent measures to meet growing needs or to protect interests. In the future, it is predicted that the conflict of interests will continue for various reasons and there will be new wars. According to Yakov Novikova, one of the representatives of the traditional theory, in many cases, armed conflicts and wars between different ethnic, ideological and religious groups continue and are repeated due to historical reasons that create a force of inertia in society (Coccia, 2019).

According to the modern approach, the reason for the emergence of war is the irrational solution of conflicts between subjects (state, ethnic, religious groups, etc.). According to this approach, conflicts have always existed, but sometimes decisions are made based on emotion or instinct when there are rational ways to resolve them and achieve peace. For example, in Armenia, which was defeated in the 44-day Patriotic War and whose army was destroyed, it is an irrational and dangerous behavior to carry out revanchism actions after the war and to refuse to sign a peace treaty with Azerbaijan. Because the opinions that the next time if the war breaks out between Azerbaijan and Armenia, the latter will suffer a heavy defeat and will end its existence have been repeatedly voiced by the leading military experts.

The successful anti-terrorist operations carried out by Azerbaijan in Karabakh after the war are proof of this (Hasan et al., 2024). If Armenia acts rationally and signs a peace treaty with Azerbaijan it will allow Erevan to join regional and international projects and get additional income. For this reason, the actions of revanchism in Armenia are not understandable. Representatives of the modern approach believe that geopolitical ambitions, the influence of chauvinist forces inside the country, failure in negotiations and domestic politics, the desire to expand the sphere of

influence of great powers are the main reasons for irrational thinking and modern wars (Matthew & Massimo, 2009).

Both of the above reasons are directly related to the human factor, its nature, as well as the result of its activity. In our opinion, the scientific and technical revolution expected in the future, mainly as a result of artificial intelligence replacing humans in many fields, will cause inter-country war or armed conflict without human will. For instance, it is a possible scenario in which artificial intelligence integrated into the strategic defense systems of any country may mistakenly assess the activities of another country as a real threat and make a decision to launch a pre-emptive strike.

Thus, the analysis of both traditional and modern approaches shows that the use of violence, including military force, is no longer one of the main means of resolving conflicts in the international world. In our opinion, in the future, there will be an increase in the number of wars on ethnic grounds compared to economic and ideological ones. In his book "The Clash of Civilizations", the American sociologist and political scientist Samuel Phillips Huntington notes that, as long as there are nations and groups belonging to different civilizations, conflicts in the world are inevitable, and this, in turn, will lead to the emergence of new wars (Assumpção, 2020).

As mentioned, along with the evolution of the social structure in human history, the characteristics of war are constantly changing. When we talk about the characteristics of the war, we mainly understand its cause, course and termination. This trend is evolving depending on domestic and foreign policy, system of social and international relations, new types of weapons and equipment. As a result of development, new methods and forms of inter-state struggle, including war, come to the fore.

Currently, the technological revolutions taking place in the field of bio, nano, material, artificial intelligence and information, on the one hand, have caused significant positive changes to human life and health, the quality of working conditions, and on the other hand, the uneven distribution of opportunities between states and within the country and increased tensions resulted in new armed conflicts and wars. New trends are observed in the conduct of armed conflicts in our time. These trends are inextricably linked to the wide application of new weapons and techniques based on artificial intelligence, information technologies in battles as an effect of rapid development. In our opinion, the widespread use of these weapons and techniques will determine the nature of future wars and significantly differentiate the forms and methods of warfare from the previous ones.

The possible nature of future warfare

Warfare is "the mechanism, method, or modality of armed conflict against the enemy". While war hasn't changed for thousands of years, warfare, specifically, the technology used to conduct war, is constantly changing. It evolved from soldiers with broadswords and bows, to soldiers on horseback with repeating rifles, to soldiers with machine guns, driving tanks, and calling in airstrikes from drones. The current security environment is characterized by rapid changes, unpredictable instability, and complexity. Wars in this modern age are no longer fought on conventional battlefields but asymmetrically over the digital world, cyberspace, social media, etc. Cyberspace is a vital component of the security environment and is essential to enhancing operational capabilities. To put it briefly, cyber security has swiftly transformed from a technical field to a strategic idea, and it is now an essential part of national and economic security policy (Hasanov et al., 2019). This approach to solving "problems" will remain prevalent for the foreseeable future. In addition, digitalization and technology will slowly penetrate all levels of society and private life (Iskandarov & Gawliczek, 2020a). The world witnessed several confrontations in the last decade, where different techniques were employed in pursuit of national objectives. However, these techniques fell far short of physical conflict. This approach does not cross the threshold of war, nevertheless the consequences are dire. The term "hybrid warfare" has dominated much of the

discussions about modern and future warfare since the 2006 Lebanon war. It has been adopted by senior military leaders and promoted as a basis for modern military strategies (Iskandarov & Gawliczek, 2020b). Hybrid warfare theorizes changes in contemporary warfare and contains key assumptions about 4th and 5th generations of warfare. In those types of warfare economic, political and social factors are used to break the opposing leadership. In this situation, military superiority alone is not helpful and knowledge of local culture and history are essential. A key concept in these types of warfare is the exploitation of emerging information technology, which allows non-state military actors to undermine the states' will by affecting the decision makers and the population through the globalized and networked media. Thus, incorporating cultural, social, legal, psychological and moral dimensions into the war makes the wider use of armed forces redundant (Iskandarov & Gawliczek, 2020b).

According to Carl Von Clausewitz, the characteristics of war change depending on circumstances and time like a chameleon (James, 2018). By characteristics, he meant the paradoxical trinity of war: passion, creativity, and politics (Cole, 2020). Passion, as the primary element of war, includes the reactions and hostile actions inherent in human nature, such as hatred, malice, enmity, and violence. Creativity is related to the art of war, the activity of the army, mainly the skills and abilities of commanders in the uncertain and confused environment of war, methods and forms of battle. The third is the rational decisions taken by the government, which turns the war into a tool of politics (Waldman, 2009). Changes in social and political life, cultures, as well as scientific and technological progress give new forms to each of the three mentioned above. As a result, new forms and methods of initiating, conducting and terminating the war appear. If the changes in the social structure of the society, as well as in the systems of political and international relations, mainly affect the first and third elements of the trinity, the scientific and technological progress significantly changes the methods and forms of the battle related to the second element.

The methods and forms of war have always played a key role in achieving the goals of war. The biggest factor on which these methods and forms have depended is weapons and equipment. In the present era, this dependence remains the same. According to an action plan approved by NATO, interoperability has three dimensions: technical (hardware and systems), procedural (doctrine and procedures) and human (language, terminology and training) (Iskandarov & Gawliczek, 2019). All three dimensions are inextricably linked to each other and it will remain all the same as far as the future nature of warfare is concerned. If in previous wars the effect of conventional weapons was measured only by the power of kinetic, chemical and thermal energy, in the future it will be measured by the ability to hit targets with high accuracy and autonomous operation. Based on the latest achievements of fundamental and applied sciences such as advanced information and communication technologies, artificial intelligence, nanoparticle and particle physics, these weapons will lead to radical changes in the methods and forms of battles.

In recent decades, great progress has been observed in the development of the production of new materials, information, communication and biotechnology. This progress has led to the production of new types of weapons, military and special equipment. In our era, the introduction of high-precision weapons based on information, artificial intelligence and other advanced technologies, their installation on unmanned aerial vehicles and other remotely controlled vehicles has significantly changed the nature of battles. These changes brought innovations called "revolution in military art". "Revolution in military art" is related to the emergence of new progressive ideas about the strategic, operational and tactical levels of war, the nature, goals, possibilities and limits of the use of military force, as well as the methods and forms of the battle. In fact, "revolution in military art" is not a new concept. As mentioned above, as military equipment and weapons developed throughout history, the methods and forms of battle also gradually changed. A so-called revolution occurs when the changes are significantly different from the previous ones, when they give a great advantage and a decisive victory to the party who introduced

them, and when there are important political and historical consequences. In the 21st century, humanity approached the threshold of a new revolution comparable to the changes in military art with the mass application of firearms in the 15th-17th centuries. The types of traditional combat, such as attack and defense, which have played a key role in achieving the goals of military operations for many years and require direct contact with the enemy, are fading away.

In new circumstances, the superiority is achieved not by concentrating forces and means in a decisive direction with the maneuver of the troops, but by precise and devastating blows from a distance, without coming into close contact with the enemy. Modern warfare has shown that it is possible to inflict heavy casualties on enemy forces, disable their equipment, and thereby debilitate them without direct contact from a long distance. In addition, the rapid development of artificial intelligence and high technologies and the significant expansion of their scope paves the way for the creation of autonomously controlled weapon systems and special equipment with greater capabilities in the future. Leading scientists predicting the development of techniques and technologies and studying their impact on the course of wars believe that the appearance of battles by the mid-21st century will be shaped by the influence of new discoveries and inventions that will occur in the following fields:

- *High energy physics*. High energy physics (also known as particle physics) is the branch of physics that studies the nature of the particles that make up matter and radiation (Fernow, 2022). High energy physics is one of the fastest growing research fields in the world and occupies an important place in the scientific research of leading countries. We believe that as a result of technological development in this field, weapons based on the use of new physical principles will be improved or new types will be created. These are directed energy (laser) weapons, as well as siper-high frequency and radio-wave, electromagnetic, geophysical and infrasound weapons. The general features of these weapons are that they can be used covertly and suddenly, they can disable electronic systems instantly, and they can destroy manpower without using conventional weapons. Currently, in developed countries, work on increasing the capabilities of these weapons is being continued. The creation of new types of directed energy (laser) weapons and increasing their effectiveness is one of the most successful activities in this field. The achieved success is due to numerous researches conducted in this direction and the emergence of new techniques. To date, leading countries have managed to develop and test directed energy (laser) weapons for various purposes. The US military announced the creation of a prototype of a high-power laser weapon in 2022, and that it will be accepted into service in the coming years (Rodgers, 2024). The biggest advantage of this weapon is that it destroys the target instantly by transferring energy at the speed of light. Due to the directed energy, the accuracy of hitting the target is very high, and this weapon does not make a sound and does not recoil when firing, unlike conventional weapons. The ability to adjust the power of another energy in this allows the weapon to be used for various purposes, such as measuring distance, disabling and destroying the target. Finally, these weapons have almost unlimited firepower, because the number of possible shots depends only on the characteristics of the energy source (Bothwell, 2023). The elimination of the shortage of currently available weapons and the rapid continuation of improvement will increase their effectiveness. In the near future, it is planned to shoot down warplanes, unmanned aerial vehicles, satellites and missiles with an improved laser weapon;

- *Artificial intelligence*. Artificial intelligence is usually defined as the development of computer systems that can perform tasks that require human intelligence, such as visual perception, speech recognition, decision making, and translation between languages (Marcin, 2019). In recent years, great progress has been made in the field of artificial intelligence (AI). Recent advances in this field make it possible to realize what previously seemed like science fiction. Thus, computers, robotics and other techniques working on the basis of artificial intelligence instantly process huge amounts of information and make decisions. Examples of autonomously controlled artificial

intelligence systems without human intervention have already been created and tested. However, with modern artificial intelligence, human-like activities such as thinking, understanding, explaining and posing problems are not yet possible. However, we believe that the improvement carried out on algorithms will increase the capabilities of artificial intelligence in the abovementioned activities in the future.

Considering that all scientific and technological achievements are widely used in military, artificial intelligence will also be integrated into weapons and weapon systems. In recent years, advanced armies have been paying special attention to the development, and application of "smart" weapon systems based on artificial intelligence. It is clear that the combat potential of the armed forces in the future will be determined by the capabilities of "smart" weapon systems. "Smart" weapon systems that will work in sync with the command center will play an important role in all stages of war as a key element of future battles. Thus, "smart" weapon systems will be able to assess the conditions in all depths of military operations and deliver an effective strike independently according to the type of target. Thus, thanks to sophisticated algorithms, the artificial intelligence will make a flexible decision to strike targets based on their type, coordinates and sequence of destruction without human intervention. Compared to artificial intelligence, this activity will take more time when performed even by the most professional people in the command center. However, in modern and future wars, where conditions change rapidly, the time factor is very important in causing damage by fire. It is for this reason that armies with "smart" weapon systems will already have an advantage at the very beginning of the war.

The abovementioned weapon systems are currently under development, but their semi-autonomous samples are already in service. The further improvement of weapon systems operating with artificial intelligence, the creation of autonomous fighting robotics, and the use of high-precision ammunition in those weapon systems will both reduce the loss of manpower and enable the destruction of targets from a long distance. Thus, since the weapon systems controlled by artificial intelligence, including military robotics, will have the capabilities of autonomously identifying the area, face and target, determining coordinates, analyzing the situation and making decisions, firing, it will greatly reduce the direct use of manpower on the battlefield. According to the specialists of the US Department of Defense, artificial intelligence will completely change the principles of armed conflicts, leading to the third revolution in military art after gunpowder and nuclear weapons (Etzioni & Etzioni, 2017). However, it is a strak reality that artificial intelligence will create certain problems for its users. These are problems such as the enemy interfering with the artificial intelligence and directing the weapon against its user, confusing the enemy and friendly forces on the battlefield, attacking the civilian population and objects. In order to achieve success in future wars, it is imperative to solve such problems in the use of artificial intelligence in weapons and equipment.

- *Nano technology.* In fact, nanotechnology has emerged as a result of great advances in bio and material engineering. This technology is related to the field of science dealing with the design, creation and use of new structures, devices and systems by interfering with substances or combinations of substances on a molecular or atomic scale (Matthew, 2024). Nanotechnology enables the development of small, miniature devices with various functions and their use as a system. We believe that military equipment, weapons and equipment developed on the basis of nanotechnology will be widely used in the future. The great progress achieved and expected in this field of technology enables the mass production and application of small-scale military robotics, drones, surveillance devices, as well as lightweight but multifunctional clothing and equipment, body armor and camouflage. In addition, as a result of the development of nano technologies, the dimensions of the active components of modern electronics have been significantly reduced. Along with reducing the size of these components to 0.1 microns or less, their memory capacity has increased to more than 10^{12} bits (Grewal et al., 2020). The speed of modern development in the

field of nanotechnology strongly suggests that these indicators will be further improved in the near future. The widespread application of the achievements in the field of nanotechnology in information and communication technologies shows that in the next two decades, the size of practical memory devices will decrease significantly, and their information processing speed (reading, writing and transmission) will increase by about four times, and the cost will decrease significantly. As a result of these achievements, the mass production and use of various equipment based on artificial intelligence, including small-sized military equipment, unmanned devices such as robotics, will begin. Because the army needs equipment that will independently destroy the enemy and defuse mines and unexploded bombs without risking the lives of its soldiers, as well as without detection.

Integrating artificial intelligence into military mini-robotics and drones will allow them to be deployed en masse on the battlefield and strike autonomously without operator intervention. Due to their small size, it will be difficult to detect and destroy them. At the same time, mini-robotics and drones will operate both independently and in close contact with each other during the execution of the mission, and will have the ability to determine the order of distribution and destruction of targets among themselves. In our opinion, in the future, high-energy physics, as well as the integration of “smart” nano-technologies into small and medium-sized weapons, will significantly increase the ability of these weapons to accurately hit the target. For example, it is planned to equip these weapons and ammunition with a laser designator and a miniature sensor, which will allow them to hit the manpower located in shelters.

- *Information and communication technology*. In our age, information plays an important role against the backdrop of relentless strategic competition between states. Thanks to the revolutionary changes in information technology, power based on information (knowledge) has been added to the power system based on material wealth and physical force. Thus, the first condition for success in the modern world is to obtain important information on time, process it quickly, and make the right decision. The analysis shows that the revolutionary changes in the abovementioned technologies are taking place in two main directions: information processing and information transmission. Today's computers have the ability to store and process large amounts of data at once. In the future, with the advent of quantum computers, the volume and speed of information to be stored and processed is expected to be much greater than today. Unlike ordinary ones, the computers that will work based on quantum mechanics are supposed to process data all at the same time, not one by one. As a result, the processing time will be reduced multiple times. For example, if the most powerful computer in use today needs a billion years to break down a number of 30-40 characters into prime factors, a quantum computer will do the same job in 18 seconds. The revolution in information technology will lead to an exponential increase in the computing power necessary to collect, store, process and analyze large volumes of data. In addition, thanks to this revolution, secret information in various forms (text, audio, video, etc.) will be transmitted and deciphered in real time at any point of the world, to any person, including those participating in military operations. At present, the achievements in the transmission and processing of large-scale information over a single network allow remote control of various operations at the same time. The ongoing development in the field of information and communication technologies indicates that the exchange of information will be much faster in the future than it is today, as well as that more complex operations will be conducted quickly over the network. In such conditions, timely and comprehensively analyzed information will play a major role in ensuring success in all cases. For this reason, continuous control of the information domain at all stages of military operations and maintaining the advantage here will be the main condition for winning future wars. Thus, the commanders who dominate the information domain will get information about the situation in real time. This will allow them to analyze the situation, make the right decision in time, and effectively use forces and resources, including high-precision weapons. All these will change the

traditional methods and forms of fighting. In our opinion, innovations in the field of information and communication, together with other high-tech products, will bring a revolutionary change to military art.

As mentioned, the development of information and communication technologies will lead to revolutionary changes in military art. The integration of high-tech network, computing, surveillance and "smart" technologies into the automated control system of troops allows for the rapid processing of a large amount of various information without operator intervention or with little intervention, predicting the development of operational conditions, simultaneously providing all levels of the battlefield, operation will allow observation of the regions, as well as an effective strike. The development of military network technologies has created the concept of "Network-centric warfare". The concept of this war was first put forward by the US Department of Defense at the end of the 90s of the last centuries, and it is based on the idea of winning the battle thanks to the advantage gained in the information and communication space (Mallick, 2020). In the "network-centric warfare" intelligence, management, navigation, fire support, systems and complexes are connected to a single information-communication network, and the transfer and reception of reliable and complete information about operational (battle) conditions is carried out in practically real time. It is intended to increase the combat power of the unit by achieving rapid and high-precision destruction. The increase in the effectiveness of combat power occurs as a result of the acceleration of the process of managing forces and assets and the pace of combat, as well as the synchronization of combat activities. The transmission and reception of real-time data over a large area allows network users to monitor the current activities of all friendly and enemy units according to their authorization levels on an electronic map or screen, and to intervene directly in battlefield activities when necessary (Jonjo, 2014).

David Steven Alberts, a former American Director of Research for the Office of the Assistant Secretary of Defense for Networks and Information Integration, noted the following advantages of "network-centric warfare" (Smith, 2010):

1. A strong and fast network greatly improves information exchange and interaction in warfare;

2. The improvement of information exchange and interaction increases the reliability and accuracy of information, as well as awareness of the general situation;

3. General situational awareness allows units to self-synchronize;

4. Self-synchronization, in turn, dramatically increases the effectiveness of activities.

The main point that stands out from the above is self-synchronization. In military organizations with a traditional centralized hierarchical structure, command, decision, information, tasking, and interaction issues are transmitted from top to bottom, and usually all activities are carried out under the command of superiors. In self-synchronization, however, many complex activities are organized from the bottom up and interactions are regulated. This is because commanders on the battlefield can interact directly with both the fighting soldiers and their superiors at various levels. This allows them to be constantly aware of the situation, to transmit that information to their superiors in real time, to quickly adapt to changing conditions, to make independent decisions and move according to the conditions, to request fire support and additional forces. In short, the commanders on the battlefield will determine the tasks and objectives, as well as the form and method of conducting the battle, according to the intentions of the higher command. Self-synchronization gives a huge advantage over the enemy in terms of speed, control, and suddenness. This advantage allows you to conduct combat operations without interruption. As a result, tactical and operational interruptions that the enemy can take advantage of are eliminated, combat activities become more dynamic, continuous and decisive. The ability of units to operate independently, as well as a high level of awareness, will enable the simultaneous conduct of combat activities at the tactical, operational and strategic levels.

Thus, having considered the revolutionary changes in military art as a result of the development of technologies and the further acceleration of these changes in the near future we may describe the characteristics of future wars. In our opinion, in the wars that will occur in the next ten years, the form of fighting “non-contact” or “from a distance” will increase, and in the future, these forms will become more advanced and widespread. The reason they are called “non-contact” or “from a distance” is that in the initial or main phase of the war, the crushing blows to the enemy will be delivered by high-precision weapons located on (flying) vehicles far from the contact line, or by remotely or autonomously controlled armed robotics (a swarm of drones). etc.) operating on the battlefield. In previous wars, the main burden fell on the ground troops, and it was impossible to win without coming into direct contact with the enemy, destroying them and capturing a certain area.

The next revolution in the military art will fundamentally change the essence of winning a war. Thus, at the beginning of the war, striking the enemy's important military and civilian infrastructure with high-precision weapons from a long distance, causing serious damage to its military, economic and combat potential, will create fear and panic among the population and military personnel. In the next phase, the enemy units, which are already in fear and panic, will be destroyed by a quick assault of special forces or tactical groups. We believe that at this stage, the use of artificial intelligence and autonomously controlled military robotics, a flock of drones together with the aforementioned forces and groups, or in a synchronized manner with them, is pretty plausible.

The revolution in military art will affect and significantly change existing understandings of the strategic, operational, and tactical levels of warfare. If in previous wars there was a certain border between tactical, operational and strategic levels in terms of territory, space, time, purpose and force, in the future this border will disappear and it will be difficult to define the levels. Thus, the scope of military operations will expand in terms of territory and space. Space, cyber domains will be added to traditional land, air and sea domains. The targets of military-technological development will make it possible to choose and destroy both tactically and operationally, as well as in strategic depth at the same time. However, if there is to be any contact with the enemy on the battlefield, it will be short-lived. As it was mentioned, in earlier conventional wars, decisive engagements were mainly fought on the ground by land forces and had a certain depth and breadth. In this war, the forces and means operating vertically above and horizontally behind (Air Force, missile-artillery units) were usually given to the support of troops conducting combat activities on land. In future non-contact wars, everything will be the other way around.

In conventional wars, battles were planned and conducted at the tactical and operational levels to achieve a strategic goal. For this, the movement and deployment of large forces was organized, reserves and logistics points were created, the main direction in attack, the direction of concentration of main efforts in defense was determined, near, far and further tasks were indicated or defense in depth was organized. In our opinion, many of these will not be needed in future wars. Because there will be no clear idea of where and how the main blow or threat will come from. A well-thought-out and well-chosen strategy will determine the fate and the winner of future wars. In addition, we think that in the future, the use of large numbers of manpower, as well as large armed units and formations in combat, will create a potential risk, not an advantage. Thus, the movement and deployment of such forces will be immediately detected by various surface and aerial (space) reconnaissance and surveillance means, and high-precision weapons will strike at their location and equipment. In these conditions, well-prepared mobile tactical groups equipped with small but multifunctional drones and robotics, as well as advanced surveillance and information-communication systems, will play a crucial role in increasig the efficiency of operations.

Since large numbers of manpower are not involved on the battlefield, maneuvering with fire, one of the most important elements of the battle, will gradually lose its importance. Terms such as “front line”, “defensive area”, “front”, “main attack direction”, will be replaced by terms such as,

"accurate strike", "main strike location", "area of responsibility", "accurate strike range", "quick strike", "network intensity". The outcome of the battle will be determined by the effectiveness of these activities: detect rapidly; analyze quickly; make decisions quickly; quickly intervene or destroy from a distance with a precision strike. The party that gains the upper hand in these activities will definitely win future wars.

Conclusion

The intense struggle for limited opportunities against the backdrop of population growth, urbanization, and environmental pollution, as well as nationalism and ethnic conflicts, international terrorism, refugee flow, illegal drug trafficking, and the spread of weapons of mass destruction will continue in the future and lead to the emergence of new wars.

War, as a part of human civilization, is certainly ever-evolving. It should be noted that this development has become more dynamic in recent years. Thus, the observed scientific and technical revolution has affected all areas of human activity and social relations, as well as the methods and forms of armed conflicts to a large extent. Today's wars are very different from the conflicts of 20 or 10 years ago. The wars of current time now include physical domains (land, air, sea) as well as information, cyber and space. In our opinion, in the next ten years, the achievements in the scientific and technical field will further expand the integration of these domains and radically change the nature of wars.

Analysis has shown that the major advances in technology, including bio-, nano-, and digital technologies, will affect the military art and cause revolutionary change. The forms and methods of fighting will change significantly compared to the past. Many of the forms and methods used successfully since the invention of gunpowder and firearms, as well as the main components of combat, will no longer be effective. So, from the main components of the battle, such as fire, strike and maneuver, which have been tested together until today, the importance of the strike will be maintained in the future. In previous wars, in order to achieve strategic goals, it was considered an important condition to come into direct contact with the enemy at the tactical and operational level, destroy its main forces by fire and maneuver, and hold the territory. A special place was reserved for land operations here. In future wars, it will be possible to disable the opponent's important facilities, including critical infrastructure, control centers, security points, and military equipment with a long-range accurate strike and thereby make it accept your conditions. In the future, countries that do not have advanced technologies for warfare, including artificial intelligence, long-range high-precision weapons, will try to replace this deficiency by increasing the number of manpower, as well as traditional weapons and equipment. However, we believe that in future wars, unprepared manpower and an abundance of conventional military equipment will be a major disadvantage rather than a superiority. Because as a result of accurate strikes, fear and confusion will arise among the people of the opponent, which will cause them lose control and several heavy equipment, and thus the fighting ability will decrease. As a last resort, it is highly likely that that party will use weapons of mass destruction, banned ammunition, or launch terrorist activities. İn addition to high-precision weapons, various robotics autonomously controlled by artificial intelligence, unmanned aerial vehicles, including a swarm of drones will play a leading role on the future battlefield. Their widespread use in armed conflicts will significantly change the structure of the Armed Forces. In the near future, traditional forces of different levels (tactical, operational and strategic) of the Land, Air and Naval Forces will be connected to a single command and control network, consisting of strategic intelligence-strike and high-precision weapon systems, as well as will be replaced by small, but mobile, prepared, fully equipped special forces (tactical groups). In future wars, events will unfold rapidly, the situation will change quickly, and the strikes will be short-term, but accurate and devastating. In such a situation, leadership qualities such as initiative,

knowledge, flexibility, deep thinking, thorough preparation, and strong motivation will come to the fore to win the battle.

Funding

This study received no specific financial support.

Competing interests

The authors declare that they have no competing interests.

References

Assumpção, C. (2020). Is Huntington's "Clash of Civilizations" a Self-fulfilled Prophecy? Available at: https://www.e-ir.info/pdf/81197 (Accessed: 06.09.2024).

Beverelli, L. (2020). Why France Lost in 1940. Available at: https://warwriters.com/why-france-lost-in-1940/ (Accessed: 06.09.2024)

Bothwell, B. (2023). Science & Tech Spotlight: Directed Energy Weapons. Available at: https://www.gao.gov/products/gao-23-106717 (Accessed: 08.09.2024).

Brychkov, A.S., Dorokhov, V.L., Nikonorov, G.A. (2019). The Hybrid Nature of Future Wars and Armed Conflicts, *Military Thought,* Vol. 28, No. 2, pp. 20-32. http://dx.doi.org/10.21557/MTH.54208774 (Accessed: 04.09.2024).

Coccia, M. (2019). Comparative Theories and Causes of War in Global Encyclopedia of Public Administration, Public Policy, and Governance, pp.1-7, Springer. Available at: https://www.researchgate.net/publication/337890175_Comparative_Theories_and_-Causes_of_War (Accessed: 23.08.2024).

Cole, B. (2020). Clausewitz's Wondrous Yet Paradoxical Trinity: The Nature of War as a Complex Adaptive System, *Joint Force Quarterly 96*, pp. 42-49. URL: https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2076059/clausewitzs-wondrous-yet-paradoxical-trinity-the-nature-of-war-as-a-complex-ada/ (Accessed: 03.09.2024).

Etzioni, A., Etzioni, O. (2017). Pros and Cons of Autonomous Weapon Systems, *Military Review*. May-June. Available at: https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2017/Pros-and-Cons-of-Autonomous-Weapons-Systems/ (Accessed: 02.09.2024).

Fernow, R. C. (1986). *Introduction to experimental particle physics*, Cambridge University Press. Available at: https://library.oapen.org/handle/20.500.12657/59210 (Accessed: 01.09.2024).

Finucane, M. (2013). Is War Primarily the Product of "Human Nature". Available at: https://www.e-ir.info/2013/10/31/is-war-primarily-the-product-of-human-nature/ (Accessed: 23.08.2024).

Fox, A. (2024). The Principles for the Future of Warfare and Stand-Off Warfare. Available at: https://www.ausa.org/publications/principles-future-warfare-and-stand-warfare (Accessed: 06.09.2024).

Grewal, D., Noble, S.M., Roggeveen, A., L., Nordfalt, J. (2020). The future of in-store technology, *Journal of the Academy of Marketing Science*, Volume 48. – p. 96-113. Available at: https://link.springer.com/article/10.1007/s11747-019-00697-z (Accessed: 01.09.2024).

Guner, E., Iskandarov, K., & Gawliczek, P. (2022). Theories of war in practice: causes and termination (in the example of the Second Karabakh War). *Wiedza Obronna*. https://yadda.icm.edu.pl/baztech/element/bwmeta1.element.baztech-89aad26d-dfd7-43bb-bd20-7a03a28fee22 (Accessed: 14.08.2024).

Hasan, A.H., Iskandarov, K. and Gawliczek, P. (2024). Azerbaijan's 2023 counterterrorism operation in Karabakh region: causes and consequences. *Social Development and Security*, *14*(3), pp.1-13. https://doi.org/10.33445/sds.2024.14.3.1

Hasanov, A.H., Iskandarov, K.I. and Sadiyev, S.S., 2019. The evolution of NATO's cyber security policy and future prospects. *Journal of Defense Resources Management*, *10*(1), pp.94-106. Available at: https://www.ceeol.com/search/article-detail?id=770728 (Accessed: 01.09.2024).

Hedges, C. (2003). *What Every Person Should Know about War*. Turtleback Books. Available at: https://www.simonandschuster.com/books/What-Every-Person-Should-Know-About-War/Chris-Hedges/9780743255127#:~:text=About%20The%20Book&text=Hedges%20allows%20U.S.%20military%20documentation,from%20medical%20and%20psychological%20studies.

Iskandarov, K. & Gawliczek, P. (2021a). Characteristic features of the second Karabakh war. *Social Development and Security*, *11*(3), pp. 30-40. https://doi.org/10.33445/sds.2021.11.3.3 (Accessed: 16.08.2024).

Iskandarov, K., & Gawliczek, P. (2020a). Hybrid warfare as an instrument of political leverage (With a special focus on the South Caucasus). *The Russian federation and international security* edited by Miroslaw Banasik, Piotr Gawliczek and Agnieszka Rogozinska (Poland: Difin publishing house, 2020), pp. 117-136.

Iskandarov, K., & Gawliczek, P. (2020b). Hybrid warfare as a new type of war. The evolution of its conceptual construct in Miroslaw Banasik, Piotr Gawliciczek and Agnieszka Rogozinska (eds) *The Russian federation and international security*, Poland: Difin publishing house, 2020, pp. 96-107.

Iskandarov, K. & Gawliczek, P. (2020c). The impact of social media on the war. Case study: The Second Karabakh War in *Information, Media, Security Environment* edited by Miroslav Banasik, Piotr Gawliczek, Agnieszka Rogozinska. Warsaw: Difin. Pp. 162-178.

Iskandarov, K., & Gawliczek, P. (2020d). The "new great game" in the south caucasus: competition for power and influence. *Social Development and Security*, *10*(1), pp. 25-33. https://doi.org/10.33445/sds.2020.10.1.4 (Accessed: 12.05.2024).

Iskandarov, K. & Gawliczek, P. (2021b). The second Karabakh war as a war of new generation. *Social Development and Security*, *11*(2), pp. 91-99. https://doi.org/10.33445/sds.2021.11.2.9 (Accessed: 18.08.2024).

Iskandarov, K., & Gawliczek, P. (2019). The south Caucasus and NATO'S defence education enhancement programme. Retrospective analysis. *Social Development and Security*, *9*(5), 3-14. https://doi.org/10.33445/sds.2019.9.5.1.

Iskandarov, K., Gawliczek, P., & Tomasik, J. (2022). Termination of war: factors affecting the outcome (in the example of the Second Karabakh War). *Civitas et Lex*, *35*(3), pp. 7-17. Available at: https://czasopisma.uwm.edu.pl/index.php/cel/article/view/7736/6136 (Accessed: 01.09.2024).

James, M.D. (2018). No guarantees when it comes to war. Available at: https://www.ausa.org/articles/no-guarantees-when-it-comes-war (Accessed: 01.09.2024).

Jonjo, R. (2014). Modern Militaries and a Network Centric Warfare Approach. Available at: https://www.e-ir.info/2014/01/09/modern-militaries-and-a-network-centric-warfare-approach/ (Accessed: 08.09.2024).

Mallick, P. (2020). Network centric warfare. Available at: https://www.researchgate.net/publication/344737587_NETWORK_-CENTRIC_WARFARE (Accessed: 02.09.2024).

Marcin, M. M. (2019). What is Artificial Intelligence? Available at: https://www.researchgate.net/publication/337089782_What_is_Artificial_Intelligence (Accessed: 01.09.2024).

Matthew, O.J., Massimo, M. (2009). The Reasons for Wars – an Updated Survey. Handbook on the Political Economy of War. Available at: https://www.researchgate.net/publication/238529380_The_Reasons_for_-Wars_-_an_Updated_Survey (Accessed: 02.09.2024).

Matthew, U. (2024). What Is Nanotechnology? Available at: https://builtin.com/hardware/nanotechnology (Accessed: 06.09.2024).

Milley, M.A., Schmidt, E. (2024). America isn't ready for the wars of the future. Available at: https://www.foreignaffairs.com/united-states/ai-america-ready-wars-future-ukraine-israel-mark-milley-eric-schmidt (Accessed: 04.09.2024).

Nasirov, E., Iskandarov, K., & Sadiyev, S. (2017). The South Caucasus: A Playground Between NATO and Russia? *Connections*, *16*(3), pp. 47-56. Available at: https://www.jstor.org/stable/26867919 (Accessed: 23.06.2024).

Rodgers, E. (2024). Directed-Energy Weapons Come of Age. Available at: https://aerospace.honeywell.com/us/en/about-us/blogs/directed-energy-weapons-come-of-age (Accessed: 07.09.2024).

Sadiyev, S. & Iskandarov, K. (2018). The evolution of the security environment in the South Caucasus since the end of the Cold War, *17th Workshop of the PfP Consortium Study Group Regional Stability in the South Caucasus, "What a New European Security Deal" could mean for the South Caucasus*, 14/2018, pp. 47-53. Available at: https://www.academia.edu/37852657/_What_a_New_European_Security_Deal_could_mean_for_the_South_Caucasus (Accessed: 19.08.2024).

Smith, C. R. (2010). Network Centric Warfare, Command, and the Nature of War. Available at: https://researchcentre.army.gov.au/sites/default/files/sp318ncwcommandandnatureofwarchristopher_smith.pdf (Accessed: 03.09.2024).

Sweijs, T., Michaels, J.H. (2024). *Beyond Ukraine: Debating the Future of War.* Hurst publishers Available at: https://www.waterstones.com/book/beyond-ukraine/tim-sweijs/jeffrey-h-michaels/9781911723165 (Accessed: 05.09.2024).

Waldman, T. (2009). War, Clausewitz, and the Trinityhttps, A Thesis Submitted for the Degree of PhD at the University of Warwick. Available at: https://core.ac.uk/download/pdf/40048786.pdf (Accessed: 05.09.2024).

Walsh, T. (2023). The defence review fails to address the third revolution in warfare: artificial intelligence. Available at: https://theconversation.com/the-defence-review-fails-to-address-the-third-revolution-in-warfare-artificial-intelligence-204619 (Accessed: 04.09.2024).

Yamin, T. (2021). Future Wars and Change in National Policy. *Strategic Thought* (3): 113-125. Available at: https://strategicthought.ndu.edu.pk/site/article/view/29 (Accessed: 06.09.2024).

Список використаних джерел

Assumpção, C. (2020). Is Huntington's "Clash of Civilizations" a Self-fulfilled Prophecy? Available at: https://www.e-ir.info/pdf/81197 (Accessed: 06.09.2024).

Beverelli, L. (2020). Why France Lost in 1940. Available at: https://warwriters.com/why-france-lost-in-1940/ (Accessed: 06.09.2024)

Bothwell, B. (2023). Science & Tech Spotlight: Directed Energy Weapons. Available at: https://www.gao.gov/products/gao-23-106717 (Accessed: 08.09.2024).

Brychkov, A.S., Dorokhov, V.L., Nikonorov, G.A. (2019). The Hybrid Nature of Future Wars and Armed Conflicts, *Military Thought,* Vol. 28, No. 2, pp. 20-32. http://dx.doi.org/10.21557/MTH.54208774 (Accessed: 04.09.2024).

Coccia, M. (2019). Comparative Theories and Causes of War in Global Encyclopedia of Public Administration, Public Policy, and Governance, pp.1-7, Springer. Available at: https://www.researchgate.net/publication/337890175_Comparative_Theories_and_-Causes_of_War (Accessed: 23.08.2024).

Cole, B. (2020). Clausewitz's Wondrous Yet Paradoxical Trinity: The Nature of War as a Complex Adaptive System, *Joint Force Quarterly 96*, pp. 42-49. URL: https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2076059/clausewitzs-wondrous-yet-paradoxical-trinity-the-nature-of-war-as-a-complex-ada/ (Accessed: 03.09.2024).

Etzioni, A., Etzioni, O. (2017). Pros and Cons of Autonomous Weapon Systems, *Military Review*. May-June. Available at: https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2017/Pros-and-Cons-of-Autonomous-Weapons-Systems/ (Accessed: 02.09.2024).

Fernow, R. C. (1986). *Introduction to experimental particle physics*, Cambridge University Press. Available at: https://library.oapen.org/handle/20.500.12657/59210 (Accessed: 01.09.2024).

Finucane, M. (2013). Is War Primarily the Product of "Human Nature". Available at: https://www.e-ir.info/2013/10/31/is-war-primarily-the-product-of-human-nature/ (Accessed: 23.08.2024).

Fox, A. (2024). The Principles for the Future of Warfare and Stand-Off Warfare. Available at: https://www.ausa.org/publications/principles-future-warfare-and-stand-warfare (Accessed: 06.09.2024).

Grewal, D., Noble, S.M., Roggeveen, A., L., Nordfalt, J. (2020). The future of in-store technology, *Journal of the Academy of Marketing Science*, Volume 48. – p. 96-113. Available at: https://link.springer.com/article/10.1007/s11747-019-00697-z (Accessed: 01.09.2024).

Guner, E., Iskandarov, K., & Gawliczek, P. (2022). Theories of war in practice: causes and termination (in the example of the Second Karabakh War). *Wiedza Obronna*. https://yadda.icm.edu.pl/baztech/element/bwmeta1.element.baztech-89aad26d-dfd7-43bb-bd20-7a03a28fee22 (Accessed: 14.08.2024).

Гасанов Хасан, А., Іскандаров, Х., & Гавлічек, П. (2024). Антитерористична операція Азербайджану в Карабахському регіоні 2023 року: причини та наслідки. *Social Development and Security*, *14*(3), 1-13. https://doi.org/10.33445/sds.2024.14.3.1

Hasanov, A.H., Iskandarov, K.I. and Sadiyev, S.S., 2019. The evolution of NATO's cyber security policy and future prospects. *Journal of Defense Resources Management*, *10*(1), pp.94-106. Available at: https://www.ceeol.com/search/article-detail?id=770728 (Accessed: 01.09.2024).

Hedges, C. (2003). *What Every Person Should Know about War*. Turtleback Books. Available at: https://www.simonandschuster.com/books/What-Every-Person-Should-Know-About-War/Chris-Hedges/9780743255127#:~:text=About%20The%20Book&text=Hedges%20allows%20U.S.%20military%20documentation,from%20medical%20and%20psychological%20studies.

Iskandarov, K. & Gawliczek, P. (2021a). Characteristic features of the second Karabakh war. *Social Development and Security*, *11*(3), pp. 30-40. https://doi.org/10.33445/sds.2021.11.3.3 (Accessed: 16.08.2024).

Iskandarov, K., & Gawliczek, P. (2020a). Hybrid warfare as an instrument of political leverage (With a special focus on the South Caucasus). *The Russian federation and international security* edited by Miroslaw Banasik, Piotr Gawliczek and Agnieszka Rogozinska (Poland: Difin publishing house, 2020), pp. 117-136.

Iskandarov, K., & Gawliczek, P. (2020b). Hybrid warfare as a new type of war. The evolution of its conceptual construct in Miroslaw Banasik, Piotr Gawliciczek and Agnieszka Rogozinska (eds) *The Russian federation and international security*, Poland: Difin publishing house, 2020, pp. 96-107.

Iskandarov, K. & Gawliczek, P. (2020c). The impact of social media on the war. Case study: The Second Karabakh War in *Information, Media, Security Environment* edited by Miroslav Banasik, Piotr Gawliczek, Agnieszka Rogozinska. Warsaw: Difin. Pp. 162-178.

Iskandarov, K., & Gawliczek, P. (2020d). The "new great game" in the south caucasus: competition for power and influence. *Social Development and Security*, *10*(1), pp. 25-33. https://doi.org/10.33445/sds.2020.10.1.4 (Accessed: 12.05.2024).

Iskandarov, K. & Gawliczek, P. (2021b). The second Karabakh war as a war of new generation. *Social Development and Security*, *11*(2), pp. 91-99. https://doi.org/10.33445/sds.2021.11.2.9 (Accessed: 18.08.2024).

Iskandarov, K., & Gawliczek, P. (2019). The south Caucasus and NATO'S defence education enhancement programme. Retrospective analysis. *Social Development and Security*, *9*(5), 3-14. https://doi.org/10.33445/sds.2019.9.5.1.

Iskandarov, K., Gawliczek, P., & Tomasik, J. (2022). Termination of war: factors affecting the outcome (in the example of the Second Karabakh War). *Civitas et Lex*, *35*(3), pp. 7-17. Available at: https://czasopisma.uwm.edu.pl/index.php/cel/article/view/7736/6136 (Accessed: 01.09.2024).

James, M.D. (2018). No guarantees when it comes to war. Available at: https://www.ausa.org/articles/no-guarantees-when-it-comes-war (Accessed: 01.09.2024).

Jonjo, R. (2014). Modern Militaries and a Network Centric Warfare Approach. Available at: https://www.e-ir.info/2014/01/09/modern-militaries-and-a-network-centric-warfare-approach/ (Accessed: 08.09.2024).

Mallick, P. (2020). Network centric warfare. Available at: https://www.researchgate.net/publication/344737587_NETWORK_-CENTRIC_WARFARE (Accessed: 02.09.2024).

Marcin, M. M. (2019). What is Artificial Intelligence? Available at: https://www.researchgate.net/publication/337089782_What_is_Artificial_Intelligence (Accessed: 01.09.2024).

Matthew, O.J., Massimo, M. (2009). The Reasons for Wars – an Updated Survey. Handbook on the Political Economy of War. Available at: https://www.researchgate.net/publication/238529380_The_Reasons_for_-Wars_-_an_Updated_Survey (Accessed: 02.09.2024).

Matthew, U. (2024). What Is Nanotechnology? Available at: https://builtin.com/hardware/nanotechnology (Accessed: 06.09.2024).

Milley, M.A., Schmidt, E. (2024). America isn't ready for the wars of the future. Available at: https://www.foreignaffairs.com/united-states/ai-america-ready-wars-future-ukraine-israel-mark-milley-eric-schmidt (Accessed: 04.09.2024).

Nasirov, E., Iskandarov, K., & Sadiyev, S. (2017). The South Caucasus: A Playground Between NATO and Russia? *Connections*, *16*(3), pp. 47-56. Available at: https://www.jstor.org/stable/26867919 (Accessed: 23.06.2024).

Rodgers, E. (2024). Directed-Energy Weapons Come of Age. Available at: https://aerospace.honeywell.com/us/en/about-us/blogs/directed-energy-weapons-come-of-age (Accessed: 07.09.2024).

Sadiyev, S. & Iskandarov, K. (2018). The evolution of the security environment in the South Caucasus since the end of the Cold War, *17th Workshop of the PfP Consortium Study Group Regional Stability in the South Caucasus, "What a New European Security Deal" could mean for the South Caucasus*, 14/2018, pp. 47-53. Available at: https://www.academia.edu/37852657/_What_a_New_European_Security_Deal_could_mean_for_the_South_Caucasus (Accessed: 19.08.2024).

Smith, C. R. (2010). Network Centric Warfare, Command, and the Nature of War. Available at: https://researchcentre.army.gov.au/sites/default/files/sp318ncwcommandandnatureofwarchristopher_smith.pdf (Accessed: 03.09.2024).

Sweijs, T., Michaels, J.H. (2024). *Beyond Ukraine: Debating the Future of War.* Hurst publishers Available at: https://www.waterstones.com/book/beyond-ukraine/tim-sweijs/jeffrey-h-michaels/9781911723165 (Accessed: 05.09.2024).

Waldman, T. (2009). War, Clausewitz, and the Trinityhttps, A Thesis Submitted for the Degree of PhD at the University of Warwick. Available at: https://core.ac.uk/download/pdf/40048786.pdf (Accessed: 05.09.2024).

Walsh, T. (2023). The defence review fails to address the third revolution in warfare: artificial intelligence. Available at: https://theconversation.com/the-defence-review-fails-to-address-the-third-revolution-in-warfare-artificial-intelligence-204619 (Accessed: 04.09.2024).

Yamin, T. (2021). Future Wars and Change in National Policy. *Strategic Thought* (3): 113-125. Available at: https://strategicthought.ndu.edu.pk/site/article/view/29 (Accessed: 06.09.2024).

Transformation of state stability amid globalisation

Трансформація стійкості держави в умовах глобалізації світу

Iryna Alieksieienko [A]
Dr of Political Sciences, Professor, e-mail: ppvch@ukr.net, ORCID: 0000-0002-6873-003X

Liudmyla Kovalyshyn [A]
Candidate of Political Sciences, Associate Professor, e-mail: k.liudmyla2000@gmail.com, ORCID: 0000-0002-1521-8577

[A] Yevhenii Bereznyak Military Academy, Kyiv, Ukraine

Ірина Алєксєєнко [A]
д.політ.н., професор, e-mail: ppvch@ukr.net, ORCID: 0000-0002-6873-003X

Людмила Ковалишин [A]
к.політ.н., доцент, e-mail: k.liudmyla2000@gmail.com, ORCID: 0000-0002-1521-8577

[A] Воєнна академія імені Євгенія Березняка, м. Київ, Україна

Received: September 16, 2024 | Revised: October 21, 2024 | Accepted: October 31, 2024

DOI: 10.33445/sds.2024.14.5.2

Purpose: is to analyse the modern process of forming state stability in the conditions of the transformation of the international political security space.

Method: The research was conducted using a neo-institutional approach, historical and systemic methods, a comparative approach, and a functional method.

Findings: Determination of the conceptual foundations of the formation of state stability in the conditions of a crisis international security environment.

Theoretical implications: It consists in forming a holistic view of modern theories of the institution of the state and the factors that ensure its stability against the background of the aggravation of contradictions in the international political and security environment caused by Russia's aggression against Ukraine.

Practical implications: The main political, economic and security factors were analysed, and a model was formed based on the neo-institutional approach to ensure the stability of the state institution in the conditions of worsening globalisation threats and the formation of a new architecture of the international security environment. This study can be a valuable resource for professional researchers, analysts in geopolitics and geostrategy, security and defence sector representatives, international organisations, and state and local authorities.

Originality: It consists of applying a neo-institutional approach to ensuring the stability of the state institution in the context of the crisis of the international political and security environment triggered by Russia's aggression against Ukraine.

Paper type: theoretical, practical.

Key words: stability of the state, sovereignty, international security environment, national security, geopolitics, national stability, armed aggression against Ukraine, threats of globalisation.

Мета роботи: проаналізувати сучасний процес формування стійкості держави в умовах трансформації міжнародного політичного простору безпеки.

Метод: неоінституційний підхід, історичний, системний методи; компаративістський підхід, функціональний метод.

Результати дослідження: Визначення концептуальних засад формування стійкості держави в умовах кризового міжнародного безпекового середовища.

Теоретичні висновки: полягає у формуванні цілісного уявлення про сучасні теорії інституту держави та фактори, що забезпечують формування її стійкості на тлі загострення протиріч в міжнародному політичному та безпековому середовищі, спричиненому агресією росії проти України.

Практичні наслідки: Проаналізовано основні політичні, економічні й безпекові фактори та сформовано на основі неоінституційного підходу модель забезпечення стійкості інституту держави в умовах загострення глобалізаційних загроз, та формування нової архітектури міжнародного безпекового середовища. Запропоноване дослідження може бути корисним фаховим дослідникам, аналітикам в царині геополітики та геостратегії, представникам сектору безпеки і оборони, міжнародним організаціям, органам державної та місцевої влади.

Оригінальність: полягає в застосуванні неоінституційного підходу до процесу забезпечення стійкості інституту держави в контексті кризи міжнародного політичного і безпекового середовища, тригером якої стала агресія росії проти України.

Тип статті: теоретичний, практичний.

Ключові слова: стійкість держави, суверенітет, міжнародне безпекове середовище, національна безпека, геополітика, національна стійкість, збройна агресія проти України, загрози глобалізації.

Introduction

The significant transformation that the political, economic, legislative, security, social and other spheres of state regulation have undergone in the process of globalisation, the high level of interaction of the state with different actors of the international political system require the study of a wide range of issues of ensuring the stability of the state in the context of the transformation of the global security space. This issue is closely related to the neo-institutional approach to the institution of the state – the leading actor in the international political space, which is undergoing significant changes under the conditions of globalisation.

Theoretical background

The question of the future of the institution of the state in a rapidly changing world is becoming central in the strategic research papers of scientists, political and military experts. Based on research from previous decades, political scientists are looking at the future of the leading political institutions in light of new trends in the world economy and global security. This problem acquires special significance in light of the close relationship between the democratic political system and the sovereign state acting as its guarantor. The question of the further fate of the institution of the state is thus transformed into a question of the stability of the state, and this explains its relevance in the context of the analysis of the international security space. The diagnosis of the incapacity and inefficiency of the state institution in the realities of a highly integrated society of the 21st century was made back in the 20th century. It is being rethought. Global political studies in this context have become one of the most critical tasks of modern political science and national security, as the period of uncertainty requires immediate responses to the threatening challenges of the time to avoid even greater instability in the future. At the end of the 20th century, the trends towards further democratisation and liberalisation of developing countries should have led to the gradual smoothing of international conflicts. Still, political and security globalisation processes have become much more complex and ambiguous. Direct analogies between economic and political integration were not as good as they seemed before. The discrepancy between the formed single world market and the nation-states that continue to exist requires a new rethinking in the conditions of military globalisation. What will happen in the process of globalisation with the institution of the state, with its monopoly right on legal violence, and with internal and external sovereignty? These are the main questions scientists of the world's leading research centres face today.

Statement of the problem

A thorough study of issues based on the neo-institutional approach related to the functioning of the state institution, the formation and ensuring of its stability, the global management of the international political system of tomorrow, the reconceptualisation of the international security space in the context of military challenges and threats acquires a new sound today in the light of military globalisation.

Results

Scientists note that at the end of the 20th century, the political hierarchy was gradually simplified: from the "concert of states" of the 19th century to the opposing "axes" of the first half of the 20th century, from the rigid bipolarity of the Cold War to the "unipolar world". The international Yalta-Potsdam order, in its modified form, which was based on the balance of power between a group of states, was hierarchical.

The hierarchy of the world order ended with the exhaustion of the opportunities it provided. Unification efforts have had the opposite effect – different nations seek to emphasise their identity and originality. At the same time, globalising countries are trying to maintain the former dominance of uniform norms and rules introduced in the international system after the Cold War by forceful methods. All this is happening against the background of the achieved balance of benefits from globalisation.

The end of the Cold War did not lead to the end of history. The thaw that began in the late 1980s accentuated Europe's long-standing animosity. We never entered unipolarity. It would be a big mistake to think that defending the mantras of globalisation and the market in the 21st century makes national security subject to global theory. The world must solve the unfinished problems of the past.

Therefore, the main reason for the current state conflict and confrontation is to preserve the elements of the former world order within the framework of the ongoing transformational processes. At the same time, a noticeable role in the change of the international security space is played by the intermediate hedging of states, aligning them with each other with an eye on the future. This process is inevitable and requires a new strategy and tactics of states in the modern international security environment, especially when it comes to considerable nuclear powers, as the risks to the security of all humanity are growing.

One of the main parameters of the modern security space of international relations is its structure. It looks like it was formed on the basis of agreements between the victorious countries in the Second World War.

In addition to the institutional framework, the architecture of international relations requires a balance of forces that affect state interaction dynamics.

In modern political realities, the concept of "rule-based order" is being actively implemented, which makes states' freedom to defend and promote their national interests increasingly conditional. This concept resonates with the theory of structural realism, which states that the realisation of national interests should be carried out within the established structure of international relations and not go beyond it.

The benefits of globalisation have led many countries to gradually limit their sovereignty and place the responsibility of ensuring welfare on the powerful core of the emerging world and the supervision of world order on the "American world policeman". Several global crises, the main one being the full-scale aggressive war unleashed by Russia against Ukraine, outlined the shortcomings in approaches to the system of governance at the national and global levels. The inevitable result of the failures faced by the liberal world order was the disenchantment of the world's majority, both with hegemony and its universalist values and principles. Unsurprisingly, many countries find themselves in turbulent waters: deprived of the opportunity to act independently, they seek to defend their ideas, ideals and identity.

The response to crises arising in the modern globalised political environment is the return of states to their basic ideological principles, which contribute to increasing their resistance to globalisation challenges. Rising tensions, outbreaks of violence, and uncontrolled escalation around the world characterise the resulting global chaos. The fragmentation of the world economy is fuelled by protectionist measures taken by countries that play a crucial role in its development. These challenges are exacerbated against the backdrop of a decline in the ability of states to act together, as was the case in the past.

Despite the lingering problems, the political process is happening, and the global landscape is becoming more colourful and complex. In international politics, actors appear to bring new global issues, and temporality is changing, characterised by the transition from post- to metamodernism, virtualisation, and accelerated diversification rates. In light of these developments, the world's return to ideological uniformity or bipolar logic becomes impossible. In the conditions of ideological diversification, the logical approach to transforming global chaos into a transitional phase is to strengthen states' subjectivity. The ability to solve their problems independently and collectively is essential for countries. This point of view, which finds more and more support in the international expert environment, is fully shared by supporters of a multipolar world.

For many years, Western politicians opposed monopolarity as the dominant principle of the global system. They argued that reducing the amount of power in the hands of numerous actors minimises the ability of international and regional players to solve the problem of a "war of all against all" in the struggle for dominance. According to this view, total peace can only be achieved when a single authoritative structure maintains order, preventing a return to the "jungle". Even in the American National Security Strategy of 1993, it was noted that the USA had no choice but to provide such a vision for the whole world. In theory, this concept seems well-founded, but practice

shows that the liberal world order led by the USA often required military interventions to accelerate transformations to "democratise" regimes or to support a balancing strategy in foreign countries [1]. According to Thomas Hobbes, its weakening will lead to the renewal of the power struggle. And today, political experts and scientists see the first manifestations of these forecasts in the full-scale war that the aggressor Russia is waging against Ukraine.

A common belief in contemporary political science is that Western values can become the basis of lasting peace worldwide, provided global players who have previously behaved aggressively abandon their deep-rooted identities. Because modern states cannot and do not want to take responsibility for the entire global system, it can be assumed that by the end of the 21st century, the world will rely on several regional systems for maintaining international security and order. Multipolarity does not mean a return to a world characterised by the presence of states, as in the 20th century. It also does not mean that in the 21st century, there will be many actors in the world, and the concept of the state, as it was once predicted, will disappear as such.

The parameters of military globalisation are determined by the crisis of the potential of individual states, the growth of global problems, the role of regional associations, military alliances, international organisations, and the emergence of a new political culture. The study of the processes of "erosion" and "devaluation" of the status of a sovereign state and the weakening of centralised institutions of state power has practically become an independent field of research today. First, researchers note several trends that indicate the gradual "eroding" of sovereignty in its traditional sense. From the point of view of the problem of state sovereignty, the main consequence of the processes of military globalisation is the contradiction between the growing economic, political and security interdependence of countries and peoples, on the one hand, and the preservation of the state's right to solve its problems independently and at its discretion, on the other. The consequence of this process is the loss by the state of a number of its functions in the international arena and the appearance of a significant number of new actors in it – regional associations of states, military alliances, international governmental organisations, international non-governmental organisations, transnational corporations, which take on several functions that they delegated by individual states, thereby actually limiting their external sovereignty. The reverse side of globalisation and the emergence of supranational authorities is ethnic separatism, the strengthening of local power, which also leads to the "devaluation" of internal sovereignty. Thus, researchers note two seemingly mutually exclusive processes – integration and decentralisation, each of which does not contribute to preserving the status quo of state power. In addition, recent events in the international arena have shown that several states that do not possess real political power are partially losing their main feature – the monopoly on legal violence on their territory due to the spread and approval of the universal ideology of human rights, which are often placed above state interests and is the reason for the sanctioned, by international structures, invasion of these countries. In contrast to the previous period of dominance of the information society theory, researchers of military globalisation refuse the method of linear extrapolation and apologise for this process, pointing to its internal contradictions and the emergence of new conflicts due to unresolved previous ones. Researchers of global political and security processes faced the problem of revising the critical provisions of science of earlier decades. Several antinomies can be pointed out between the predictions of scientists of the 20th century and the realities of today's political and military globalisation process. The prophecies of the Club of Rome members about the imminent demise of sovereign states and the emergence of new multiple centres of power at the global, local and intermediate levels have not justified themselves. However, we are witnessing a crisis and weakening of the state with tendencies towards decentralising power. International organisations, which were assigned the role of leading actors in the system of international relations and a dominant position over national organisations, still have a relatively weak political weight despite the rapid growth of their number. The forecast regarding the nature of international relations, which

were supposed to become flexible and polycentric, also did not come true. The leading role, as before, continues to be played by solid states – globalists, who dictate the rules of the game in the international arena. All these facts could not help but affect the development of political research at the turn of the millennium, forcing us to look for new approaches to analysing global political and security processes of our time and determining trends in their development. Studying the scale of the crisis of the international political system, the international space of security and searching for ways to overcome it is becoming the master direction of specialists in global military and political forecasting. Most scholars agree that the idea of the demise of the nation state and the demise of nation-state sovereignty is a gross exaggeration. However, the restructuring of state institutions is evident. One of the most important reasons for the high level of conflict in globalisation processes is fundamental differences in the socio-economic, political, and security development of human communities, in the way of life, and the main problems of existence. The unevenness of globalisation processes in various spheres of public life creates inconsistencies in the relations between its subjects.

The most widespread opinion is about preserving the dominant position of the state institution as the leading actor in the international arena. It concerns significant, economically and strategically vital states that will continue the struggle for leadership at the beginning of the third millennium without demanding restrictions on the interests of small sovereign states. In this context, the debate is primarily about whether the world will be unipolar or whether several centres of power will still be capable of influencing world processes.

This point of view is also held by representatives of left-wing organisations that have recently sufficiently declared themselves under the banner of "anti-globalism". Criticising neoliberal ideology, they seek to prove that the US is not losing its position as a world leader and is not renouncing its sovereignty, but, on the contrary, is using the slogans of democratisation and liberalisation to strengthen its world domination. In this connection, the "golden billion" concept is gaining particular popularity, according to which only one billion of the planet's population will enjoy all the advantages of modern civilisation. Other inhabitants of the earth are assigned the role of service personnel and suppliers of cheap labour and raw materials for developed countries. Since this situation causes discontent, which will only intensify with the growth of the population in poor countries, it will be increasingly difficult for the countries of the West to restrain this pressure. The confrontation will result in a West-Non-West conflict and threaten the entire planet's stability. That is why, according to representatives of radical attitudes, the USA invented a neoliberal ideology that proclaims the inevitable strengthening of interdependence and integration on a global scale [11]. A globalised economy should gradually equalise the economic and cultural differences between different regions and the level of inequality. This will hurt the status of a sovereign state, which will be challenging to maintain with almost complete transparency of borders and the inefficiency of state institutions in general. Therefore, power will gradually pass into the hands of supranational organisations that will implement a unified coordination policy. According to the radicals, this model of the "new world order" is a fiction that representatives of the financial and political circles of the West impose on the rest of the world to suppress its resistance to the growing inequality between different regions of the planet [12].

Of course, a sovereign state will continue to play a leading role in international relations in the XXI century. Still, new actors will appear whose influence on political processes will grow. Today, we are observing the formation of a transnational world in which states and peoples will retain a significant role, levers, and functions.

In general, the picture of the future world order appears to modern researchers to be quite controversial and not conflict-free compared to the previous era. Therefore, the search for alternative development methods is becoming a significant direction of political science and

forecasting. This also applies to the problem of the transformation of sovereignty, which is gaining a pronounced ideological dimension and the related security problems of our time.

In a world with growing competition for resources and influence without a hegemonic state, sovereignty will become a scarce commodity for states, so scientists are convinced that in 2040, the state will be assigned a new role. This shift would see the state viewed as a privilege rather than an automatic right in the passing Westphalian world. If the people of Russia, China, Iran, Turkey, Saudi Arabia and India still prefer public administration, then in Western countries, people's trust in the state has recently fallen to a historic low. This makes it possible to assume that some state-centric entities will remain active subjects in the emerging world order, while others will be transnational associations with blurred borders, thereby creating competition between sovereign states.

Conclusions.

Thus, the concept of the modern state, formed under the profound influence of the ideas of T. Hobbes and J. Locke, will retain its relevance in the future, contributing to the revival of movements for the protection of the sovereignty of states led by both global powers (USA, Russia and China) and regional players (EU, Turkey, Iran and Saudi Arabia). These countries will shape the landscape of globalisation, strengthening and establishing strong ties within specific geographic boundaries [13].

A group of political experts believes that international actors, disappointed by the failure of Pax Americana in the 2020s, will prioritise the sovereignty of their regions, which will lead to the formation of comprehensive techno-economic blocs in which they will have political power [14]. During the development of globalisation, deprived areas of sovereignty will become the arena of competition between these blocs. Citizens who have abandoned the principle of belonging to one state or another will prefer global civil societies and populate these spaces, taking advantage of the blocs' political and economic benefits. The question is whether they will be able to provide financial, food and physical security, which is usually guaranteed by the state.

Funding

This study received no specific financial support.

Competing interests

The authors declare that they have no competing interests.

References

1. Leonard M. The age of unpeace: how connectivity causes conflict. London: Bantam press. 2021.240 p.
2. Hasenclever A., Mayer P., Rittberger V. Integrating Theories of International Regimes. *Review of International Studies.* 2000. Vol. 26. No. 1. P. 3-33.
3. Anghel S., Immenkamp B., Lazarou E., Saulnier J., Wilson A. On the path to strategic autonomy. The EU in an evolving geopolitical environment. European Parliamentary Research Service. PE 652.096. September 2020. Available from : https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652096/EPRS_STU(2020)652096_EN.pdf.
4. O'Neill A. European Union: share in global gross domestic product based on purchasing-power-parity from 2018 to 2028. Statista. New York.28.04.2023. Available from : https://www.statista.com/statistics/253512/share-of-the-eu-in-the-inflation-adjusted-global-gross-domestic-product/.

5. Hemmer C., Katzenstein P. J. Why Is There No NATO in Asia? Collective Identity, Regionalism, and the Origins of Multilateralism. *International Organization.* 2022. Vol. 56. No. 3. P. 575-607.
6. Pugliese G. A Global Rorschach test: Responding to China's Belt Road Initiative. Defense Strategic Communication. The Official Journal of the NATO Strategic Communications Centre of Excellence 2019. Vol. 7.
7. Panda J.P. EU's global gateway strategy and building a global consensus vis-a-vis BRI. Ordnungspolitische Diskurse. No. 2022.10. Ordnungspolitisches Portal. 2022. Available from : https://www.econstor.eu/bitstream/10419/266145/1/1820680134.pdf.
8. Manners I. Normative power Europe: a contradiction in terms? J. of common market studies. Hoboken, NJ: John Wiley & Sons.2022. Vol. 40. Issue 2. P. 235 – 258.
9. Sjöholm F. Navigating the new normal: the European Union's changing stance on globalization in the era of trade conflicts. IFN. Stockholm. 2023. 21 p. Available from : https://www.ifn.se/media/p34dyzls/wp1466.pdf.
10. Lohmann S. European strategic autonomy: the test case of Iran. *European review of international studies*. Hague: Brill.2021. Vol. 8. Issue 3. P. 443-477.
11. Initiative pour l'Europe: discours d'Emmanuel Macron pour une Europe sou-veraine, unie démocratique. Élysée. Paris. 26.09.2017. Available from : https://www.elysee.fr/emmanuel-macron/2017/09/26/initiative-pour-l-europe-discours-d-emmanuel-macron-pour-une-europe-souveraine-unie-democratique.
12. Kamphof R., Wessel R. Analysing shared competences in EU external action: the case for a politico-legal framework . Europe and the world: a law review. UCL. London: UCL press. 2018. Vol. 2. N 1. P. 38–64.
13. Strategic Plan 2020–2024. DG Research and Innovation. European Commission. Available from : https://commission.europa.eu/system/files/2020.1/rtd_sp_2020_2024_en.pdf
14. Adler E. Europe as a civilizational community of practice. Civilizations in world politics: plural and pluralist perspectives. P.J. Katzenstein (Ed). New York: Routledge.2019. 248 p.

Список використаних джерел

1. Leonard M. The age of unpeace: how connectivity causes conflict. London: Bantam press. 2021.240 p.
2. Hasenclever A., Mayer P., Rittberger V. Integrating Theories of International Regimes. *Review of International Studies.* 2000. Vol. 26. No. 1. P. 3-33.
3. Anghel S., Immenkamp B., Lazarou E., Saulnier J., Wilson A. On the path to strategic autonomy. The EU in an evolving geopolitical environment. European Parliamentary Research Service. PE 652.096. September 2020. URL : https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652096/EPRS_STU(2020)652096_EN.pdf.
4. O'Neill A. European Union: share in global gross domestic product based on purchasing-power-parity from 2018 to 2028. Statista. New York.28.04.2023. URL : https://www.statista.com/statistics/253512/share-of-the-eu-in-the-inflation-adjusted-global-gross-domestic-product/.
5. Hemmer C., Katzenstein P. J. Why Is There No NATO in Asia? Collective Identity, Regionalism, and the Origins of Multilateralism. *International Organization.* 2022. Vol. 56. No. 3. P. 575-607.
6. Pugliese G. A Global Rorschach test: Responding to China's Belt Road Initiative. Defense Strategic Communication. The Official Journal of the NATO Strategic Communications Centre of Excellence 2019. Vol. 7.

7. Panda J.P. EU's global gateway strategy and building a global consensus vis-a-vis BRI. Ordnungspolitische Diskurse. No. 2022.10. Ordnungspolitisches Portal. 2022. URL : https://www.econstor.eu/bitstream/10419/266145/1/1820680134.pdf.
8. Manners I. Normative power Europe: a contradiction in terms? J. of common market studies. Hoboken, NJ: John Wiley & Sons.2022. Vol. 40. Issue 2. P. 235 – 258.
9. Sjöholm F. Navigating the new normal: the European Union's changing stance on globalization in the era of trade conflicts. IFN. Stockholm. 2023. 21 p. URL : https://www.ifn.se/media/p34dyzls/wp1466.pdf.
10. Lohmann S. European strategic autonomy: the test case of Iran. *European review of international studies*. Hague: Brill.2021. Vol. 8. Issue 3. P. 443-477.
11. Initiative pour l'Europe: discours d'Emmanuel Macron pour une Europe sou-veraine, unie démocratique. Élysée. Paris. 26.09.2017. URL : https://www.elysee.fr/emmanuel-macron/2017/09/26/initiative-pour-l-europe-discours-d-emmanuel-macron-pour-une-europe-souveraine-unie-democratique.
12. Kamphof R., Wessel R. Analysing shared competences in EU external action: the case for a politico-legal framework . Europe and the world: a law review. UCL. London: UCL press. 2018. Vol. 2. N 1. P. 38–64.
13. Strategic Plan 2020–2024. DG Research and Innovation. European Commission. URL : https://commission.europa.eu/system/files/2020.1/rtd_sp_2020_2024_en.pdf
14. Adler E. Europe as a civilizational community of practice. Civilizations in world politics: plural and pluralist perspectives. P.J. Katzenstein (Ed). New York: Routledge.2019. 248 p.

Strategic Localization for Ukraine's Defense Industry

Стратегічна локалізація для оборонної промисловості України

Michael J. McCarthy [A]
e-mail: michaelxmccarthy@hotmail.com, ORCID: 0009-0003-0855-6038
Taras Yemchura [A]
e-mail: michaelxmccarthy@hotmail.com

[A] Defence Advisor, Kyiv, Ukraine

Майкл Дж. Маккарті [A]
e-mail: michaelxmccarthy@hotmail.com, ORCID: 0009-0003-0855-6038
Тарас Ямчура [A]
e-mail: michaelxmccarthy@hotmail.com

[A] Радник з питань оборони, Київ, Україна

Received: October 6, 2024 | Revised: October 20, 2024 | Accepted: October 31, 2024

DOI: 10.33445/sds.2024.14.5.3

Purpose: to evaluate the options for strategic localization for the defence industrial sector of Ukraine and to provide practical recommendations for the implementation of the policy.

Method: comparative analysis, synthesis, and case studies.

Findings: Rebuilding Ukraine's degraded defence industry is vital for its long-term security and strategic interests, and a robust Ukrainian defence industry supports partner nation security interests as well. While continued foreign assistance remains essential in the short term, Ukraine needs to progressively localize repair, assembly, and repair capabilities for its most critical military equipment.

Theoretical implications: The paper enhances our understanding of key concepts relating to the contributions of the local defence industry to the security of Ukraine, and how those industries can be developed to support the capabilities of the Armed Forces of Ukraine. The Russia-Ukraine war serves as a contemporary case study to explore these theories in practice. The paper provides new insights for understanding the practical application of the policy of localization.

Value: Examining the practical implications of the policy of localization in Ukraine's defence industry in the context of the Russia-Ukraine war involves understanding how these theories translate into real-world recommendations, both for Ukraine and for its international partners. that can contribute to the development and sustainment of Ukraine's military capabilities.

Research limitations: The classification of much information relating to Ukraine's defence industry and defence capabilities, along with the contributions of international partners, forms a limitation on the scope and depth of the study.

Paper type: practical.

Key words: Ukraine defence industry, localization, Russia-Ukraine War, international military assistance, government-to-government, industry-to-industry.

Мета: оцінити варіанти стратегічної локалізації для ОПК України та надати практичні рекомендації щодо реалізації політики.

Метод дослідження: порівняльний аналіз, синтез і тематичні дослідження.

Результати дослідження: Відбудова деградованої оборонної промисловості України має життєво важливе значення для її довгострокової безпеки та стратегічних інтересів, а міцна українська оборонна промисловість також підтримує інтереси безпеки нації партнера. Хоча подальша зовнішня допомога залишається важливою в короткостроковій перспективі, Україні необхідно поступово локалізувати можливості ремонту, складання та ремонту свого найважливішого військового обладнання.

Теоретична цінність дослідження: Стаття покращує наше розуміння ключових концепцій, що стосуються внеску місцевої оборонної промисловості в безпеку України, а також того, як ці галузі можна розвивати для підтримки можливостей Збройних Сил України. Російсько-українська війна служить сучасним тематичним дослідженням для дослідження цих теорій на практиці. Стаття надає нові ідеї для розуміння практичного застосування політики локалізації.

Цінність: Вивчення практичних наслідків політики локалізації в оборонній промисловості України в контексті російсько-української війни передбачає розуміння того, як ці теорії перетворюються на реальні рекомендації як для України, так і для її міжнародних партнерів, які можуть сприяти розвитку та підтримці військового потенціалу України.

Обмеження дослідження: Класифікація великої кількості інформації, що стосується оборонної промисловості та оборонних можливостей України, разом із внеском міжнародних партнерів, створює обмеження щодо обсягу та глибини дослідження.

Тип статті: практична.

Ключові слова: українська оборонна промисловість, локалізація, російсько-українська війна, міжнародна військова допомога, від уряду до уряду, від галузі до галузі.

Introduction

Ukraine's defence industry has been severely degraded after years of neglect and extensive damage from the Russian invasion and now is largely incapable of meeting anything other than the most basic requirements. This has forced Ukraine into dependence on international assistance and – to a lesser degree–procurement of foreign defence equipment. However, boosting domestic defence repair and production capabilities is vital for its security and self-sufficiency as reliance on international donations will be insufficient to meet the nation's growing defence requirements. Ukraine must focus on the strategic localization of its defence needs by investing heavily in its

indigenous defence industrial base, and partner nations should support this initiative with funding, technology transfer, and cooperative production agreements.

Although the challenges facing Ukrainian defence industry are well known (Tkach, M., Hrytsyuk, Y., Tkachenko, V., & Kivliuk, O. (2023); Yurkiv, N., & Shemaev, V. (2023); Pysmennyi, O., Krechko, S., & Bestiuk, A. (2024); Nikitchenko, V., Hmyria, V., Kostiuk, O. (2024), and the need for localization has been addressed both in Ukrainian government policy statements (Ukraine will increase the localization, March 14, 2024) and in the media (Dmytro Pavlenko, October 10, 2023; Halyna Yanchenko, March 26, 2024), the concept has not been fully explored in the academic literature. Most academic literature published since the beginning of the full-scale invasion in February 2022 regarding this topic has focused on the need for reforms in the defence industrial sector. Stepan A. Davymuka addresses the ongoing innovation within the defence industrial sector, stressing the need for conception foundations of ecosystems to improve the technological level of Ukrainian arms production (Stepan A. Davymuka, 2023). Volodymyr Mozharovskyi and Serhii Hodz of the Central Research Institute of the Armed Forces of Ukraine address the need for centralization of the management of Ukrainian defense industry and the establishment of a State Agency for the Defense Industry of Ukraine (Mozharovskyi, V., & Hodz, S., 2024). Yuliia Kerpatenko fully discusses the importance of financial strategies in the development of the defence industrial sector (Yuliia Kerpatenko, 2024). Kateryna Stepanenko, George Barros, and Fredrick W. Kagan with Grace Mappes, Nicole Wolkov, Angelica Evans, and Christina Harward at the Institute for the Study of War address Ukraine's joint ventures and partnerships with western partners in the defence industrial sphere in "Ukraine's Long-Term Path to Success: Jumpstarting a Self-Sufficient Defense Industrial Base with US and EU Support" (Kateryna Stepanenko, January 14, 2024). S.V. Kovalevskyy, V.M. Osipov, and M.S. Kukosh address the issue of localization within the broader context of ensuring overall capability of the armed forces, arguing that the "gradual localization of Western technology production in Ukraine will contribute to reducing dependence on imports and increasing production volumes", also noting that the development of such localization opportunities, particularly with regard to service, repair, and restoration of weapon systems and military equipment can have a positive social and economic benefit by providing employment and the infusion of resources to local economies (Kovalevskyy, S.V., Osipov, V.M., Kukosh, M.S., 2023). This article seeks to expand the topic by addressing the context of localization, its requirements, practical applications, and policy approaches which would help ensure the implementation of this approach.

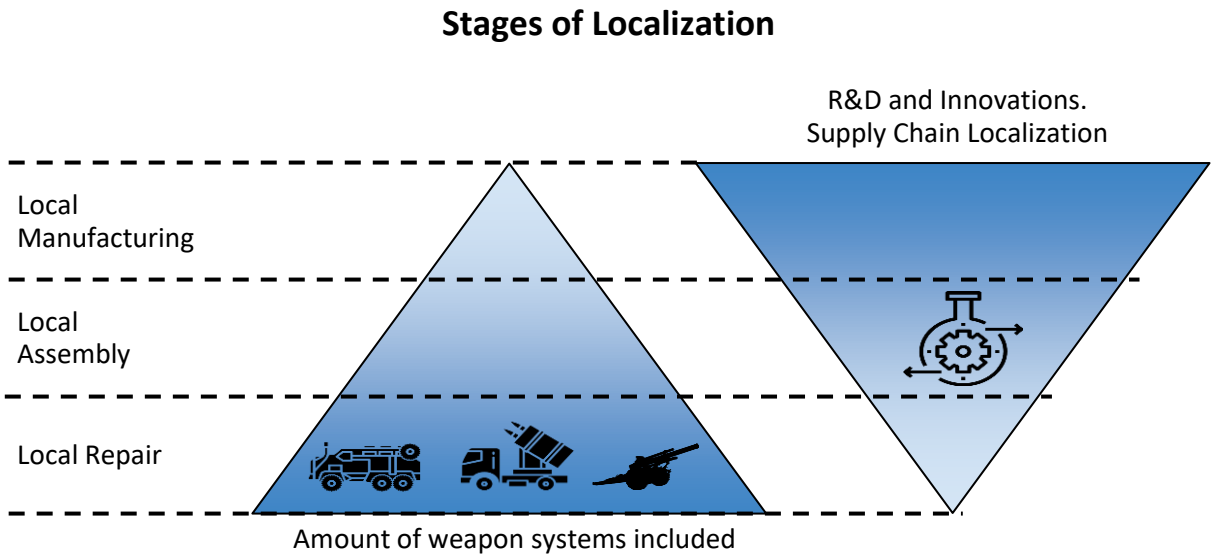
The United States, Ukraine's most generous supporter, has provided over USD 44.2 billion (U.S. Security Cooperation with Ukraine) in military assistance between January 24, 2022, and December 12, 2023, and seeks to continue supporting Ukraine's defence. But providing such support without a process of the localization of repair and manufacturing will be complicated, expensive, and logistically challenging. It will also impact Ukraine's ability to conduct sustained operations, as the requirement to return damaged equipment to repair facilities in Western Europe takes time, effort, and resources. Long-term development of the Ukrainian defence industry may help overcome these obstacles, but both countries lack experience cooperating on initiatives even during times of peace. Likewise, barriers around transfers of sensitive technology have hindered cooperation in the past and corruption, legal protections on intellectual property, and bureaucratic hurdles also remain significant impediments.

New policy solutions are required to enhance Ukraine's long-term defence capabilities and facilitate US-Ukraine defence industry cooperation. A bilateral initiative to establish localized production and repair facilities for key defence items in Ukraine would strategically drive cooperation. But regulatory barriers must be addressed, adequate financial and technical assistance provided, and anti-corruption measures prioritized to ensure success.

Such an effort would be best suited with three levels: local repair, local assembly, and local production. While many weapon systems can benefit from local repair, a smaller set would be

available for local assembly, and an even smaller set for local production. This tiered approach would ensure the Ukrainian Armed Forces can sustain its capabilities through the course of this conflict, while ensuring the Ukraine can begin to build the industrial capabilities necessary to respond to future conflicts.

Results



Local Repair

Many, if not most, of the weapon systems provided by the United States and other partners should be subject to local repair. Establishing in-country repair capabilities are needed to ensure high operational readiness and fast recovery of battle-damaged equipment. Local repair reduces cost and time compared to reliance on the remote maintenance and distribution cell in eastern Poland, known as the Tele-Maintenance and Distribution Center–Ukraine (TDC-U). While TDC-U provides an intermediary solution for much intermediate and depot level repair, localization of maintenance and overhaul for some priority equipment is still necessary. Starting with basic servicing, a phased approach to advance to rebuilds and overhauls of entire platforms is optimal. Investments in repair infrastructure, technical skills training, diagnostic equipment, and localized spare part stocks can increase the efficiency of foreign support.

Local Assembly

At the second level, a smaller group of weapon systems would be subject to local assembly. Again, through largely the same set of mechanisms, the U.S. government can encourage U.S. defence companies to partner with Ukrainian firms to create manufacturing facilities that can assemble weapon systems from materials and parts delivered from the U.S. Transitioning from the import of finished defence systems to domestic assembly using Semi Knock Down (SKD (Semi Knock Down) This refers to dismantling and packaging up certain parts of a system for shipment to other assembly plants where the parts will then be re-assembled) and Complete Knock Down (CKD (Completely Knocked Down) Refers to a product that is delivered in individual parts and then assembled on site) kits transfers product know-how and puts in place assembly lines. Assembly operations should focus on priority areas (see below). The skills and facilities established create a pathway towards local manufacturing.

Local Manufacturing

Licensed production, joint ventures, and technology transfers are key enablers for establishing local manufacturing capacity. Gradually increasing the locally produced content and value-addition should be mandated. Investments in machine tools, quality control systems, and certified production processes are critical. Building reliable local supply chains expands opportunities.

Research, Development, and Innovation

Ukraine has strong engineering talent and hands-on experience countering Russian military capabilities. The high equipment usage rates in Ukraine also help identify areas for improvement. Modifications and enhancements based on real-world experience can be scaled up and integrated into existing fleets globally. This enhances capabilities and survivability while leveraging Ukraine's skills. Collaborative research and development projects with allies should focus on rapid prototyping and testing of innovations that align with global requirements. Focused investments matched with strong intellectual property protections are essential to realize successful domestic products that can be exported.

Local Repair, Local Assembly, Local Manufacturing, and Research and Development

Some of what is proposed, particularly with regard to local repair, is being done already, but often without official sanction or support. BAE Systems, for example, is currently assessing five Ukrainian defence companies which are unofficially repairing its products following damage on the battlefield, with the view of picking one or more to serve as authorized BAE repair facilities. But an *ad-hoc* approach is insufficient and too slow. Ukraine needs a commitment by the U.S. government to encourage and assist these local repair facilities through Third Party Transfer approvals, provision of technical documentation and training, public-private partnerships with U.S. defence companies, and the establishment of a reliable mechanism for obtaining spare parts, would ensure the Ukrainian Armed Forces can adequately sustain these weapon systems for years.

Forms of Cooperation

There are various avenues for facilitating defence industry cooperation between the United States and Ukraine across government, industry, and multilateral domains. Bilateral government agreements can provide frameworks for collaboration. Domestic policies can incentivize industry partnerships. Direct industry relationships can enable technology transfers and joint ventures. Multilateral platforms can attract additional resources and diversify opportunities. Each option has its pros and cons.

Government-to-Government (G2G) Model

The United States has been the primary supporter of Ukraine's defence capabilities through direct G2G initiatives, including programs like Foreign Military Financing, Ukraine Security Assistance Initiative, and Presidential Drawdown. Thanks to this support, the Armed Forces of Ukraine (AFU) have acquired essential repair capabilities, benefiting from U.S. equipment, spare parts, and training. Strengthened self-sufficiency and repair capacity within the Ukrainian Armed Forces ensure high operational readiness and rapid recovery of battle-damaged equipment, underscoring the tangible impact of US-Ukraine defence industry collaboration.

Example of Cooperation: HMMWV Repair Capabilities

A notable example of defence industry cooperation is the establishment of the *5th Joint Electrogas Welding and Automobile Repair Center* at Zhytomyr, in central Ukraine. Through collaboration with the U.S., Ukraine gained advanced repair capabilities for HMMWV vehicles. This strategic localization ensured high operational readiness, sometimes surpassing even U.S. standards. The

partnership exemplifies the benefits of government-to-government cooperation, strengthening Ukraine's self-sufficiency in defence maintenance and enhancing mutual security interests.

A major advantage of the government-to-government model

A major advantage of the government-to-government model is the ability to channel substantial resources rapidly based on high-level commitments between the United States and Ukraine. This allows large-scale equipment, technical skills, and funding transfers directly to the Armed Forces of Ukraine, bypassing potential legal hurdles. Housing repair and maintenance capacities directly within military units, rather than private industry, enable agile fixing of battle-damaged equipment. The dedicated military-to-military cooperation structure facilitates the establishment of advanced repair centers for urgent operational needs.

A major limitation of the government-to-government model

A major limitation of this approach is that it focuses narrowly on building repair and overhaul capabilities rather than licensed production or manufacturing. Establishing localized production facilities is not a core military function and would require direct industry-to-industry or government-to-industry partnerships. The government-to-government model also relies heavily on political will and aligned priorities between both administrations. Changes in leadership or policies may disrupt cooperation. Additionally, flexibility to respond rapidly to emerging needs may be more restricted compared to private industry partnerships.

Government-to-Industry (G2I) Model

The Government-to-Industry model involves policies and incentives aimed at encouraging private defence companies in partner nations to collaborate, transfer technology, and jointly develop capabilities. This enables leveraging industry expertise for focused cooperation.

Example of Cooperation: US-Israel FMF support for domestic industry

Israel was first granted permission to use a portion of Foreign Military Financing (FMF) funds for domestic defence projects in 1977, supporting the development of the Merkava tank. Congress later allowed over $250 million in FMF to be spent in Israel on the Lavi fighter aircraft. By 1991, offsets reached 25% of total FMF. Legislation in 2009 enabled 26.3% of Israel's FMF to be spent on joint ventures and local production with US firms resulting in advanced projects like the F-35, which contains technology from Israeli Elbit Systems.

A major advantage of the government-to-industry model

The Government-to-Industry approach taps into the agility and innovation of private defence firms unconstrained by political bureaucracies. Companies can deliver rapid, targeted cooperation in areas of mutual commercial interest. Governments play an enabling role by incentivizing

partnerships through policies and funding mechanisms. This market-driven model allows outcomes to be shaped organically based on economic factors.

A major limitation of the government-to-industry model

A major limitation of the government-to-industry model is dependence on the business case for companies to commit resources. Many initiatives lack financial viability without committed government subsidies and incentives. There are also corruption risks associated with providing state funds to private Ukrainian firms. Additional bureaucratic steps may be required for approvals, such as third-party transfer permissions. Governments have less control over cooperation outcomes under this model than under direct participation models, so careful oversight is needed to ensure efficiency and sustained alignment with strategic priorities.

Industry-to-Industry (I2I) Model

The Industry-to-Industry model involves direct partnerships between private defence companies in the partner nations, with minimal government involvement. Collaboration is driven by commercial interests rather than political factors.

Example of Cooperation: L3Harris & Radio Satcom Group

L3Harris has partnered with Ukrainian company Radio Satcom Group to provide quick access to Harris products and certified repairs for Ukraine's military. L3Harris was considering localizing the radio production in Ukraine, but it required a long-term contract from Ukrainian defence forces – still unrealized – to make it financially viable.

A Major Advantage of the Industry-to-Industry Model

A key advantage of direct industry-to-industry cooperation is the ability to leverage market principles to shape partnerships based on aligned capabilities and incentives. Companies can cooperate rapidly without bureaucratic hurdles.

A Major Limitation of the Industry-to-Industry Model

A major limitation is government restrictions on technology transfers and war-related risks that prevent foreign firms from investing in Ukrainian production capacities. Partnerships under this model may not fully align with strategic national priorities, especially if government long-term plans are unclear. Sustaining cooperation requires strong commercial cases despite political headwinds.

Multilateral Frameworks

In addition to bilateral initiatives, Ukraine should more extensively utilize multilateral platforms to support its defence industry and military capability development, including:

- NATO Support and Procurement Agency (NSPA) – Using its international procurement mechanisms, it can provide vital spare parts and contracted maintenance/repair services to help sustain Ukraine's equipment fleets.
- NATO Trust Funds – Allow partner nations to jointly fund key cooperation projects with Ukraine. Relevant NATO-Ukraine trust funds cover areas like explosive ordnance disposal and counter improvised explosive devices (EOD/C-IED); small arms destruction; command, control, communications, and computers (C4); cyber defence; logistics standardization; and others.
- EU Defense Integration – Ukraine should pursue closer integration with European defence ecosystems, including cooperation with Polish and Central European defence industries and collaboration on PESCO projects.

- Multilateral Development Banks – Institutions like the European Bank for Reconstruction and Development can provide financing for major Ukrainian defence industry modernization projects.

Strategically leveraging these multilateral tools can attract additional resources, capabilities, and expertise to complement bilateral cooperation. But Ukraine needs to prioritize forums which provide the most significant impact on critical defence industry gaps.

Possible Areas of Future Cooperation

Initial strategic localization efforts of the US and Ukraine can focus on the following priority equipment areas:

HMMWVs:

- Ukraine operates around **2,000 HMMWVs** and has extensive experience sustaining and repairing them, achieving even higher operational readiness rates than the US.
- The US has stockpiles of excess HMMWV frames that could be transferred to Ukraine as donor vehicles for battle damage repairs. More may become available as the HMMWV gets phased out by the armed forces of the US and other countries.
- The HMMWV is reliable, flexible and has potential for the future upgrades.

MaxxPro MRAPs:

- Around **500 MaxxPros** operated by Ukraine provide protected mobility for personnel movement.
- The MaxxPro design uses bolted assemblies rather than welded armour. This enables rapid field repairs of battle damage without specialized tools.
- Ukraine could leverage this maintainability by localizing spare parts, repairs, and upgrades to keep MaxxPros operational.

M113 Armored Personnel Carriers:

- Ukraine has around **800 M113s** forming a large part of its mechanized forces.
- Many M113s and spares are available globally as the platform gets phased out of the inventory of most nations. More than 88,000 were produced since 1960. The M113's aluminum hull resists corrosion, meaning surplus systems available worldwide are likely in good condition.
- M113 is superior to Soviet BMPs and, despite the age, has a strong upgrade potential.

M777 Howitzers:

- Having around **160 M777s** and using it extensively on the frontline, self-sufficient local repair and ammo production is vital.
- Life extension programs on the howitzer fleet would maximize effectiveness.
- Opportunities exist to co-develop specialized ammunition variants.

Conclusion

Rebuilding Ukraine's degraded defence industry is vital for its long-term security and strategic interests, and a robust Ukrainian defence industry supports partner nation security interests as well. While continued foreign assistance remains essential in the short term, Ukraine needs to progressively localize repair, assembly, and repair capabilities for its most critical military equipment.

Recommendations for the Ukrainian Government

- Develop a national-level policy document framing International Defense Cooperation and strategic localization.
- Develop a strategy and an implementation roadmap aligning strategic localization goals with defence acquisition plans.
- Pass legislation to enable public-private partnerships and joint ventures in the defence industry.
- Create favourable tax conditions supporting Ukrainian production. Lift import taxes on manufacturing equipment and components for weapon production.
- Develop and implement a program for veterans' employment at defence companies.
- Improve national secrecy legislation to allow greater exchange of industrial information and to ensure an appropriate level of intellectual property and investment protection.
- Revise export control legislation to enable rapid military and dual-use goods movement, especially for defence production.
- Improve governance and implement robust anti-corruption mechanisms.
- Request localization initiatives as part of future security assistance packages to ensure long-term sustainability of Ukraine's defence requirements.

Recommendations for the US Government

- Establish a reciprocal defence industry cooperation agreement which includes expedited approval processes for joint initiatives with Ukraine.
- Incentivize US defence companies to engage in co-production, licensed production, and joint ventures in Ukraine.
- Allocate part of the Foreign Military Financing (FMF) budget to procure localized goods and services from Ukraine.
- Utilize US loan guarantees, grants, and public-private partnerships to facilitate investment in Ukraine's defence industry.
- Fund exchange programs and organize networking and study tours for industry representatives.
- Support localizing initiatives that are, among others, promoting veterans' employment.
- Use the seized Russian Central Bank reserves to guarantee investments in Ukraine's defence industry modernization.

Effective execution across these dimensions will enable the progressive development of strategic localization initiatives. But political will, stakeholder alignment, and resolute

implementation will be critical for success. The window for impactful cooperation is now. Ukrainian and allied policymakers must seize the opportunity to rebuild Ukraine's defence industrial base through partnerships at each level – laying the foundations for the sovereignty of Ukraine and strategic security in Europe.

Funding

This study received no specific financial support.

Competing interests

The authors declare that they have no competing interests.

References

Tkach, M., Hrytsyuk, Y., Tkachenko, V., & Kivliuk, O. (2023). Trends in the development of defense capabilities of Ukraine and NATO member states: war experience. *Social Development and Security*, *13*(6), 104-118. https://doi.org/10.33445/sds.2023.13.6.10.

Yurkiv, N., & Shemaev, V. (2023). Defense industry as a driver of the national economy. *Social Development and Security*, *13*(6), 95-103. https://doi.org/10.33445/sds.2023.13.6.9.

Pysmennyi, O., Krechko, S., & Bestiuk, A. (2024). The development of the defense industry of Ukraine in the conditions of war and post-war recovery. *Social Development and Security*, *14*(2), 74-81. https://doi.org/10.33445/sds.2024.14.2.8;

Nikitchenko, V., Hmyria, V., Kostiuk, O. (2024). The Defence Industry of Ukraine and its Role in Ensuring the Security and Defence of the State. Наукові праці Державного науково-дослідного інституту випробувань і сертифікації озброєння та військової техніки 20(2), 65-71. https://doi.org/10.37701/dndivsovt.20.2024.09.

"Ukraine will increase the localization of its own production, in particular, in the defence industry: Yuliia Svyrydenko" Ministry of Economy of Ukraine, March 14, 2024 Available from : https://me.gov.ua/News/Print?lang=en-GB&id=8c8ceca2-1be7-4450-8b79-5ec76e38d15e

Dmytro Pavlenko, "How to strengthen the Ukrainian military and defense industry: A business perspective," NV Business, October 10, 2023. Available from : https://www2.deloitte.com/ua/en/pages/press-room/deloitte-press/2023/10-10.html

Halyna Yanchenko, "Defense Technology Investment in Ukraine Is Attractive but Awaits Greater Risk Insurance," Kennan Institute, march 26, 2024, Available from : https://www.wilsoncenter.org/blog-post/defense-technology-investment-ukraine-attractive-awaits-greater-risk-insurance

Stepan A. Davymuka. (2023). Innovation ecosystem of the defense industry of Ukraine: conceptual foundations and practice of establishment. Regional Economy (December 2023). https://doi.org/10.36818/1562-0905-2024-1-7.

Mozharovskyi, V., & Hodz, S. (2024). Military-economic aspects of maintaining the state's defence capability in the current military and strategic situation. *Baltic Journal of Economic Studies*, *10*(1), 185-193. https://doi.org/10.30525/2256-0742/2024-10-1-185-193

Yuliia Kerpatenko. (2024). Financial strategies for the development of the military-industrial complex in the national security system of Ukraine. Economics Finances Law (7/2024)/ 55-58. https://doi.org/10.37634/efp.2024.7.10.

Kateryna Stepanenko, George Barros, and Fredrick W. Kagan with Grace Mappes, Nicole Wolkov, Angelica Evans, and Christina Harward, "Ukraine's Long-Term Path to Success: Jumpstarting a Self-Sufficient Defense Industrial Base with US and EU Support," Institute for the Study of War, January 14, 2024, Available from : https://understandingwar.org/backgrounder/ukraine%E2%80%99s-long-term-path-success-jumpstarting-self-sufficient-defense-industrial-base

Kovalevskyy, S.V., Osipov, V.M., Kukosh, M.S. (2023). The Role of the Machine-Building Cluster in Ensuring the Defence Capability of Ukraine. Economic Innovations 25(4(89)), 58-67. https://doi.org/10.31520/ei.2023.25.4(89).58-67.

U.S. Security Cooperation with Ukraine. Available from : https://www.state.gov/u-s-security-cooperation-with-ukraine/

Список використаних джерел

Ткач, М., Грицюк, Ю., Ткаченко, В., & Кивлюк, О. (2023). Тенденції в розвитку обороноздатності України та країн-членів НАТО: досвід війни. *Social Development and Security*, *13*(6), 104-118. https://doi.org/10.33445/sds.2023.13.6.10.

Юрків, Н., & Шемаєв, В. (2023). Оборонно-промисловий комплекс як драйвер національної економіки. *Social Development and Security*, *13*(6), 95-103. https://doi.org/10.33445/sds.2023.13.6.9.

Письменний, О., Кречко, С., & Бестюк, А. (2024). Розвиток ОПК України в умовах війни та повоєнного відновлення. *Social Development and Security*, *14*(2), 74-81. https://doi.org/10.33445/sds.2024.14.2.8.

Нікітченко, В., Гмиря, В. і Костюк, О. (2024) Оборонна промисловість України та її роль у забезпеченні безпеки і оборони держави, *Збірник наукових праць; Державного науково-дослідного інституту випробувань і сертифікації озброєння та військової техніки*, 20(2), С. 65-71. https://doi.org/10.37701/dndivsovt.20.2024.09.

Україна посилить локалізацію власного виробництва, зокрема, в ОПК: Юлія Свириденко. Мінекономіки України, березень 14, 2024. URL : https://me.gov.ua/News/Print?lang=en-GB&id=8c8ceca2-1be7-4450-8b79-5ec76e38d15e

Dmytro Pavlenko, “How to strengthen the Ukrainian military and defense industry: A business perspective,” NV Business, October 10, 2023. Available from : https://www2.deloitte.com/ua/en/pages/press-room/deloitte-press/2023/10-10.html

Halyna Yanchenko, “Defense Technology Investment in Ukraine Is Attractive but Awaits Greater Risk Insurance,” Kennan Institute, march 26, 2024, Available from : https://www.wilsoncenter.org/blog-post/defense-technology-investment-ukraine-attractive-awaits-greater-risk-insurance

Давимука С. А. Інноваційна екосистема оборонної промисловості України: концептуальні засади та практика формування. *Регіональна економіка*. 2024. №1(111). С. 65-80. https://doi.org/10.36818/1562-0905-2024-1-7.

Mozharovskyi, V., & Hodz, S. (2024). Military-economic aspects of maintaining the state’s defence capability in the current military and strategic situation. *Baltic Journal of Economic Studies*, *10*(1), 185-193. https://doi.org/10.30525/2256-0742/2024-10-1-185-193

Керпатенко Ю. В. (2024). Фінансові стратегії розвитку військово-промислового комплексу в системі національної безпеки України. Економіка, фінанси, правою 7/2024. С. 55-58. https://doi.org/10.37634/efp.2024.7.10.

Kateryna Stepanenko, George Barros, and Fredrick W. Kagan with Grace Mappes, Nicole Wolkov, Angelica Evans, and Christina Harward, “Ukraine’s Long-Term Path to Success: Jumpstarting a Self-Sufficient Defense Industrial Base with US and EU Support,” Institute for the Study of War, January 14, 2024, Available from : https://understandingwar.org/backgrounder/ukraine%E2%80%99s-long-term-path-success-jumpstarting-self-sufficient-defense-industrial-base

Kovalevskyy, S., Osipov, V., & Kukosh, M. (2023). Роль машинобудівного кластеру в забезпеченні обороноздатності України. *Фаховий науковий журнал Економічні інновації*, *25*(4(89), 58-67. https://doi.org/10.31520/ei.2023.25.4(89).58-67.

U.S. Security Cooperation with Ukraine. Available from : https://www.state.gov/u-s-security-cooperation-with-ukraine/

Науково-методичний апарат протидії нелегальній міграції на ділянці відповідальності прикордонного загону

The scientific and methodical apparatus for combating illegal migration in the area of responsibility of the border detachment

Юрій Михайлюк [A]

Corresponding author: ад'юнкт, e-mail: mihailukuo01@ukr.net, ORCID: 0000-0003-4926-4886

Олег Башнянин [A]

старший викладач кафедри, e-mail: oleg.bashnyanin@icloud.com, ORCID: 0000-0002-0427-9526

Yurii Mykhailiuk [A]

Corresponding author: PhD studend, e-mail: mihailukuo01@ukr.net, ORCID: 0000-0003-4926-4886

Oleh Bashnianyn [A]

Senior Teacher of the Department, e-mail: oleg.bashnyanin@icloud.com, ORCID: 0000-0002-0427-9526

[A] Національна академія Державної прикордонної служби України імені Богдана Хмельницького, м. Київ, Україна

[A] National Academy of the State Border Service of Ukraine named after Bohdan Khmelnytskyi, Khmelnytskyi, Ukraine

Received: September 7, 2024 | Revised: October 20, 2024 | Accepted: October 31, 2024

DOI: 10.33445/sds.2024.14.5.4

Мета роботи: розробка науково-методичного апарату вибору раціонального варіанта застосування прикордонного підрозділу для виконання завдань в умовах ймовірного сценарію розвитку загрози нелегальної міграції на ділянці відповідальності прикордонного загону.

Метод: математичні моделі та методи.

Результати дослідження: сформовано систему показників і критеріїв визначення стану протидії нелегальній міграції на ділянці відповідальності органу охорони державного кордону; обґрунтовано модель вибору раціонального варіанта застосування прикордонного підрозділу для виконання завдань в умовах ймовірного сценарію розвитку загрози нелегальної міграції на ділянці відповідальності прикордонного загону; розроблено методику прогнозування можливих сценаріїв обстановки на ділянці відповідальності прикордонного загону.

Теоретична цінність дослідження: даний науково-методичний апарат дозволяє з достатньою адекватністю запровадити основні підходи щодо протидії нелегальній міграції на ділянці відповідальності прикордонного загону.

Цінність дослідження: дозволяє приймати обґрунтовані рішення щодо вибору та подальшого формування раціонального варіанту застосування прикордонних підрозділів прикордонного загону у відповідності до конкретних сценаріїв розвитку обстановки, що дозволить гарантувати забезпечення ефективної протидії нелегальній міграції на конкретних ділянках відповідальності.

Майбутні дослідження: у ході подальших досліджень доцільно опрацювати рекомендації штабу прикордонного загону щодо ефективної протидії нелегальній міграції на ділянці відповідальності.

Тип статті: теоретична.

Purpose: the development of a scientific and methodological apparatus for choosing a rational option for the use of a border unit to perform tasks in the conditions of a probable scenario of the development of the threat of illegal migration in the area of responsibility of the border detachment.

Method: mathematical models and methods.

Findings: a system of indicators and criteria for determining the state of combating illegal migration in the area of responsibility of the state border protection body was formed; the model for choosing a rational option for the use of a border unit to perform tasks in the conditions of a probable scenario of the development of the threat of illegal migration in the area of responsibility of the border detachment is substantiated; a method of forecasting possible scenarios of the situation in the area of responsibility of the border detachment was developed.

Theoretical implications: this scientific and methodological apparatus allows to implement with sufficient adequacy the main approaches to countering illegal migration in the area of responsibility of the border detachment.

Value: it allows making informed decisions regarding the selection and further formation of a rational option for the use of border units of the border detachment in accordance with specific scenarios of the development of the situation, which will guarantee the provision of effective countermeasures against illegal migration in specific areas of responsibility.

Future research: in the course of further research, it is advisable to work out the recommendations of the headquarters of the border detachment regarding effective countermeasures against illegal migration in the area of responsibility.

Papertype: theoretical.

Ключові слова: загрози, спроможності, управління, планування, безпека державного кордону, прикордонна безпека, оперативно-службова діяльність, нелегальна міграція.

Key words: threats, capabilities, management, planning, security of the state border, border security, operational service activity, illegal migration.

Вступ

Вторгнення російських військ в Україну, введення воєнного стану та проведення загальної мобілізації призвело до збільшення спроб незаконного перетину державного кордону поза

пунктами пропуску. Потенційними порушниками державного кордону є громадяни України – особи чоловічої статі призовного віку (18-60 років) що мають на меті ухилення від призову на військову службу під час мобілізації.

Особливістю у тактиці дій осіб – ухилянтів при незаконному перетинанні державного кордону є те, що на відмінну від "класичних" нелегальних мігрантів (іноземців, осіб без громадянства) громадяни України добре орієнтуються на місцевості та в більшості випадків не потребують послуг організаторів та пособників у їх незаконному переміщенні. Також, проблемним питанням у процесі організації заходів щодо протидії зазначеним правопорушенням є відмова суміжної сторони від передачі громадян України представникам ДПСУ на підставі звернень затриманих осіб про надання їм притулку та статусу біженця.

Теоретичні основи дослідження

Даний науково-методичний апарат дозволяє з достатньою адекватністю запровадити основні підходи щодо протидії нелегальній міграції на ділянці відповідальності прикордонного загону.

Постановка проблеми

Статистичні дані вказують на недостатню протидію зазначеним видам правопорушень в прикордонній сфері. Запропонований науково-методичний апарат дає можливість штабу прикордонного загону ефективно побудувати роботу щодо зниження рівня нелегальної міграції на ділянці відповідальності.

Результати

1. Формування системи показників та критеріїв визначення стану нелегальній міграції на ділянці відповідальності органу охорони державного кордону

Отриманий досвід в ході проведення ССПО "Полісся", результат аналізу обстановки щодо нелегальної міграції в сучасних умовах та логічні висновки щодо подальшого розвитку подій в державі, дають можливість виокремити зовнішні та внутрішні показники та критерії, параметри яких характеризують стан нелегальної міграції, що є основою для прийняття управлінських рішень щодо використання наявних сил та засобів в охороні ДК України.

При цьому, корисність обираних показників для мети дослідження визначається наявністю у них відомих властивостей:

- відповідність цілям і завданням ОСД;
- ясний фізичний зміст;
- чутливість до значимих для дій прикордонних підрозділів факторів і до прийнятих рішень;
- зручність обчислення й використання.

Проведене експертне опитування фахівців, які мають досвід з прийняття управлінських рішень щодо охорони ДК в умовах невизначеності та можливості різкого загострення обстановки за рахунок впливу на її (обстановки) стан нелегальної міграції поза пунктами пропуску були синтезовані основні показники та критерії кількісна міра яких дає можливість оцінити реальний та прогнозований стан обстановки на конкретній ділянці ДК та формувати варіанти раціональної організації ОСД.

Із практики ОСД експертним шляхом та з урахуванням методичного апарату було встановлено складові етапів протиправної діяльності (нелегальна міграція) у прикордонній сфері та середній час, який витрачають порушники на їх реалізацію, основними з яких є:

1) вивчення тактики дій прикордонних підрозділів у прикордонних районах України та суміжної держави;

2) пошук пособників у конкретній протиправній діяльності (як правило,

5–6 осіб з відповідним оснащенням);

3) пошук місць перетину державного кордону (як правило, організатори нелегальної міграції мають 2–3 місця перетину);

4) вивчення місцевості (конкретних ділянок кордону) з метою реалізації майбутніх протиправних дій (як правило, за місцем проживання організаторів);

5) пошук нелегальних мігрантів (ухилянтів);

6) накопичення нелегальних мігрантів (ухилянтів) поблизу кордону та їх переміщення;

7) приховане переміщення правопорушників від місця початку руху до лінії державного кордону;

8) приховане переміщення нелегальних мігрантів (ухилянтів) через державний кордон на конкретній ділянці.

Основними показниками, які характеризують ступінь загрози “нелегальна міграція” є: кількість нелегальних мігрантів, час необхідний для реалізації порушення державного кордону, рівень оснащення та екіпіровка правопорушників, наявність транспортних засобів підвищеної прохідності, сприяння (відсутність реагування на порушення) суміжної сторони, протяжність ділянки кордону що використовується порушниками (Залож та інші, 2024).

2. Модель вибору раціонального варіанта застосування прикордонного підрозділу для виконання завдань в умовах ймовірного сценарію розвитку загрози нелегальної міграції на ділянці відповідальності прикордонного загону

Вибір способів виконання завдань прикордонними підрозділами залежить від мети їх застосування. Під час виконання завдання з ОДК прикордонні підрозділи проводять дії в межах контрольованого прикордонного району у визначених районах та на напрямках зосередження основних зусиль. Ці дії ґрунтуються на активному пошуку порушників законодавства про ДК, оперативній реалізації випереджувальної інформації та своєчасному реагуванні на відповідні зміни обстановки. У свою чергу, сфера (призначення, мета, місце й умови) та особливості застосування прикордонних підрозділів для виконання завдань щодо протидії нелегальній міграції визначають необхідність проведення ретельного аналізу існуючих моделей, які надають можливість оцінювати певні загальні складові задекларованої моделі (Братко, 2023).

Модель вибору раціонального варіанта застосування прикордонного підрозділу для виконання завдань в умовах ймовірного сценарію розвитку загрози нелегальної міграції на ділянці відповідальності прикордонного загону складається із наступних блоків:

- збір і накопичення даних: ознаки портрету загрози нелегальної міграції, умов та елементів рельєфу місцевості, тощо; параметрів рівня потенційної спроможності ПРИКЗ виконувати завдання щодо протидії НМ з урахуванням сценаріїв розвитку подій, стану взаємодіючих підрозділів;

- модель оцінки та прогнозу ступеня достовірності інформації про можливу протиправну діяльність у районі відповідальності прикордонного загону;

- модель оцінки та прогнозу рівня загострення обстановки щодо НМ у визначених районах і на напрямках підвищеної оперативної активності;

- модель визначення сценарію розвитку загрози НМ;

- модель оцінки необхідного складу прикордонного підрозділу при виконанні завдань щодо нейтралізації сценарію розвитку подій;

- формування характеристик раціонального варіанта застосування прикордонного підрозділу:

1) місце (напрямок);

2) супротивник (вид сценарію розвитку загрози НМ);

3) наявний час;

4) достовірність інформації й заходи для її підвищення;
5) кількість прикордонних нарядів;
6) кількість і інтенсивність потоку правопорушників;
7) очікувана ефективність виконання завдань. Прийняття рішення, постановка завдань.

3. Методика прогнозування ефективності протидії нелегальній міграції на ділянці відповідальності прикордонного загону

Якість виконання завдань прикордонними підрозділами залежить від урахування зазначених та інших особливостей при підготовці таких варіантів дій, та надають можливість виконати завдання з необхідною ефективністю (Кириленко, Олійник, 2023). Це породжує потребу розробки методики прогнозування ефективності протидії нелегальній міграції на ділянці прикордонного загону, адекватної наведеним завданням та умовам.

Алгоритм методики, який подано на рисунку 1, надає можливість спрогнозувати ефективність дій та підбирати значення керованих параметрів.

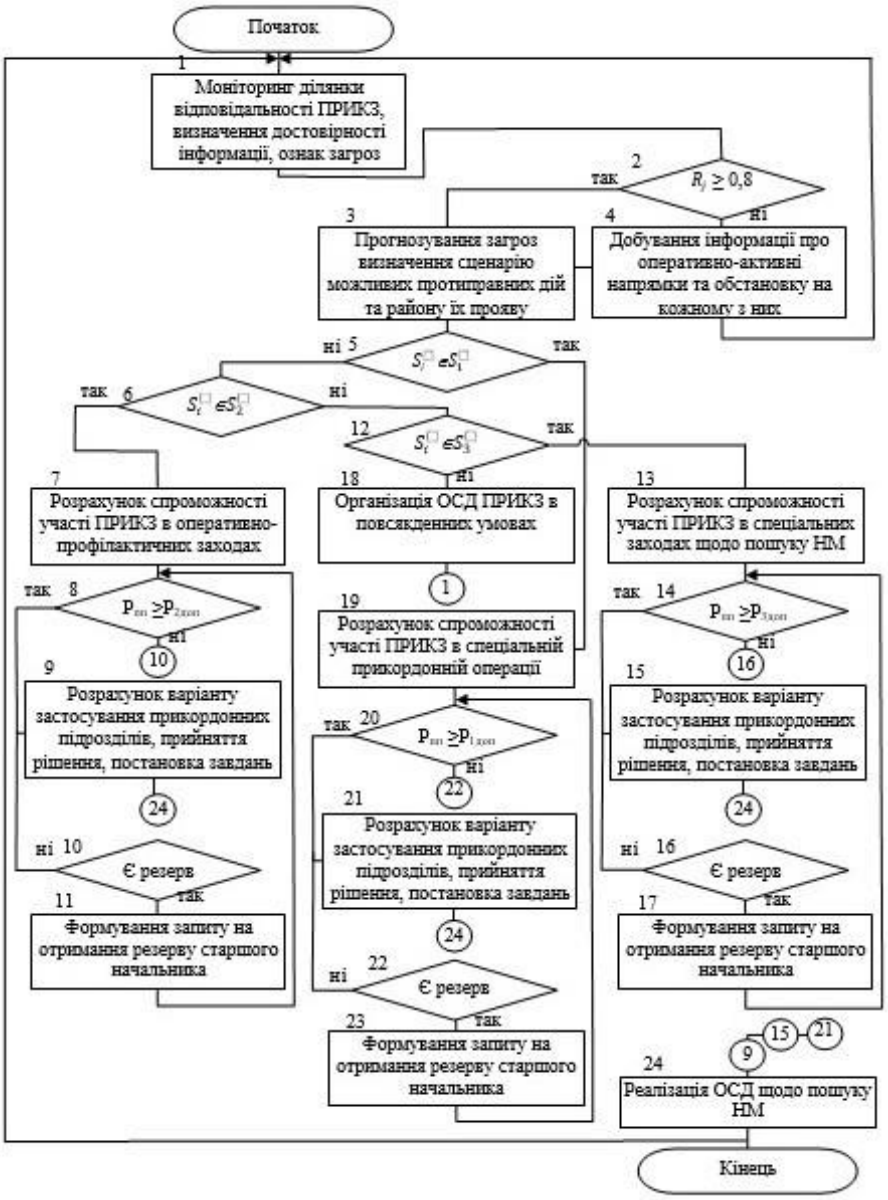


Рисунок 1 – Алгоритм методики прогнозування ефективності протидії нелегальній міграції на ділянці прикордонного загону
Джерело: *Розроблено автором*

Покращення кожного з керованих параметрів потребує потенційних затрат ресурсів, але може призводити до покращення результатів виконання завдань, яке може бути оцінено за допомогою даного алгоритму методики. Це надає змогу приймати обґрунтовані рішення щодо вибору раціонального варіанту застосування прикордонних підрозділів прикордонного загону під час визначених сценаріїв розвитку нелегальної міграції на конкретних ділянках місцевості.

Висновки

Таким чином, на підставі використання відомих методичних підходів, наявного досвіду та з урахуванням нових тенденцій розвитку загрози нелегальної міграції обґрунтовано, що основними показниками, які характеризують ступінь загрози нелегальної міграції є: кількість нелегальних мігрантів, час необхідний для реалізації порушення державного кордону, рівень оснащення та екіпіровка правопорушників, наявність транспортних засобів підвищеної прохідності, сприяння (відсутність реагування на порушення) суміжної сторони, протяжність ділянки кордону що використовується порушниками представлено їх описові характеристики (Самойленко, Дягель, 2023).

З урахуванням отриманих даних сформовані формальні вирази критеріального апарату, які надали можливість визначити можливі сценарії дій прикордонних підрозділів, що у подальшому надає можливість побудувати відповідну модель організації заходів протидії загрозі, що розглядається.

На засадах проведеного аналізу існуючого та розробленого науково-методичного апарату, було обґрунтовано модель вибору раціонального варіанта застосування прикордонного підрозділу для виконання завдань в умовах ймовірного сценарію розвитку загрози нелегальної міграції на ділянці відповідальності прикордонного загону (Братко, 2023).

Отримана модель надає можливість виконувати моделювання варіантів розвитку сценаріїв нелегальної міграції, прогнозувати ефективність та вибирати параметри варіанта застосування прикордонного підрозділу для виконання завдань щодо протидії сценарію розвитку загрози нелегальної міграції на ділянці відповідальності конкретного прикордонного загону.

Розроблена методика прогнозування можливих сценаріїв обстановки на ділянці відповідальності прикордонного загону. Відповідний алгоритм дає можливості реалізувати раціональну організацію ОСД щодо протидії нелегальній міграції в залежності від прогнозованих загроз на ділянці відповідальності.

Даний науково-методичний апарат дозволяє з достатньою адекватністю запровадити основні підходи щодо протидії нелегальній міграції на ділянці відповідальності прикордонного загону.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

Залож В. В., Михайлюк Ю. О., Овчаренко В. В. (2023). Методичний підхід щодо формування системи показників і критеріїв визначення стану протидії нелегальній міграції на

ділянці відповідальності органу охорони державного кордону. *Збірник наукових праць Національної академії державної прикордонної служби України,* 2(91), 35–45.

Братко А. (2023). Аналіз стану загроз для безпекового середовища в прикордонному просторі. *Social Development and Security*, 13 (4), 8–17. https://doi.org/10.33445/sds.2023.13.4.2

Кириленко В. А., Олійник А. А. (2023). Модель формування раціонального варіанта застосування сил і засобів прикордонного загону щодо збирання (добування) та обробки даних обстановки. *Збірник наукових праць Національної академії державної прикордонної служби України,* 2(91), 46–56.

Самойленко О. О., Дягель Д. А. (2023). Модель формування системи показників раціонального розподілу сил і засобів прикордонних підрозділів у міжнародних пунктах пропуску для автомобільного сполучення в умовах воєнного стану. *Збірник наукових праць Національної академії державної прикордонної служби України,* 3(92). 111–125.

Братко А. (2023). Методика організації роботи органів управління Державної прикордонної служби України щодо планування оперативно-службової діяльності. *Social Development and Security,* 13(1), 29-37. https://doi.org/10.33445/sds.2023.13.1.4

References

Bratko A. (2023). Analiz stanu zahroz dlya bezpekovoho seredovyshcha v prykordonnomu prostori. Social Development and Security, 13 (4), 8–17. https://doi.org/10.33445/sds.2023.13.4.2

Bratko A. (2023). Metodyka orhanizatsiyi roboty orhaniv upravlinnya Derzhavnoyi prykordonnoyi sluzhby Ukrayiny shchodo planuvannya operatyvno-sluzhbovoyi diyal'nosti. Social Development and Security, 13(1), 29-37. https://doi.org/10.33445/sds.2023.13.1.4.

Kyrylenko V. A., Oliynyk A. A. (2023). Model' formuvannya ratsional'noho varianta zastosuvannya syl i zasobiv prykordonnoho zahonu shchodo zbyrannya (dobuvannya) ta obrobky danykh obstanovky. Zbirnyk naukovykh prats' Natsional'noyi akademiyi derzhavnoyi prykordonnoyi sluzhby Ukrayiny, 2(91), 46–56.

Samoylenko O. O., Dyahel' D. A. (2023). Model' formuvannya systemy pokaznykiv ratsional'noho rozpodilu syl i zasobiv prykordonnykh pidrozdiliv u mizhnarodnykh punktakh propusku dlya avtomobil'noho spoluchennya v umovakh voyennoho stanu. Zbirnyk naukovykh prats' Natsional'noyi akademiyi derzhavnoyi prykordonnoyi sluzhby Ukrayiny, 3(92). 111–125.

Zalozh V. V., Mykhaylyuk YU. O., Ovcharenko V. V. (2023). Metodychnyy pidkhid shchodo formuvannya systemy pokaznykiv i kryteriyiv vyznachennya stanu protydiyi nelehal'niy mihratsiyi na dilyantsi vidpovidal'nosti orhanu okhorony derzhavnoho kordonu. Zbirnyk naukovykh prats' Natsional'noyi akademiyi derzhavnoyi prykordonnoyi sluzhby Ukrayiny, 2(91), 35–45.

Аналітична метрика реалій та перспектив розвитку людського ресурсу як елементу оборонної достатності держав

Analytical metric of realities and prospects of human resources development as an element of defense sufficiency of states

Олег Семененко [A]

Corresponding author: д. військ. н., професор, заступник начальника Центрального науково-дослідного інституту ЗС України з наукової роботи, e-mail: aosemenenko@ukr.net, ORCID: 0000-0001-6477-3414

Марина Абрамова [A]

к. екон. н., старший дослідник, старший науковий співробітник, e-mail: elaira3@gmail.com, ORCID: 0000-0001-7644-9988

Віктор Царинник [A]

начальник науково-дослідного відділу кадрового менеджменту та мобілізації, e-mail: viktor_0202@i.ua, ORCID:0009-0003-8638-6353

Наталія Снапкова [B]

аспірант, Національний педагогічний університет імені М.П. Драгоманова, e-mail: NatalyaS_2023@meta.ua, ORCID: 0000-0002-2706-9687

Марія Ярмольчик [C]

доктор філософії, начальник науково-дослідної лабораторії, e-mail: LinkinFan357@ukr.net, ORCID: 0000-0001-9917-0189

Максим Поливода [C]

старший викладач, e-mail: polivodamo@ukr.net, ORCID:0000-0002-4673-008X

Oleh Semenenko [A]

Corresponding author: Dr of military Sciences, Professor, deputy head of the Central Research Institute of the Armed Forces of Ukraine for scientific work, e-mail: aosemenenko@ukr.net, ORCID: 0000-0001-6477-3414

Maryna Abramova [A]

Candidate of Economic Sciences, Senior Researcher, Senior Research Fellow, e-mail: elaira3@gmail.com, ORCID: 0000-0001-7644-9988

Viktor Tsarynnyk [A]

Chief of the Personnel Management and Mobilization Research Section, e-mail: viktor_0202@i.ua, ORCID:0009-0003-8638-6353

Nataliia Snapkova [B]

graduate student, National Pedagogical Dragomanov University, e-mail: NatalyaS_2023@meta.ua, ORCID: 0000-0002-2706-9687

Mariia Yarmolchyk [C]

Doctor of Philosophy, head of the research laboratory, e-mail: LinkinFan357@ukr.net, ORCID: 0000-0001-9917-0189

Maksym Polyvoda [C]

senior lecturer, e-mail: polivodamo@ukr.net, ORCID:0000-0002-4673-008X

[A] Центральний науково-дослідний інститут Збройних Сил України, м. Київ, Україна
[B] Національний педагогічний університет імені М.П. Драгоманова, м. Київ, Україна
[C] Кафедра військової підготовки Національного авіаційного університету, Київ, Україна

[A] Central Research Institute of the Armed Forces of Ukraine, Kyiv, Ukraine
[B] National Pedagogical Dragomanov University, Kyiv, Ukraine
[C] Department of Military Training of the National Aviation University, Kyiv, Ukraine

Received: October 7, 2024 | Revised: October 20, 2024 | Accepted: October 31, 2024

DOI: 10.33445/sds.2024.14.5.5

Мета роботи: полягає у висвітленні проблематики неоднорідності динаміки людського ресурсу порівняно до частки населення працездатного віку, що у довгостроковій перспективі може мати негативний вплив на оборону достатність держав.

Метод дослідження: аналізу; синтезу; порівняння; формалізації та оцінювання матеріалу; абстрагування та кон'юнктурного аналізу (мислення).

Результати дослідження: здійснено екстраполяцію даних коефіцієнтів вікової залежності деяких країн до 2029 року, що у поєднанні із порівнянням прогнозованих значень динаміки та темпів змін людського ресурсу дали можливість виділити держави, у котрих людський фактор може бути загрозою\поштовхом до зниження\підвищення оборонної достатності у довгостроковій перспективі.

Теоретична цінність дослідження: полягає у донесенні до читачів важливості порівняння динаміки людського ресурсу до частки населення працездатного віку під час планування довгострокової оборонної політики.

Тип статті: теоретичний**,** описовий, практичний, методичний.

Purpose: is to highlight the problem of the heterogeneity of human resource dynamics in terms of the proportion of the population of working age, which may have a negative impact on the defence sufficiency of states in the long run.

Method: analysis; synthesis; comparison; formalization and evaluation of the material; abstraction and conjunctural analysis (thinking).

Findings: extrapolation of the age dependency ratios of some countries to 2029, which, combined with a comparison of the projected values of the dynamics and rates of change of human resources, made it possible to identify countries in which the human factor could be a threat/impetus to reduce/increase defence sufficiency in the long term.

Theoretical implications: is to convey to the reader the importance of comparing the dynamics of human resources with the proportion of the population of working age when planning long-term defence policy.

Paper type: theoretical, descriptive, practical, methodical.

Ключові слова: людський ресурс, оборонна достатність, іноземні країни, прогноз, працездатне населення.

Key words: human resource, defense sufficiency, foreign countries, forecast, working population.

Вступ

Людські ресурси відіграють ключову роль у розвитку держави, функціонуючи як опора економічного та соціального прогресу. За своєю суттю вони охоплюють не лише робочу силу, але й інтелектуальний та творчий потенціал держави. У наш час важливість людських ресурсів лише зросла. У сучасній глобалізованій економіці такі тенденції, як віддалена робота та цифрова співпраця, ще більше підкреслюють цінність людських ресурсів; компанії все більше покладаються на кваліфіковану робочу силу, яка може адаптуватися до динамічних потреб ринку. Ця еволюція відображає глобальне визнання того, що компетенції та здібності людей є найважливішими для процвітання держави, що робить людські ресурси життєво важливим активом у прагненні до розвитку. Через історичні приклади та сучасні тенденції стає очевидним, що кваліфікована та здорова робоча сила є рушієм інновацій, продуктивності та соціальної згуртованості. Однак проблеми нерівності, відтоку кваліфікованих кадрів і технологічних змін створюють значні перешкоди, які необхідно вирішити для ефективної оптимізації людських ресурсів.

Їх роль у зміцненні національної безпеки є багатогранною та незамінною. Потенціал персоналу безпосередньо впливає на оперативну ефективність оборонних і розвідувальних операцій, тоді як надійні стратегії найму та навчання гарантують, що робоча сила готова відповідати сучасним викликам. Крім того, сприяння співпраці та стійкості в рамках системи безпеки підвищує загальну здатність протистояти загрозам і зміцнювати суспільну довіру. Взаємодія між кваліфікованим персоналом, всебічною підготовкою та залученням громади зрештою визначатиме успіх зусиль у сфері національної безпеки у все більш взаємопов’язаному світі. Тому збереження та поповнення людського ресурсу є вирішальним компонентом для підвищення достатності національної оборони. Проблематика забезпечення оборонної достатності держави втілює не лише апаратне забезпечення чи технологічні досягнення у військовій техніці, але також охоплює людський чинник — кваліфікований персонал, який може ефективно працювати, обслуговувати та впроваджувати інновації й в оборонному секторі.

Теоретичні основи дослідження

Такі теоретики, як Клаус Райгель, зробили свій внесок у цей розвиток, описавши складну, взаємозалежну природу людського зростання та обороноздатності країни [1]. Крім того розвиток таких психологічних теорій, як біхевіоризм і когнітивна психологія забезпечили структуровані рамки для вивчення того, як стимули навколишнього середовища і психічні процеси впливають на людський потенціал [2]. Ці теорії ґрунтувалися на емпіричних наукових методах, що дозволило більш ретельно дослідити чинники, які сприяють людському розвитку та потенціалу [3]. Як наслідок, у 20-му столітті зростає інтерес до розуміння того, як різні психологічні конструкти можуть бути використані для покращення індивідуального розвитку та благополуччя країни. Кількісні методи в дослідженні людського ресурсу необхідні для узагальнення даних, виявлення закономірностей, прогнозування та перевірки причинно-наслідкових зв’язків [4; 5]. Забезпечуючи структурований підхід до аналізу даних, кількісні дослідження дають змогу узагальнювати висновки для ширших груп населення, підвищуючи таким чином надійність і достовірність результатів. Акцент на теоретичних засадах у кількісних дослідженнях має вирішальне значення, оскільки вони спрямовують методичний збір та інтерпретацію даних, гарантуючи, що отримані результати є значущими та застосовними [6]. Міждисциплінарні методи дослідження мають глибокий вплив на вивчення людського потенціалу, оскільки вони інтегрують знання з різних дисциплін для вирішення складних дослідницьких питань [7]. Спираючись на різні точки зору, міждисциплінарні дослідження поглиблюють глибину і широту розуміння, що призводить до більш комплексних та

інноваційних висновків. Такий підхід особливо важливий у таких сферах, як дослідження небезпек і катастроф, де перетинаються складні соціальні, екологічні та технологічні фактори [8]. Вчені, які займаються міждисциплінарними дослідженнями, часто мають можливість отримати результати з високою суспільною видимістю і актуальністю, тим самим розвиваючи галузь і роблячи внесок у розробку практичних рішень [9]. Динамічна природа міждисциплінарних досліджень сприяє співпраці та творчості, що, зрештою, сприяє вивченню та реалізації людського ресурсу в різних контекстах. Їхнє значення можна простежити в історії; наприклад, промислова революція в 18 і 19 століттях продемонструвала, як кваліфікована робоча сила може трансформувати економіку та підвищити оборонну достатність держави. Поява механізованого виробництва в Британії, підживлювана обсягами людського ресурсу призвела до безпрецедентного економічного зростання та урбанізації. Деякі провідні країни свідомо інвестували в людський капітал, віддаючи пріоритет освіті та професійній підготовці, що призвело до швидкого економічного розвитку, високого рівня життя та підвищило.

Постановка проблеми

Старіння населення створює значні проблеми для найму та утримання військового персоналу. У міру того, як робоча сила скорочується через демографічні зміни, кількість відповідних і фізично здатних новобранців зменшується, що робить збройним силам все важче підтримувати належний рівень укомплектованості. Дефіцит робочої сили посилюється тим, що молоді покоління, які традиційно становлять кістяк військового призову, скорочуються [10]. Отже, військові повинні конкурувати з іншими секторами за обмежену кількість молодих працівників, що може призвести до збільшення витрат на наймання та більшого акценту на стратегіях утримання. У відповідь на ці виклики оборонним організаціям може знадобитися вивчити інноваційні підходи до залучення та утримання талантів, наприклад, пропонувати більш гнучкі варіанти служби або покращити можливості кар’єрного зростання, щоб зробити військову службу більш привабливою.

Фінансовий тиск зростає, оскільки старіння населення збільшує попит на пенсії та витрати на охорону здоров’я, тим самим обтяжуючи бюджети національної оборони. Демографічні зміни призводять до дисбалансу у фінансових системах, де менше працівників підтримує зростаючу кількість пенсіонерів, що нагадує фінансову піраміду, яка більше не функціонує ефективно [11]. Цей сценарій змушує уряди виділяти більше ресурсів на програми соціального забезпечення, потенційно відволікаючи кошти від оборонних потреб. Ситуація ще більше погіршується через зростання вартості медичної допомоги для старіючого населення, що вимагає значних інвестицій у медичну інфраструктуру та послуги. Ці фінансові обмеження змушують політиків збалансувати конкуруючі вимоги щодо соціальної підтримки людей похилого віку та підтримки надійної оборонної інфраструктури, що вимагає стратегічного розподілу ресурсів та інноваційного фінансового планування.

Необхідність технологічного прогресу стає першочерговою для компенсації скорочення робочої сили, спричиненого старінням населення. Оскільки дефіцит робочої сили стає все більш помітним, впровадження передових технологій може підвищити продуктивність і ефективність, компенсуючи зменшення доступних людських ресурсів. Цей технологічний прогрес має вирішальне значення не лише для підтримки економічної стабільності, але й для забезпечення достатності оборони шляхом модернізації військового потенціалу та операцій [12]. Застосування автоматизації, штучного інтелекту та інших інновацій може дозволити військовим ефективніше виконувати завдання з меншою кількістю персоналу, таким чином зберігаючи оперативну готовність, незважаючи на скорочення робочої сили. Однак результати російсько-українського конфлікту показали, що інноваційне забезпечення воєнних дій є занадто коштовним для бюджету не лише самої України, а й країн-партнерів, тому збереження

та збільшення людського ресурсу працездатного віку все ще залишається актуальною проблематикою сьогодення. Тому є доцільним вчасне виявлення негативних тенденцій щодо його зменшення та побудови дієвих стратегій до примноження людського потенціалу для забезпечення належного рівня оборонної достатності у довгостроковій перспективі.

Результати

Для дослідження поточної динаміки людського ресурсу були використані результати емпіричного аналізу статистичних даних динаміки та темпів змін людського ресурсу України, Китаю, Литви, Угорщини, США, рф та Польщі з прогнозом до 2050 року, а також коефіцієнти вікових залежностей з екстраполяцією даних до 2029 року включно, що розкриває проблематику забезпечення країн людським ресурсом працездатного віку у довгостроковій перспективі.

Українська нація стоїть на переломному етапі свого шляху щодо забезпечення розвитку людського потенціалу. Країна може похвалитися міцною освітньою базою, про що свідчить високий рівень грамотності та збільшення кількості випускників у таких галузях, як наука, технології, інженерія та математика. Проте, незважаючи на те, що навчальні досягнення заслуговують похвали, між теоретичними знаннями та практичними навичками існує розрив. Значній частині робочої сили бракує компетенцій, які б відповідали вимогам ринку, що призводить до невідповідності навичок, що підриває економічну продуктивність. Крім того, демографічні тенденції, такі як зниження народжуваності та старіння населення, становлять суттєву загрозу для майбутньої робочої сили. Відплив молодих спеціалістів, які шукають можливості за кордоном у зв'язку із воєнними діями, ще більше загострює цю проблему, що призводить до відтоку кваліфікованих кадрів, що зменшує інноваційний потенціал країни. Головною загрозою щодо розвитку людського потенціалу є наявна економічна нестабільність, у зв'язку із наявною війною, у свою чергу політична нестабільність призвела до відсутності довгострокового стратегічного планування, що змусило багатьох талановитих людей шукати можливості реалізації закордоном (рис. 1).

Для подолання існуючих викликів необхідні комплексні стратегії, спрямовані на покращення освіти, професійної підготовки, а також зменшення міграції, що включає в себе інтеграцію навчання практичним навичкам в академічні навчальні програми, щоб забезпечити відповідність випускників вимогам ринку праці. Поява технологій та інновацій відіграє вирішальну роль у цій еволюції; використання цифрових платформ для дистанційного навчання та отримання навичок може розширити доступ і демократизувати освіту.

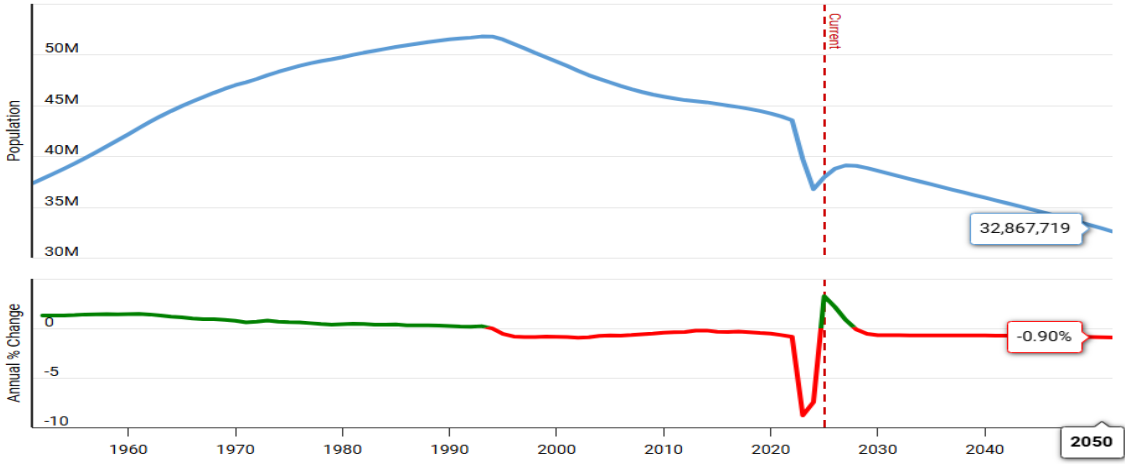


Рисунок 1 – З прогнозом до 2050 року

Джерело: *https://www.macrotrends.net/global-metrics/countries/RUS/russia/population*

Крім того, сприяння міжнародному партнерству та залучення іноземних інвестицій у розвиток людського капіталу може прискорити зростання. Програми, які сприяють передачі знань, наставництву та спільним дослідницьким ініціативам, можуть зміцнити робочу силу в Україні та позиціонувати країну як регіональний центр талантів (рис. 2).

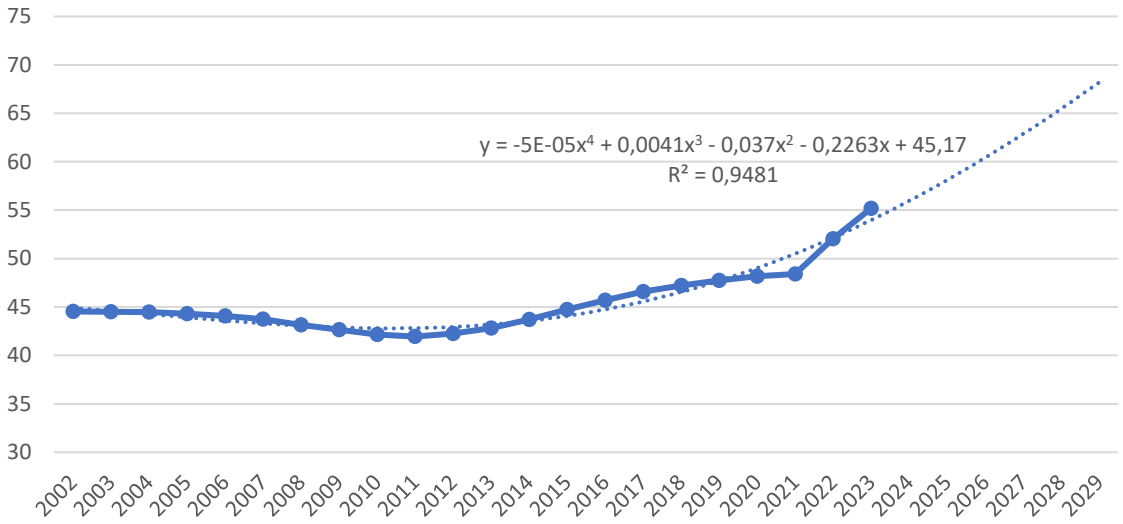


Рисунок 2 – Коефіцієнт вікової залежності України (% населення працездатного віку)
Джерело: *https://data.worldbank.org/indicator/SM.POP.REFG?end=2023&locations*

Як найбільш густонаселена нація у світі, Китай має різноманітну та динамічну робочу силу, яка історично відігравала ключову роль у його швидкому економічному підйомі.

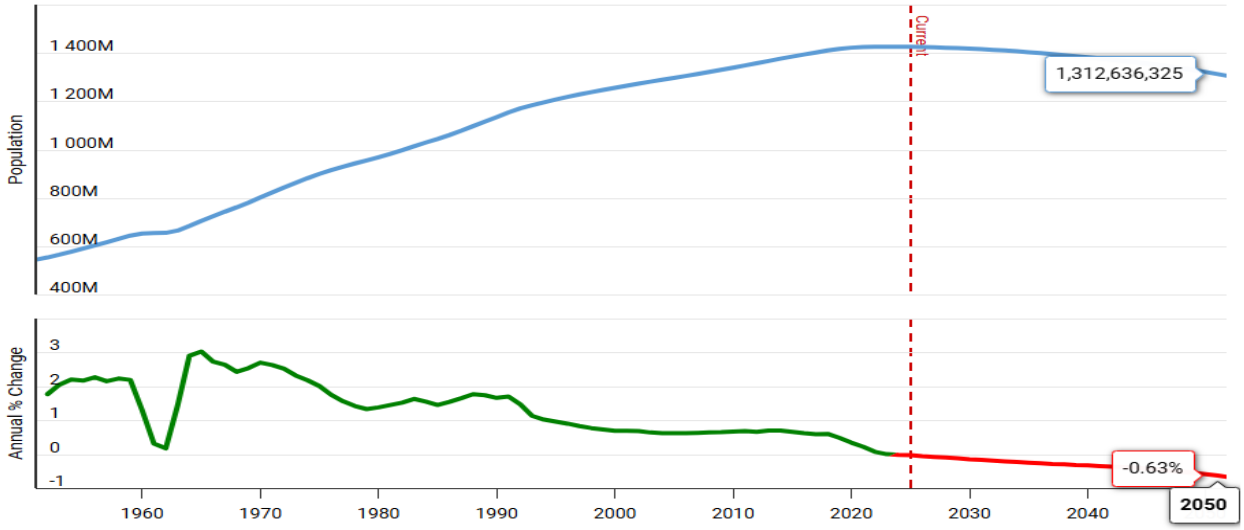


Рисунок 3 – Динаміка та темпи змін людського ресурсу Китаю з прогнозом до 2050 року
Джерело: *https://www.macrotrends.net/global-metrics/countries/RUS/russia/population*

У демографічному плані Китай переживає суттєві зміни: рівень народжуваності знижується, а частка людей похилого віку зростає. За даними Національного бюро статистики Китаю, очікується, що до 2050 року частка осіб віком від 60 років досягне 35%. Цей демографічний перехід створює як проблеми, так і можливості, оскільки меншій кількості населення працездатного віку (рис. 4) доведеться адаптуватися, щоб підтримувати зростаюча демографічна група людей похилого віку. Крім того, рівень освіти в Китаї помітно покращився, особливо в міських районах, де різко розширився доступ до вищої освіти. Міністерство освіти

повідомило, що валовий коефіцієнт охоплення вищою освітою досяг 54% у 2020 році, що свідчить про прихильність країни реформі освіти. Проте відмінності в якості освіти залишаються проблемою, особливо в сільській місцевості, де ресурси обмежені. Крім того, здоров'я та добробут відіграють вирішальну роль у максимізації людського потенціалу; незважаючи на прогрес у сфері охорони здоров'я, такі проблеми, як забруднення повітря, стигматизація психічного здоров'я та недостатній рівень медичних послуг у сільській місцевості продовжують заважати загальному добробуту робочої сили.

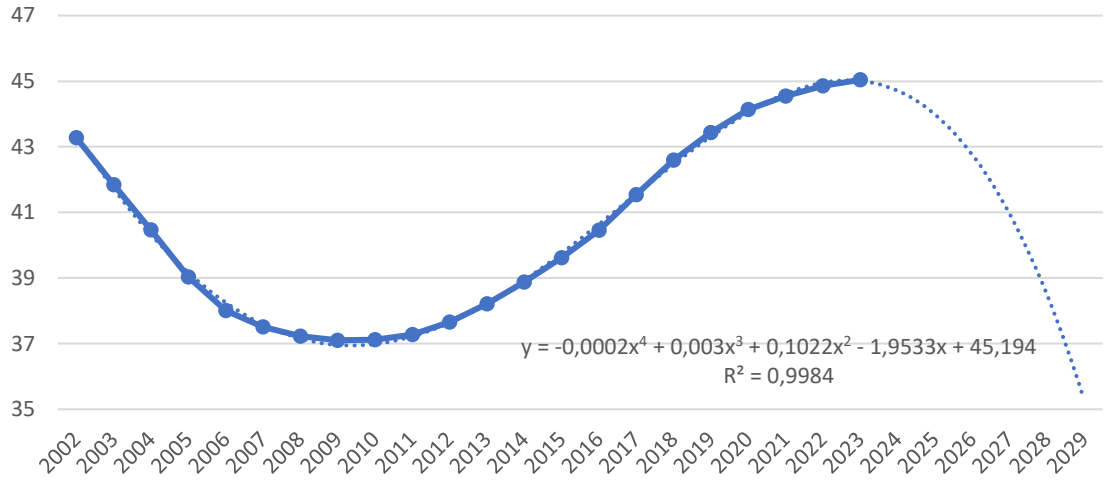


Рисунок 4 – Коефіцієнт вікової залежності Китаю (% населення працездатного віку)
Джерело: *https://data.worldbank.org/indicator/SM.POP.REFG?end=2023&locations*

Незважаючи на величезну кількість можливостей для розкриття людського потенціалу в Китаї, необхідно вирішити кілька проблем і перешкод, щоб повністю його реалізувати. Сільське населення, зокрема, продовжує стикатися з системними недоліками, які увічнюють цикли бідності та обмежують висхідну мобільність. Складні бюрократичні процеси та відсутність прозорості часто заважають малому бізнесу та новачкам отримати доступ до фінансування та підтримки. Крім того, культурне ставлення до ризику та невдач також створює проблему для підприємницького середовища. У суспільстві, яке традиційно цінує стабільність і конформізм, стигма, пов'язана з невдачею, може стримувати людей від інноваційних починань.

Литва - невелика держава, що володіє багатством невикористаного людського потенціалу Поки країна продовжує проходити пострадянські перехідні періоди та приймає членство в Європейському Союзі, вона стоїть на роздоріжжі, де стратегічні інвестиції в її людський капітал можуть принести значні вигоди. Розуміння поточного стану демографічних тенденцій Литви, складу робочої сили та рівня освіти має вирішальне значення для визначення можливостей, які відкриються попереду.

Станом на 2023 рік Литва стикається зі значними демографічними проблемами, включаючи старіння населення та тенденції еміграції (рис. 5), які призвели до зменшення населення працездатного віку. За даними Департаменту статистики Литви, з 1990 року населення скоротилося більш ніж на 20%, головним чином через еміграцію, спричинену економічними можливостями за кордоном. Однак ця тенденція також відкриває можливість для решти робочої сили, яка має високий рівень освіти та кваліфікації.

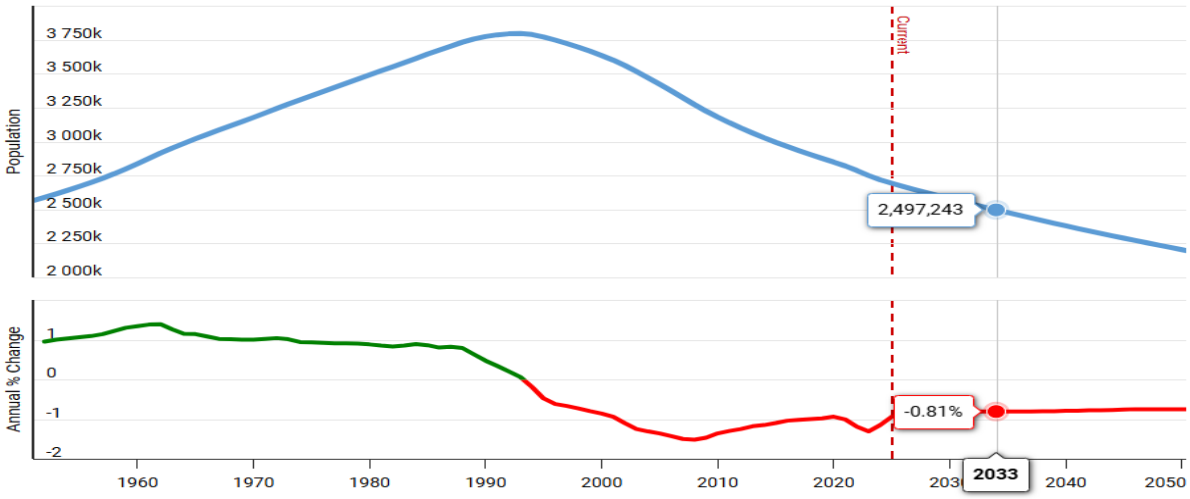


Рисунок 5 – Динаміка та темпи змін людського ресурсу Литви з прогнозом до 2050 року
Джерело: *https://www.macrotrends.net/global-metrics/countries/RUS/russia/population*

Литва може похвалитися одним із найвищих показників вищої освіти в Європейському Союзі, де понад 50% населення у віці 25-34 років мають вищу освіту. Такі ключові сектори, як інформаційні технології, біотехнології та відновлювані джерела енергії, демонструють великий потенціал для зростання, особливо в умовах зростання глобального попиту на стійкі рішення. Використовуючи наявні навички освіченої робочої сили та узгоджуючи їх із потребами цих швидко зростаючих секторів, Литва могла б вирішити поточні демографічні проблеми, одночасно відкриваючи нові шляхи економічного розвитку.

У звіті Європейської комісії зазначено, що витрати Литви на дослідження та розробки є значно нижчими, ніж у середньому по ЄС, що стримує зростання цінних секторів, які могли б поглинути освічену робочу силу. Крім того, системні проблеми в освітніх та навчальних програмах сприяють невідповідності між кваліфікацією та потребами ринку. Хоча випускників вищих навчальних закладів багато, часто існує розрив між навичками, отриманими в рамках формальної освіти, і тими, які потрібні роботодавцям на ринку праці, що швидко розвивається. Крім того, суспільне ставлення до підприємництва та інновацій залишається консервативним, з переважаючою тенденцією до пошуку стабільної роботи, а не до підприємницької діяльності. Таке культурне мислення може стримати потенційних інноваторів від ризику, який зрештою може сприяти економічному зростанню та розвитку людського капіталу. Щоб подолати ці перешкоди, необхідний багатогранний підхід, який не лише сприяє економічним інвестиціям, але й розвиває культуру інновацій та адаптивності серед робочої сили (рис. 6).

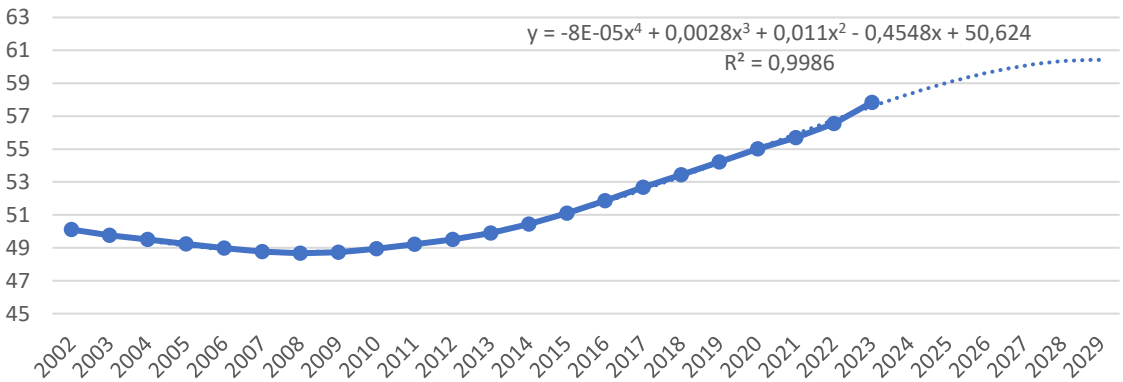


Рисунок 6 – Коефіцієнт вікової залежності Литви (% населення працездатного віку)
Джерело: *https://data.worldbank.org/indicator/SM.POP.REFG?end=2023&locations*

Угорщина, нація з багатою історією та культурною спадщиною, стоїть на роздоріжжі, де її невикористаний людський потенціал створює як виклики, так і можливості. Незважаючи на добре освічене населення, людський капітал Угорщини стикається зі значним недовикористанням, особливо в ключових секторах, які могли б стимулювати економічне зростання та інновації. Аналізуючи демографічні тенденції, історичні впливи та поточний стан освіти, можна краще зрозуміти рушійні сили людського потенціалу нації. Крім того, визначення конкретних можливостей для розвитку в галузях, що розвиваються, удосконалення освітніх рамок і сприяння підприємницькому духу має вирішальне значення для розкриття цього потенціалу.

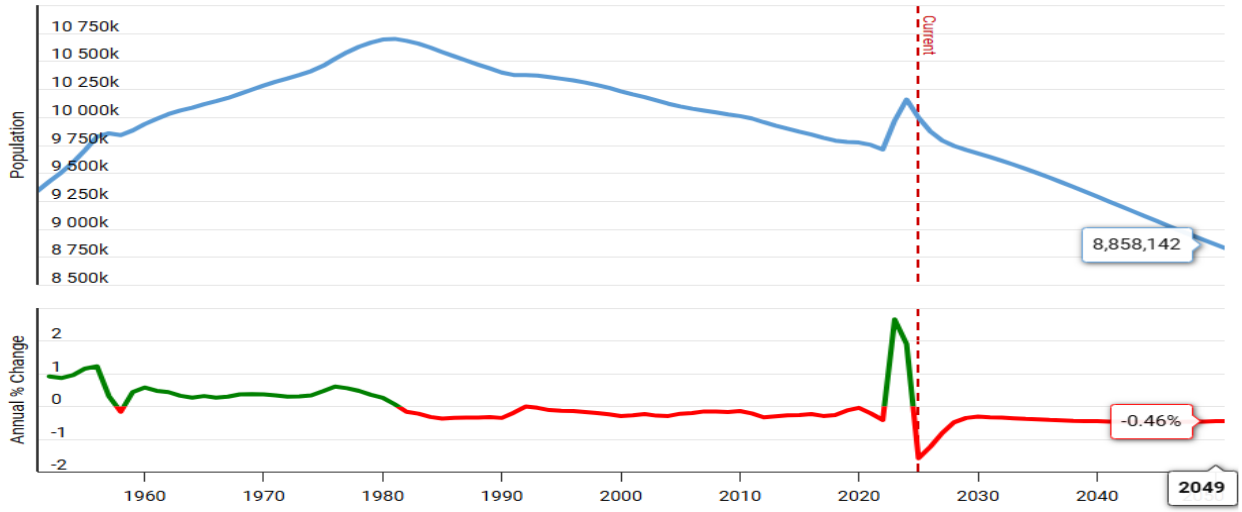


Рисунок 7 – Динаміка та темпи змін людського ресурсу Угорщини з прогнозом до 2050 року

Джерело: *https://www.macrotrends.net/global-metrics/countries/RUS/russia/population*

Зрештою, вивчення перспектив максимізації людського капіталу через цільові політичні рекомендації та стратегічні ініціативи може висвітлити шлях до більш процвітаючого майбутнього для Угорщини.

Хоча в Угорщині розвивається технологічна індустрія з численними стартапами, попит на кваліфікованих розробників програмного забезпечення та інженерів часто перевищує пропозицію. Це недостатнє використання людського потенціалу посилюється відсутністю співпраці між навчальними закладами та промисловістю, де перші не можуть належним чином підготувати студентів до практичних потреб робочої сили. Таким чином, необхідно проаналізувати цю динаміку, щоб визначити, як Угорщина може краще використовувати свій людський капітал перед обличчям цих історичних і сучасних викликів.

Виявлення можливостей розвитку людського потенціалу Угорщини, що розвивається, має ключове значення для використання її у досягненні необхідного рівня оборонної достатності. У країні спостерігається зростання в різних галузях, таких як інформаційні технології, відновлювана енергетика та туризм. IT-сектор став центром економічного зростання, а Будапешт стає регіональним технологічним центром, який залучає значні інвестиції. Крім того, сприяння підприємництву та інноваціям є критично важливим у цьому контексті; В Угорщині є жвава екосистема стартапів, але багато підприємців-початківців стикаються з такими перешкодами, як доступ до капіталу та наставництва. Заохочення культури, яка сприймає ризик, підкріплене доступним фінансуванням та інкубаторами, могло б стимулювати створення робочих місць та інновації. Оскільки Угорщина продовжує модернізувати свою економіку, розуміння та заохочення цих можливостей для розвитку буде життєво важливим для максимізації людського потенціалу та забезпечення сталого економічного зростання (рис. 8).

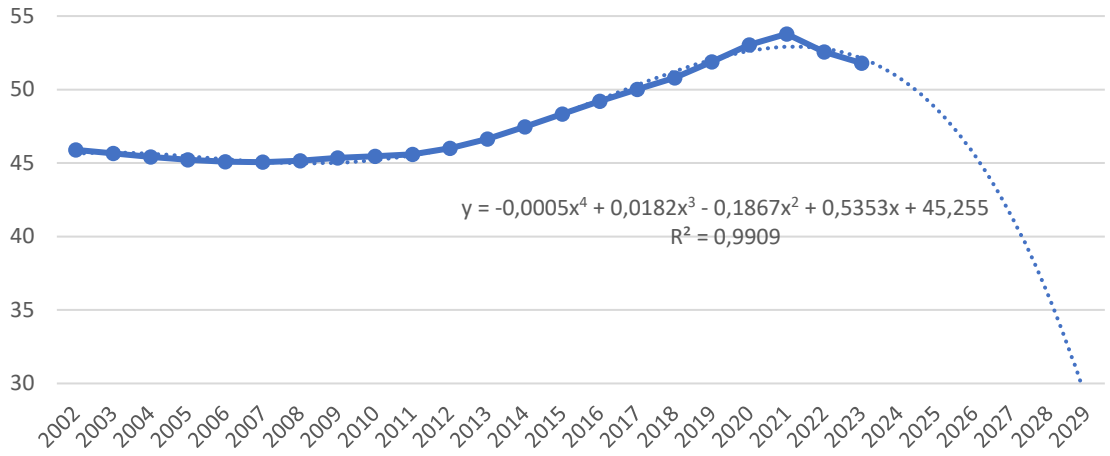


Рисунок 8 – Коефіцієнт вікової залежності Угорщини (% населення працездатного віку)
Джерело: *https://data.worldbank.org/indicator/SM.POP.REFG?end=2023&locations*

Дивлячись у майбутнє, максимізація людського потенціалу в Угорщині потребує узгоджених зусиль як уряду, так і освітніх закладів для впровадження ефективної політики та стратегій. Створюючи сприятливі умови, такі як податкові пільги, спрощена бюрократія та надійна підтримка досліджень і розробок, країна може спонукати міжнародні компанії розпочинати діяльність у межах її кордонів. Крім того, покращення людського капіталу може мати серйозні наслідки як для економіки, так і для суспільства в цілому. Підвищення навичок і кваліфікації може призвести до підвищення продуктивності, підвищення заробітної плати та покращення рівня життя, що зрештою сприятиме більш динамічній та стійкій економіці. Стратегічно вирішуючи ці сфери, Угорщина може повністю розкрити свій людський потенціал, прокладаючи шлях до більш світлого та процвітаючого майбутнього.

Російсько-український конфлікт, який спалахнув у 2014 році, мав глибокі наслідки для геополітичного ландшафту Східної Європи, зокрема для самої рф. Війна, що триває, суттєво вплинув на розвиток людського потенціалу, призвівши до зменшення можливостей для отримання освіти та зміщення уваги від інновацій та критичного мислення (рис. 9).

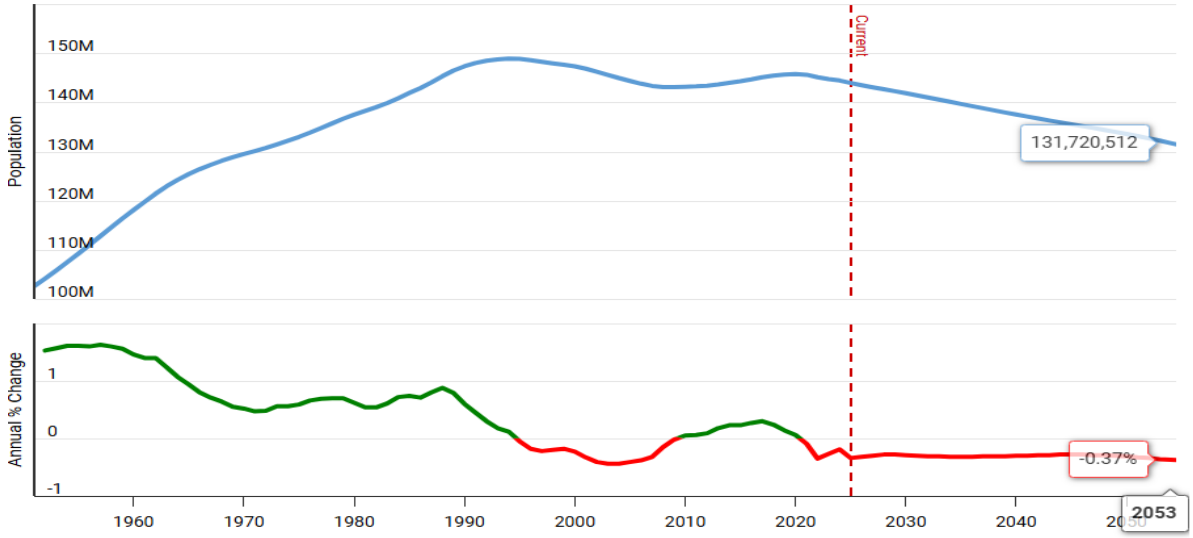


Рисунок 9 – Динаміка та темпи змін людського ресурсу рф з прогнозом до 2050 року
Джерело: *https://www.macrotrends.net/global-metrics/countries/RUS/russia/population*

Якість вищої освіти в рф зіткнулася з проблемами через брак фінансування, посилений бюрократичний контроль і навчальну програму, яка часто ставить пріоритет ідеологічній

відповідності над академічною свободою. Крім того, конфлікт утримав багатьох молодих спеціалістів від кар'єри в секторах, які могли б сприяти національному розвитку, оскільки економічні санкції та політична ізоляція зменшили перспективи працевлаштування у життєво важливих галузях (рис. 10). Ця ситуація призвела до відтоку кваліфікованих кадрів за кордон, що ще більше загострює проблеми, з якими стикається рф у підвищенні своєї оборонної достатності.

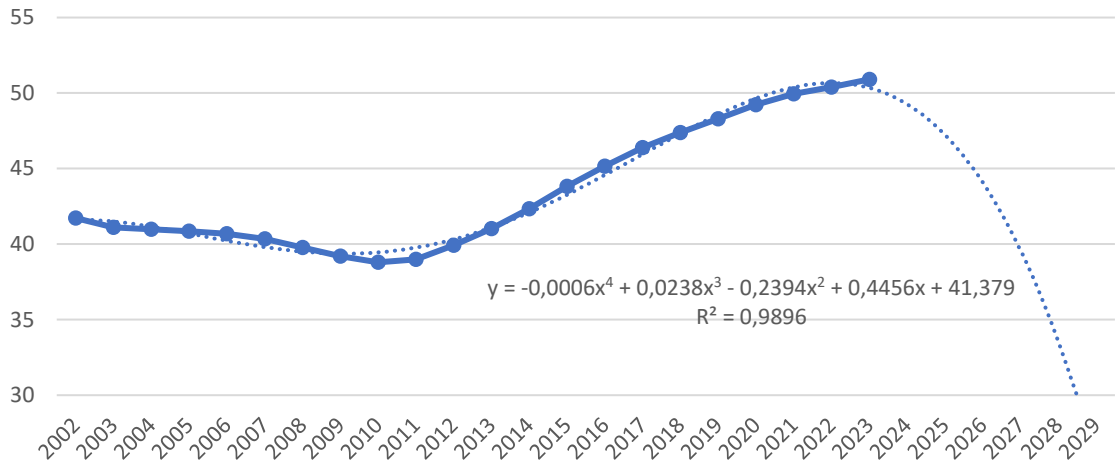


Рисунок 10 – Коефіцієнт вікової залежності рф (% населення працездатного віку)
Джерело: *https://data.worldbank.org/indicator/SM.POP.REFG?end=2023&locations*

Польща, нація з багатою історичною спадщиною та яскравою культурою, зараз переживає етап трансформації, який характеризується значним економічним зростанням та інтеграцією до Європейського Союзу. Одним із найважливіших активів Польщі є її людський потенціал — динамічна та різноманітна робоча сила, здатна стимулювати інновації та економічне процвітання. Однак, незважаючи на багатообіцяючу перспективу, на польському ринку праці існує парадокс, який позначається неповною зайнятістю та невідповідністю кваліфікації, що перешкоджає оптимальному використанню цього потенціалу (рис. 11).

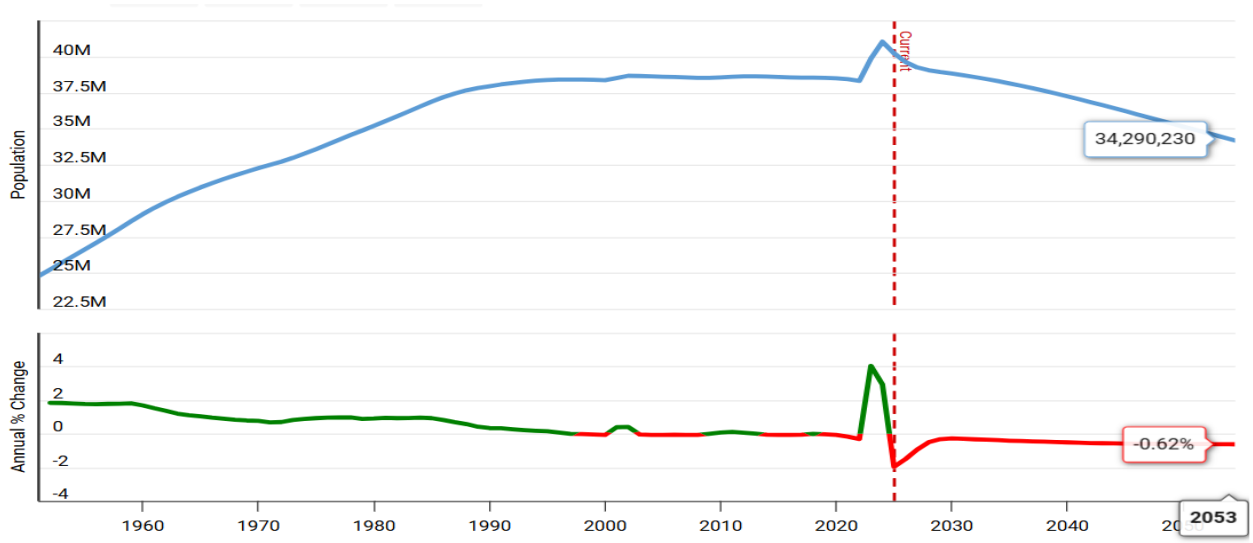


Рисунок 11 – Динаміка та темпи змін людського ресурсу Польщі з прогнозом до 2050 року
Джерело: https://www.macrotrends.net/global-metrics/countries/RUS/russia/population

Незважаючи на сприятливий демографічний профіль та освітні досягнення Польщі, зберігаються значні області невикористаного потенціалу, що в першу чергу проявляється через неповну зайнятість і невідповідність кваліфікацій на ринку праці. Звіти Головного статистичного управління Польщі свідчать про те, що приблизно 40% випускників знаходять роботу, яка не вимагає рівня їхньої освіти, що не тільки підриває індивідуальне задоволення від роботи, але й обмежує загальну продуктивність. Крім того, деякі регіони, особливо у східних частинах країни, продовжують стикатися з високим рівнем безробіття, що посилюється нижчим рівнем освіти та обмеженим доступом до програм професійної підготовки. Наприклад, у Підкарпатському воєводстві постійний рівень безробіття перевищує 10%, що часто пояснюється відсутністю місцевої промисловості та недостатніми інвестиціями в розвиток людського капіталу. Крім того, сектори, які готові до зростання, такі як технології та зелена енергетика, стикаються з гострою нестачею кваліфікованих працівників. Наприклад, IT-сектор, що розвивається, спостерігав попит на понад 50 000 нових спеціалістів щорічно, але освітня система не відповідала належним чином цьому попиту. Усунення цих розбіжностей через цільові навчальні ініціативи та програми регіонального розвитку має вирішальне значення для невикористаного людського потенціалу та забезпечення справедливого економічного зростання по всій Польщі. Польський уряд визнав необхідність інвестування в освітні та навчальні програми, які відповідають потребам ринку, прикладом чого є такі ініціативи, як Національна стратегія навичок до 2030 року, яка спрямована на підвищення якості професійного навчання та сприяння навчанню протягом усього життя. Таким чином, майбутні перспективи розвитку Польщі залежать від ефективного використання її людського потенціалу через цілеспрямовану політику, інвестиції в освіту та сприяння міжнародним партнерствам, які можуть підштовхнути країну до більш процвітаючого та збалансованого економічного майбутнього. (рис. 12).

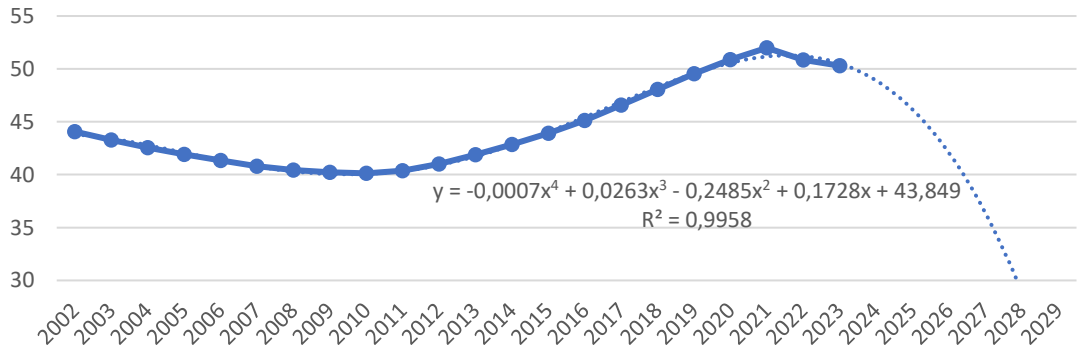


Рисунок 12 – Коефіцієнт вікової залежності Польщі (% населення працездатного віку)
Джерело: *https://data.worldbank.org/indicator/SM.POP.REFG?end=2023&locations*

Сучасний стан людського потенціалу в Америці характеризується складним взаємовпливом демографічних показників, рівня освіти та економічних проблем. Сполучені Штати є домом для понад 330 мільйонів осіб, однак, незважаючи на цей величезний резерв людських ресурсів, відмінності в освіті та кваліфікації зберігаються. За даними Бюро статистики праці США, приблизно 34% американської робочої сили мають ступінь бакалавра або вищу, тоді як багато інших не мають доступу до якісної освіти та професійного навчання. Економічні проблеми, такі як наслідки пандемії COVID-19, посилили ці відмінності в освіті та призвели до значних змін у попиті на робочу силу (рис. 13). Тому розуміння поточного стану людського потенціалу в Америці має вирішальне значення для розробки ефективних стратегій використання та підвищення цього потенціалу в майбутньому.

Виявлення та розкриття прихованих талантів і навичок серед американської робочої сили має важливе значення для сприяння більш інклюзивній та динамічній економіці. Професійне навчання та освітні програми відіграють важливу роль у цьому. Такі ініціативи, як учнівство та професійне навчання, часто в партнерстві з місцевими підприємствами, надають людям практичний досвід і відповідні навички, які відповідають вимогам галузі. Наприклад, такі програми, як ініціатива Apprenticeship USA, успішно об'єднали тисячі працівників із високооплачуваною роботою в професійних і технічних сферах, демонструючи силу цілеспрямованого розвитку навичок. Крім того, громадські ініціативи, спрямовані на розвиток навичок, такі як некомерційні організації, які надають безкоштовне навчання технологіям і підприємництву, набувають популярності.

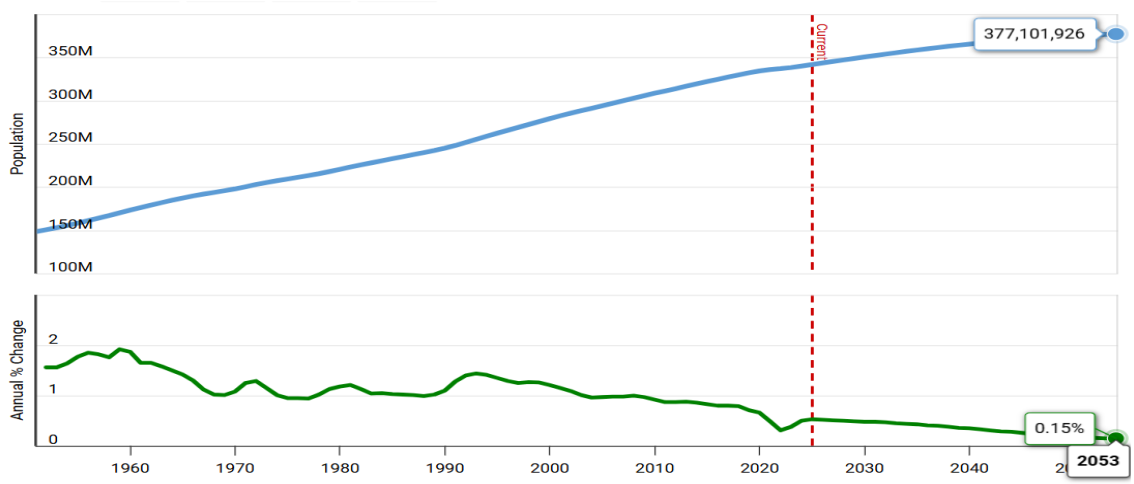


Рисунок 13 – Динаміка та темпи змін людського ресурсу США з прогнозом до 2050 року
Джерело: *https://www.macrotrends.net/global-metrics/countries/RUS/russia/population*

Навчальні онлайн-платформи, такі як Coursera та Udacity, демократизували доступ до високоякісних освітніх ресурсів, дозволяючи людям продовжувати навчання у власному темпі та відповідно до своїх інтересів. Цей технологічний зсув не тільки допомагає людям виявити свої приховані таланти, але й забезпечує постійне вдосконалення та підвищення кваліфікації, що є важливим на сучасному швидкому ринку праці (рис. 14). Таким чином, комплексний підхід, який поєднує формальне навчання, залучення громади та технологічні інновації, є життєво важливим для виявлення та виховання прихованих навичок серед американського населення.

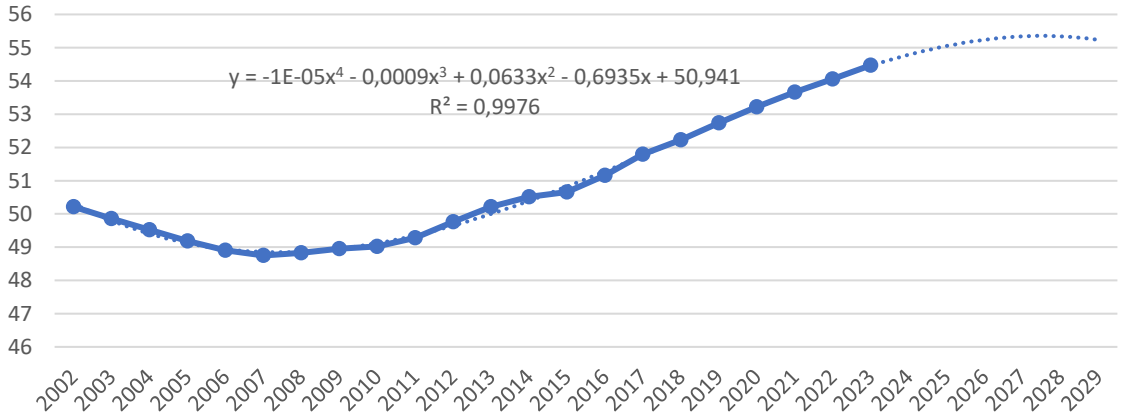


Рисунок 14 – Коефіцієнт вікової залежності США (% населення працездатного віку)
Джерело: *https://data.worldbank.org/indicator/SM.POP.REFG?end=2023&locations*

Галузі, що розвиваються, такі як відновлювана енергетика, біотехнології та штучний інтелект, відкривають значні перспективи на ринку праці, які можна використовувати для стимулювання економічного зростання. За даними Всесвітнього економічного форуму, лише перехід до "зеленої" економіки може створити 24 мільйони нових робочих місць до 2030 року, що підкреслює потребу в робочій силі, яка адаптується та кваліфікована у відповідних сферах.. Наприклад, впровадження політики, яка передбачає фінансові стимули для компаній інвестувати в навчання співробітників, може перенести тягар розвитку навичок з окремих осіб на роботодавців, сприяючи спільним зусиллям для створення більш кваліфікованої робочої сили.

Висновки

Україна стоїть на порозі суттєвої трансформації свого людського потенціалу. Хоча поточний стан освітніх досягнень і компетенцій робочої сили є міцною основою, перешкоди економічної, політичної нестабільності та соціальної нерівності створюють величезні виклики, які необхідно вирішити. Однак у середньостроковій перспективі відкриваються численні можливості для розвитку завдяки стратегічним освітнім реформам, технологічним досягненням і міжнародній співпраці. Використовуючи ці можливості, Україна може повністю розкрити потенціал свого людського капіталу, створюючи кваліфіковану робочу силу, яка не лише сприяє економічному зростанню, але й покращить оборону достатність країни. Натомість вивчаючи поточний стан робочої сили Литви, усуваючи перешкоди, які заважають розвитку, і досліджуючи майбутні перспективи, стає очевидним, що для розкриття всього людського потенціалу необхідні стратегічні дії. У той час як демографічні зміни та економічні обмеження створюють проблеми, високий рівень освіти серед населення та поява інноваційних секторів створюють унікальну можливість для зростання. *(Хоча динаміка та темпи змін людського ресурсу України та Литви з прогнозом до 2050 року має тенденцію до поступового спаду, однак екстраполяція значень коефіцієнту вікової залежності до 2029 року свідчить про його зростання, що є позитивним для розвитку людського потенціалу та підвищення за рахунок цього оборонної достатності у середньостроковій перспективі.)*

Затягування російсько-української війни для рф підвищують ризики регіональних розбіжностей і сепаратистських настроїв, що загрожує національній єдності. Певні регіони, особливо ті, що мають значну кількість етнічних меншин, можуть дедалі більше розчаровуватися в політиці центрального уряду та підході до управління. Розуміючи поточний стан людського капіталу, визначаючи області недостатнього використання та досліджуючи майбутні можливості, Польща може позиціонувати себе як конкурентоспроможного гравця на європейській арені. Взаємодія між освітніми реформами, державною підтримкою та міжнародним співробітництвом матиме вирішальне значення для розкриття її потенціалу та вирішення проблем, пов'язаних із зміною ринку праці. Оскільки Польща продовжує рухатися шляхом до модернізації та зростання, ефективне залучення її людських ресурсів, безсумнівно, слугуватиме підвищенню її оборонної достатності. Потенціал для розвитку людського капіталу Китаю величезний, але він тісно пов'язаний із взаємодією демографічних тенденцій, освітньої реформи, технологічного прогресу та культурного ставлення. Хоча поточний стан людського потенціалу представляє як можливості, так і проблеми, майбутня траєкторія значною мірою залежатиме від того, наскільки ефективно ці елементи будуть розглянуті. Однак не менш важливо протистояти соціально-економічним відмінностям, регуляторним перешкодам і культурним уявленням, які гальмують прогрес, що має безпосередній вплив на оборону достатність країни. Невикористаний людський потенціал Угорщини являє собою значну можливість для країни підняти свій економічний і соціальний статус на світовій арені. Розуміючи ключові сектори, які можуть бути використані для зростання, і впроваджуючи

стратегічну довгострокову політику, Угорщина може використовувати свої демографічні переваги для сприяння зростанню, інноваціям та підвищенню власної оборонної достатності *(Динаміка та темпи змін людського ресурсу Польщі, рф , Китаю та Угорщини з прогнозом до 2050 року, а також екстраполяція значень коефіцієнту вікової залежності до 2029 року має тенденцію до поступового спаду, що є негативним для розвитку людського потенціалу та підвищення за рахунок цього оборонної достатності у середньостроковій перспективі).*

Єдиною країною, у якої динаміка та темпи змін людського ресурсу з прогнозом до 2050 року, а також екстраполяція значень коефіцієнту вікової залежності до 2029 року має тенденцію до поступового зростання є США, що є свідченням сталої політики уряду щодо підтримки розвитку людського потенціалу країни.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Spengler, L. (2018). 5. Sufficiency as policy: potential solutions. У Sufficiency as Policy (с. 234–283). Nomos Verlagsgesellschaft mbH & Co. KG. https://doi.org/10.5771/9783845284743-234
2. DEFENSE. (2020). У Human Nature (с. 47–48). New York University Press. https://doi.org/10.18574/nyu/9780814705490.003.0017
3. Gurov, O. N., & Petrunina, M. A. (2020). Digital transformation: human measurement. Humanities Bulletin of BMSTU, (82). https://doi.org/10.18698/2306-8477-2020-2-654
4. 1944-, R. A. A., National Defense Research Institute (U.S.) & United States. Dept. of Defense. Office of the Secretary of Defense. (Ред.). (1997). *Differentiation in military human resource management*. RAND.
5. Syzov, A., & Koval, O. (2021). HUMAN POTENTIAL IN THE PART OF THE DEFENSE ECONOMY STATE. *Visnyk Taras Shevchenko National University of Kyiv. Military-Special Sciences*, (4 (48)), 42–49. https://doi.org/10.17721/1728-2217.2021.48.42-49
6. Wijaya, S. W., Dwiatmoko, A., Surendro, K., & Sastramihardja, H. S. (б. д.). A Statistical Analysis of Priority Factors for Local e-Government in a Developing Country. У *Human Resources Management* (с. 215–231). IGI Global. https://doi.org/10.4018/978-1-4666-1601-1.ch014
7. Головко, Л. С. (2014). Людський капітал як ресурс економічного розвитку. *Економічний нобелівський вісник*, (1 (7)), 122–127.
8. Яковенко, Р. В. (2013). Людський капітал та людський потенціал. *Наукові праці Кіровоградського національного технічного університету. Економічні науки*, (вип. 24), 186–193.
9. University, N. D. (Ред.). (1983). *Human resources and defense manpower*. National Defense University.
10. Яковенко, Р. В. (2008). Людський потенціал: економічний зміст, структура та характеристика. *Зовнішня торгівля: право та економіка*, (5 (40)), 126–130.
11. Bandow, D. (1989). *Human resources and defense manpower*. Institute of Higher Defense Studies, National Defense University.
12. United States. Defense Science Board. Task Force on Human Resources Strategy. (2000). *The* Defense *Science Board Task Force on Human Resources Strategy.* Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics.

References

1. Spengler, L. (2018). 5. Sufficiency as policy: potential solutions. U Sufficiency as Policy (s. 234–283). Nomos Verlagsgesellschaft mbH & Co. KG. https://doi.org/10.5771/9783845284743-234
2. DEFENSE. (2020). U Human Nature (s. 47–48). New York University Press. https://doi.org/10.18574/nyu/9780814705490.003.0017
3. Gurov, O. N., & Petrunina, M. A. (2020). Digital transformation: human measurement. Humanities Bulletin of BMSTU, (82). https://doi.org/10.18698/2306-8477-2020-2-654
4. 1944-, R. A. A., National Defense Research Institute (U.S.) & United States. Dept. of Defense. Office of the Secretary of Defense. (Red.). (1997). Differentiation in military human resource management. RAND.
5. Syzov, A., & Koval, O. (2021). HUMAN POTENTIAL IN THE PART OF THE DEFENSE ECONOMY STATE. Visnyk Taras Shevchenko National University of Kyiv. Military-Special Sciences, (4 (48)), 42–49. https://doi.org/10.17721/1728-2217.2021.48.42-49
6. Wijaya, S. W., Dwiatmoko, A., Surendro, K., & Sastramihardja, H. S. (b. d.). A Statistical Analysis of Priority Factors for Local e-Government in a Developing Country. U Human Resources Management (s. 215–231). IGI Global. https://doi.org/10.4018/978-1-4666-1601-1.ch014
7. Holovko, L. S. (2014). Liudskyi kapital yak resurs ekonomichnoho rozvytku. Ekonomichnyi nobelivskyi visnyk, (1 (7)), 122–127.
8. Yakovenko, R. V. (2013). Liudskyi kapital ta liudskyi potentsial. Naukovi pratsi Kirovohradskoho natsionalnoho tekhnichnoho universytetu. Ekonomichni nauky, (vyp. 24), 186–193.
9. University, N. D. (Red.). (1983). Human resources and defense manpower. National Defense University.
10. Yakovenko, R. V. (2008). Liudskyi potentsial: ekonomichnyi zmist, struktura ta kharakterystyka. Zovnishnia torhivlia: pravo ta ekonomika, (5 (40)), 126–130.
11. Bandow, D. (1989). Human resources and defense manpower. Institute of Higher Defense Studies, National Defense University.
12. United States. Defense Science Board. Task Force on Human Resources Strategy. (2000). The Defense Science Board Task Force on Human Resources Strategy. Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics.

Обґрунтування підходу до оптимального підбору показників діяльності сектору оборони України

Justification of the approach to the optimal selection of performance indicators of the defense sector of Ukraine

Віталій Ткаченко [A]
Corresponding author: Заступник начальника Головного управління персоналу, e-mail: vitalik000000@ukr.net, ORCID: 0009-0003-7825-1811

Олексій Чорненький [B]
молодший науковий співробітник відділу, e-mail: nososek@gmail.com, ORCID: 0000-0002-1609-1950

Сергій Гаценко [C]
к. тех. наук, доцент, e-mail: verb388097@proton.me, ORCID: 0000-0002-0957-6458

Сергій Мордвінов [C]
провідний науковий співробітник. e-mail: mordvinoff@meta.ua. ORCID: 0000-0002-0451-9868

Vitaly Tkachenko [A]
Corresponding author: Deputy Chief of the Main Personnel, e-mail: vitalik000000@ukr.net, ORCID: 0009-0003-7825-1811

Oleksii Chornenkyi [B]
Junior Researcher of the Department, e-mail: nososek@gmail.com, ORCID: 0000-0002-1609-1950

Serhii Hatsenko [C]
Candidate of Technical Sciences, e-mail: verb388097@proton.me, ORCID: 0000-0002-0957-6458

Serhii Mordvinof [C]
Leading researcher of the research. e-mail: mordvinoff@meta.ua. ORCID: 0000-0002-0451-9868

[A] Генеральний штаб ЗС України, м. Київ, Україна
[B] Науково-дослідний інститут воєнної розвідки. м. Київ, Україна
[C] Національний університет оборони України. м. Київ, Україна

[A] General Staff of the Armed Forces of Ukraine. Kyiv, Ukraine
[B] Defence Intelligence Research Institute, Kyiv, Ukraine
[C] National University of Defense of Ukraine, Kyiv, Ukraine

Received: October 2, 2024 | Revised: October 20, 2024 | Accepted: October 31, 2024

DOI: 10.33445/sds.2024.14.5.6

Мета роботи: сформувати рекомендації щодо удосконалення системи показників діяльності сектору оборони України.
Метод: метод комплексного аналізу та узагальнення.
Результати дослідження: підвищення ефективність реалізації заходів з розвитку сектору оборони України та запровадити зрозумілу, прозору, всебічну систему оцінювання діяльності складових сектору оборони.
Теоретична цінність дослідження: теоретичні положення, висновки та рекомендації, викладені в роботі, можуть стати основою для подальших наукових досліджень й дискусій з питань підвищення продуктивності діяльності сектору оборони України.
Практична цінність дослідження: реалізація рекомендацій і пропозицій, обґрунтованих у роботі, дозволить вдосконалити процес стратегічного управління діяльністю сектору оборони України.
Оригінальність/Цінність дослідження: в даному дослідженні побудова комплексної системи показників діяльності сектору оборони України ще не були предметом комплексного наукового дослідження.
Обмеження дослідження: обмеження дослідження полягає у використанні джерел, що знаходяться у відкритому доступі.
Тип статті: теоретичний, практичний.

Ключові слова: безпекове середовище; стратегія розвитку; сектор оборони держави.

Purpose: formulate recommendations for improving the system of performance indicators of the defense sector of Ukraine.
Method: method of complex analysis and generalization.
Findings: an attempt to increase the efficiency of the implementation of measures for the development of the defense sector of Ukraine and to introduce a clear, transparent, comprehensive system for evaluating the activities of the components of the defense sector.
Theoretical value of the study: theoretical provisions, conclusions and recommendations presented in the work can become the basis for further scientific research and discussions on the issues of increasing the productivity of the defense sector of Ukraine.
Practical value of the study: the implementation of recommendations and proposals substantiated in the work will allow to improve the process of strategic management of the activities of the defense sector of Ukraine.
Originality/value of the study: in this study, the construction of a complex system of performance indicators of the defense sector of Ukraine has not yet been the subject of a comprehensive scientific study.
Limitations of the study: a limitation of the study is the use of publicly available sources.
Type of article: theoretical, practical.

Key words: security environment; development strategy; the defense sector of the state.

Вступ

Ефективні системи оцінки продуктивності мають вирішальне значення для того, щоб організації оцінювали ефективність своїх співробітників і приймали обґрунтовані рішення для зростання та розвитку. Однак традиційний підхід до оцінки продуктивності, заснований

виключно на одному критерії, виявляється недостатнім для охоплення усієї складності та багатьох вимірів ефективності. Багатокритеріальна оптимізація передбачає інтеграцію кількох критеріїв ефективності для створення цілісного уявлення про ефективність організації. Розглядаючи різні параметри, такі як продуктивність, якість, інновації, командна робота та задоволеність замовників чи клієнтів, організації можуть краще оцінити свою загальну ефективність.

Теоретичні основи дослідження

Різні аспекти, сфери і підходи до оцінювання діяльності сектору оборони держави досліджував ряд вітчизняних вчених. Серед них виділяються праці Олександра Георгадзе, присвячені методикам оцінювання, зокрема, рівня організації об'єднаної підготовки сил оборони; Ольги Резнікової, присвячені аналізу безпекового середовища України; Володимира Абрамова, Григорія Ситника, Андрія Дацюка, Олексія Полторака, присвячені різноманітним аспектам забезпечення глобальної та національної безпеки, Івана Руснака, Івана Ткача, В.С.Корендовича, Миколи Ткача, присвячені оборонному плануванню на основі спроможностей та оборонному менеджменту в діяльності Збройних Сил України, а також роботи інших дослідників. Серед актуальних зарубіжних наукових праць, присвячених дослідженню показників ефективності діяльності в різних сферах, обґрунтуванню вибору індикаторів ефективності для узгодження стратегій розвитку з бажаними результатами, покращення розподілу ресурсів і підвищення підзвітності, варто відмітити такі, як «Управління ефективністю стратегічної оборони», де підкреслюється вирішальна роль управління ефективністю стратегічної оборони в загальному процесі управління системою оборони [1], "Ефективність і перспективи аерокосмічної та оборонної промисловості (A&D): PwC" з ключовими показниками ефективності, сучасними розробками та майбутніми перспективами глобальної комерційної аерокосмічної та оборонної промисловості [2]; серію публікацій RAND «Вимірювання продуктивності» щодо оцінювання та вимірювання продуктивності в різних сферах, включаючи цивільну, військову, освітню, медичну і судову [3]; "Показники ефективності для боєздатних сил у Збройних Силах", де розглянуто розробку показників ефективності у військовому контексті, з особливим акцентом на боєздатних силах [4].

У той же час питання обґрунтування рекомендацій щодо побудови комплексної системи показників діяльності сектору оборони України ще не були предметом комплексного наукового дослідження, що і визначає актуальність і важливість дійсного дослідження.

Постановка проблеми

В умовах сучасного світу, який динамічно змінюється, проблема забезпечення національної безпеки для будь-якої держави світу є однією з ключових у контексті забезпечення її розвитку [5]. Це повною мірою стосується і України, особливо з врахуванням її геополітичного становища та сучасної ролі у забезпеченні існування мирної і спокійної Європи [6]. Національна безпека споконвіку була тісно пов'язана з боротьбою за виживання, причому не тільки у фізичному сенсі в умовах несприятливого оточення, а й у політико-економічному, з точки зору діяльності сусідніх держав. Аналізу цих проблем, а також проблем взаємодії між безпекою, населенням, урядом та державою присвятив свої труди Томас Гоббс. У своїх роботах від зробив висновок про те, що "людина – це істота цивілізована страхом смерті". Тому кожна людина шукає засоби, як персонального так й колективного захисту від різного роду загроз, які виникають у процесі її життєдіяльності. Це змушує людину жити у суспільстві. Безпеку слід розглядати як одну із важливих функцій соціальної системи (включно до цивілізаційного рівня), яка характеризує її відповідний стан дієздатності та готовності до вирішування складних завдань. У такому розумінні зміст безпеки можна визначати, як ціль,

спосіб та умови існування соціальної системи. Це підтверджує роль безпеки, що займає ключову позицію в теорії національної безпеки та є головною передумовою прогресивного розвитку цивілізації [7].

Мета статті. На основі аналізу існуючих підходів щодо оцінювання діяльності урядових організацій в Україні та в країнах-членах ЄС і НАТО сформувати рекомендації щодо удосконалення системи показників діяльності сектору оборони України.

Методологія дослідження

Для досягнення сформульованої мети та поставлених завдань статті використано комплекс загальнонаукових та спеціальних методів дослідження, а саме: системний підхід – для теоретичного узагальнення знань про явища та процеси у взаємозв'язку та розвитку; аналізу і синтезу – для узагальнення підходів до оцінювання діяльності сектору оборони України; систематизації та порівняння – для аналізу зарубіжних та вітчизняних методик оцінювання діяльності сектору оборони; індукції, дедукції та абстрагування – для розробки практичних рекомендацій щодо модернізації системи критеріїв оцінювання діяльності сектору оборони з урахуванням досвіду країн-членів НАТО; метод комплексного аналізу та узагальнення – для формулювання наукових визначень та висновків.

Результати

У традиційній оптимізації одна цільова функція оптимізується для пошуку найкращого рішення. Однак у реальних сценаріях організації часто мають кілька цілей, які необхідно враховувати. В контексті сектору оборони, можна прагнути мінімізувати вартість витрат на забезпечення його роботи, максимізуючи отримувані результати його діяльності. Подібним чином, при проектуванні кількості і якості збройних сил держави можна прагнути максимізувати їх продуктивність при мінімізації споживання державних ресурсів. Оптимізація за багатьма критеріями визнає, що часто існують суперечливі цілі та компроміси між ними. Вона прагне знайти набір рішень, які представляють оптимальні компроміси між різними критеріями. Ці рішення відомі як оптимуми Парето і представлені на фронті Парето, який є графічним зображенням компромісів між цілями. Щоб проілюструвати цю концепцію далі, розглянемо приклад сектору оборони держави. Держава може мати кілька цілей, таких як максимізація ступеню своєї безпеки, мінімізація витрат на досягнення цього результату і забезпечення ефективності, але компактності своїх збройних сил. Ці цілі можуть суперечити одна одній, оскільки збільшення рівня забезпеченої безпеки може призвести до підвищення витрат або погіршити компактність збройних сил. Застосовуючи багатокритеріальну оптимізацію, держава може визначити набір рішень, які представляють найкращі компроміси між цими цілями, дозволяючи їм приймати обґрунтовані рішення, які врівноважують ці компроміси. Багатокритеріальна оптимізація широко застосовується в різних галузях, включаючи техніку, економіку, логістику та процеси прийняття рішень, що включають складні компроміси, і що найбільш притаманне публічному управлінню та адмініструванню. Для тих, хто приймає рішення, вона забезпечує структуру оцінювання та порівнювання різних рішень на основі кількох критеріїв, беручи до уваги внутрішні компроміси між ними.

Визначення відповідних критеріїв ефективності. Першим кроком багато-критеріальної оптимізації є визначення найбільш відповідних критеріїв ефективності для організації, що є вирішальним кроком у розробці комплексної системи оцінки ефективності, яка охоплює ключові аспекти діяльності організації. Це вимагає ретельного аналізу цілей, завдань і ключових показників ефективності (KPI) організації для визначення критеріїв, які найбільше відповідають її успіху. Залучаючи ключових зацікавлених сторін, таких як менеджери, співробітники та клієнти, організації можуть отримати цінну інформацію та

переконатися, що вибрані критерії відповідають їхнім стратегічним пріоритетам. Щоб проілюструвати цей процес, розглянемо сектор оборони держави. Деякі потенційні критерії ефективності, які можуть мати відношення до цієї організації, можуть включати:

1. Задоволеність замовників, тобто держави і суспільства: Цей критерій вимірює рівень задоволеності бенефіціарів діяльності сектору оборони, фактично замовників його послуг. Його можна оцінити за допомогою опитувань, механізмів зворотного зв'язку або відгуків клієнтів.

2. Швидкість реагування на зовнішні загрози: цей критерій вимірює швидкість, з якою сектор оборони запускає реакцію на зовнішні загрози, наявні чи передбачувані.

3. Якість функціонування сектору оборони, виконання його функцій: цей критерій оцінює надійність, функціональність і продуктивність діяльності сектору. Його можна виміряти за допомогою процесів тестування, звітів про помилки та відгуків замовників.

4. Продуктивність співробітників: цей критерій вимірює ефективність і результативність виконання співробітниками своєї роботи.

5. Інновації: цей критерій оцінює здатність сектору оборони впроваджувати інновації та розробляти нові технології, продукти або функції.

6. Фінансова ефективність: цей критерій зосереджується на фінансовому стані сектору, наприклад, зростанні результативності досягнення цілей, зниженні видатків та ефективності вкладених інвестицій. Важливо залучати ключових зацікавлених сторін, таких як менеджери, співробітники та замовники, до процесу визначення відповідних критеріїв ефективності. Їхні точки зору та ідеї можуть надати цінний внесок і забезпечити відповідність вибраних критеріїв стратегічним пріоритетам організації. Після визначення відповідних критеріїв ефективності організації повинні визначити їх пріоритетність на основі їх важливості та впливу на успіх організації.

Критерії зважування та пріоритетності. Після визначення відповідних критеріїв ефективності наступним кроком є призначення вагових коефіцієнтів кожному критерію на основі їх відносної важливості. Цей процес зважування гарантує, що певним критеріям приділяється більше уваги, ніж іншим, що відображає пріоритети організації. Визначення критеріїв пріоритетності дозволяє організаціям зосередитися на сферах, які мають найбільший вплив на їх продуктивність і стратегічні цілі. Держава визначила три критерії ефективності: рівень досягнутої безпеки, вартість утримання збройних сил і задоволеність замовників (тобто суспільства). Тепер потрібно призначити ваги для кожного критерію, щоб відобразити їх відносну важливість.

1. Рівень досягнутої безпеки. Держава вважає рівень досягнутої безпеки ключовим критерієм свого успіху. Вона призначає цьому критерію вагу 50%, що вказує на його високу важливість для оцінки загальної продуктивності.

2. Вартість утримання збройних сил: держава визнає, що вартість утримання збройних сил має значення не тільки для досягнення бажаного рівня безпеки, а й для можливостей державного бюджету їх утримувати. Вона призначає цьому критерію вагу 25%, що відображає його важливість для загальної продуктивності.

3. Задоволеність замовників (суспільства): держава приділяє значну увагу задоволенню суспільства і надає цьому критерію вагу 25%. Задоволені громадяни, швидше за все, залишатимуться лояльними та легше погоджуватимуться на збільшення видатків на утримання збройних сил.

Ваги, призначені кожному критерію, повинні відображати стратегічні пріоритети організації та відносну важливість кожного критерію для досягнення цих пріоритетів. Ваги можна визначити шляхом обговорення з ключовими зацікавленими сторонами, такими як керівники, співробітники та замовники, або через структурований процес прийняття рішень. Призначення вагових коефіцієнтів критеріям дозволяє організаціям визначати пріоритети

своїх зусиль і відповідно розподіляти ресурси.

Розробка інструментів вимірювання. Для ефективного вимірювання продуктивності за кількома критеріями організаціям необхідно розробити комплексні інструменти вимірювання. Ці інструменти необхідні для збору даних і оцінки продуктивності за визначеними критеріями і можуть включати опитування, інтерв'ю, оцінювання ефективності та механізми зворотного зв'язку.

1. Визначення показників: Першим кроком у розробці інструментів вимірювання є визначення конкретних показників або показників для кожного критерію ефективності. Ці показники мають бути вимірними та відповідати обраним критеріям.

2. Вибір методів збору даних: після того, як метрики визначені, організації повинні визначити найбільш відповідні методи збору даних. Це може включати опитування, інтерв'ю, спостереження, аналіз документів або комбінацію методів.

3. Розробка опитувань і анкет: опитування та анкети є широко використовуваними інструментами для збору даних у системах оцінки ефективності. Розробляючи опитування, важливо створювати чіткі та лаконічні запитання, які фіксують відповідну інформацію. Питання мають бути адаптовані до конкретного критерію, що оцінюється як якість послуг чи досвід взаємодії з сектором за шкалою від 1 до 5.

4. Впровадження збору даних: після того, як інструменти вимірювання, такі як опитування чи анкети, розроблені, організаціям необхідно впровадити процес збору даних.

5. Аналіз та інтерпретація даних: після того, як дані зібрані, їх потрібно проаналізувати та інтерпретувати, щоб отримати значущу інформацію.

6. Зворотній зв'язок і звітність: Останнім кроком у розробці інструментів вимірювання є надання зворотного зв'язку та звітності на основі зібраних і проаналізованих даних. Розробивши відповідні інструменти вимірювання, організації можуть збирати надійні та актуальні дані для оцінки ефективності за визначеними критеріями. Ці інструменти дозволяють організаціям відстежувати прогрес, визначати сфери вдосконалення та приймати обґрунтовані рішення для оптимізації продуктивності та досягнення своїх стратегічних цілей.

Інтеграція та аналіз даних. Після збору даних за допомогою засобів вимірювання, розроблених для системи оцінки продуктивності, наступним кроком є інтеграція та аналіз даних. Цей процес передбачає агрегування даних із різних джерел, виявлення закономірностей і тенденцій, а також отримання значущої інформації. Аналізуючи дані, організації можуть приймати обґрунтовані рішення та вживати необхідних заходів для оптимізації продуктивності.

1. Інтеграція даних: інтеграція даних – це процес консолідації даних із різних джерел в одному централізованому місці, часто сховищі даних. Ця інтеграція дає змогу отримувати комплексне уявлення про ефективність організації за різними критеріями.

2. Очищення та підготовка даних: перед початком аналізу важливо очистити та підготувати дані.

3. Методи аналізу даних: Існують різні техніки та методи, доступні для аналізу інтегрованих даних.

4. Виявлення моделей і тенденцій: під час процесу аналізу важливо визначити закономірності, тенденції та зв'язки в даних.

5. Дослідження та прийняття рішень: Кінцева мета аналізу даних полягає в тому, щоб отримати значущі висновки з даних, які можуть стати основою для прийняття рішень. Аналізуючи інтегровані дані, організації можуть визначити сильні сторони, області для вдосконалення та потенційні стратегії для оптимізації продуктивності.

6. Звітування та комунікація: після завершення аналізу важливо ефективно повідомити результати відповідним зацікавленим сторонам. Інтегруючи та аналізуючи зібрані дані, організації можуть отримати цінну інформацію про свою ефективність за визначеними

критеріями. Це дозволяє їм приймати рішення на основі даних, визначати сфери, які потрібно вдосконалити, і оптимізувати свою систему оцінки ефективності відповідно до своїх стратегічних цілей.

Постійне вдосконалення. Багатокритеріальний підхід до оптимізації оцінки продуктивності є безперервним процесом, який вимагає постійного вдосконалення – системного підходу, який організації застосовують для вдосконалення своїх операцій, процесів, продуктів або послуг. Це передбачає постійне визначення областей для вдосконалення, внесення поступових змін і прагнення до ефективності та результативності. Цей ітеративний процес гарантує, що система оцінки діяльності організації залишається ефективною та відповідає її стратегічним цілям. Інтеграція безперервного вдосконалення в культуру організації спонукає всіх співробітників брати активну участь у виявленні можливостей для вдосконалення. Це може включати пропонування ідей, оцінку поточних процесів і пошук способів усунення непродуктивної роботи. Для ефективного впровадження постійного вдосконалення організації дотримуються структурованого підходу, який зазвичай включає наступні етапи:

1. Визначте сфери для вдосконалення: організації регулярно оцінюють свою діяльність, щоб визначити сфери, які можна впорядкувати або оптимізувати.

2. Встановіть чіткі цілі: після визначення областей для вдосконалення організації встановлюють чіткі та конкретні цілі, які відповідають їхнім стратегічним цілям.

3. Плануйте та впроваджуйте зміни: організації розробляють плани дій для впровадження необхідних змін.

4. Вимірюйте та відстежуйте прогрес: організації встановлюють метрики та ключові показники ефективності (KPI) для вимірювання впливу впроваджених змін. Регулярний моніторинг і вимірювання дозволяють організаціям відстежувати прогрес, виявляти вузькі місця та вносити необхідні корективи.

5. Аналізуйте результати та навчайтеся: постійне вдосконалення передбачає аналіз результатів впроваджених змін для визначення їх ефективності.

6. Стандартизувати та підтримувати: успішні ініціативи щодо вдосконалення стандартизовані, щоб гарантувати, що зміни стануть частиною стандартних операційних процедур організації. Стандартизація допомагає підтримувати вдосконалення та гарантує, що організація продовжує отримувати користь від запроваджених змін. Для постійної оцінки процесів для подальшого вдосконалення встановлюються цикли зворотного зв’язку.

Реформування сектору оборони є необхідним кроком для забезпечення ефективності, сучасності та конкурентоспроможності української оборонної системи в умовах мінливого світового порядку та нових викликів безпеки. Оцінювання діяльності сектору оборони України є важливим завданням, яке дозволяє визначити ефективність його функціонування та рівень готовності до виконання завдань щодо оборони держави. Однак, існуюча система оцінювання має ряд недоліків, які ускладнюють її ефективність. Для вивчення вимог громадян до результатів та якості діяльності сектору оборони України і подальшого їх врахування у діяльності ОПВ щодо організації управління цим сектором важливо здійснити систематизацію чинників, що впливають на оцінювання відповідної діяльності. На основі аналізу підходів до оцінювання діяльності сектору оборони України, можна сформулювати наступну класифікацію чинників за групами: військова готовність, забезпечення та логістика, кадровий потенціал та навчання військовослужбовців, кібербезпека та інформаційна відкритість, міжнародна співпраця, реагування на загрози, розвиток та інновації, контроль та нагляд за діяльністю.

Група показників військової готовності включає рівень готовності збройних сил, наявність технічно сучасного озброєння та військової техніки, рівень тренувань і рівень мобілізаційної готовності.

Група показників забезпечення та логістики включає наявність ефективної системи

постачання; рівень забезпечення військовим обладнанням; рівень забезпечення амуніцією; відношення кількості зброї та військової техніки до встановлених норм забезпеченості; ступінь відповідності обсягу фінансування загрозам і завданням національної безпеки; наявність палива, боєприпасів, запасних частин, медичної підтримки та інших важливих ресурсів, необхідних для підтримки боєздатності армії; рівень фінансування з національного бюджету на потреби оборони; вартість військових проектів та вплив витрат на економіку країни; наявність та стан військових об'єктів; наявність та стан засобів зв'язку та розвідки; наявність та стан систем забезпечення безпеки.

Група показників кадрового потенціалу та навчання військовослужбовців включає кількість військовослужбовців; якість військовослужбовців (рівень їх професійної підготовки); рівень навчання та підготовки військовослужбовців; відношення кількості військово-службовців та працівників сектору оборони до встановлених норм забезпеченості.

Група показників кібербезпеки та інформаційної відкритості включає рівень захисту від кібератак; ефективність кіберзаходів та захист інформаційної інфраструктури.

Група показників міжнародної співпраці включає рівень участі у міжнародних альянсах; рівень участі в міжнародних військових операціях і спільних військових вправах; розрахунки захисту спільних інтересів; готовність до спільних миротворчих операцій.

Група показників реагування на загрози включає здатність сектору оборони реагувати на військові конфлікти; здатність сектору оборони реагувати на тероризм; здатність сектору оборони реагувати на кіберзагрози; здатність сектору оборони реагувати на гібридну війну; швидкість реакції сектору оборони на загрози (окремо нові та еволюційні).

Група показників розвитку та інновацій включає рівень інновацій у секторі оборони; впровадження нових технологій; розробка сучасного військового обладнання і зброї; рівень інвестицій в оборону.

Група показників контролю та нагляду за діяльністю включає рівень прозорості сектору оборони; рівень звітності сектору оборони; задоволеність замовників, тобто держави і громадян. Таким чином, наведені чинники впливають на оцінку якості діяльності сектору оборони України, і їх необхідно враховувати ОПВ у своїх зусиллях щодо удосконалення управління цією діяльністю. Завдання знаходження оптимальної системи оцінювання діяльності сектору оборони України полягає в знаходженні такої системи оцінювання, яка компромісне оптимізує показники якості при обмеженні вхідних даних та спектра визначених умов. Аналіз наукових джерел свідчить, що вже здійснювались спроби відшукання узагальненого критерію для такої задачі багатокритеріальної оптимізації [4, 8], проте знайдені рішення характеризувались, крім достоїнств, низкою вад, які не дозволяли пропонувати такі рішення для широкого застосування. Розгляд зазначених у попередньому підрозділі показників якості такої складної системи, якою є сектор оборони України, доводить, що результуюча система оцінки має бути багатокритеріальною.

Оптимізація системи управління сектором оборони України як великої складної системи має бути векторною, тобто виконуватися з урахуванням значень сукупності показників (векторів) якості $K(k_1, k_2, ..., k_n)$, в тому числі економічних, які заздалегідь враховані (прогнозуються) в критерії переваги (критерії оптимальності системи). Отже, при проведенні векторної оптимізації потрібно визначити такі значення змінних управління x, що належать допустимій області D і забезпечують одночасно мінімум усіх уведених критеріїв оптимальності $Q_k(x)$, $k = 1, 2, ..., s$ – характеристик, що вказують на відносну перевагу одного варіанту порівняно з іншим. Звичайно, ці критерії є суперечливими. Оптимізація за кожним з них приводить до різних значень змінних управління. Для врахування усієї сукупності часткових критеріїв необхідно проаналізувати векторний критерій оптимальності $Q(x) = [Q_1(x), ..., Q_s(x)]$, який приводить до розв'язання завдання багатокритеріальної оптимізації.

Таблиця 1 – Показники оцінювання якості діяльності сектору оборони України

Характеристика діяльності	Показники якості
1. Військова готовність	1.1. рівень готовності збройних сил 1.2. наявність технічно сучасного озброєння та військової техніки 1.3. рівень тренувань 1.4. рівень мобілізаційної готовності
2. Забезпечення та логістика	2.1. наявність ефективної системи постачання 2.2. рівень забезпечення військовим обладнанням 2.3. рівень забезпечення амуніцією 2.4. відношення кількості ОВТ до встановлених норм забезпеченості 2.5. ступінь відповідності обсягу фінансування загрозам і завданням нац. безпеки 2.6. наявність ПММ, боєприпасів, запасних частин, мед.підтримки та інших важливих ресурсів, необхідних для підтримки боєздатності 2.7. рівень фінансування з національного бюджету на потреби оборони 2.8. вартість військових проектів та вплив витрат на економіку країни 2.9. наявність та стан військових об'єктів 2.10. наявність та стан засобів зв'язку та розвідки 2.11. наявність та стан систем забезпечення безпеки
3. Кадровий потенціал та навчання військовослужбовців	3.1. кількість військовослужбовців 3.2. якість військовослужбовців (рівень їх професійної підготовки) 3.3. рівень навчання військовослужбовців 3.4. відношення кількості військовослужбовців та працівників сектору оборони до встановлених норм забезпеченості
4. Кібербезпека	4.1. рівень захисту від кібератак 4.2. ефективність кіберзаходів та захист інформаційної інфраструктури
5. Міжнародна співпраця	5.1. рівень участі у міжнародних альянсах 5.2. рівень участі в міжнародних військових операціях 5.3. розрахунки захисту спільних інтересів 5.4. готовність до спільних миротворчих операцій
6. Реагування на загрози	6.1. здатність сектору оборони реагувати на військові конфлікти 6.2. здатність сектору оборони реагувати на тероризм 6.3. здатність сектору оборони реагувати на кіберзагрози 6.4. здатність сектору оборони реагувати на гібридну війну 6.5. швидкість реакції сектору оборони на загрози (окремо нові та еволюційні)
7. Розвиток та інновації	7.1. рівень інновацій у секторі оборони 7.2. впровадження нових технологій 7.3. розробка сучасного військового обладнання і зброї 7.4. рівень інвестицій в оборону
8. Контроль та нагляд за діяльністю	8.1. рівень прозорості сектору оборони 8.2. рівень звітності сектору оборони 8.3. задоволеність замовників, тобто держави і громадян

Для сектору оборони України, наприклад, можна ввести такі часткові критерії: $Q_1(x)$ – функція, яка характеризує рівень військової готовності сектору оборони; $Q_2(x)$ – функція, яка характеризує рівень забезпечення та логістики сектору оборони; $Q_3(x)$ – функція, яка

характеризує рівень кадрового потенціалу та навчання військовослужбовців; $Q_4(x)$ – функція, яка характеризує рівень кібербезпеки та інформаційної відкритості; $Q_5(x)$ – функція, яка характеризує рівень міжнародної співпраці; $Q_6(x)$ – функція, яка характеризує рівень реагування на загрози; $Q_7(x)$ – функція, яка характеризує рівень розвитку та інновацій сектору оборони; $Q_8(x)$ – функція, яка характеризує рівень контролю та нагляду за діяльністю сектору оборони; $Q_9(x)$ – функція, що характеризує вартість утримання сектору оборони з урахуванням усіх перелічених властивостей.

При однокритеріальному розв'язуванні такого завдання оптимізації системи перевага зазвичай надається одному з вищенаведених критеріїв, а для інших визначається область допустимих розв'язків. Для розглядуваної системи такий підхід не є ефективним, оскільки перелічені часткові критерії суперечать один одному. Наприклад, критерій Q_5 – "рівень міжнародної співпраці" – суперечить критерію Q_6 – "рівень реагування на загрози", адже чим більша включеність сектору оборони у різноманітні міжнародні альянси і спільні миротворчі операції, тим більше необхідно часу для формування спільного виклику на загрози, що виникають. А виконання усіх критеріїв Q_1-Q_8 суперечить критерію Q_9 – "мінімум вартості".

Розв'язок завдання багатокритеріальної оптимізації в загальному випадку є неоптимальним для жодного з часткових критеріїв, але є компромісним для вектору $Q(x)$ у цілому. Потрібно зазначити, що розв'язок задачі багатокритеріальної оптимізації (компромісний розв'язок) $x^* \notin D$ є ефективною точкою, якщо для неї справедлива нерівність $Q(x^*) \leq Q(x)$ при $x \notin D$. Тобто, будь-який компонент $Q_k(x^*) \leq Q_k(x)$, де $k = 1, 2, ..., s$, але хоча б для одного з s чисел знайдеться точка $x \notin D$, в якій виконується жорстка нерівність $Q_j(x^*) \leq Q(x)$. З визначення ефективної точки випливає, що вона не єдина. Оптимальність векторного критерію $Q(x)$ означає, що не можна далі зменшувати значення одного з часткових критеріїв, не збільшуючи значення хоча б одного з інших. Для визначення мінімуму векторного критерію $Q(x)$ слід перейти від задачі векторної оптимізації до задачі нелінійної оптимізації зі спеціально сформульованою цільовою функцією $Q(x) = \Phi[Q_1(x), ..., Q_s(x)]$. Зробимо це.

Розглядаючи вимоги до складної системи, можна встановити, що рівень якості управління сектором оборони достатньо повно і правильно характеризується єдиним показником якості K_p. Крім цього, з'являється можливість з'ясувати, від яких часткових показників якості $K_1, ..., K_n$ системи S та у який спосіб залежить величина вектора K_p. Це означає, що вдається встановити залежність виду $K_p = f_p(K_1, ..., K_m)$. Тут $f_p(K_1, ..., K_n)$ – функція змінних $K_1, ..., K_n$, а K_p – величина, однозначно пов'язана з якістю системи S: чим менший вектор K_p, тим краща система. Надалі будемо припускати, що величина K_p невід'ємна і чим менший K_p, тим більш якісно функціонує система. При цьому найкращою (оптимальною) вважається така система S, для якої величина K_p мінімальна, тобто критерій оптимальності має вигляд:

$$\begin{gathered} K_p = \min_{S \in M_Д} f_p(K_1, \dots, K_i, \dots K_n), \\ K_i = K_i(S), i = \overline{1,n}, \\ K_i \leq K_{im}(S), i = \overline{1,n}, \end{gathered} \tag{1}$$

де $M_Д$ – множина усіх припустимих систем S;

K_{im} – значення показника якості K_i, що є гранично припустимим для системи. Очевидно, значення $K_{im}\left(i = \overline{1,n}\right)$ також мають бути обґрунтованими, виходячи з призначення системи.

Увести достатньо обґрунтований результуючий показник якості K_p, що є відомою функцією $f_p(K_1, \dots K_n)$ показників якості $K_1, \dots K_n$ для такої великої складної системи, якою є

сектор оборони України, не вдається. Тому доцільно сформулювати залежності $K_p = f_p(K_1, \dots K_n)$ іншим, суб'єктивним способом. Суб'єктивність обґрунтування виду результуючої цільової функції (і значень її параметрів) при цьому полягає в тому, що воно проводиться не шляхом кількісного аналізу впливу різних комбінацій значень показників $K_1, \dots, K_n$ на якість виконання системою її функцій, а шляхом інтуїтивних оцінок, які даються одним або кількома (краще – спільнотою) експертами.

Суб'єктивна результуюча цільова функція (СРЦФ) відносно грубо враховує вплив показників $K_1, \dots, K_n$ на якість системи. Тому при її застосуванні потрібно мати гарантії того, що оптимізована на основі цієї функції система виявиться строго припустимою і при тому не гіршою. Можна довести, що система, знайдена в результаті розв'язання задачі (1), обов'язково буде не гіршою, якщо функція $f_p(K_1, \dots, K_n)$ є монотонно зростаючою за кожним з аргументів.

Для багатокритеріальної оптимізації великої складної системи, якою є сектор оборони України, доцільно використовувати таку СРЦФ, яка дасть змогу врахувати нелінійний характер залежності результуючого показника якості K_p від показників $K_1, \dots, K_n$. Такою функцією пропонується обрати адитивну функцію втрат: де V_i – вагові коефіцієнти, вибрані за значимістю, виходячи з відносної важливості кожного з показників $K_1, \dots, K_n$: чим вагомішим вважається даний показник K_i (тобто, чим більше вдається мінімізувати цей показник у процесі оптимізації), тим більшою вибирається відповідна йому вага V_i; $f_i(K_i)$ – деяка безрозмірна у загальному випадку нелінійна функція значень показників якості K_i, що вибирається (обґрунтовується) фахівцями, виходячи з вимог до сектору оборони України, і яка має зміст втрати, пов'язаної зі зростанням (погіршенням) даного показника якості.

$$K_p = \sum_{i=1}^{n} V_i f_i(K_i),$$

$$\sum_{i=1}^{n} V_i = 1, V_i > 0, i = \overline{1,n},$$

Нехай K_{i0} є мінімально можливим значенням показника якості K_i при заданій сукупності вихідних даних та ігноруванні значень усіх інших (n – 1) показників якості. Інакше кажучи, K_{i0} є тим найкращим значенням даного (часткового) показника якості K_i (наприклад, K_1), що можна було б одержати при заданих вихідних даних, якби значення усіх інших показників якості (наприклад, $K_2, \dots, K_n$) не брати до уваги, тобто припустити будь-яке їх погіршення. Тоді, очевидно, що функцію $f_i(K_i)$ варто вибирати такою, щоб вона задовольняла умови:

$$f_i(K_{i0}) = 0, f_i(K_i) > 0 \text{ при } K_i > K_{i0}$$

При цьому передбачається, що значення $K_{i0}, \left(i = \overline{1,n}\right)$ вдається попередньо знайти, розв'язуючи спрощені задачі з одним показником K_i при ігноруванні усіх інших (n – 1) показників. Зазначимо, що на практиці при аналізі сектору оборони реально $K_i > 0$, наприклад, з урахуванням імовірних помилок, затримки інформації управління, вартості тощо. Тобто $K_{i0} > 0$ і відповідно потрібно попередньо обчислювати значення K_{i0}. Якщо вибрати функцію $f_i(K_i)$ лінійною, то згідно з викладеним вище маємо

$$f_i(K_i) = |K_i - K_{i0}| / K_{im}. \quad (2)$$

Якщо $K_{i0} > 0$, то в (3.2) також можна вважати $K_{i0} = 0$ без втрат для результатів оптимізації системи. Це зумовлено тим, що у виразі (2) величини $K_{i0}, \left(i = \overline{1,n}\right)$ входять лише у вигляді адитивних членів, що не змінюються в процесі оптимізації (тобто при варіації структури розглядуваного сектору оборони або його параметрів). Звідси виходить, що при пошуку шляхів оптимізації аналізованої системи та при лінійній СРЦФ моделі можна вважати $f_i(K_i)=K_i/K_m$

навіть, якщо $K_{i0} \neq 0$. Проте, у випадку, коли метою є лише оцінка існуючої системи управління сектором оборони з метою з'ясування відповідності її наявним вимогам і нормативам, то приймати $K_{i0} = 0$ не можна. Оскільки не завжди можливо зібрати належну групу компетентних експертів для практичного втілення цієї методики, подальші розвідки доцільно проводити у напрямку універсалізації методу шляхом визначення величин вагових коефіцієнтів V_i та показників якості K_{im} та K_{i0} з урахуванням регіональної, політичної, військової, тощо, специфіки. З урахуванням суб'єктивної оцінки експертами показників якості системи управління сектором оборони, СРЦФ доцільно записати у такому вигляді:

$$\begin{cases} K_p = C_1K_1 + C_2K_2 + C_3K_3 + C_4K_4 + C_5K_5 + C_6K_6 + \\ \quad +C_7K_7 + C_8K_8 + \ldots + C_nK_n; \\ K_i = \dfrac{|K_i - K_{i0}|}{K_{im}}, i = \overline{1,n}, n = 11; \\ \sum\limits_{i=1}^{n} C_i = 1\,, C_i > 0, i = \overline{1,n}. \end{cases} \quad (3)$$

Як уже зазначалося, K_{i0} – деяке опорне значення показника якості K_i; K_{im} – значення показника якості K_i, гранично припустиме з точки зору вимог замовника до системи управління сектором оборони; C_i – вагові коефіцієнти, які вибираються, виходячи з відносної важливості кожного з показників якості K_i, …, K_n, чим вагомішим вважається даний показник K_i. Іншими словами, чим більш суттєво показник K_i мінімізується у процесі аналізу, тим більшим обирається відповідний йому коефіцієнт C_i. Будемо вважати оптимальною таку систему управління сектором оборони, яка забезпечує виконання умов:

$$\begin{gathered} K_p = f_p(K_1, \ldots, K_i, \ldots, K_m) = \min_{S \in M_a}, \\ K_i = K_i(S), i = \overline{1,n}, \\ K_i \leq K_{im}, i = \overline{1,n}. \end{gathered} \quad (4)$$

Відповідно, за K_1, K_2, K_3, K_4 … K_8 приймаємо такі показники якості діяльності сектору оборони:

K_1 – показник рівня військової готовності;

K_2 – показник якості забезпечення та логістики;

K_3 – оцінка рівня кадрового потенціалу та навчання військовослужбовців;

K_4 – оцінка рівня кібербезпеки та інформаційної відкритості;

K_5 – показник якості міжнародної співпраці;

K_6 – оцінка швидкості реагування на загрози;

K_7 – показник рівня розвитку та інновацій;

K_8 – показник якості контролю та нагляду за діяльністю сектору оборони.

Визначення кожного з максимально припустимих з точки зору вимог замовника послуг показників якості K_{im} є окремими самостійними завданнями. Таким чином, при оцінці рівня якості діяльності сектору оборони України або при порівнянні різних варіантів побудови і способів фінансування сектору оборони, можна використовувати критерій (3), де інтегральний показник якості системи K_p визначається за (2). Відповідно до введених позначень, показник якості діяльності сектору оборони K_p має вигляд:

$$\begin{cases} K_p = C_1 \dfrac{|K_1 - K_{1o}|}{K_{1m}} + C_2 \dfrac{|K_2 - K_{2o}|}{K_{2m}} + \cdots + C_{11} \dfrac{|K_{11} - K_{11o}|}{K_{11m}} \\ \sum\limits_{i=1}^{11} C_i = 1\,, C_i > 0, K_i \le K_{im}, K_{io} \le K_{im}, i = \overline{1,11}, \end{cases} \quad (5)$$

Величини опорних значень показників якості K_{i0} підлягають окремому визначенню з метою забезпечення можливості порівняння ступеня організації управління сектором оборони в різних сферах, наприклад, економічній, кадровій, матеріально-технічній, організаційній, міжнародній взаємодії, тощо. Отже, у попередніх підрозділах було показано, що основною метою діяльності ОПВ у сфері надання ПЗ є організація забезпечення ТГ необхідними обсягами якісних ПЗ. Рівень якості забезпечення такими послугами, як це доведено у попередньому підрозділі, можна оцінити за допомогою показника якості (4). Можна показати, що програмний підхід до формування системи надання послуг ТГ полягає в організації заходів щодо покращення показника якості (5), тобто, фактично, у покращенні часткових показників якості. Часткові показники якості, зокрема, наявність технічно сучасного озброєння та військової техніки, рівень тренувань і рівень мобілізаційної готовності, наявність та стан військових об’єктів; наявність та стан засобів зв'язку та розвідки; наявність та стан систем забезпечення безпеки, наявність палива, боєприпасів, запасних частин, медичної підтримки та інших важливих ресурсів, необхідних для підтримки боєздатності армії та низка інших, перш за все визначаються характеристиками сектору оборони як фізичної системи і найбільшою мірою залежать від характеристик використовуваного обладнання, досягнутого технологічного рівня і рівня кваліфікації обслуговуючого персоналу. З цієї точки зору діяльність ОПВ щодо покращення діяльності сектору оборони полягає у сприянні щонайскорішій модернізації технологічних систем та обладнання, впровадженню цифрових і супутникових технологій тощо. Це, з одного боку, значно сприятиме підвищенню якості управління сектором оборони, що відповідно відобразиться і на показнику якості (4), а з іншого – сприятиме розширенню можливостей досягнення результатів цим сектором поза норми існуючих стандартів, встановлених державою. Отже, інтегральний показник якості K залежить від властивостей системи управління сектором оборони як фізичного, економічного і кібернетичного об’єкта. Відповідно, більш комплексними мають бути заходи ОПВ щодо його покращення. Для проведення оцінювання запропонованої моделі автор здійснив опитування низки експертів та узагальнив їх оцінки рівня якості діяльності сектору оборони України у 2014-2023 роках за кожним із розглянутих вище критеріїв. Результати опитування представлені у вигляді лінійного графіка, що показує середні значення експертних оцінок за роками, а стовпчики похибок – діапазон розкиду їхніх оцінок. Рівень якості був нормалізований до значень від 0 до 1, де 1 – абсолютний успіх, 0 – повна невдача. Смуги помилок на графіку представляють розкид оцінок, візуально демонструючи представлення діапазону експертних думок.

Сектор оборони України в сучасних умовах стоїть перед великими викликами і завданнями. Забезпечення національної безпеки та обороноздатності країни вимагає ефективного управління ресурсами, стратегічного планування та постійного вдосконалення. Оцінювання діяльності сектору оборони грає важливу роль у забезпеченні ефективності цього сектору. Перш за все, необхідно впровадити систему збору та аналізу даних щодо оборонної діяльності. Це дозволить отримувати об’єктивну інформацію про стан галузі, рівень використання ресурсів та результати роботи. Важливо враховувати як кількісні показники, так і якісні аспекти, такі як готовність військ, ступінь модернізації озброєння та військово-технічної спеціалізації.

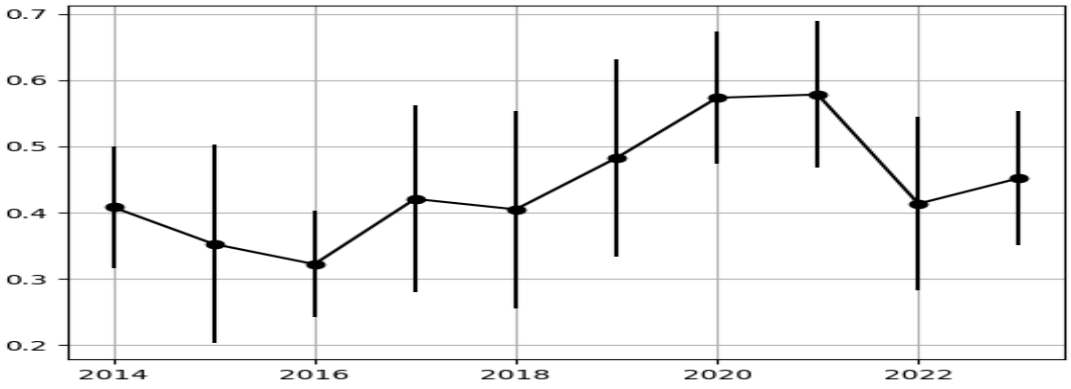


Рисунок 1 – Результати експертного оцінювання якості діяльності сектору оборони України у 2014-2023 рр. *(обраховано автором)*

Для ефективного оцінювання сектору оборони необхідно розвивати систему контролю та нагляду. Це означає забезпечення прозорості та відкритості в діяльності оборонних структур, а також незалежного аудиту та зовнішнього контролю. Такий підхід сприятиме запобіганню корупції та зловживанням, а також підвищить довіру громадськості до сектору оборони. Удосконалення оцінювання діяльності сектору оборони також вимагає розвитку інформаційних технологій та аналітичних інструментів. Використання сучасних технологій дозволить ефективно аналізувати великі обсяги даних та прогнозувати розвиток ситуації в галузі оборони. Необхідно також підвищувати кваліфікацію персоналу, який займається оцінюванням діяльності сектору оборони. Це включає навчання аналітиків, експертів та керівників, які мають розуміти специфіку оборонної справи та мати навички аналізу та прийняття стратегічних рішень.

Одним із основних недоліків є відсутність єдиної нормативно-правової бази, яка б визначала принципи, методи та критерії оцінювання. Це призводить до того, що різні органи оцінювання використовують власні підходи та методики, що ускладнює порівняння результатів оцінювання. Іншим недоліком є недостатня деталізованість оцінювання. В існуючій системі оцінювання акцент робиться на загальних показниках, таких як рівень фінансування, чисельність особового складу, стан озброєння та військової техніки. Це не дозволяє повною мірою оцінити ефективність діяльності сектору оборони, зокрема, його здатність до виконання завдань щодо оборони держави. Також, існуюча система оцінювання не передбачає достатнього рівня прозорості та підзвітності. Це ускладнює контроль за ефективністю діяльності сектору оборони та унеможливлює внесення необхідних коректив. Для удосконалення оцінювання діяльності сектору оборони України пропонуються такі рекомендації:

Затвердження єдиної нормативно-правової бази, яка б визначала принципи, методи та критерії оцінювання. Це дозволить уніфікувати підходи до оцінювання та забезпечити порівнянність результатів.

Деталізоване оцінювання діяльності сектору оборони. Необхідно оцінювати не лише загальні показники, але й конкретні аспекти діяльності, такі як готовність до виконання завдань щодо оборони держави, ефективність використання ресурсів, рівень професійної підготовки особового складу тощо.

Посилення прозорості та підзвітності оцінювання. Необхідно забезпечити відкритість інформації про результати оцінювання та можливість громадськості надавати відгуки та пропозиції.

Оцінювання діяльності сектору оборони України є важливим інструментом для

забезпечення його ефективності та результативності. Воно дозволяє оцінити рівень досягнення визначених цілей, стан ресурсного забезпечення, ефективність використання ресурсів, а також рівень відповідності діяльності сектору оборони національним інтересам. Оцінювання національної безпеки України є важливим інструментом для забезпечення її стабільності та розвитку. Воно дозволяє оцінити рівень загроз національній безпеці, стан її захисту, а також ефективність заходів, що вживаються для її забезпечення.

Міністерство оборони України (МОУ) є центральним органом виконавчої влади, який забезпечує формування та реалізацію державної політики у сфері оборони. МОУ відіграє ключову роль у процесі оцінювання національної безпеки України. МОУ має виконувати наступні функції в процесі оцінювання національної безпеки України:

Участь у розробці Стратегії національної безпеки України. МОУ бере участь у розробці Стратегії національної безпеки України, яка визначає основні напрями та пріоритети державної політики у сфері національної безпеки.

Здійснення оцінки стану національної безпеки України. МОУ здійснює оцінку стану національної безпеки України, враховуючи внутрішні та зовнішні загрози, а також стан її захисту.

Вироблення рекомендацій щодо підвищення ефективності заходів з забезпечення національної безпеки України.

Громадська думка є важливим фактором, який необхідно враховувати в процесі оцінювання діяльності сектору оборони. Громадськість може надати цінну інформацію про стан сектору оборони, його ефективність та відповідність національним інтересам.

Громадськість може виконувати наступні функції в процесі оцінювання діяльності сектору оборони:

Контрольна функція. Громадськість може контролювати діяльність сектору оборони та забезпечувати її відповідність національним інтересам. Громадськість може брати участь у заходах з оцінювання діяльності сектору оборони, таких як проведення перевірок, опитувань, круглих столів тощо.

Освітня функція. Громадськість може сприяти підвищенню обізнаності населення про сектор оборони та його роль у захисті країни.

Участь у процесі прийняття рішень. Громадськість може брати участь у процесі прийняття рішень щодо діяльності сектору оборони. Громадськість може надавати інформацію про стан сектору оборони, його ефективність та відповідність національним інтересам.

Для підвищення ролі громадськості в процесі оцінювання діяльності сектору оборони необхідно вжити наступних заходів:

Забезпечити прозорість та відкритість процесу оцінювання. Процес оцінювання діяльності сектору оборони необхідно зробити більш прозорим та відкритим для громадськості.

Сприяти розвитку громадянського суспільства. Необхідно сприяти розвитку громадянського суспільства, а також підвищенню рівня обізнаності населення про сектор оборони та його роль у захисті країни.

Створити механізми для участі громадськості в процесі оцінювання. Необхідно створити механізми для участі громадськості в процесі оцінювання діяльності сектору оборони.

Нами розроблено та рекомендуються до впровадження практичні рекомендації щодо впровадження наступних заходів:

Створити веб-сайт, на якому будуть публікуватися звіти про оцінювання діяльності сектору оборони.

Проводити відкриті слухання щодо результатів оцінювання діяльності сектору оборони.

Створити громадські ради з питань оцінювання діяльності сектору оборони.

Сприяти розвитку громадянського суспільства.

Сприяти розвитку громадських організацій, які займаються питаннями безпеки та оборони.

Проводити освітні заходи з питань безпеки та оборони для населення.

Розробити правила та процедури для участі громадськості в процесі оцінювання діяльності сектору оборони.

Забезпечити фінансування заходів з участі громадськості в процесі оцінювання.

Отже, реалізація цих заходів дозволить підвищити роль громадськості в процесі оцінювання діяльності сектору оборони України, а також зробити цей процес більш ефективним та результативним.

Обговорення

Наукова новизна результатів дослідження та їх практичне значення підтримані у ході дискусії щодо побудови комплексної системи показників діяльності сектору оборони України ще не були предметом комплексного наукового дослідження, що і визначає актуальність і важливість проведеного в межах статті дослідження. Адже наукове обґрунтування рекомендацій щодо побудови міцної та контекстуально відповідної системи показників діяльності сектору оборони України передбачає детальний аналіз існуючих рамок, адаптацію до конкретних потреб та викликів України і обґрунтування практичних пропозицій щодо впровадження.

Висновки

Розроблені методологічні положення та рекомендації з удосконалення оцінювання діяльності сектору оборони, які передбачають раціональне вирішення питань оцінки і управління сектором оборони, дозволяють зробити наступні висновки.

Розроблено метод багатокритеріальної оптимізації системи управління сектором оборони України, який дозволяє здійснювати оцінку рівня якості роботи такої системи, знаходити шляхи підвищення рівня цієї якості, порівнювати ефективність таких систем, реалізованих у різних сферах. Запропоновано здійснювати теоретико-системний розгляд та обґрунтування методологічних підходів до вирішення часткових проблем з управління діяльністю сектором оборони на основі такої багатокритеріальної оптимізації, на урахуванні рекомендацій якої повинно ґрунтуватися прийняття управлінських рішень.

У результаті системного розгляду діяльності сектору оборони розроблено систему критеріїв для оцінювання функціонування сектору оборони на основі побудови суб’єктивної результуючої цільової функції, яка враховує як об’єктивні показники функціонування сектору як фізичної і економічної системи, так і суб’єктивні оцінки громадян якості функціонування цієї системи. На базі цієї системи критеріїв побудовано систему оцінки якості діяльності сектору оборони, яку ОПВ можуть використовувати для реалізації як владних повноважень щодо організації діяльності сектору оборони. Розроблено пропозиції щодо методичних основ комплексної оцінки якості діяльності сектору оборони, які включають виміри технічних, технологічних, економічних, соціальних та інших параметрів діяльності сектору оборони, виміри характеристик її об’єктів, вивчення думки громадян, спостереження за діяльністю сектору з використанням зовнішніх засобів тощо.

Сформульовано основні засади діяльності ОПВ у сфері організації діяльності сектору оборони, які включають принципи системності, постійного підвищення якості діяльності, планомірності, наукового обґрунтування й об’єктивності.

Підсумовано, що у сучасному динамічному зовнішньому середовищі сектору оборони

держави варто застосувати підхід багатокритеріальної оптимізації до оцінки продуктивності, щоб отримати повне розуміння своєї загальної ефективності. Інтегруючи численні критерії ефективності, сектор оборони зможе цілісно оцінювати свою ефективність і приймати обґрунтовані рішення щодо покращення. Важливо пам'ятати, що система оцінювання ефективності повинна бути адаптована до унікальних потреб і цілей сектору оборони держави. Завдяки безперервному вдосконаленню та адаптації сектор оборони може оптимізувати свої системи оцінки ефективності та стимулювати стійкий розвиток відповідно до вимог динамічно змінного середовища.

Реформування сектору оборони спрямоване на стратегічну адаптацію до мінливих геополітичних умов та нових викликів безпеки. Це включає зміну доктрини оборони, перегляд стратегічних пріоритетів, адаптацію до гібридної війни та кіберзагроз, а також впровадження інноваційних підходів у військову сферу. Крім того, воно спрямоване на забезпечення ефективного використання оборонних ресурсів, які обмежені. Це включає раціоналізацію бюджетних видатків, оптимізацію структури та кадрового складу, впровадження ефективного управління та контролю. Реформування сектору оборони має на меті підвищення професіоналізму та кваліфікації військового персоналу. Це включає вдосконалення системи набору, навчання та підготовки військових, розвиток лідерських якостей та підтримку соціального захисту військовослужбовців. Реформування сектору оборони спрямоване на підтримку інтеграції України в міжнародну оборонну спільноту, зокрема до НАТО. Це включає адаптацію до стандартів та процедур НАТО, підвищення сумісності та взаємодії з партнерськими країнами, а також сприяння обміну досвідом та технологіями.

Розроблено та рекомендуються до впровадження практичні рекомендації щодо впровадження наступних заходів:

Створити веб-сайт, на якому будуть публікуватися звіти про оцінювання діяльності сектору оборони.

Проводити відкриті слухання щодо результатів оцінювання діяльності сектору оборони.

Створити громадські ради з питань оцінювання діяльності сектору оборони.

Сприяти розвитку громадянського суспільства.

Сприяти розвитку громадських організацій, які займаються питаннями безпеки та оборони.

Проводити освітні заходи з питань безпеки та оборони для населення.

Розробити правила та процедури для участі громадськості в процесі оцінювання діяльності сектору оборони.

Забезпечити фінансування заходів з участі громадськості в процесі оцінювання.

Реалізація цих заходів дозволить підвищити роль громадськості в процесі оцінювання діяльності сектору оборони України, а також зробити цей процес більш ефективним та результативним.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Stojković D., Stojanović L. Strategic Defence Performance Management. SYMORG 2012 – XIII

International Symposium on Innovative Management and Business Performance at: Zlatibor, Serbia. – 2012. – URL : https://www.researchgate.net/publication/287996266_strategic_defence_performance_management (дата звернення: 04.02.2023).
2. PwC's global aerospace and defense: Annual performance and outlook. 2023 edition. URL : https://www.pwc.com/us/en/industries/industrial-products/library/aerospace-defense-review-and-forecast.html (дата звернення: 04.02.2023).
3. RAND: Performance Measurement. URL : https://www.rand.org/topics/performance-measurement.html (дата звернення: 04.02.2023).
4. Engelbrecht G., Schmitz P., Bean W. Performance measures for combat-ready forces in the military. – 2009. URL : https://www.researchgate.net/publication/37851886_Performance_measures_for_combat-ready_forces_in_the_military. (дата звернення: 04.02.2023).
5. Стратегія забезпечення державної безпеки України : затв. указом Президента України від 16 лют. 2022 р. № 56/2022. Верховна Рада України. – URL : https://zakon.rada.gov.ua/laws/show/56/2022#Text (дата звернення: 04.02.2023).
6. Світова гібридна війна: український фронт : монографія / за заг. ред. В. П. Горбуліна. Харків : Фоліо, 2017. – 496 с.
7. Основи воєнної безпеки держави: підручник / Грицай П.М., Грищенко В.П. та інші. – К.: НУОУ, 2021. – 204 с.
8. Ткач, М., Ткач, І., Ясенко, С., Брітченко, І., & Лошонці, П. (2022). Методичні підходи щодо оцінювання воєнно-економічної спроможності країни. *Social Development and Security*, *12*(3), 81-97. https://doi.org/10.33445/sds.2022.12.3.8 (дата звернення: 04.02.2023).

References

1. Stojković D., Stojanović L. Strategic Defence Performance Management. SYMORG 2012 - XIII International Symposium on Innovative Management and Business Performance at: Zlatibor, Serbia. – 2012. – Available from : https://www.researchgate.net/publication/287996266_strategic_defence_performance_management (date of application : 04.02.2023).
2. PwC's global aerospace and defense: Annual performance and outlook. 2023 edition. Available from : https://www.pwc.com/us/en/industries/industrial-products/library/aerospace-defense-review-and-forecast.html (date of application: 04.02.2023).
3. RAND: Performance Measurement. Available from : https://www.rand.org/topics/performance-measure ment.html (date of application : 04.02.2023).
4. Engelbrecht G., Schmitz P., Bean W. Performance measures for combat-ready forces in the military. – 2009. Available from : https://www.researchgate.net/publication/37851886_Performance_measures_for_combat-ready_forces_in_the_military. (date of application: 04.02.2023).
5. Strategy for ensuring the state security of Ukraine: approved. by decree of the President of Ukraine dated February 16 2022 No. 56/2022. Verkhovna Rada of Ukraine – Available from : https://zakon.rada.gov.ua/laws/show/56/2022#Text (date of application: 04.02.2023).
6. World hybrid war: the Ukrainian front: a monograph / by General ed. V. P. Horbulina. Kharkiv: Folio, 2017. – 496 p.
7. Basics of military security of the state: a textbook / Hrytsai P.M., Hryshchenko V.P. and others. – Kyiv: NUOU, 2021. – 204 p.
8. Tkach, M., Tkach, I., Yasenko, S., Britchenko, I., & Lošonczi, P. (2022). Methodical approaches to assessing the military and economic capacity of the country. *Social Development and Security*, *12*(3), 81-97. https://doi.org/10.33445/sds.2022.12.3.8

Роль і місце роїв безпілотних систем в операціях (бойових діях) та варіанти їх застосування

The role and place of swarms of unmanned systems in operations (combat operations) and options for their use

Олег Семененко [A]
Corresponding author: д. військ. н., професор, заступник начальника Центрального науково-дослідного інституту Збройних Сил України з наукової роботи, e-mail: aosemenenko@ukr.net, ORCID: 0000-0001-6477-3414

Сергій Островський [A]
к. в. н, начальник науково-дослідного управління, e-mail: ostrovserg@ukr.net, ORCID: 0000-0002-4702-9808

Артур Мовчан [A]
к. т. н, начальник науково-дослідного відділу, e-mail: asesciencepost4@ gmail.com, ORCID: 0009-0006-0559-4962

Андрій Мельниченко [B]
ад'юнкт наукового відділу, e-mail: gatling.511@gmail.com, ORCID: 0000-0002-6072-4989

Сергій Столінець [C]
старший викладач кафедри, e-mail: aosemenenko@ukr.net, ORCID: 0000-0001-9202-0057

Станіслав Петренко [C]
викладач, e-mail: aosemenenko@ukr.net, ORCID: 0000-0001-5369-1683

Oleh Semenenko [A]
Corresponding author: Dr of military Sciences, Professor, deputy head of the Central Research Institute of the Armed Forces of Ukraine for scientific work, e-mail: aosemenenko@ukr.net, ORCID: 0000-0001-6477-3414

Serhii Ostrovskyi [A]
Candidate of Military Sciences, Head of the Research Department, e-mail: ostrovserg@ukr.net, ORCID: 0000-0003-2767-0891

Artur Movchan [A]
Candidate of Technical Sciences, Head of the Research Department, e-mail: asesciencepost4@ gmail.com, ORCID: 0009-0006-0559-4962

Andrii Melnychenko [B]
PhD student, e-mail: gatling.511@gmail.com, ORCID: 0000-0002-6072-4989

Serhii Stolinets [C]
Senior Lecturer of the Department, e-mail: aosemenenko@ukr.net, ORCID: 0000-0001-9202-0057

Stanislav Petrenko [C]
Lecturer, e-mail: aosemenenko@ukr.net, ORCID: 0000-0001-5369-1683

[A] Центральний науково-дослідний інститут Збройних Сил України, м. Київ, Україна
[B] Національний університет оборони України, м. Київ, Україна
[C] Кафедра військової підготовки Національного авіаційного університету, Київ, Україна

[A] Central Research Institute of the Armed Forces of Ukraine, Kyiv, Ukraine
[B] National Defense University of Ukraine, Kyiv, Ukraine
[C] Department of Military Training of the National Aviation University, Kyiv, Ukraine

Received: October 8, 2024 | Revised: October 24, 2024 | Accepted: October 31, 2024

DOI: 10.33445/sds.2024.14.5.7

Мета роботи: визначити роль, місце, завдання роїв безпілотних систем в операціях (бойових діях) та варіанти їх застосування.

Метод дослідження: методи аналізу та синтезу, методи індукції та дедукції, методи експертного опитування, методи дослідження операцій.

Практична цінність дослідження: приведено ключові складові роїв безпілотних систем; визначено основні завдання та місце роїв безпілотних систем в операціях (бойових діях); наведено раціональні варіанти застосування роїв безпілотних систем у операціях (бойових діях); розглянуто окремі рекомендації щодо застосування роїв безпілотних систем.

Теоретична цінність дослідження: визначено, роль, місце та завдання роїв безпілотних систем, як нових елементів сучасних бойових дій. Приведено раціональні варіанти застосування у операціях (бойових діях) з урахуванням досвіду відбиття широкомасштабної збройної агресії російської федерації.

Тип статті: теоретичний, описовий, практичний.

Ключові слова: рої безпілотних систем; операції; бойові дії, система управління.

Purpose: Determine the role, place, tasks of swarms of unmanned systems in operations (combat operations) and options for their application

Method: methods of analysis and synthesis, methods of induction and deduction, methods of expert survey, methods of operations research.

Practical implications: the key components of swarms of unmanned systems are given; the main tasks and the place of swarms of unmanned systems in operations (combat actions) are determined; rational options for the use of swarms of unmanned systems in operations (combat actions) are given; separate recommendations for the use of swarms of unmanned systems are considered.

Theoretical implications: the role, place and tasks of swarms of unmanned systems as new elements of modern warfare are defined. Rational options for use in operations (combat actions) are given, taking into account the experience of repelling large-scale armed aggression of the russian federation.

Paper type: theoretical, descriptive, practical.

Key words: swarms of unmanned systems; operations; combat operations, control system.

Вступ

Досвід сучасних воєнних конфліктів і відбиття широкомасштабної збройної агресії рф проти України свідчить про зростання ролі на полі бою різноманітних зразків дронів. Для виконання різних завдань все активніше застосовують не лише окремі безпілотні літальні апарати (БпЛА), а й одночасно значну їх кількість у групі. Перспективним способом застосування дронів є перехід до їх роїв. При цьому постає низка організаційних, технічних, правових та етичних питань, пов'язаних зі створенням роботизованої зброї із застосуванням штучного інтелекту. Варто розуміти термін "дрон" у більш широкому розумінні, ніж просто БпЛА, а як мобільний, автономний безпілотний апарат (БпА) (повітряний, наземний, надводний або підводний), призначений для виконання конкретних завдань [1–5].

Уже сьогодні, в багатьох державах світу проводяться дослідження з тактики застосування "роїв" розвідувальних та розвідувально-ударних безпілотних систем на основі безпілотних апаратів різного призначення. Такі дослідження базуються на створенні самоорганізованих груп ("роїв") БпА (БпЛА) великої кількості, що мають спільну мету щодо виявлення та ураження об'єктів, наприклад, засобів ППО, великогабаритних надводних об'єктів (кораблів), пунктів управління тощо. Рій таких БпА (БпЛА) дуже складно знищити повністю, а зміна його завдань вимагатиме лише зміни елементів програмного забезпечення в системі управління ним. Застосування роїв БпА наземного (повітряного) типу дозволить вести ефективну розвідку та вражати об'єкти обраного типу (визначені цілі) з мінімальними матеріальними затратами та без втрат особового складу. Таким чином, у світі відбувається поступовий перехід від застосування поодиноких БпЛА до групового та зосередженого застосування, кульмінацією якого стає роїння дронів (БпА) для виконання визначених бойових завдань[6–9].

Розвиток технологій застосування рою БпА ґрунтується на безперешкодовому інформаційному обміні між ними, зменшенні їх габаритних параметрів, підвищенні маневреності та здешевленні конструкції, застосування за різним призначенням з різними підходами до управління та самоорганізації. Це забезпечує зменшення ефективності протидії (виявлення та ураження) БпА (роїв безпілотних систем), тим самим збільшує результативність застосування роїв безпілотних систем в інтересах виконання завдань угрупованнями військ (сил).

Теоретичні основи дослідження

Особливістю сучасної організації складних систем є те, що переважною організаційною структурою стає не ієрархія, а мережа. З'являються інтелектуальні мережі, здатні до аналізу і планування своєї поведінки і розумної організації деякого інтелектуального середовища. Мережеві структури мобільніші, більш стійкі, більш надійні; вихід з ладу деяких елементів мережі не призводить до відмови функціонування всієї мережі, по мережі більш оперативно поширюється різноманітна інформація і здійснюється взаємодія між різними організаційно-технічними рівнями.

В даний час поведінка безпілотних апаратів вже формується складним інтелектуальним чином. Наприклад, в даний час у ході планування застосування БпЛА розглядається і враховується, що БпЛА, які рухаються в групі можуть, наприклад, "жертвувати" собою заради виконання групою загального цільового завдання, змінювати по "домовленості між собою" цілерозподіл в реальному масштабі часу, здійснювати групові маневри, діючи колективно, тощо. Так безпілотні апарати можуть приймати рішення самостійно, виходячи з ситуації, що складається і "сповіщаючи" про свій стан і заходи, що вживаються інші апарати, здійснюють самостійний вибір цілей і раціональної поведінки для їх досягнення.

Проведений аналіз показує, що визначальною і реалізованою з високим ступенем довіреності інновацією при бойовому застосування безпілотних систем є можливість активного обміну інформацією між об'єктами управління у реальному часі, організації колективної поведінки бойових і хибних засобів і прийняття колективних рішень з їх ефективною індивідуальною реалізацією. Тоді головною компонентою в інфраструктурі бойового застосування стане єдина мережа інтелектуальних безпілотних систем зі спеціально організованою системою управління.

Сумісне застосування великої кількості апаратів дозволяє:

– спеціалізувати окремі БпА у групі на окремі функції розвідки, зв'язку, радіоелектронної протидії тощо;

– оперативно виявляти та вибірково уражати стаціонарні та рухомі цілі (мобільні, замасковані об'єкти).

Можливість функціональної спеціалізації БпА визначає доцільність розгляду варіанту їх бойового застосування, коли умова виконання поставленого завдання буде еквівалентна досягненню зони об'єкту противника одразу декількома апаратами.

Постановка проблеми

Отже, головною метою статті є визначення ролі, місця, завдань роїв безпілотних систем в операціях (бойових діях) та варіантів їх застосування.

Результати

Одним із перспективних напрямків підвищення ефективності застосування безпілотних систем є перехід до їх групового застосування (роїв) [6]. Це підтверджується бойовими діями під час відбиття широкомасштабної збройної агресії російської федерації проти України. Зокрема, в ході бойових дій рф широко використовує практику нанесення групових ударів БпЛА-камікадзе "Shahed-136" ("Герань-2"), як прообраз застосування, так званих, роїв безпілотних систем повітряного типу. У цьому випадку засоби протиповітряної оборони мають обмежені можливості з виявлення та знищення таких цілей, внаслідок чого частина БПЛА влучає в об'єкти (ціль) [3].

Крім того, досвід збройних сил інших держав світу показує, що одним із перспективних напрямів є застосування ударних БпЛА (БпА) зі штучним інтелектом на основі алгоритмів самоорганізації. Застосування штучного інтелекту дає можливість об'єднувати БпЛА (БпА) у рої та організовувати обмін інформацією між ними, а також забезпечити самостійне взаємоузгоджене вирішення завдань зі збирання та оброблення інформації щодо складних об'єктів і групових цілей, ідентифікувати їх елементи, здійснювати розподіл між ударними БпА (БпЛА) та уражати їх.

Хоча сучасні бойові дії характеризуються значною кількістю застосувань БпА різних класів, однак є ряд завдань, де застосування одиничних БпА не дозволяє вирішити бойові завдання. До таких завдань можна віднести:

- виявлення, розпізнавання і ураження наземних (повітряних) складних об'єктів і групових цілей;
- порушення та дезорганізація функціонування об'єктової та військової ППО шляхом формування віртуальної оперативної обстановки;
- ретрансляція і формування інформаційних мереж;
- груповий повітряний бій;
- боротьба з великогабаритними надводними об'єктами (цілями);
- завдання ударів по групах наземних малорозмірних цілей (живій силі, легкоброньованій техніці, артилерійських позиціях, інфраструктурних об'єктах тощо);

- коригування та цілерозподіл вогню артилерії на великих ділянках лінії зіткнення;

- деморалізація та підрив морально-психологічного стану особового складу противника та ін.

Рої безпілотних систем на полі бою, сьогодні, можуть відігравати важливу роль через високу ймовірність успішного виконання ними різних (багатьох) бойових завдань. Такий результат досягається з урахуванням низької ефективності протидії рою БпА, а саме:

по-перше, застосування на БпА адаптивних антенних решіток у складі приймачів супутникової системи навігації, підвищення точності бортових безплатформних інерційних навігаційних систем, встановлення малогабаритних оптичних та радіолокаційних датчиків, що реалізують відносні та кореляційно-екстремальні способи автономної навігації, знижують дальність дії та ефективність застосування засобів радіоелектронного подавлення;

по-друге, відбиття масованого нальоту БпЛА засобами зенітного ракетного артилерійського прикриття економічно нераціонально через використання дорогих ракет для ураження значної кількості відносно дешевих БпЛА та швидкого вичерпання гарматного боєкомплекту, що може призвести до подальшої нездатності відбиття основного удару ешелонами крилатих ракет та тактичної авіації;

по-третє, значну частину засобів повітряного нападу, які реалізовані на міні- та мікро-БпЛА, через їх малу ефективну площу розсіювання (до 0,01 м2), низькі висоти та швидкість польоту, традиційні засоби розвідки та ураження ППО (оглядові РЛС, зенітні ракетні комплекси та системи (ЗРК), ЗРС), винищувачі) не здатні не тільки вражати, а й виявляти їх. Тому, рої мікро- та міні-БпЛА, а також хибні цілі становитимуть особливу небезпеку для системи ППО;

четверте, застосування керованих роїв ударних БпЛА, що завдають одночасні удари по об’єктах і елементах систем управління (розвідки, ППО) з різних напрямків різко зменшує ймовірність прикриття останніх [7–10].

Разом з тим, поява великої кількості ударних БпА (БпЛА) потребує організації оборони значно більшої загальної кількості об’єктів безпосередньо з початком воєнних дій, а також оборони низки важливих об’єктів державного управління, промисловості, паливно-енергетичного комплексу, екологічно небезпечних об’єктів, об’єктів інфраструктури та масових заходів у мирний час.

Перевагою рою безпілотних систем є здатність автономно або напівавтономно виконувати завдання у режимі часу близькому до реального з мінімальним контролем з боку операторів та спроможністю адаптуватись до мінливих умов середовища.

Надійність, масштабованість, взаємозамінність і мультизадачність БпА, недетермінована поведінка рою БпА створює передумови набуття нових спроможностей угруповань військ (сил) Збройних Сил України. Крім того, застосування у рою недорогих БпА робить кожен з них менш вимогливим до ресурсів і більш енергоефективним.

Не дивлячись на те, що переваги застосування рою БпА є очевидними, цей напрям у Збройних Силах України перебуває на початковому етапі розвитку. Тому місце роїв безпілотних систем у структурі Збройних Сил України залежатиме від загальної стратегії розвитку безпілотних систем ЗС України та потреби для вирішення конкретних бойових завдань.

Загалом, рої БпА доцільно розглядати як складову вогневої підтримки в операціях, де вони будуть застосовуватися за єдиним замислом та планом вогневої підтримки.

Таким чином, можна стверджувати, що рій безпілотних систем – це багатокомпонентна система, в якій кожен компонент (БпА) функціонує самостійно в тісно узгодженій взаємодії з іншими складовими, з метою досягнення спільної мети (виконання поставленого завдання). Кожен окремий БпА в рою являється компонентом єдиної інформаційної мережі. Також, під роєм слід розуміти групу (сукупність) БпА, управління якою здійснюється за різними підходами в тому числі і за допомогою штучного інтелекту із застосуванням алгоритмів самоорганізації [6, 9].

У низці досліджень стосовно варіантів застосування роїв безпілотних систем, на сьогодні, розроблено загальну теорію ройового (групового) застосування БпА (БпЛА) в умовах динамічних, недетермінованих середовищ. Особливу увагу у дослідженні питань щодо варіантів застосування роїв БпА (роїв безпілотних систем) для реалізації розвідувальних (розвідувально-ударних) завдань приділяють у таких державах як США, КНР, Південна Корея та Індія, а також у Франції, Великій Британії, Ізраїлі, Туреччині, Ірані, рф та Естонії. Такі дослідження зосереджуються на питаннях управління застосуванням роїв БпА. При цьому рої БпА (безпілотних систем) можуть застосовуватися для виявлення засобів протиповітряної оборони та наземних цілей та їхнього ураження, радіоелектронної боротьби, розвідки тощо. Однією з основних проблем є організація управління застосуванням рою БпА (безпілотних систем), яке може бути централізованим, децентралізованим або змішаним та бути визначальним для формування варіантів застосування роїв безпілотних систем [9–11]. На рис. 1 наведені окремі (типові) форми координації роїв та міжройових зв'язків.

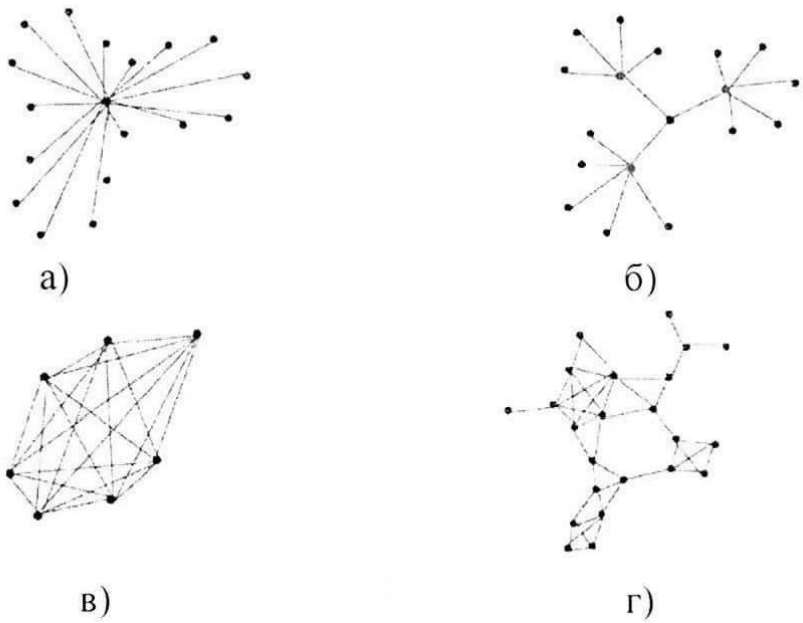


Рисунок 1 – Моделі управління та координації роїв: а) централізована, б) ієрархічна, в) консенснусна, г) емерджентна

Централізоване управління – елементи рою передають інформацію центральному планувальнику, який ставить задачі кожному елементу окремо.

Ієрархічне управління полягає в тому, що окремі елементи рою контролюються агентами нарівні "підрозділу", який в свою чергу управляється агентом більш високого рівня, і так далі.

Координація на основі консенсусу, де елементи рою спілкуються один з одним і приймають рішення шляхом голосування або методом аукціону.

Емерджентна координація виникає природнім шляхом між окремими елементами рою, що реагують на інших, подібно зграям живих істот.

Отже, можна зробити висновок, що варіанти застосування роїв безпілотних систем будуть визначатися метою їх застосування та бойовими завданням, а також вибором схеми (способу) управління роєм безпілотних систем.

Крім того, в умовах насичення військ різнотипними багатофункціональними БпА актуальним питанням є пошук адекватних поведінкових алгоритмів управління ройовим застосуванням роїв безпілотних систем.

Прийнято вважати, що колективна (ройова) поведінка групи БпА має виникати у результаті взаємодії між окремими БпА у рої та взаємодії БпА із навколишнім середовищем. Прості правила, визначені для кожного окремого БпА, можуть створювати багато варіантів складної поведінки рою. Циклічність процесу управління роєм безпілотних систем (БпА) полягає в тому, що взаємодія між окремими агентами рою впливає на стійкість рою в умовах впливу зовнішнього середовища, а поведінка рою, яка пов'язана з швидкоплинністю обстановки, призводить до коригування поведінки кожного окремого агента рою (безпілотних систем) та, як наслідок – до зміни поведінки усіх задіяних БпА (рис. 3). Відповідно до цього варіанту, тактика застосування рою безпілотних систем може передбачати зміну його структури під час виконання завдання, а також передбачає оперативну (залежно від ситуації) зміну тактики (варіанта) застосування.

Структура рою безпілотних систем передбачає ітеративну поведінку кожного окремого БпА одного того самого класу (ударний БпЛА, БпЛА розвідки, РЕБ, наземний БпА тощо) до моменту, коли буде досягнуто бажаний результат колективної поведінки рою безпілотних систем (тобто, коли завдання буде виконано). За цим підходом, можна виділити наступний варіант застосування роїв безпілотних систем:

- оператор рою безпілотних систем (БпА) призначає завдання для суброїв або окремих БпА (тобто, визначає мету та порядок їх дій);

- рій БпА здійснює пошук цілі (об'єктів) противника, стеження за ними та, за досягнення певних умов, – атаку на них.

Як уже зазначалося вище, управління роїв безпілотних систем може бути централізованим, децентралізованим або змішаним. При цьому функції оператора щодо контролю БпА можуть суттєво відрізнятись. З урахуванням зазначеного, виділимо наступні основні варіанти застосування роїв безпілотних систем наземного (повітряного) типу для реалізації розвідувальних (розвідувально-ударних) завдань:

1. Застосування роїв безпілотних систем із централізованим управлінням.

2. Застосування роїв безпілотних систем із децентралізованим управлінням за допомогою алгоритмів штучного інтелекту.

3. Застосування роїв безпілотних систем із змішаним управлінням.

Слід також враховувати перспективний варіант, який може бути реалізовано вже найближчим часом. За цим варіантом припускається можливість застосування роїв БпЛА (безпілотних систем) проти подібних ворожих роїв. Тоді, враховуючи специфіку завдання, алгоритм управління роями (варіант застосування) повинен передбачати виявлення і перехоплення БпЛА ворожого рою в умовах динамічної зміни взаємного положення БпЛА-контрагентів, поступової втрати частки функціональності рою, зміни пріоритетів завдань, втрати зв'язку з іншими БпЛА рою тощо.

Таким чином, виходячи із змісту основних завдань роїв безпілотних систем наземного (повітряного) типу (розвідка, корегування вогню сил і засобів ракетних військ та артилерії, ураження об'єктів (цілей) противника), доцільно для оцінювання ефективності застосування роїв безпілотних систем використовувати наступні показники.

1. Під час виконання завдань з розвідки та корегування вогню сил і засобів РВіА:

- математичне сподівання кількості (або частки) розвіданих об'єктів (цілей) противника;

- математичне сподівання кількості (або частки) цілей під час ведення вогню, по яких здійснювалось його корегування;

- час нанесення заданого ступеня ураження;

- математичне сподівання кількості (або частки) уражених (подавлених) об'єктів.

Інтегральний показник ефективності (по чисельному значенню якого приймаються рішення):

- математичне сподівання втрат бойового потенціалу угруповання противника, за яким вимірюється (оцінюється) “ефект” від нових властивостей (можливостей) роїв безпілотних систем наземного (повітряного) типу;

- “затрати” – математичне сподівання кількості уражених (втрачених) безпілотних систем наземного (повітряного) типу зі складу рою та їх вартість;

- витрати на підготовку та застосування.

2. Під час виконання завдань з ураження об’єктів (цілей) роєм безпілотних систем наземного (повітряного) типу:

- математичне сподівання кількості (або частки) розвіданих об’єктів (цілей) противника;

- математичне сподівання кількості (або частки) об’єктів (цілей) противника, по яких застосовувались ударні (розвідувально-ударні) безпілотних систем наземного (повітряного) типу;

- математичне сподівання кількості (або частки) уражених об’єктів (цілей) противника.

Інтегральний показник ефективності (по чисельному значенню якого приймаються рішення):

- математичне сподівання бойового потенціалу угруповання противника;

- “затрати” – математичне сподівання кількості уражених (втрачених) безпілотних систем наземного (повітряного) типу (у тому числі знищених ППО) зі складу рою та їх вартість;

- витрати на підготовку та застосування.

Під час виконання завдань (розвідки, коригування вогню сил і засобів РВіА) ефект за визначеними показниками від застосування роїв безпілотних систем може бути досягнутий за рахунок раціонального розподілу зусиль БпА-розвідників по районах (зонах, напрямках) з урахуванням їх важливості, автоматичного вирішення задач виявлення, ідентифікації та оброблення інформації, яка надходить від декількох джерел практично одночасно.

Під час виконання завдань з ураження об’єктів (цілей) противника ефект за визначеними показниками від застосування роїв безпілотних систем може бути досягнутий за рахунок раціонального цілерозподілу (централізованого, змішаного).

Під час підготовки та ведення операцій (бойових дій) доцільно розглядати рої безпілотних систем як невід’ємний елемент складу сил і засобів об’єднаної вогневої підтримки. Тому, застосування роїв безпілотних систем повинно здійснюватись за єдиним замислом та планом об’єднаної вогневої підтримки. Враховуючи особливості роїв безпілотних систем, зокрема:

- високоточість та можливість ефективного ураження складних об’єктів (групових цілей);

- значна дальність застосування;

- маневреність;

- висока швидкість;

рекомендується визначити пріоритетними завданнями, під час виконання яких доцільно застосовуються рої безпілотних систем:

- ведення розвідки з метою систематичної тактичної (оперативної) обізнаності командирів (штабів) щодо положення та дій противника в масштабі часу наближеного до реального;

- здійснення коригування вогню сил і засобів РВіА, у тому числі в складі РВК (РУК);

- нанесення ударів за планом об’єднаної вогневої підтримки переважно по складних об’єктах (групових цілях) противника (в районах зосередження, на марші та під час розгортання);

- створення маневрених резервів для вирішення раптово виникаючих (ситуативних) завдань з вогневого ураження.

Крім того, враховуючи обмежений час на виконання завдань роями безпілотних систем (обмежену ємкість бортових енергоносіїв), доцільно планувати періодичну заміну роїв безпілотних систем (їх складових) під час операцій (бойових дій).

Найбільш перспективними та реалістичними завданнями для роїв безпілотних систем є їх застосування для виявлення та ураження засобів ППО, важливих, переважно групових наземних цілей, ведення радіоелектронної боротьби (радіоелектронного подавлення, радіоелектронної розвідки) та інші подібні. При цьому варіант застосування рою безпілотних систем буде залежати від організації (вибору) управління їх застосуванням.

У разі централізованого управління роєм безпілотних систем управління здійснюється з єдиного центру управління кожним БпА. За такого способу управління можливе управління групою БпА складом до 20 дронів.

Децентралізоване управління роєм безпілотних систем передбачає застосування штучного інтелекту з алгоритмами самоорганізації. За такого способу управління можливе управління роєм БпА складом до 200 дронів.

При змішаному способі управління роєм безпілотних систем застосовується принцип поділу БпА на окремі суброї. При цьому централізоване управління здійснюється суброями, а управління всередині суброю здійснюється штучним інтелектом. За такого способу управління можливе управління роєм безпілотних систем складом до 1200 дронів.

Загалом, для успішного виконання завдань в операції (бойових діях), покладених на рої безпілотних систем, доцільно розглядати ситуативне створення роїв безпілотних систем для досягнення мети їх застосування за визначеним варіантом. У такому випадку, важливим питанням є визначення вихідних даних щодо принципів та логіки формування рою розвідувальних (розвідувально-ударних) безпілотних систем. Зокрема, цільовим призначенням рою, як варіант, може бути пошук та ураження наземних цілей заданого типу у визначеному районі (області простору). Також, принципово важливим є визначення типу рою (однорідний, різнорідний), що суттєво впливає на склад рою безпілотних систем (роїв та суброїв). Тому, під час планування операції (бойових дій) із ситуативним створенням рою безпілотних систем, з метою успішного (раціонального) його застосування, рекомендовано створювати (орієнтуватись на) логіко-часову (поетапну) модель застосування рою безпілотних систем. Для прикладу, на рис. 2 відображено застосування рою ударних БпЛА у логіко-часовій моделі за етапами їх застосування [8–11].

Таким чином, виходячи із змісту основних завдань роїв безпілотних систем наземного (повітряного) типу (розвідка, корегування вогню сил і засобів ракетних військ та артилерії, ураження об’єктів (цілей) противника), доцільно для оцінювання ефективності застосування роїв безпілотних систем використовувати наступні показники.

1. Під час виконання завдань з розвідки та корегування вогню сил і засобів РВіА:

- математичне сподівання кількості (або частки) розвіданих об’єктів (цілей) противника;
- математичне сподівання кількості (або частки) цілей під час ведення вогню, по яких здійснювалось його корегування;
- час нанесення заданого ступеня ураження;
- математичне сподівання кількості (або частки) уражених (подавлених) об’єктів.

Інтегральний показник ефективності (по чисельному значенню якого приймаються рішення):

- математичне сподівання втрат бойового потенціалу угруповання противника, за яким вимірюється (оцінюється) “ефект” від нових властивостей (можливостей) роїв безпілотних систем наземного (повітряного) типу;
- “затрати” – математичне сподівання кількості уражених (втрачених) безпілотних систем наземного (повітряного) типу зі складу рою та їх вартість;
- витрати на підготовку та застосування.

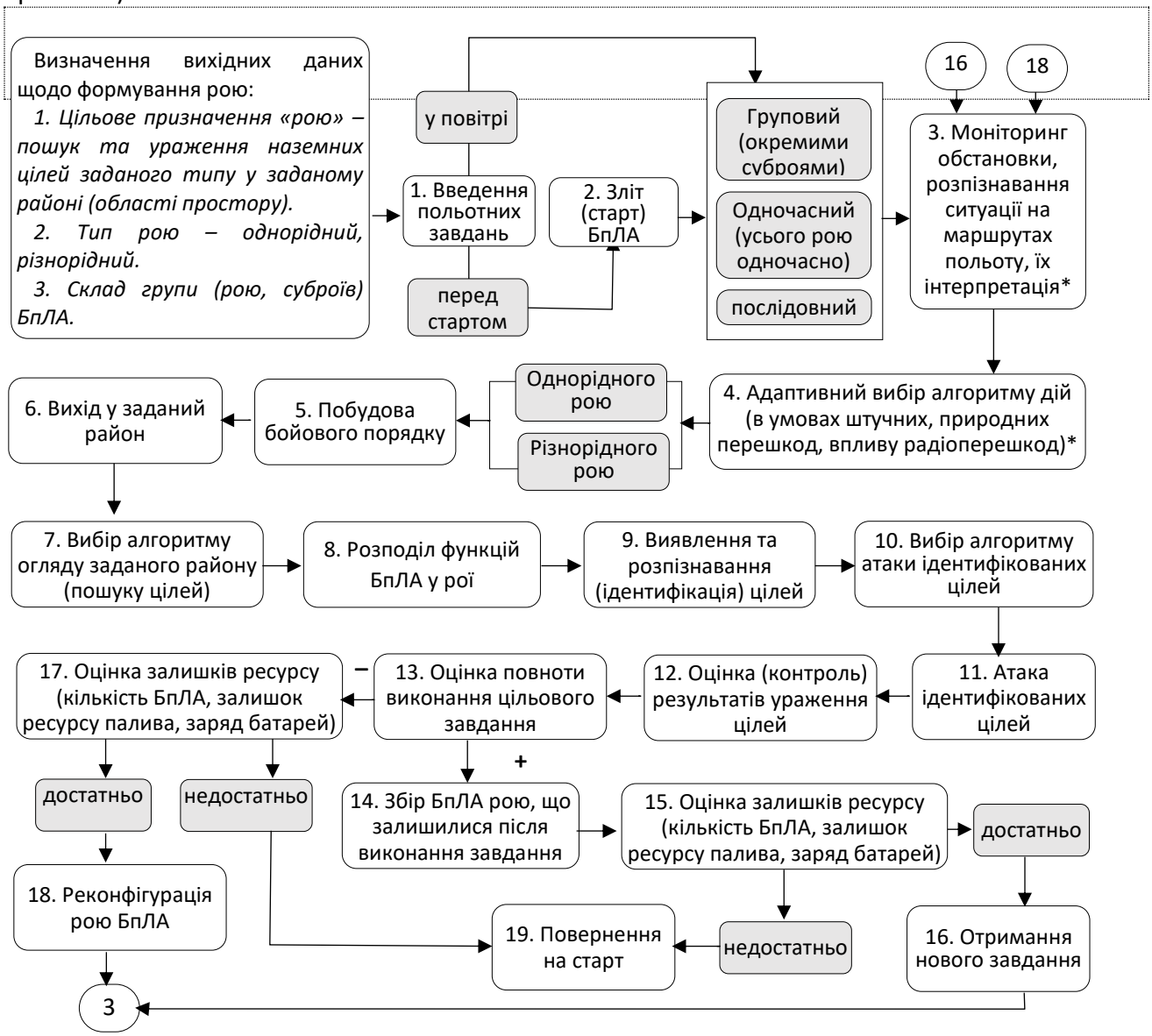
2. Під час виконання завдань з ураження об’єктів (цілей) роєм безпілотних систем наземного (повітряного) типу:

- математичне сподівання кількості (або частки) розвіданих об’єктів (цілей) противника;

- математичне сподівання кількості (або частки) об'єктів (цілей) противника, по яких застосовувались ударні (розвідувально-ударні) безпілотних систем наземного (повітряного) типу;

- математичне сподівання кількості (або частки) уражених об'єктів (цілей) противника.

Інтегральний показник ефективності (по чисельному значенню якого приймаються рішення):



Примітка. Заходи, позначені зіркою (*) виконуються безперервно протягом усього часу від зльоту до завершення виконання цільового завдання групою (роєм) БпЛА.

Рисунок 2 – Логіко-часова поетапна модель застосування рою ударних БпЛА (варіант)

- математичне сподівання бойового потенціалу угруповання противника;

- "затрати" – математичне сподівання кількості уражених (втрачених) безпілотних систем наземного (повітряного) типу (у тому числі знищених ППО) зі складу рою та їх вартість;

- витрати на підготовку та застосування.

Під час виконання завдань (розвідки, коригування вогню сил і засобів РВіА) ефект за визначеними показниками від застосування роїв безпілотних систем може бути досягнутий за рахунок раціонального розподілу зусиль БпА-розвідників по районах (зонах, напрямках) з урахуванням їх важливості, автоматичного вирішення задач виявлення, ідентифікації та оброблення інформації, яка надходить від декількох джерел практично одночасно.

Під час виконання завдань з ураження об’єктів (цілей) противника ефект за визначеними показниками від застосування роїв безпілотних систем може бути досягнутий за рахунок раціонального цілерозподілу (централізованого, змішаного).

Висновки

Досвід сучасних воєнних конфліктів і відбиття широкомасштабної збройної агресії рф проти України свідчить про активне збільшення ролі застосування не лише окремих дронів, а й їх груп та навіть роїв. Така ситуація потребує формування загальної картини щодо тактики роїння дронів та формалізації їх завдань. При цьому існує низка невирішених організаційних, технічних та правових питань, пов’язаних зі створенням роїв безпілотних систем (роботизованої зброї) із застосуванням штучного інтелекту.

Розвиток варіантів застосування роїв безпілотних систем ґрунтується на безперешкодовому інформаційному обміні між його елементами (БпА), зменшенні габаритних параметрів, підвищенні маневреності та здешевленні конструкції БпА, застосування за різним призначенням з різними підходами до управління та самоорганізації в інтересах виконання завдань угрупованнями військ (сил).

Загалом прийнято, що рій безпілотних систем – це багатокомпонентна система, в якій кожен компонент (БпА) функціонує самостійно в тісно узгодженій взаємодії з іншими складовими для досягнення спільної мети (виконання поставленого завдання). Також, під роєм слід розуміти групу (сукупність) БпА, управління якою здійснюється за різними підходами, в тому числі, і за допомогою штучного інтелекту із застосуванням алгоритмів самоорганізації.

До типових завдань застосування роїв безпілотних систем слід віднести: виявлення, розпізнавання і ураження наземних (повітряних) складних об’єктів і групових цілей, порушення та дезорганізація функціонування об’єктової та військової ППО, ретрансляція і формування інформаційних мереж, боротьба з великогабаритними надводними об’єктами (цілями), завдання ударів по групах наземних малорозмірних цілей (живій силі, легкобронюваній техніці, артилерійських позиціях, інфраструктурних об’єктах тощо), коригування вогню артилерії на великих ділянках лінії зіткнення, деморалізація та підрив морально-психологічного стану особового складу противника, та в перспективі, груповий повітряний бій.

Рекомендується розглядати рої безпілотних систем як невід’ємний елемент складу сил і засобів об’єднаної вогневої підтримки під час підготовки та ведення операцій (бойових дій). Застосування роїв безпілотних систем повинно здійснюватися за єдиним замислом та планом об’єднаної вогневої підтримки. При цьому варіант застосування рою безпілотних систем буде суттєво залежати від організації (вибору способу) управління їх застосуванням. У подальшій перспективі місце роїв безпілотних систем у структурі Збройних Сил України залежатиме від загальної стратегії розвитку безпілотних систем у ЗС України та потреби для вирішення конкретних бойових завдань.

Можна виділити наступні основні варіанти управління застосуванням роїв безпілотних систем наземного (повітряного) типу для реалізації розвідувальних (розвідувально-ударних) завдань: застосування роїв безпілотних систем із централізованим способом управління, застосування роїв безпілотних систем із децентралізованим способом управління за допомогою алгоритмів штучного інтелекту та застосування роїв безпілотних систем із змішаним способом управлінням.

На цей час не визначено єдиного погляду щодо комплексної оцінки ефективності роїв безпілотних систем застосування. Тому, виходячи із змісту можливих завдань роїв безпілотних систем наземного (повітряного) типу доцільно проводити оцінювання ефективності застосування роїв безпілотних систем за частковими та основними показниками ефективності.

Для вибору раціонального варіанта застосування роїв безпілотних систем у Збройних

Силах України можуть використовуватися критерії придатності та математичного очікування втрат бойового потенціалу угруповання військ (сил) противника.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Лупандін В.А., Мегельбей Г.В., Самойленко В.М., Тюріна В.Ю. Обґрунтування напрямків захисту об’єктів та озброєння і військової техніки від роїв безпілотних літальних апаратів. Наука і техніка Повітряних Сил Збройних Сил України. Харків. 2021. № 4(45). С. 58–64.
2. Лупандін В.А., Сотніков О.М., Мегельбей Г.В., Танцюра О.Б. Модель захисту об’єктів і військової техніки від роїв безпілотних літальних апаратів Системи обробки інформації. 2022. Випуск 4 (171). С. 41–47.
3. Авілов А.І., Ткачук С.С. Ієрархічна модель взаємодії оператора з “роєм” безпілотних літальних апаратів. Збірник наукових праць Харківського національного університету Повітряних Сил. Харків. 2023. № 1(75). С. 37–40.
4. Єфремов О.В., Горбенко В.М., Коршець О.А. Методика оцінювання ефективності застосування підрозділів безпілотних авіаційних комплексів. Збірник наукових праць Харківського національного університету Повітряних Сил. Харків. 2018. 4(58) С. 30–36
5. Горбулін В.П., Мосов С.П. Рої дронів – кульмінація дронізації воєн. Вісн. НАН України, 2024. № 3. С. 3–11.
6. Шовкошитний І.І., Василенко О.А. Проблемні питання ройового застосування ударних безпілотних літальних апаратів. Modern Information Technologies in the Sphere of Security and Defence. 2023. № 3(48). С. 27–34.
7. Гусак Ю.А., Василенко О.А. Mathematical model for controlling the use of a swarm of striking unmanned aerial vehicles based on artificial intelligence algorithms. Міжнародний академічний форум “Воєнні інновації в сучасних війнах”: Збірник тез міжнародного форуму. ЦНДІ ЗС України. Київ. 7 БЦ, 2024. С. 36–37 (м. Київ, 18–19 квітня). ЦНДІ ЗС України
8. Шовкошитний І. І., Василенко О. А. Проблемні питання ройового застосування ударних безпілотних літальних апаратів. Сучасні інформаційні технології у сфері безпеки та оборони: наук. журн. Нац. ун-т оборони України. Київ. 2023. № 3 (48). С.27–34.
9. Василенко О.А., Ярошенко Я. В. Деякі питання управління роями безпілотних літальних апаратів та їх адаптація до потреб Збройних Сил України. Інтеграція закордонних платформ у структуру Сил оборони України. Спроможності, застосування, підтримка : Зб. матеріалів наук.-практ. семінару 07 лютого 2024 року. Київ. НУОУ, 2024. С. 35–40.
10. Гусак Ю.А., Василенко О.А., Коломієць Ю.М. Розроблення алгоритму дій групи ударних безпілотних літальних апаратів. Сектор безпеки і оборони України на захисті національних інтересів: актуальні проблеми та завдання в умовах воєнного стану : тези II Міжнародної науково-практичної конференції (Хмельницький, 23 листопада 2023 року). Хмельницький. Видавництво НАДПСУ. 2024. С. 123–125.
11. Шовкошитний І. І., Василенко О. А. Перспективи та проблемні питання впровадження ройових принципів застосування ударних безпілотних літальних апаратів. Спільні дії

військових формувань і правоохоронних органів держави: проблеми та шляхи вирішення в умовах воєнного стану : тези V міжнародної науково-практичної конференції (Одеса, 20 жовтня 2023 року). С. 137–138.

References

1. Lupandin V.A., Megelbey G.V., Samoilenko V.M., Tyurina V.Yu. Justification of directions for the protection of objects and weapons and military equipment from swarms of unmanned aerial vehicles. *Science and technology of the Air Force of the Armed Forces of Ukraine*. Kharkiv. 2021. No. 4(45). P. 58–64.
2. Lupandin V.A., Sotnikov O.M., Megelbey G.V., Tansyura O.B. a model of protection of objects and military equipment from swarms of unmanned aerial vehicles Information processing systems. 2022. Issue 4 (171). P. 41–47
3. Avilov A.I., Tkachuk C.S. A hierarchical model of operator interaction with a “swarm” of unmanned aerial vehicles. *Collection of scientific works of the Kharkiv National University of the Air Force*. Kharkiv. 2023. No. 1(75). P. 37–40.
4. Yefremov O.V., Horbenko V.M., Korshets O.A. Methodology for evaluating the effectiveness of the use of units of unmanned aviation complexes. *Collection of scientific works of the Kharkiv National University of the Air Force*. Kharkiv. 2018. 4(58) P. 30–36
5. Gorbulin V.P., Mosov S.P. Swarms of drones are the culmination of the droneization of wars. Visn. NAS of Ukraine, 2024. No. 3. P. 3–11.
6. Shovkoshitny I.I., Vasylenko O.A. Problematic issues of swarm use of attack unmanned aerial vehicles. *Modern Information Technologies in the Sphere of Security and Defense*. 2023. No. 3(48). P. 27–34.
7. Husak Yu.A., Vasylenko O.A. Mathematical model for controlling the use of a swarm of striking unmanned aerial vehicles based on artificial intelligence algorithms. International academic forum “Military innovations in modern wars”: Collection of theses of the international forum. Central Research Institute of the Armed Forces of Ukraine. Kyiv. 7 BC, 2024. P. 36–37 (Kyiv, April 18–19). Central Research Institute of the Armed Forces of Ukraine
8. Shovkoshitny I. I., Vasylenko O. A. Problematic issues of the swarm application of attack unmanned aerial vehicles. Modern information technologies in the field of security and defense: *science. journal National University of Defense of Ukraine*. Kyiv. 2023. No. 3 (48). P.27–34.
9. Vasylenko O.A., Yaroshenko Ya.V. Some issues of control of swarms of unmanned aerial vehicles and their adaptation to the needs of the Armed Forces of Ukraine. Integration of foreign platforms into the structure of the Defense Forces of Ukraine. Capabilities, application, support: Coll. scientific and practical materials. seminar on February 7, 2024. Kyiv. NDUU, 2024. P. 35–40.
10. Husak Yu.A., Vasylenko O.A., Kolomiets Yu.M. Development of an algorithm of actions of a group of attack unmanned aerial vehicles. The security and defense sector of Ukraine in defense of national interests: current problems and tasks in the conditions of martial law: theses of the 2nd International Scientific and Practical Conference (Khmelnytskyi, November 23, 2023). Khmelnytskyi. NADPSU Publishing House. 2024. P. 123–125.
11. Shovkoshitny I. I., Vasylenko O. A. Prospects and problematic issues of implementation of swarm principles of use of attack unmanned aerial vehicles. Joint actions of military formations and law enforcement agencies of the state: problems and solutions in the conditions of martial law: theses of the 5th international scientific and practical conference (Odesa, October 20, 2023). P. 137–138.

Безпека України та глобальна стабільність: стратегії та шляхи забезпечення в умовах війни

Ukraine's security and global stability: strategies and ways of ensuring in conditions of war

Іван Гаврилюк [A]
к.в.н., старший дослідник, перший заступник Міністра оборони України, e-mail: ivan_havryliuk@ukr.net, ORCID: 0000-0002-3514-0738

Олег Семененко [B]
Corresponding author: д. військ. н., професор, заступник начальника Центрального науково-дослідного інституту Збройних Сил України з наукової роботи, e-mail: aosemenenko@ukr.net, ORCID: 0000-0001-6477-3414

Олександр Водчиць [C]
к.т.н., доцент, начальник кафедри військової підготовки Національного авіаційного університету, e-mail: agv64agv@gmil.com, ORCID: 0000-0002-3294-7632

Юзеф Добровольський [C]
к.т.н., доцент, заступник начальника кафедри, e-mail: kataza@i.ua, ORCID: 0000-0002-1077-1402

Сергій Митченко [D]
к.т.н., доцент, старший викладач кафедри військової підготовки, e-mail: vvkorotya@gmail.com, ORCID: 0000-0002-6720-1451

Володимир Коротя[C]
к.т.н., доцент, старший викладач кафедри військової підготовки, e-mail: vvkorotya@gmail.com, ORCID: 0000-0002-6720-1451

Ivan Havryliuk[A]
Ph.D., senior researcher, First Deputy Minister of Defense of Ukraine, e-mail: ivan_havryliuk@ukr.net, ORCID: 0000-0002-3514-0738

Oleh Semenenko [B]
Corresponding author: Dr of military Sciences, Professor, deputy head of the Central Research Institute of the Armed Forces of Ukraine for scientific work, e-mail: aosemenenko@ukr.net, ORCID: 0000-0001-6477-3414

Oleksandr Vodchyts [C]
Candidate of Technical Sciences, Associate Professor, Head of the Department, e-mail: avg64avg@gmail.com, ORCID: 0000-0002-3294-7632

Yuzef Dobrovolskyi [C]
Candidate of Technical Sciences Associate Professor, Deputy Head of the Department, e-mail: kataza@i.ua, ORCID: 0000-0002-1077-1402

Serhii Mytchenko [D]
Doctor of Philosophy, Associate Professor of the Department, e-mail: serhii.mytchenko@gmail.com, ORCID: 0000-0003-3711-2033

Volodymyr Korotia[C]
Candidate of Technical Sciences, Associate Professor, Senior Lecturer of the Department, e-mail: vvkorotya@gmail.com, ORCID: 0000-0002-6720-1451

[A] Міністерство оборони України, м. Київ, Україна
[B] Центральний науково-дослідний інститут Збройних Сил України, м. Київ, Україна
[C] Кафедра військової підготовки Національного авіаційного університету, Київ, Україна
[D] Національний університет оборони України, м. Київ, Україна

[A] Ministry of Defense of Ukraine, Kyiv, Ukraine
[B] Central Research Institute of the Armed Forces of Ukraine, Kyiv, Ukraine
[C] Department of Military Training of the National Aviation University, Kyiv, Ukraine
[D] National Defense University of Ukraine, Kyiv, Ukraine

Received: October 10, 2024 | Revised: October 27, 2024 | Accepted: October 31, 2024

DOI: 10.33445/sds.2024.14.5.8

Мета роботи: визначення основних стратегій забезпечення перемоги України у російсько-українській війні та шляхів забезпечення її національної безпеки через глобальну стабільність у світі.

Метод дослідження: методи аналізу та синтезу, дедукції та індукції, метод аналогій та порівняння.

Практична цінність дослідження: визначені основні стратегії забезпечення перемоги України у російсько-українській війні; сформовані шляхи практичної реалізації цих стратегій, а також розкрито перелік заходів необхідних для реалізації цих шляхів; сформовані загальні висновки стосовно реалізації кожної зі стратегій в глобальній системі забезпечення перемоги України у війні та глобальної світової стабільності і безпеки.

Цінність дослідження: у статті проведено аналіз основних стратегій та шляхів реалізації перемоги України у війні та розкрито сучасні особливості її забезпечення.

Майбутні дослідження: напрямами подальших досліджень можу бути розроблення та вдосконалення стратегій кібербезпеки; інформаційна безпека та протидія дезінформації; реформування оборонного сектору та модернізація збройних сил; співпраця з міжнародними безпековими організаціями; енергетична безпека та диверсифікація енергопостачання; економічна стійкість як фактор національної безпеки;.

Тип статті: теоретичний, практичний.

Ключові слова: безпека України, глобальна стабільність, стратегії та шляхи забезпечення національної безпеки.

Purpose: determining the main strategies for ensuring Ukraine's victory in the Russian-Ukrainian war and ways to ensure its security through global stability.

Method: methods of analysis and synthesis, deduction and induction, method of analogies and comparison.

Practical implications: the main strategies for ensuring Ukraine's victory in the Russian-Ukrainian war are determined; the ways of practical implementation of these strategies have been formed, and the list of measures necessary for the implementation of these ways has been revealed; general conclusions were formed regarding the implementation of each of the strategies in the global system of ensuring Ukraine's victory in the war and global world stability and security.

Value: the article analyzes the main strategies and ways of realizing Ukraine's victory in the war and reveals the modern features of its support.

Future research: areas of further research may be the development and improvement of cyber security strategies; information security and countering disinformation; reforming the defense sector and modernizing the armed forces; cooperation with international security organizations; energy security and diversification of energy supply; economic stability as a factor of national security; the influence of international politics on the security of Ukraine; psychological stability and readiness of the population for crisis situations; innovations in defense technologies.

Paper type: theoretical, practical.

Key words: security of Ukraine, global stability, strategies and ways of ensuring national security.

Вступ

У сучасних геополітичних умовах, коли глобальна стабільність постійно перебуває під загрозою через численні конфлікти, терористичні акти та агресивні дії деяких держав, перемога України у російсько-українській війні стає ключовим фактором, що здатний суттєво вплинути на стабілізацію міжнародної обстановки. Гібридна війна, розв'язана на території України після 2014 року та активна її фаза після 24.02.2022 року, не лише має катастрофічні наслідки для країни та її народу, а й породжує економічні, політичні та соціальні кризи, які відчуваються далеко за межами регіону та дестабілізують ситуацію у світі в цілому [1–3].

Перемога України у цій війні не лише свідчитиме про відновлення територіальної цілісності та суверенітету держави, а й стане важливим сигналом для міжнародної спільноти про неприпустимість агресивних дій з боку держав, що порушують міжнародне право та здійснюють зміни сталих кордонів країн силовими методами, а також створить передумови для зміцнення міжнародних інститутів безпеки та допомагатиме формувати нові, більш ефективні механізми вирішення конфліктів.

Крім того, підтримка України на її шляху до перемоги має стратегічне значення для світових демократій, адже вона демонструє солідарність і рішучість у відстоюванні демократичних цінностей та прав людини. Стратегічне партнерство з Україною відкриває нові можливості й для економічного співробітництва та інноваційного розвитку, що сприятиме глобальній стабільності та процвітанню.

Теоретичні основи дослідження

Аналіз останніх досліджень і публікацій [1–15] за тематико статті показує, що сучасні загрози безпеці України тісно пов'язані з глобальними викликами, такими як військова агресія, інформаційна війна, кіберзагрози та економічні санкції. Дослідження підкреслюють, що ефективна стратегія забезпечення безпеки України має спиратися на комплексний підхід, що поєднує дипломатичні зусилля, міжнародну співпрацю та внутрішні реформи оборонного сектору. Також велике значення надається участі України в міжнародних безпекових структурах, таких як НАТО та ООН, для посилення обороноздатності та стримування потенційних загроз. Важливим аспектом залишається впровадження інноваційних технологій і посилення інформаційної безпеки, що допоможе протистояти пропаганді та маніпуляціям.

Загалом, стратегічні підходи, що пропонуються в сучасних дослідженнях, зосереджені на зміцненні альянсів з демократичними державами, диверсифікації енергетичних джерел, покращенні економічної стійкості та активізації реформ. Це дозволить Україні ефективніше реагувати на внутрішні та зовнішні загрози, сприяючи глобальній стабільності в цілому.

Постановка проблеми

Отже метою статті є визначення основних стратегій забезпечення перемоги України у російсько-українській війні та шляхів забезпечення її національної безпеки через глобальну стабільність у світі.

Результати

Аналіз стратегій та шляхів реалізації перемоги України є надзвичайно актуальним та необхідним для розуміння ролі цієї перемоги у забезпеченні глобальної стабільності, що є важливим орієнтиром для формування політики держав та міжнародних організацій у сфері безпеки, економіки та міжнародних відносин.

До основних стратегій забезпечення перемоги України у російсько-українській війні та шляхів їх реалізації належать:

1. *Адекватне забезпечення потреб сил оборони України озброєнням та військовою технікою.* Забезпечення сил оборони сучасним озброєнням і військовою технікою (ОВТ) є ключовим фактором для досягнення успіху на полі бою, що передбачає постачання сучасних артилерійських систем, танків, авіації, систем протиповітряної оборони (ППО), а також засобів зв'язку і розвідки. Основними напрямами реалізації цієї стратегії є: активний розвиток власних зразків ОВТ, а також державна підтримка підприємств оборонно-промислового комплексу України; забезпечення партнерами достатніх показників озброєння для ефективної протидії противнику; постачання в Україну озброєння, здатного завдавати ударів по території агресора з метою зниження ефективності атак з повітря (ракетами, керованими авіаційними бомбами), ураження скупчення військ (сил) противника, пунктів управління військами (силами), важливих інфраструктурних об'єктів противника, які забезпечують функціонування його угруповань; виділення нашій державі якісних та ефективних зразків озброєння з метою підвищення спроможностей сил оборони України протидіяти сучасним російським аналогам тощо.

До основних шляхів реалізації такої стратегії належать:

- налагодження тісної співпраці з країнами-партнерами та організаціями, такими як НАТО, ЄС для отримання військової допомоги – необхідних зразків озброєння. На сучасному етапі найбільш необхідними зразками озброєння є: літаки F-16 та ракети для них з метою ураження авіації противника до моменту скидання керованих авіаційних бомб, а також комплексів С-300 в місцях розгортання та пуску ракет;

- модернізація наявних зразків ОВТ за рахунок спроможностей ОПК України шляхом впровадження передових технологій, підвищення бойових характеристик, удосконалення систем керування та автоматизації, а також навчання кадрів для ефективного використання та обслуговування оновлених і модернізованих зразків ОВТ;

- використання програм, які дозволяють Україні отримувати озброєння та техніку на вигідних умовах. Реалізація процедур хоча б часткового ленд-лізу, формування можливості орендування складних систем озброєння та військової техніки в інших країнах з реалізацією процедур їх страхування та повернення до країн, які дали зразки в оренду на визначений час (період);

- реалізація процедур прямих закупівель озброєння та військової техніки у виробників, зокрема, з країн, які не є традиційними партнерами України у війні проти росії, але готові постачати необхідне озброєння та обладнання. Зменшення заборон та обмежень співпраці України з країнами, які не належать до кола її країн-партнерів.

Основними заходами реалізації стратегії забезпечення потреб сил оборони України озброєнням та військовою технікою є: організація військових навчань та тренінгів для ефективного використання нового озброєння та військової техніки; пошук шляхів збереження складних систем озброєння (літаки, системи ППО, складні системи космічної, повітряної та наземної розвідки); адаптування логістичної інфраструктури для швидкого постачання і розподілу озброєння на фронті; залучення іноземних та вітчизняних військових експертів для оцінювання потреб і планування подальших закупівель озброєння та військової техніки для сил оборони України тощо.

2. *Реалізація принципів справедливої, прозорої та гнучкої мобілізації.* Перехід від практики примусу та невідомості після мобілізації до чітких правил вибору контракту різного змісту із силами оборони, а також удосконалення системи ротацій військовослужбовців. Справедлива та гнучка мобілізація передбачає залучення всіх доступних людських ресурсів, з урахуванням індивідуальних навичок і професійного досвіду, для максимального підвищення боєздатності. Реалізація принципів формування противаги системи контрактів за принципом "timeline" (1, 3, 4, 5, 7 років) можливим наслідкам вибору режиму "blackline" (штрафи, зменшення свобод). Захист суверенітету та територіальної цілісності України є обов'язком кожного її громадянина, але виконувати цей обов'язок можна за різними сценаріями: чим

менше ти ризикуєш, тим довше служиш за контрактом, отримуєш менше грошове забезпечення, маєш менший ступінь соціальних гарантій. Чим більше ти ризикуєш, тим менше термін контракту, а також ти та твоя сім'я отримуєте максимальний соціальний пакет, максимальні фінансові надбавки, привілеї та державні гарантії за різних сценаріїв проходження служби на лінії бойового зіткнення, максимальний термін обов'язкових відпусток та строків реабілітації.

До основних шляхів реалізації такої стратегії належать:

- удосконалення системи ротацій військовослужбовців і підвищення інформативності та якості системи рекрутингу, а також прозорості процедур вибору військової частини для проходження військової служби;

- швидке оновлення законодавства та внесення змін до законів, які регламентують порядок проходження військової служби, порядок організації заходів мобілізації та забезпечення соціальних гарантій військовослужбовців та членів їхніх сімей;

- реалізація принципів цільової мобілізації щодо залучення фахівців із конкретних галузей (наприклад, IT, медицина, інженерія) для виконання специфічних завдань, забезпечення справедливого розподілу обов'язків між спеціалістами вузького профілю, формування інструментів дотримання умов та правил контракту як з боку громадянина України, так і з боку держави. Виконання свого обов'язку щодо захисту суверенітету та територіальної цілісності України громадянином України за одним із видів контрактів гарантує йому користування всіма правами без обмежень, а саме: виїзд за межі України як на відпочинок, так і в інших справах; користування всіма пільгами та привілеями для себе та сім'ї, які він отримав відповідно до свого контракту; можливість підвищення фінансової стабільності родини; гарантування громадянам України, які прибули з інших країн після евакуації, можливості повернення до родини після виконання військового обов'язку за будь-яким видом контракту тощо;

- удосконалення системи бронювання спеціалістів критичних галузей національної економіки України, формування правил заміни громадянами України, які не змогли до кінця закрити будь-який контракт, за принципом "timeline" тощо.

Основними заходами реалізації стратегії справедливої та гнучкої мобілізації є: розроблення та впровадження системи обліку навичок мобілізованих громадян; зміна технологій інформування громадян України щодо реалізації контрактів із силами оборони за принципом "timeline", а також наслідків у разі вибору режиму "blackline"; проведення регулярних тренувань та навчань для підвищення кваліфікації мобілізованих; забезпечення не менш як двомісячного періоду навчання після мобілізації; забезпечення надання обов'язкових відпусток для реабілітації після перебування на лінії зіткнення за визначеним часовим проміжком відповідно до вибору одного із видів контракту; застосування сучасних технологій для планування і координації мобілізаційних заходів; розроблення переліку критичних галузей національної економіки, які мають можливості бронювання співробітників.

3. *Достатність забезпечення сил оборони боєприпасами та матеріально-технічними засобами.* Безперебійне постачання боєприпасів та матеріально-технічних засобів є критично важливим для підтримання високої бойової готовності та ефективності застосування сил оборони України. Ситуація на фронті потребує постійного поповнення ресурсів, зокрема боєприпасів, амуніції, палива та медичного обладнання, що забезпечить стійкість і маневреність українських військ, дозволяючи їм оперативно реагувати на зміни обстановки та проводити успішні бойові операції проти агресора.

До основних шляхів реалізації такої стратегії належать:

- нарощування власного виробництва боєприпасів та матеріально-технічних засобів. Особливого значення набувають боєприпаси, які використовуються під час застосування безпілотних систем;

- розширення можливостей імпорту боєприпасів шляхом закупівлі необхідних ресурсів у міжнародних постачальників, що передбачає встановлення довгострокових контрактів із надійними постачальниками з різних країн, а також дасть можливість забезпечити стабільність постачання й уникнути перебоїв. Але такий підхід передбачає налагодження партнерських відносин з країнами, які мають високі стандарти виробництва і перевірені методи забезпечення якості продукції. Крім того, важливим аспектом є розвиток логістичної інфраструктури для швидкого й ефективного транспортування боєприпасів до місць призначення, а також забезпечення прозорості та ефективності закупівельних процедур з метою уникнення корупційних ризиків і забезпечення раціонального використання фінансових ресурсів. Систематичний аналіз ринку і вивчення нових технологій у виробництві боєприпасів дозволить Україні залишатися конкурентоспроможною та адаптивною до змінних умов війни;

- оптимізація логістики шляхом створення ефективної системи логістики для швидкого транспортування та розподілу боєприпасів, що передбачає впровадження сучасних технологій управління ланцюгами постачання, таких як системи відстеження та моніторингу вантажів у режимі реального часу, використання спеціалізованих програмних рішень для планування маршрутів, управління запасами та координації між різними логістичними центрами. Створення децентралізованих складських комплексів з автоматизованими системами управління запасами, залучення досвідчених іноземних та вітчизняних логістичних фахівців і проведення регулярних навчань для персоналу сприятиме підвищенню ефективності логістичних операцій. Крім того, розвиток транспортної інфраструктури, зокрема залізничних та автомобільних шляхів, забезпечить надійне і безпечне транспортування боєприпасів навіть в умовах активних бойових дій. Співпраця з міжнародними логістичними компаніями й організаціями допоможе впровадити кращі практики та інноваційні рішення в систему логістики України.

- Основними заходами реалізації стратегії достатності забезпечення сил оборони боєприпасами та матеріально-технічними засобами є: інвестування у модернізацію та розширення існуючих виробничих потужностей; встановлення довгострокових контрактів з надійними постачальниками; використання сучасних технологій для управління складськими запасами і транспортуванням боєприпасів та матеріально-технічних засобів з країн-партнерів.

4. *Удосконалення технологій безконтактних війн (розвиток безпілотних систем і роботизація, кіберборотьба та електронна війна).* Використання безпілотних систем та роботизованих комплексів дає можливість мінімізувати втрати серед особового складу та підвищити ефективність бойових операцій. Розвиток технологій кіберборотьби та електронної війни сприяє захисту критичної інфраструктури, порушенню роботи систем управління та комунікацій противника, а також забезпеченню інформаційної безпеки. Усе це передбачає створення спеціалізованих підрозділів для проведення кібероперацій та електронних атак, розроблення програмного забезпечення для виявлення та нейтралізації кіберзагроз, а також підготовку фахівців з кібербезпеки.

Сьогодні стає зрозумілим, що найбільш раціональним шляхом підвищення спроможностей військових частин (підрозділів) ЗС України під час ведення бойових дій та захисту особового складу є розвиток безпілотних і роботизованих комплексів (систем) (Бп і РК(С)). Це дозволить досягти як паритету у вогневій міці з противником, так і завоювати перевагу за рахунок асиметричних дій у повітрі, на землі та на морі. Поширене застосування розвідувальних безпілотних авіаційних комплексів (систем) (БпАК(С)) як у складі розвідувально-ударних комплексів, так і автономно на окремих напрямах забезпечує створення єдиної системи ситуаційної обізнаності, яка вже зараз призводить до підвищення точності ураження ОВТ, особового складу противника, у першу чергу на їх тактичну глибину, за рахунок своєчасного їх виявлення та корегування вогню ракетних військ і артилерії своїх військ, а також запобігає непомітному підведенню резервів.

Насичене застосування ударних (розідувально-ударних) БпАК(С) як одноразового (камікадзе), так і багаторазового використання (“БпАК(С), що здійснюють скид боєприпасів”) на певній місцевості, зайнятій противником, призводить до зниження боєздатності його військ як за рахунок втрат, так і через падіння морально-психологічного стану особового складу внаслідок підвищення ризику ураження. За таких умов противник не може ефективно здійснювати наступ та вимушений перейти до оборони.

До основних шляхів реалізації такої стратегії належать:

- підтримка науково-дослідних і дослідно-конструкторських робіт у галузі розвитку безпілотних технологій, кіберборотьби та електронної війни;

- закупівля готових безпілотних систем і їх адаптування до специфічних умов бойових дій в Україні;

- співпраця з міжнародними партнерами шляхом реалізації спільних проєктів та обмін досвідом з країнами, що мають передові технології у цій сфері.

Основними заходами реалізації стратегії удосконалення технологій безконтактних війн (розвиток безпілотних систем та роботизація) є: створення спеціалізованих центрів (полігонів) для розроблення і тестування безпілотних систем; вивчення та аналіз аналогічного трофейного озброєння противника; підготовка та навчання операторів для роботи з новими технологіями; розроблення програмного забезпечення для управління безпілотними апаратами і системами; інтеграція безпілотних та роботизованих систем у загальну стратегію військових дій, що передбачає щільну координацію між різними родами військ (сил) і використання спільних інформаційних платформ для обміну даними в режимі реального часу.

5. *Зміна технологій інформаційного впливу на свідомість українців, аудиторії росії та країн світу.* Ефективна інформаційна стратегія є критично важливою для підтримки морального духу населення, протидії ворожій пропаганді та формування позитивного іміджу України у світі.

До основних шляхів реалізації такої стратегії належать:

- негайне створення потужних медіа-платформ шляхом запуску нових та підтримка існуючих платформ для донесення правдивої інформації;

- активізація заходів контрпропаганди шляхом розроблення та впровадження програм контрпропаганди для нейтралізації ворожих інформаційних атак;

- активне залучення міжнародних медіа-кампаній та проведення інформаційних кампаній, спрямованих на зарубіжну аудиторію, для формування підтримки України.

Основними заходами реалізації стратегії зміни технологій інформаційного впливу на свідомість українців, аудиторії росії та країн світу є: збільшення випуску якісного медіа-контенту, включаючи відео, статті та соціальні мережі, відхід від шаблонності в загальній системі інформування населення; створення більш агресивної інформаційної політики по відношенню до країни-агресора; співпраця з міжнародними медіа-організаціями та журналістами щодо донесення до світу інформації про події в Україні; залучення PR-компаній (агенцій) до розроблення PR-стратегій та їх супроводження з питань підвищення репутації бойових підрозділів та популяризації військової служби у Збройних Силах України; підвищення якості інформаційного впливу на свідомість громадян України щодо незворотності мобілізації та формування загальних правил зміни інформаційної політики в масштабах держави; проведення тренінгів для українських журналістів та медіа-менеджерів.

6. *Санкційна політика країн світу проти росії та зняття обмежень щодо військових дій на її території для сил оборони України.* Ефективні санкції та зняття обмежень на військові дії дозволяють послабити економічний і військовий потенціал агресора і тим самим збільшити шанси України на перемогу.

До основних шляхів реалізації такої стратегії належать:

- посилення та підтримання міжнародного тиску шляхом роботи з міжнародними

організаціями та урядами;

- безперервні дипломатичні переговори з країнами-партнерами щодо зняття обмежень на військові дії на території агресора з метою зниження його військового потенціалу та створення умов, коли підтягування військ (сил) до кордонів України є неможливим.

Основними заходами реалізації стратегії розвитку санкційної політики та зняття обмежень щодо військових дій на території росії є: постійна дипломатична робота щодо підсилення санкцій проти країни агресора та країн-сателітів, які підтримують війну; активна участь у міжнародних форумах і конференціях для підтримки санкційної політики; проведення роз'яснювальних кампаній про необхідність та ефективність санкцій.

7. *Нарощування системи протиповітряної оборони України.* Покращення та розширення системи протиповітряної оборони (ППО) є критичним для захисту населення, стратегічних цивільних та військових об'єктів від повітряних атак противника. Росія активно використовує керовані авіаційні бомби, адже їх багато у російській федерації, вони дешевші за ракети, і мають середню або високу точність і велику потужність. Найкращий спосіб боротьби з КАБ це літаки F-16, які здатні як вражати носіїв КАБ, так і створювати додатковий фактор психологічного впливу на противника, обмежуючи його ініціативу у повітрі. Наразі найпоширенішим варіантом комплексу озброєння винищувача F-16A/C є використання ракет малої дальності AIM-9 і ракети середньої дальності AIM-120, а також ракети AMRAAM, AIM-54 Phoenix, Meteor тощо. Ці ракети забезпечать базові можливості для ведення повітряного бою на різних дистанціях, і можливості перехоплення ворожих цілей. Крім цього є нагальна потреба у постачанні засобів ППО, зокрема ЗРК типу "Patriot" з ракетами MIM-104 D/E та ЗРК "SAMP T" з ракетою ASTER-30.

До основних шляхів реалізації такої стратегії належать:

- отримання як допомоги від країн-партнерів та закупівля сучасних систем ППО, а саме: Патріот (Patriot PAC-3); NASAMS (Norwegian Advanced Surface to Air Missile System); SAMP/T (Surface-to-Air Missile Platform/Terrain); MEADS (Medium Extended Air Defense System); IRIS-T SLM (Infra Red Imaging System Tail/Surface Launched Medium);

- налагодження співпраці з країнами-партнерами для отримання технологій і підтримки в розробленні власних систем ППО;

- модернізація існуючих систем ППО для підвищення ефективності їх застосування;

- отримання допомоги від країн-партнерів щодо технічного обслуговування та ремонту наявних в Україні іноземних зразків ППО.

Основними заходами реалізації стратегії нарощування системи протиповітряної оборони України є: продовження дипломатичної роботи з країнами-партнерами щодо удосконалення системи ППО України; збільшення інвестицій в науково-дослідні роботи щодо створення нових технологій ППО; підготовка і навчання фахівців для роботи з сучасними системами ППО іноземного виробництва; розширення мережі радіолокаційних станцій для раннього виявлення повітряних загроз тощо.

8. *Постійний розвиток систем радіоелектронної та кіберборотьби від тактичної до стратегічної ланки управління.* Україні сьогодні вкрай необхідний постійний розвиток систем радіоелектронної та кіберборотьби від тактичної до стратегічної ланки управління для забезпечення національної безпеки, захисту критичної інфраструктури та ефективної протидії сучасним загрозам.

Сучасні системи та засоби радіоелектронної боротьби (РЕБ) дозволяють ефективно боротися з російськими безпілотними засобами ураження та розвідки, які сьогодні є ключовим аспектом ефективного ведення бойових дій. Ці системи здатні виявляти, глушити та перехоплювати сигнали безпілотників, знижуючи їхню ефективність та запобігаючи їх використанню для коригування артилерійського вогню, збору розвідувальної інформації або здійснення атак. Завдяки цьому підвищується безпека українських військ та цивільного

населення, а також створюються умови для більш успішного проведення власних операцій з використанням власних безпілотних систем та комплексів.

Враховуючи зростаючі виклики в сфері кібербезпеки та інформаційних воєн, інтеграція передових технологій, інновацій та співпраця з міжнародними партнерами є ключовими елементами для створення надійної та стійкої системи оборони. Розвиток систем радіоелектронної та кіберборотьби є необхідним для захисту від кібератак з боку росії, забезпечення безпеки комунікацій та управління військовими операціями.

До основних шляхів реалізації такої стратегії належать:

- розроблення, прийняття на озброєння та масоване виробництво власних систем РЕБ типу “Буран”, “Буковель”, “Мандат”, “Нота” тощо;

- отримання як допомоги від країн-партнерів та закупівля сучасних систем РЕБ (AN/ALQ-99 (США), SPYDER (Ізраїль), SPECTRA (Франція), CERBERUS (Німеччина), Hensoldt Kalaetron Attack (Німеччина), Leonardo Elettronica (Італія), SABRE (Великобританія) тощо);

- збільшення інвестицій у підтримку науково-дослідних і дослідно-конструкторських робіт у сфері радіоелектронної боротьби та кібербезпеки;

- залучення міжнародних партнерів до випробування власних засобів у реальних бойових умовах та реалізація заходів для обміну досвідом та отримання нових технологій радіоелектронної та кіберборотьби;

- підготовка фахівців з радіоелектронної та кіберборотьби на всіх рівнях управління сил оборони держави.

Основними заходами реалізації стратегії постійного розвитку систем радіоелектронної та кіберборотьби від тактичної до стратегічної ланки управління є: впровадження сучасних технологій для захисту від кібератак та радіоелектронного подавлення; розроблення і впровадження стратегій для ефективного управління кібероперaціями та радіоелектронною боротьбою на тактичному і стратегічному рівнях.

Комплексна реалізація наведених заходів та стратегій допоможе наблизити перемогу України у війні, а також сприяє зміцненню глобальної стабільності, чинити опір агресивним діям і підтримувати міжнародний правопорядок.

Висновки

У статті розглянуто основні стратегії, спрямовані на забезпечення перемоги України у російсько-українській війні. Перемога України у цій війні є ключовим аспектом підтримання світової стабільності та гарантією дієвості норм міжнародного права у світі. До основних висновків стосовно реалізації кожної зі стратегій в глобальній системі забезпечення перемоги України у війні можна віднести те, що:

- постачання сучасного озброєння і техніки є критично важливим для успішного ведення бойових дій силами оборони України, що можливо тільки завдяки міжнародній співпраці, програмам ленд-лізу та прямим закупівлям озброєння;

- прозорість, справедливість та гнучкість мобілізації є основою залучення кваліфікованих кадрів з урахуванням їхніх навичок та професійного досвіду, а також реальним кроком зміни кадрової політики, яка гарантує права вибору, що забезпечить ефективну мобілізацію. Важливими кроками є оновлення законодавства, цільова мобілізація та використання сучасних технологій для управління мобілізаційними процесами;

- безперебійне постачання боєприпасів є важливим для підтримки боєготовності. Необхідно розширювати власне виробництво, здійснювати імпорт, оптимізувати логістику та створювати ефективну систему управління запасами;

- використання безпілотних систем та роботизованих комплексів мінімізує втрати особового складу і підвищує ефективність бойових дій. Інвестиції в НДДКР, закупівля сучасних

систем та міжнародна співпраця є важливими кроками для реалізації цієї стратегії;

- ефективна інформаційна стратегія підтримує моральний дух населення, протидіє ворожій пропаганді та формує позитивний імідж України у світі. Створення медіа-платформ, програми контрпропаганди та міжнародні медіа-кампанії є ключовими заходами;

- ефективні санкції та зняття обмежень на військові дії на території агресора значно послаблять потенціал росії, підвищуючи шанси на перемогу України. Важливими кроками є міжнародний тиск, дипломатичні переговори та активна участь у міжнародних форумах;

- покращення систем ППО захищає населення та стратегічні об'єкти від повітряних атак противника. Необхідними заходами є закупівля сучасних систем ППО, модернізація існуючих та міжнародна співпраця;

- постійний розвиток систем радіоелектронної та кіберборотьби дозволить силам оборони України ефективно боротися з російськими безпілотними засобами ураження та розвідки, які сьогодні є ключовим аспектом ефективного ведення бойових дій. Активізація кіберборотьби та розробка нових технологій кіберзахисту дозволить підвищити захист критичної інфраструктури та ефективне управління кіберопераціями, що забезпечить інформаційну безпеку як сил оборони, так і держави в цілому. Інвестиції в НДДКР, співпраця з міжнародними партнерами та підготовка фахівців за цим напрямом є необхідними кроками забезпечення перемоги України.

Ефективна комплексна реалізація стратегій забезпечення перемоги України у російсько-українській війні сприяє не лише перемозі України, а й зміцненню глобальної безпекової стабільності у світі. Поступове виконання запропонованих заходів забезпечить ефективну оборону, підтримку міжнародного правопорядку та стабільний розвиток України. Але треба розуміти, що процес забезпечення ефективної реалізації зазначених стратегій та заходів можливий тільки за умов безперервної підтримки України країнами-партнерами за допомогою спільних оборонних ініціатив, взаємної підтримки в міжнародних організаціях та розвитку міжнародних партнерств у сфері безпеки та оборони.

До основних напрямів подальших досліджень за тематикою статті можна віднести:

- розроблення та вдосконалення стратегій кібербезпеки. Аналіз потенційних загроз та створення ефективних механізмів для захисту критичної інфраструктури України, зокрема у сфері енергетики, телекомунікацій та фінансових систем;

- інформаційна безпека та протидія дезінформації. Дослідження методів боротьби з інформаційною війною, аналіз впливу пропаганди та розробка механізмів захисту національного інформаційного простору;

- реформування оборонного сектору та модернізація збройних сил. Вивчення потреб оборонного сектору України для підвищення його ефективності, зокрема в контексті міжнародних стандартів, що можуть сприяти інтеграції України в НАТО;

- співпраця з міжнародними безпековими організаціями. Аналіз ролі міжнародних організацій (НАТО, ООН, ОБСЄ) у забезпеченні безпеки України та можливостей поглиблення співпраці для стримування зовнішніх загроз;

- енергетична безпека та диверсифікація енергопостачання. Дослідження енергетичної незалежності як елементу національної безпеки, включаючи альтернативні джерела енергії та зниження залежності від імпорту енергоносіїв;

- економічна стійкість як фактор національної безпеки. Аналіз ролі економічних санкцій, інвестиційної привабливості та економічного розвитку як елементів стратегії національної безпеки;

- вплив міжнародної політики на безпеку України. Оцінка політики основних світових держав і міжнародних організацій щодо України та їхній вплив на ситуацію в регіоні та глобальну стабільність;

- психологічна стійкість та готовність населення до кризових ситуацій. Дослідження методів підвищення стійкості суспільства до кризових ситуацій, таких як війни чи природні катастрофи, шляхом громадянської освіти та формування національної ідентичності;

- інновації в оборонних технологіях. Розвиток сучасних технологій у сфері оборони (дрони, штучний інтелект, системи раннього попередження) та їхнє застосування для захисту державного суверенітету;

- аналіз впливу глобальних кліматичних змін на національну та регіональну безпеку. Дослідження наслідків зміни клімату для України, таких як нестача води, природні катастрофи, міграційні потоки, та розробка планів їхнього стримування.

Ці напрямки дозволять розширити розуміння сучасних загроз та сприяти підготовці нових стратегій, спрямованих на захист інтересів України і підтримання глобальної стабільності.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Семененко, О., Добровольський, Ю., Ярмольчик , М., Рахманий , О., Тарасов , О., & Ремез , А. (2022). Українська військово-економічна ядерна бомба вже розірвалася у економіці Росії (ретроспектива, дійсне та майбутнє). *Social Development and Security*, *12*(1), 179-197. https://doi.org/10.33445/sds.2022.12.1.17
2. Семененко, О., Онофрійчук, А., Толок, П., Онофрійчук, В., Гетьман, А., & Пєхота, С. (2023). Щодо оцінювання потенційних воєнно-економічних можливостей країн-партнерів України у війні проти росії. *Social Development and Security*, *13*(5), 218-229. https://doi.org/10.33445/sds.2023.13.5.21
3. Семененко, О., Чернишова, І., Таран, О., Капля, І., Мусієнко, В., & Побережець, Т. (2022). Щодо оцінювання економічних збитків України внаслідок російської агресії та прогнозування їх впливу на стан її національної економіки і рівень воєнно-економічної безпеки (лютий-квітень 2022 року). *Social Development and Security*, *12*(2), 78-91. https://doi.org/10.33445/sds.2022.12.2.7
4. Elizabeth Bodine-Baron, Todd C. Helmus, Madeline Magnuson, Zev Winkelman. (2018). Countering Russian Social Media Influence. RAND Corporation. Santa Monica. P. 200.
5. Michael Kofman, Richard Connolly. (2019). Russia's Global Ambitions in Perspective. Center for Naval Analyses. Virginia. P. 150.
6. Stephen J. Flanagan, James Black. (2020). Deterring Russian Aggression in the Baltic States: What it Takes to Win. RAND Corporation. Santa Monica. P. 175.
7. Anders Fogh Rasmussen. (2019). Transatlantic Security and the Challenges of NATO Defense. Atlantic Council. Washington, D.C. P. 95.
8. Timothy Thomas. (2017). Russia’s Military Strategy and Doctrine. Foreign Military Studies Office. Kansas. P. 210.
9. Jeffrey A. Larsen, Kerry Kartchner. (2018). On Limited Nuclear War in the 21st Century. Stanford University Press. Stanford. P. 305.
10. Наталія Гончарова. (2021). Інформаційна безпека України в умовах гібридної війни. Видавництво Київського університету. Київ. С. 220.

11. Олександр Литвиненко. (2020). Стратегічні пріоритети національної безпеки України. Національний інститут стратегічних досліджень. Київ. С. 180.
12. Іван Мельник. (2019). Інтеграція України до європейської системи безпеки. Центр Разумкова. Київ. С. 150.
13. Олена Корольова. (2022). Кібербезпека та кіберзагрози для України. Інститут міжнародних відносин. Київ. С. 135.
14. Василь Гуменюк. (2020). Україна в системі колективної безпеки: виклики та перспективи. Видавництво "Український пріоритет". Львів. С. 190.
15. Марія Петренко. (2021). Вплив міжнародної співпраці на національну безпеку України. Інститут зовнішньополітичних досліджень. Харків. С. 110.

References

1. Semenenko, O., Dobrovolskyi , Y., Yarmolchyk , M., Rakhmanyi , O., Tarasov , O., & Remez , A. (2022). Ukrainian military-economic nuclear bomb has already exploded in Russia's economy (retrospective, present and future). *Social Development and Security*, *12*(1), 179-197. https://doi.org/10.33445/sds.2022.12.1.17.
2. Semenenko, O., Onofriichuk, A., Tolok, P., Onofriichuk, V., Hetman, A., & Piekhota, S. (2023). Regarding the assessment of the potential military and economic capabilities of Ukraine's partner countries in the war against russia. *Social Development and Security*, *13*(5), 218-229. https://doi.org/10.33445/sds.2023.13.5.21
3. Semenenko, O., Chernyshova, I., Taran, O., Kaplia, I., Musienko, V., & Poberezhec, T. (2022). On assessing Ukraine's economic losses due to Russian aggression and forecasting their impact on the state of its national economy and the level of military and economic security (February-April 2022). *Social Development and Security*, *12*(2), 78-91. https://doi.org/10.33445/sds.2022.12.2.7
4. Elizabeth Bodine-Baron, Todd C. Helmus, Madeline Magnuson, Zev Winkelman. (2018). Countering Russian Social Media Influence. RAND Corporation. Santa Monica. R. 200.
5. Michael Kofman, Richard Connolly. (2019). Russia's Global Ambitions in Perspective. Center for Naval Analyses. Virginia. P. 150.
6. Stephen J. Flanagan, James Black. (2020). Deterring Russian Aggression in the Baltic States: What it Takes to Win. RAND Corporation. Santa Monica. R. 175.
7. Anders Fogh Rasmussen. (2019). Transatlantic Security and the Challenges of NATO Defense. Atlantic Council. Washington, D.C. R. 95.
8. Timothy Thomas. (2017). Russia's Military Strategy and Doctrine. Foreign Military Studies Office. Kansas. R. 210.
9. Jeffrey A. Larsen, Kerry Kartchner. (2018). On Limited Nuclear War in the 21st Century. Stanford University Press. Stanford. R. 305.
10. Natalia Goncharova. (2021). Information security of Ukraine in conditions of hybrid warfare. Kyiv University Publishing House. Kyiv. P. 220.
11. Oleksandr Lytvynenko. (2020). Strategic priorities of national security of Ukraine. National Institute of Strategic Studies. Kyiv. P. 180.
12. Ivan Melnyk. (2019). Integration of Ukraine into the European security system. Razumkov Center. Kyiv. P. 150.
13. Olena Koroleva. (2022). Cyber security and cyber threats for Ukraine. Institute of International Relations. Kyiv. P. 135.
14. Vasyl Humenyuk. (2020). Ukraine in the system of collective security: challenges and prospects. "Ukrainian Priority" Publishing House. Lviv. P. 190.
15. Maria Petrenko. (2021). The impact of international cooperation on the national security of Ukraine. Institute of Foreign Policy Studies. Kharkiv. P. 110.

Метод оцінювання ефективності заходів щодо підвищення енергетичної та воєнної безпеки держави

Method of assessing the efficiency of measures to enhance energy and military security of the state

Юрій Клят [A]
Corresponding author: : к. т. н., доцент, начальник Центрального науково-дослідного інституту Збройних Сил України, e-mail: klyatt@ukr.net, ORCID: 0000-0002-8267-3748

Поліна Толок [B]
к. екон. н., начальник кафедри оборонного менеджменту, e-mail: tolok100@meta.ua, ORCID: 0000-0002-2481-8152

Олег Дєгтяр [C]
доктор наук з державного управління, професор, провідний науковий співробітник, e-mail: oleh.diehtiar@viti.edu.ua, ORCID: 0000-0001-6413-3580

ТетянаЧернега [D]
здобувач, e-mail: chtetiana888@gmail.com, ORCID: 0009-0000-5534-6664

Yurii Kliat [A]
Corresponding author: Ph.D., associate professor, head of the Central Research Institute of the Armed Forces of Ukraine for scientific work, e-mail: klyatt@ukr.net, ORCID: 0000-0002-8267-3748

PolinaTolok[B]
Candidate of Economic Sciences, Senior Research Fellow, Head of the Department, e-mail: tolok100@meta.ua, ORCID: 0000-0002-2481-8152

Oleg Diegtiar[C]
Dr of Science in Public Administration, Professor, Leading Researcher, e-mail: oleh.diehtiar@viti.edu.ua, ORCID: 0000-0001-6413-3580

Tetiana Cherneha [D]
Recipient, e-mail: chtetiana888@gmail.com, ORCID: 0009-0000-5534-6664

[A] Центральний науково-дослідний інститут Збройних Сил України, м. Київ, Україна
[B] Національний університет оборони України, Київ, Україна
[C] Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна
[D] Міністерство оборони України, м. Київ, Україна

[A] Central Research Institute of the Armed Forces of Ukraine, Kyiv, Ukraine
[B] National Defence University of Ukraine, Kyiv, Ukraine
[C] Military Institute of Telecommunications and Informatization named after Heroes of Kruty, Kyiv, Ukraine
[D] Ministry of Defense of Ukraine, Kyiv, Ukraine

Received: October 12, 2024 | Revised: October 26, 2024 | Accepted: October 31, 2024

DOI: 10.33445/sds.2024.14.5.9

Мета роботи: викладення основних положень методу оцінювання ефективності заходів щодо підвищення енергетичної та воєнної безпеки держави.
Метод дослідження: використовуються методи системного аналізу та векторної алгебри.
Практична цінність дослідження: запропонований метод оцінювання ефективності заходів щодо підвищення енергетичної та воєнної безпеки держави можна використовувати під час розроблення програмних документів стосовно розвитку енергетичної сфери держави, визначення шляхів протистояння негативним зовнішнім та внутрішнім факторам, проведення досліджень з енергетичної безпеки держави, зокрема визначення можливостей держави щодо протидії загрозам.
Тип статті: теоретична.

Ключові слова: енергетична безпека, воєнна безпека, оцінювання ефективності, енергетична система, критична інфраструктура.

Purpose: method of assessing the effectiveness of measures to improve the energy and military security of the state.
Method: methods of system analysis and vector algebra are used.
Practical implications: the proposed method of assessing the effectiveness of measures to increase the state's energy and military security can be used when developing program documents for the development of the state's energy sector, determining ways to counter negative external and internal factors, conducting research on the state's energy security, in particular, determining the state's capabilities in countering threats.
Paper type: theoretical.

Key words: energy security, military security, performance evaluation, energy system, critical infrastructure.

Вступ

Оцінювання ефективності заходів щодо підвищення енергетичної безпеки (енергобезпеки) держави має важливе значення для визначення раціональних шляхів забезпечення (підвищення) воєнної безпеки. Це особливо важливо у наш час, коли вся енергетична система України перебуває під ударами противника.

Воєнна безпека як структурний елемент національної безпеки характеризує здатність країни та її збройних сил протидіяти або перешкоджати завданню збитків її національній безпеці засобами збройного насильства. Для підтримання воєнної безпеки держави

необхідне відповідне економічне забезпечення, зокрема, все більшого значення набувають енергетичні ресурси. Зараз спостерігається взаємозалежність – підтримання воєнної безпеки потребує певного рівня енергобезпеки, а енергобезпека забезпечується військовими засобами. Тому оцінювання впливу енергетичної безпеки на воєнну безпеку є актуальним науковим завданням, розв'язавши яке, ми отримаємо можливість обґрунтовувати відповідні рішення щодо забезпечення належного рівня воєнної безпеки держави, що у свою чергу підтримуватиме енергобезпеку.

Теоретичні основи дослідження

Результати проведеного аналізу свідчать про те, що дослідженню питань щодо енергобезпеки приділяють багато уваги [1–10], однак слід зазначити, що питання стосовно впливу енергетичної безпеки на воєнну безпеку держави практично не розглядається.

Це призводить до того, що під час прийняття рішень щодо забезпечення потрібного рівня воєнної безпеки держави не враховують енергетичну складову й навпаки – не враховують зворотний зв'язок, що негативно відбивається на загальних результатах. Крім цього, навіть у Стратегії енергетичної безпеки [1] воєнні загрози критичній інфраструктурі в енергетичному секторі не згадуються.

Постановка проблеми

Мета статті полягає у викладенні основних положень розробленого методу оцінювання ефективності заходів щодо підвищення енергетичної та воєнної безпеки держави.

Результати

Мета запропонованого методу полягає в оцінюванні ефективності заходів щодо підвищення енергетичної безпеки для забезпечення воєнної безпеки держави, а також визначенні досягнутого шляхом втілення цих заходів рівня воєнної безпеки та його відповідності потрібному рівню. Тобто в отриманні значення певного показника, за допомогою якого можна буде оцінити її стан. Відповідно, під системою критеріїв у методі будемо розуміти таку мінімальну сукупність умов (нерівностей), яка дає можливість зробити відповідні висновки.

Для вирішення поставленого завдання наведено такий порядок розрахунків за запропонованим методичним апаратом (рис. 1).

У блоці формування бази вихідних даних за результатами огляду енергетичної сфери держави (стосовно впливу на воєнну безпеку) формується масив вихідних даних, до якого включається інформація щодо стану складових енергосистеми держави, стану енергозабезпеченості ЗС України та факторів, які впливають на її стан.

На основі отриманих у першому блоці даних у блоці оцінювання стану енергобезпеки визначається стан енергетичної безпеки у воєнній та невоєнній сферах. Для визначення стану воєнної безпеки держави пропонується підхід, який передбачає послідовне її оцінювання. Для реалізації такого підходу представлено відповідну систему показників [11].

Для розрахунку значення стану енергетичної безпеки необхідно здійснити згортку часткових показників.

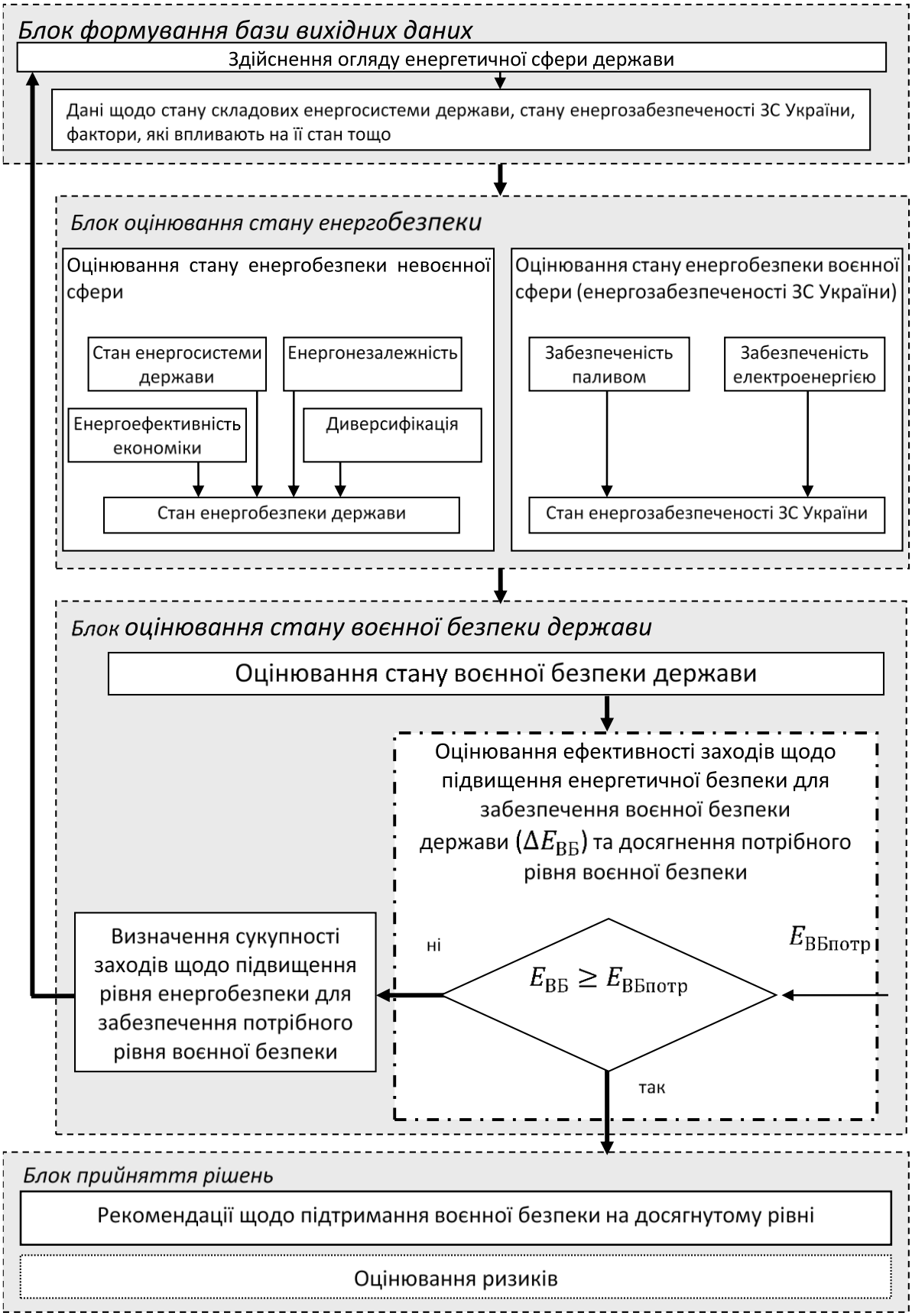


Рисунок 1 – Порядок оцінювання ефективності заходів щодо підвищення енергетичної безпеки для забезпечення воєнної безпеки держави

Згортку пропонується здійснювати з використанням елементів векторної алгебри, з урахуванням величини вкладу α_i від *i*-ї групи *m* факторів у загальну ефективність E_i об'єкта. Відповідно, можна записати:

$$E(m) = \sum_{s=1}^{n} \alpha_i E_i,$$

$$\sum_{s=1}^{n} \alpha_i = 1,$$

де E_i – ефективність *i*-ї групи факторів.

Для реалізації цього способу необхідно визначити залежність E_i від *i*-х груп факторів та оцінити експертним чи іншим шляхом величини вкладів α_i кожної з груп факторів у загальну ефективність.

Тобто завдання зводиться до того, щоб за допомогою відомих функцій $E_i(m_{ij})$ від m_{ij} факторів кожної *i*-ї групи ($i = \overline{1,n}$) оцінити загальну ефективність системи. З позиції векторної алгебри функцію ефективності $E_i(m_{ij})$ може бути представлено багатовимірним ($j = \overline{1,m_{ij}}$) вектором $\overline{E_i}$ у координатному вигляді таким чином:

$$\overline{E_i} = E_{i1}\bar{t} + E_{i2}\bar{j} + E_{i3}\bar{k} + \cdots + E_{ij}\bar{s} + \cdots + E_{im}\bar{l},$$

де $E_{i1}, E_{i2}, E_{i3}, E_{ij}, E_{im}$ – координати вектора E_i в *m*-вимірному просторі з ортонормованим базисом, який являє собою попарно ортогональні одиничні вектори $\bar{t}, \bar{j}, \bar{k}, \bar{s}, \bar{l}$;

m_{ij} – кількість ($j = \overline{1,m_{ij}}$) факторів, які враховуються в *i*-й складовій ($i = \overline{1,n}$) системи.

Множина координат (елементів) $E_{ij} (i = \overline{1,n}, j = \overline{1,m_{ij}})$ утворює матрицю такого виду:

$$\|E_{ij}\| = \begin{Vmatrix} E_{11} & E_{12} & \cdots & E_{1j} & \cdots & E_{im} \\ E_{21} & E_{22} & \cdots & E_{2j} & \cdots & E_{2m} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ E_{i1} & E_{i2} & \cdots & E_{ij} & \cdots & E_{im} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ E_{n1} & E_{n2} & \cdots & E_{nj} & \cdots & E_{nm} \end{Vmatrix},$$

елементи рядків якої є координатами відповідних векторів E_i. Ці координати є вихідними даними для розрахунку значень модуля вектора E_i, який визначається як скалярний добуток цього вектора на самого себе (дорівнює сумі добутків однойменних координат) або як квадрати елементів *i*-х рядків матриці $\|E_{ij}\|$ у такий спосіб:

$$|\overline{E_i}| = E_i = \sqrt{E_i \cdot E_i} = \sqrt{E_{i1}^2 + E_{i2}^2 + \cdots + E_{ij}^2 + \cdots + E_{im}^2} = \sqrt{\sum_{j=1}^{m} E_{ij}^2},$$

що, власне, й визначає величину ефективності E_i тієї чи іншої складової всієї системи.

Кожна координата E_i-го вектора (*i*-ї складової) у свою чергу є функцією від відповідного (m_{ij}-го) фактора, який сприяє її зростанню, вона може мати, наприклад, за результатами аналізу роботи цієї складової, такий вигляд, що не суперечить фізичному смислу розглядуваної функції:

$$E_{ij} = f(m_{ij}) = 1 - e^{-m_{ij}}.$$

У цьому випадку ефективність *i*-ї складової, що досягається, розраховується за формулою:

$$E_i = \sqrt{E_i \cdot E_i} = \sqrt{\sum_{j=1}^{m} (1 - e^{-m_{ij}})^2}.$$

Однак, варто зауважити, що в деяких випадках значення параметра може виражатися константою (дискретною величиною) або визначатися за принципом тригера – у цьому випадку необхідно нормувати це значення у такий спосіб, щоб воно знаходилось в інтервалі від 0 до 1.

Знаючи з підсумкових даних за минулий період величину внеску α_i кожної зі складових до загальної ефективності системи (або визначивши її в інший спосіб, наприклад, за допомогою експертних методів), можна визначити цю ефективність як:

$$E = \sum_{i=1}^{n} \alpha_i E_i = \sum_{i=1}^{n} \alpha_i \sqrt{\overline{E_i}\overline{E_\iota}} = \sum_{i=1}^{n} \alpha_i \sqrt{\sum_{j=1}^{m} E_{ij}^2} = \sum_{i=1}^{n} \alpha_i \sqrt{\sum_{j=1}^{m} (1 - e^{-m_{ij}})^2},$$

при цьому:

$$\sum_{i=1}^{n} \alpha_i = 1.$$

У *блоці оцінювання стану воєнної безпеки держави* визначається рівень воєнної безпеки залежно від стану енергетичної безпеки $Q(E)$ (з огляду на мету дослідження, групами факторів, що не пов'язані з енергобезпекою, можна знехтувати та вважати їх константами).

$$Q(E) = 1 - e^{-E}.$$

Ефективність заходів щодо підвищення енергетичної безпеки $E_{\text{зах}}$ розраховується як:

$$E_{\text{зах}} = \frac{Q_2(E)}{Q_1(E)},$$

де $Q_1(E), Q_2(E)$ – рівень воєнної безпеки держави до реалізації заходів та після, відповідно.

Крім цього, у цьому блоці оцінюється досягнення потрібного рівня воєнної безпеки:

$$Q_{\text{потр}}^{min} \le Q(E) < Q_{\text{потр}}^{max}, \quad (1)$$

де $Q_{\text{потр}}^{min}, Q_{\text{потр}}^{max}$ – мінімальний та максимальний потрібний рівень воєнної безпеки.

Границі діапазонів $Q_{\text{потр}}^{min}, Q_{\text{потр}}^{max}$ визначаються окремо особою, яка приймає рішення (ОПР), або за результатами експертного опитування, або за результатами спостереження та аналізу ситуацій (процесів), які вже призвели до погіршення стану енергетичної безпеки будь-де у світі. Слід зазначити, що у більшості випадків не ставиться завдання досягти максимально можливого рівня воєнної безпеки. Зазвичай границі діапазону обирають виходячи з аналізу загроз та наявних ресурсів.

Графік функції $Q(E)$ наведено на рис. 2.

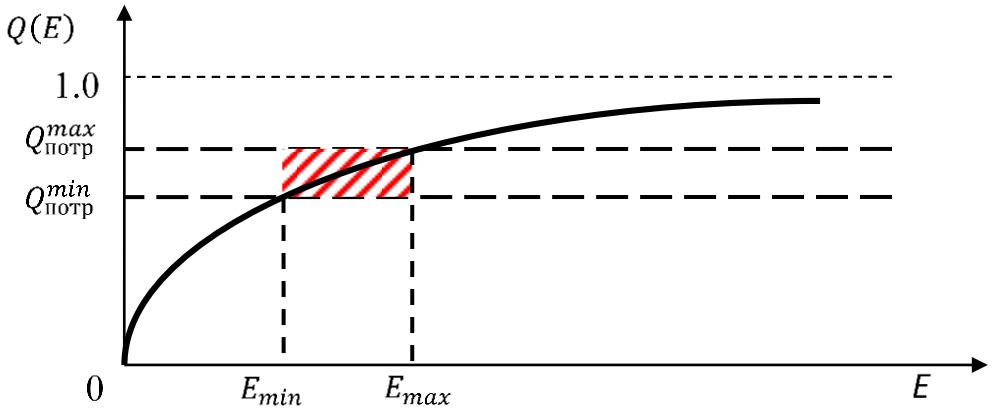


Рисунок 2 – Залежність воєнної безпеки від енергетичної безпеки держави

У випадку, коли умова (1) не виконується, здійснюється визначення сукупності заходів щодо підвищення рівня енергобезпеки для забезпечення потрібного рівня воєнної безпеки. Заходи визначаються з урахуванням критичних показників енергетичної безпеки за окремою методикою. Після впровадження цієї сукупності заходів здійснюється повторне оцінювання.

За умови досягнення потрібного значення рівня воєнної безпеки у блоці прийняття рішень розробляються рекомендації щодо підтримання енергетичної та, відповідно, воєнної безпеки на досягнутому рівні, взявши до уваги розраховану ефективність заходів щодо підвищення енергетичної безпеки для забезпечення воєнної безпеки держави або поступового збільшення рівнів безпеки з урахуванням наявних ресурсів та прогнозів.

Останнім етапом оцінювання може бути процедура оцінювання ризиків, які можуть виникнути внаслідок прийняття того чи іншого рішення [12]. У разі, якщо прогнозований ризик перевищує припустимий, процедуру прийняття рішення може бути повторено.

Висновки

Отже, у статті викладено основні положення методу оцінювання ефективності заходів щодо підвищення енергетичної безпеки для забезпечення воєнної безпеки держави.

За допомогою запропонованого методу, на відміну від наявних, є можливість визначити залежність стану воєнної безпеки від енергетичної, отримати інтегральне значення показника енергетичної безпеки, а також створити передумови для визначення критичних показників та розроблення рекомендацій щодо їх нейтралізації.

Напрямом подальших досліджень може бути розроблення методики прогнозування тенденцій змін енергетичної безпеки, що допоможе підвищити обґрунтованість управлінських рішень у сфері енергетичної та воєнної безпеки.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Україна. Кабінет Міністрів. Розпорядження. Про схвалення Стратегії енергетичної безпеки: розпорядження Каб. Міністрів від 4 серпня 2021 р. № 907-р. URL:

https://zakon.rada.gov.ua/laws/show/907-2021-%D1%80#Text.
2. Arnold C. Dupuy, Dan Nussbaum, Vytautas Butrimas, Alkman Granitsas Energy security in the era of hybrid warfare // NATO Review. URL: https://www.nato.int/docu/review/articles/2021/01/13/energy-security-in-the-era-of-hybrid-warfare/index.html.
3. Сафонов О. В. Оценка региональной энергетической безопасности в контексте интересов Украины. Економічні інновації. 2011. № 44. С. 267–275.
4. Мусіна Л. А., Кваша Т. К. Стан та оцінка енергетичної безпеки в Україні. Науково-технічна інформація. 2005. № 4. С. 23–32.
5. Шевцов А. І., Земляний М. Г., Дорошкевич А. З. Енергетична безпека України: стратегія та механізми забезпечення. Донецьк: Пороги, 2002. 264с.
6. Kui-Nang M. Energy and Sustainable Development: Issues And Options, Strategies And Actions: World Energy Council / 18th Congress, Buenos Aires, 2011. URL: http://www.worldenergy.org.
7. Rosario, Antonio V. del., Challenges, risks and energy security. URL: http://212.125.77.15/wec-geis/publications/default/archives/speeches/pritchard7802.pdf.
8. Суходоля О. М., Харазішвілі Ю. М., Бобро Д. Г., Сменковський А. Ю., Рябцев Г. Л., Завгородня С. П. Енергетична безпека України: методологія системного аналізу та стратегічного планування: аналіт. доп. Київ: НІСД, 2020. 178 с.
9. NATO Energy Security Centre of Excellence. URL: https://www.enseccoe.org.
10. Шаповал Л. Ю. Обґрунтування рекомендацій щодо забезпечення воєнної безпеки України за рахунок підвищення її енергетичної безпеки: дис. … к-та військ. наук: 21.02.01 / Шаповал Леонід Юрійович. Київ, 2014. 196 с.
11. Клят, Ю., Соломицький, О., Семененко, О., Водчиць, О., Войцеховський, Р., & Поливода, М. (2024). Визначення та класифікація загроз енергетичній безпеці України в сучасних умовах військових викликів. *Social Development and Security*, *14*(2), 272-285. https://doi.org/10.33445/sds.2024.14.2.22
12. Кушлик-Дивульська О.І., Кушлик Б.Р. Основи теорії прийняття рішень. Київ, 2014. 94 с.

References

1. Ukraina. Kabinet Ministriv. Rozporiadzhennia. Pro skhvalennia Stratehii enerhetychnoi bezpeky: rozporiadzhennia Kab. Ministriv vid 4 serpnia 2021 r. № 907-r. Available from : https://zakon.rada.gov.ua/laws/show/907-2021-%D1%80#Text.
2. Arnold C. Dupuy, Dan Nussbaum, Vytautas Butrimas, Alkman Granitsas Energy security in the era of hybrid warfare // NATO Review. Available from : https://www.nato.int/docu/review/articles/2021/01/13/energy-security-in-the-era-of-hybrid-warfare/index.html.
3. Safonov O. V. Ocenka regional'noj energeticheskoj bezopasnosti v kontekste interesov Ukrainy. *Ekonomichni innovacii*. 2011. № 44. S. 267–275.
4. Musina L. A., Kvasha T. K. Stan ta otsinka enerhetychnoi bezpeky v Ukraini. *Naukovo-tekhnichna informatsiia*. 2005. № 4. S. 23–32.
5. Shevtsov A. I., Zemlianyi M. H., Doroshkevych A. Z. Enerhetychna bezpeka Ukrainy: stratehiia ta mekhanizmy zabezpechennia. Donetsk: Porohy, 2002. 264s.
6. Kui-Nang M. Energy And Sustainable Development: Issues And Options, Strategies And Actions: World Energy Council / 18th Congress, Buenos Aires, 2011. Available from : http://www.worldenergy.org.
7. Rosario, Antonio V. del., Challenges, risks and energy security. Available from : http://212.125.77.15/wec-geis/publications/default/archives/speeches/pritchard7802.pdf.
8. .Sukhodolia O. M., Kharazishvili Yu. M., Bobro D. H., Smenkovskyi A. Yu., Riabtsev H. L.,

Zavhorodnia S. P. Enerhetychna bezpeka Ukrainy: metodolohiia systemnoho analizu ta stratehichnoho planuvannia: analit. dop. Kyiv: NISD, 2020. 178 c.
9. NATO Energy Security Centre of Excellence. Available from : https://www.enseccoe.org.
10. Shapoval L. Yu. Obgruntuvannia rekomendatsii shchodo zabezpechennia voiennoi bezpeky Ukrainy za rakhunok pidvyshchennia yii enerhetychnoi bezpeky: dys. … k-ta viisk. nauk: 21.02.01 / Shapoval Leonid Yuriiovych. Kyiv, 2014. 196 s.
11. Kliat, Y., Solomitsky, A., Semenenko, O., Vodchyts, O., Voytsehovskiy, R., & Polyvoda, M. (2024). Substantiation of security recommendations energy security of the state. *Social Development and Security*, *14*(2), 272-285. https://doi.org/10.33445/sds.2024.14.2.22
12. Kushly`k-Dy`vul`s`ka O.I., Kushly`k B.R. Osnovy` teoriyi pry`jnyattya rishen`. Ky`yiv, 2014. 94 s.

Потенціал застосування надлегких сталей для виробництва елементів броні військової техніки

The potential of lightweight steels application for the production of armor elements for military technique

Михайло Ворон [A]
Corresponding author: к.тех.н., старший дослідник, заст. зав. відділу, e-mail: mihail.voron@gmail.com, ORCID: 0000-0002-0804-9496

Юлія Скоробагатько [A]
к.тех.н., старший дослідник, старший науковий співробітник, e-mail: yulka.ukr@gmail.com, ORCID 0000-0002-1724-9895

Андрій Тимошенко [A]
к.тех.н., старший дослідник, старший науковий співробітник, e-mail: marschal@i.ua, ORCID: 0000-0003-4038-1744

Анастасія Семенко [A]
к.тех.н., старший дослідник, старший науковий співробітник, e-mail: semenko.au@gmail.com, ORCID: 0000-0002-0448-1636

Сергій Шваб [B]
к.тех.н., старший дослідник, старший науковий співробітник, e-mail: serg.schwab@gmail.com, ORCID 0000-0002-4627-9786

Олексій Смірнов [A]
д-р.техн.наук, проф., зав. відділу, e-mail: stalevoz@i.ua, ORCID: 0000-0001-5247-3908

Mykhailo Voron [A]
Corresponding author: Candidate of Technical Sciences, Deputy Head of Department, e-mail: mihail.voron@gmail.com, ORCID: 0000-0002-0804-9496

Yuliia Skorobagatko [A]
Candidate of Technical Sciences, Senior Researcher, e-mail: yulka.ukr@gmail.com, ORCID: 0000-0002-1724-9895

Andrii Tymoshenko [A]
Candidate of Technical Sciences, Senior Researcher, e-mail: marschal@i.ua, ORCID: 0000-0003-4038-1744

Anastasiia Semenko [A]
Candidate of Technical Sciences, Senior Researcher, e-mail: semenko.au@gmail.com, ORCID: 0000-0002-0448-1636

Serhiy Schwab [B]
Candidate of Technical Sciences, Senior Researcher, e-mail: serg.schwab@gmail.com, ORCID 0000-0002-4627-9786

Oleksiy Smirnov [A]
Dr. Sci.(Engin.), Professor, Head of the Department; e-mail: stalevoz@i.ua, ORCID: 0000-0001-5247-3908

[A] Фізико-технологічний інститут металів та сплавів НАН України, м. Київ, Україна
[B] Інститут електрозварювання ім. Є.О. Патона НАН Україна, м. Київ, Україна

[A] Physico-Technological Institute of Metals and Alloys of the National Academy of Sciences of Ukraine, Kyiv, Ukraine
[B] E.O. Paton Electric Welding Institute of the National Academy of Sciences of Ukraine, Kyiv, Ukraine

Received: October 6, 2024 | Revised: October 20, 2024 | Accepted: October 31, 2024

DOI: 10.33445/sds.2024.14.5.10

Мета роботи: Проведення аналізу хімічного складу і властивостей сучасних сталей для виготовлення елементів бронезахисту військової техніки з надлегкими сталями в контексті пошуку нових матеріалів, які можуть зменшувати масу засобів озброєння та захисту.

Метод дослідження: аналіз, експертна оцінка.

Результати дослідження Показано актуальність застосування матеріалів з низькою, по відношенню до звичайних сталей, густиною для виробництва елементів бронезахисту. Проведено порівняльний аналіз сталей, які використовуються у виробництві броні та вказано на потенційну технологічну і економічну доцільність використання з цією метою надлегких сталей.

Теоретична цінність дослідження: Запропоновано і обґрунтовано використання інноваційних матеріалів для потреб створення і модернізації військової техніки, зокрема для виробництва елементів бронезахисту, що може сприяти покращенню її тактико-технічних характеристик.

Практична цінність дослідження: Проведено коротке системне порівняння складу і властивостей найбільш відомих і надійних марок броньових сталей з перспективними надлегкими сталями, які мають схожі механічні та експлуатаційні характеристики. Описано технологічні прийоми для підвищення комплексу властивостей та потенціалу надлегких сталей для виготовлення бронезахисту військової техніки.

Purpose: Providing an analysis of the chemical composition and properties of modern steels for the manufacture of armor protection elements of military equipment with ultra-light steels in the context of searching a new materials that can reduce weight of weaponry and defense technique.

Method: analysis, expert assessment.

Findings: The relevance of using materials with a low density compared to ordinary steels for the production of armor protection elements is shown. A comparative analysis of steels used in the production of armor was carried out and the potential technological and economic feasibility of using lightweight steels for this purpose was indicated.

Theoretical implications: The use of innovative materials for the needs of creating and modernizing military eyсртшйгу is proposed and justified, in particular for the production of armor protection elements, which can contribute to the improvement of its tactical and technical characteristics.

Practical implications: A brief systematic comparison between most well-known and reliable grades of armor steels and promising lightweight steels, which have similar mechanical and operational characteristics, was carried out. Technological methods for increasing the complex of properties and potential of lightweight steels for the production of armor protection of military technique are described.

Value: The study is aimed to draw an attention to the possibilities of large-scale modernization of already existing and creation of

Цінність дослідження: Дослідження покликане привернути увагу до можливостей масштабної модернізації існуючих та створення нових зразків військової техніки за рахунок застосування нових матеріалів.
Майбутні дослідження: Буде здійснено пошук партнерів для практичного впровадження наявних розробок авторів і проведення експлуатаційних та балістичних випробувань.
Тип статті: Теоретично-експериментальний.

Value of the research: The research is called to draw attention to the possibilities of large-scale modernization of existing and the creation of new samples of military equipment by the use of new materials.
Future research: The search for partners will be carried out for the practical implementation of the authors' existing developments and providing operational and ballistic tests.
Papertype: Theoretical–experimental.

Ключові слова: оборонно-промисловий комплекс, нові матеріали для військової техніки, броня, модернізація, надлегкі сталі.

Key words: military-industrial complex, new materials for military technique, armor, modernization, lightweight steels.

Вступ

Створення і застосування нових конструкційних матеріалів з низькою густиною відноситься до числа найважливіших задач розвитку багатьох технологічних напрямків і є особливо важливим для оборонно-промислового комплексу. Зменшення маси елементів озброєння та військової техніки дозволяє підвищити мобільність і маневреність, а також зменшити габарити, або збільшити допустимі навантаження для зразків легко- та важкоброньованої наземної техніки, літаків, катерів, безпілотних та безекіпажних засобів, елементів індивідуального захисту, тощо. Перелічені переваги зниженої густини конструкційних матеріалів у ВПК використовуються та розвиваються багато десятиліть і залишаються в переліку постійних тенденцій удосконалення озброєння та військової техніки [1, 2].

Такі відомі світові лідери з виробництва озброєння, як Lockheed Martin, Boeing, BAE systems, Leonardo, Airbus, Dassault, Rheinmetall AG та Ingalls постійно розвивають і збільшують використання легких матеріалів для своєї техніки [3]. Класичне застосування високоміцних алюмінієвих сплавів та полімерів поступово збільшується для виробництва легкоброньованої техніки та безпілотних літальних апаратів. Для більш важкої техніки, яка потребує підвищення маневреності та одночасного збереження високого рівня захисту (танки, БМП, БТР) постійно зростає потреба в збільшенні відсотка використання легких та надміцних сталей на заміну класичних конструкційних та броньових залізо-вуглецевих сплавів [4].

Теоретичні основи дослідження

В якості відомого і досить контрастного прикладу використання легких матеріалів для виробництва елементів броні військової техніки варто навести алюмінієві сплави. Їх застосовують, починаючи з часів В’єтнамської війни, що показано на прикладі легендарного бронетранспортера М113. Він виготовлявся майже п’ятдесят років, а використовується понад шістдесят, має багато сучасних модернізацій та аналогів. Багато в чому така популярність та ефективність пов’язані саме з використанням алюмінієвої броні, для якої було застосовано сплави на основі системи Al-Mg-Mn. Вони забезпечували надійний захист від осколкових уражень та стрілецької зброї звичайних калібрів. Основними марками алюмінієвих сплавів для виробництва елементів броні є 2024, 2519, 5059, 6061, 7039, 7075 та 2139 [2, 5].

Логічним продовженням процесу створення легких матеріалів для бронезахисту повинні були стати сплави на основі титану та магнію. Тим не менш, титан може бути придатним лише в якості частини багатошарової композитної броні та як структурний екран для захисту від куль. Низькі балістичні характеристики титану пов’язані з утворенням адіабатичного розтріскування при взаємодії з балістичним фактором ураження, що викликає розшарування матеріалу та утворення сколів. Однією з причин такого ефекту є тип кристалічної ґратки титану (гексагональна компактна). Таку саму ґратку має і магній, тому він та його сплави також поки не використовуються в якості елементів броні. Перспективи його використання, при цьому, є досить високими, проте впровадження вимагає проведення великої кількості досліджень та розробки спеціальних технологій деформування [5].

Відповідно, запит на максимальне зменшення маси військової техніки при збереженні її високого рівня захищеності має велику актуальність, а розробки в цьому напрямку постійно продовжуються.

Постановка проблеми

Метою статті є експертний аналіз придатності нового типу надлегких сталей для виробництва елементів броні військової техніки та порівняння їх характеристик з деякими найбільш відомими і надійними марками броньових сталей, які використовуються в Україні та світі.

Результати

Серед класичних конструкційних матеріалів саме сталі продовжують залишатися основою для виробництва броні. Їх удосконалення в контексті зменшення ваги пов'язано із суттєвим додаванням до складу алюмінію, а також незначного підвищення вмісту кремнію та вуглецю. Таким чином можливо зменшити густину сталі з 7,9 до 6,2 г/см^3, тобто – на величину до 20% [6-8].

Додавання алюмінію, яке сприяє суттєвому зниженню густини, також спричиняє утворення крихких інтерметалідних фаз, які негативно впливають на весь комплекс механічних характеристик надлегких сталей. Задля компенсації тнегативного впливу сталь має містити велику кількість марганцю, яка повинна приблизно в два рази переважати вміст алюмінію [6, 9]. При такому хімічному складі сталі з високим вмістом марганцю та алюмінію можуть мати багатофазову будову, зміцнюватись деформаційною, термічною і термомеханічною обробками, а також нанорозмірними к-карбідами в умовах старіння сплавів після гартування. За рахунок такої великої кількості можливих механізмів зміцнення та регулювання основних механічних характеристик, в межах одного сплаву міцність може змінюватись в 2-2,5 рази, а твердість зростати з 42 до 58 HRC, в залежності від послідовності деформаційної та термічної обробки [6, 10].Міцність деяких представників таких сталей може складати 2 ГПа, а пластичність та ударна в'язкість при цьому становлять не менше 8-12 % та 25-35 Дж/см2 відповідно. Твердість сплавів може знаходитись в межах 52-58 HRC без деформаційної обробки, тобто в литому стані [6].

При масовому виробництві сталей, як звичайних, так і надлегких, важливу роль відіграють складність і точність їх хімічного складу, вартість легуючих елементів та здатність до вторинної переробки. Ці фактори найбільше впливають на вартість матеріалів, так само як і подальша складність їх деформаційної, термічної обробки, зварювання та ін.

Якщо порівняти хімічний склад найбільш розповсюджених броньових сталей, які використовуються в Україні, з надлегкими високоміцними сталями (табл. 1), можна помітити, що до останніх висувається менше вимог у дотриманні точності хімічного складу, а їх вартість може бути меншою за класичні сталі через переважну відсутність високовартісного нікелю. Крім того, при виробництві надлегких високоміцних сталей може використовуватись значна кількість вторинної сировини, включаючи відходи звичайних сталей, брухт військової техніки, моторний лом, феросплави та ін., що суттєво здешевлює виробництво.

Механічні властивості перелічених сталей приведено в табл. 2. З цих даних можна помітити, що необхідний рівень твердості знаходиться в межах 54-60 HRC. При значеннях вище 58-60 HRC зазвичай важко зберегти ударну в'язкість вище 10 Дж/см^2, тому можна сказати, що оптимальна твердість броньової сталі повинна знаходитись в межах 54-58 HRC.

Мінімальними бажаними значеннями межі плинності та межі міцності комерційних сталей найвищого класу захисту є показники на рівні 1300 та 1600 МПа відповідно. Пластичність сталей має бути не нижчою 5-7 %, що вказує на високий опір крихкому руйнуванню. Також не бажано, щоб цей показник перевищував 12-15 % через небезпеку надто сильного деформування бронеелементу.

Таблиця 1 – Порівняння хімічних складів сталей, які використовуються, або можуть бути використані для виробництва броні [6, 10-14]

Найменування сталей	Хімічний склад, % мас. (Fe – основа)									
	Mn	Al	Si	C	Cr	Ni	Mo	S	P	Інше
Armox 600 T, Armox Advance	≤ 1	–	≤ 0.7	≤ 0.47	≤ 1.5	≤ 3	≤ 0.7	≤ 0.003	≤0.01	≤0.005 B
Hardox 600, Hardox extreme	≤1.4	–	≤0.7	≤0.47	≤1.2	≤2.5	≤0.7	≤0.01	≤0.015	≤0.005 B
Ramor 550, 600	≤1.5	–	≤0.7	≤0.36-0.4	≤1.5	≤2.5	≤0.8	≤0.01	≤0.015	≤0.005 B
Mars 600, Mars 650	0.7	–	1	0.55	0.4	2.4-4.5	0.5	≤0.002	≤0.01-0.02	0.003 B
Сталь 71	0,6-1	0,015-0,05	1,2-1,5	0,29-0,36	1,5-2	2-2,4	0,45-0,55	≤0.003	≤0.012	0,005-0,025 Ti
45ХН2МФА	0,5-0,8	–	0,17-0,37	0,42-0,5	0,8-1,1	1,3-1,8	0,2-0,3	≤0,025	≤0,025	0,1-0,18 V, ≤ 0.3 Cu
Fe-24Mn-11Al-1,4C	23,8-24,5	10,5-11	0,25-0,35	1,3-1,4	–	–	–	–	–	–
Fe-30Mn-9Al-0,9C-1Si	29.5-30.5	8.8-9.1	0.5-1	0.85-1.05	–	–	–	–	–	–
Fe-18Mn-10Al-0.9C-5Ni	17.5-18.5	9.5-10.2	0.2-0.3	0.85-0.92	–	4.7-5.1	–	–	–	–

Ударна в’язкість, яка найбільш сильно корелює з твердістю і пластичністю матеріалу, також сильно залежить від структурних характеристик і анізотропії. Загалом вона також відповідає за недопущення крихкого руйнування елементів захисту, їх надійність і довговічність. Високий рівень ударної в’язкості з одночасно високою твердістю і пластичністю в межах 5-10 % є пріоритетним поєднанням властивостей, при якому межа міцності має другорядне значення і може мати значення порядку 1200 МПа.

Таблиця 2 – Механічні властивості сталей, хімічний склад яких наведений у табл. 1 [6-10, 12-14]

Сталі	Механічні властивості				
	HRC	$\sigma_т$, МПа	$\sigma_в$, МПа	δ, %	KCV, Дж/см^2
Armox 600 T	55-60	≥1400	1600-2000	≥7	≥ 12
Armox Advance	58-63				
Hardox 600	54-60				
Hardox extreme	57-63				
Ramor 500	54-60	≥1500	1800-2000	≥8	≥60
Ramor 600	54-60				
Mars 600, Mars 650	54-62	≥1300	≥2000	≥7	≥8, ≥16
Сталь 71	54-58	≥1600	≥1800	≥8	25-30
45ХН2МФА	54-62	≥1275	≥1420	≥7	≥39
Fe-24Mn-11Al-1,4C (литий)	44-52	≥1220	≥1250	≥8	~25
Fe-30Mn-9Al-0,9C-1Si	42-48	1200	≥1400-1600	≥9	71
Fe-18Mn-10Al-0.9C-5Ni	35-46	≥1150	≥1230	≥12	≥28

Власне, комерційні сталі Ramor 500, Ramor 600 та вітчизняна сталь 71 є найбільш надійними, в контексті сказаного вище. Порівнюючи їх властивості з деякими надлегкими сталями, можна помітити відповідність всіх основних показників потрібному рівню, окрім значень твердості.

Додаткове легування надлегких сталей хромом, термічна обробка і деформаційна пост-обробка здатні забезпечити підвищення їх твердості до 58 HRC. Оптимальний вміст основних легуючих елементів надлегких сталей, які можна застосовувати для виготовлення елементів бронезахисту військової техніки, враховуючи оптимальні значення механічних характеристик, буде наступним: (25-28)Mn, (10-12)Al, (1,1-1,4)C, (0,5-1)Si, (0-5)Cr (% мас.), залізо – основа [6]. Мікролегування, модифікування та додавання нікелю до 5 % мас. є опціональним. Вартість і недефіцитність компонентів надлегких сталей сприяє формуванню їх адекватної кінцевої вартості, яку можна порівняти зі звичайними інструментальними сталями, особливо за умов використання вторинної сировини.

Кінцеве регулювання механічних характеристик надлегких сталей, як було сказано вище, може здійснюватися комбінацією деформаційної та термічної обробки і холодною пластичною деформацією в якості пост-обробки. При цьому, менша міцність і вища пластичність є технологічними перевагами для забезпечення більш якісного зварювання [13], а особливості структурно-фазового стану матеріалу забезпечують максимальне розподілення ударних навантажень і одночасне стрибкоподібне зміцнення зони контакту з уражаючим елементом, що надаватиме матеріалу зміцнення в процесі експлуатації та підвищуватиме надійність бронезахисту [7].

Висновки

Розглянуто актуальність і наведено приклади застосування легких елементів броні для військової техніки. Порівняння хімічного складу та механічних властивостей деяких з найбільш відомих комерційних марок броньових сталей та кількох надлегких високоміцних сталей показали близькість властивостей обох типів сплавів, що безпосередньо вказує на доцільність і перспективність застосування надлегких сталей саме в якості елементів захисту броньованої військової техніки. Враховуючи високий потенціал надлегких сталей до зміцнення за допомогою застосування деформаційної, термічної обробки та їх комбінування, можливо досягти в них комплексу механічних характеристик на рівні сталей Ramor 600 та Mars 650. Вартість розглянутих сталей, що мають низьку густину є співставною або нижчою за звичайні інструментальні сталі через можливість застосування у виробництві великої кількості вторинної сировини, особливо – військового та моторного лому. Надлегкі сталі є достатньо технологічними і можуть піддаватися зварюванню.

Фінансування

Дослідження проведено в рамках виконання Проєкту 2023.04/0021 “Одержання елементів броні з надлегких сталей для військової техніки з використанням вторинної сировини”. Проєкт реалізовано за рахунок грантової підтримки Національного фонду досліджень України, конкурс “Наука для зміцнення обороноздатності України”.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Чепков І. Б. і Нор П.І. (2014). Загальні тенденції розвитку озброєння та військової техніки. *Озброєння та військова техніка*, 1, 4-13.
2. Teoman A., Gode E. and Cetin B. (2021). Advanced aluminum alloys used in land combat vehicle applications*. Proceedings of the International 10th Automotive Technologies Congress,* September 6-7, At: Bursa, Türkiye, 840-844.

3. Siengchin S. (2023). A review on lightweight materials for defence applications: Present and future developments. *Defence Technology*, 24., 1-17. https://doi.org/10.1016/j.dt.2023.02.025
4. Bowles N. (2020) *$20 million grant funds effort to develop ultra-high strength and lightweight steels for U.S. Army* Retrieved from: https://news.mst.edu/2020/12/20-million-grant-funds-effort-to-develop-ultra-high-strength-and-lightweight-steels-for-u-s-army/
5. Yunanda W.W., Gunadi G.I. and Kasim K. (2022). Metal as a Ballistic-Resistant Lightweight Protective Material in the Military Field. *International Journal of SocialScience Research and Review,* 5, 287-296. http://dx.doi.org/10.47814/ijssrr.v5i12.808
6. Ringer Nature Switzerland AG 2020R. Rana (ed.), High-Performance Ferrous Alloys, Chapter 6, Low-density steels. https://doi.org/10.1007/978-3-030-53825-5_6
7. Howell, R.A., Montgomery, J.S. and Van Aken, D.C. (2009). Advancements in Steel for Weight Reduction of P900 Armor Plate*, AIST, PR-PM0709-7*.
8. Sebek K. et al. (2018). High Mn, high Al steels for thick plate armor applications. *Ndia ground vehicle systems engineering and technology symposium materials & advance manufacturing (M&AM) technical session,* August 7-9, Nova, Michigan
9. Верзілов О.П., Ворон М.М. та ін. (2021) Сучасний стан та перспективи розробки високопластичних надміцних сталей Fe-Mn-Al-C. Повідомлення 1. *Метал та лиття України* (2), 101-109. https://doi.org/10.15407/steelcast2021.02.101
10. Ворон М.М., Семенко А.Ю. та ін. (2023). Структурно-фазові характеристики та механічні властивості TWIP-сталі Fe-24Mn-11Al-1.4C. *Металознавство та обробка металів* (4), 50-57. https://doi.org/10.15407/mom2023.04.050
11. Chemical composition of Ssab steels. URL: https://www.ssab.com/en
12. МСК Україна. URL: https://mskukraine.com/uk/katalog-produkcziyi/bronestal-uk/
13. Костін В. А., Позняков В. Д. та ін. (2020). Вплив структурних перетворень на механічні властивості зварних з'єднань броньованих сталей. *Фізико-хімічна механіка матеріалів* (4), 36-43.
14. Piston M., Bartlett L. et al. (2020). Microstructural Influence on Mechanical Properties of a Lightweight Ultrahigh Strength Fe-18Mn-10Al-0.9C-5Ni (wt.%) *Steel. Metals* (10), 1305. https://doi.org/10.3390/met10101305

References

1. Chepkov I. B. and Nor P. I. (2014). General trends in the development of weapons and military equipment. *Arms and Military Equipment*, 1, 4-13.
2. Teoman A., Gode E. and Cetin B. (2021). Advanced aluminum alloys used in land combat vehicle applications*. Proceedings of the International 10th Automotive Technologies Congress,* September 6-7, At: Bursa, Türkiye, 840-844.
3. Siengchin S. (2023). A review on lightweight materials for defence applications: Present and future developments. *Defence Technology*, 24., 1-17. https://doi.org/10.1016/j.dt.2023.02.025
4. Bowles N. (2020) *$20 million grant funds effort to develop ultra-high strength and lightweight steels for U.S. Army* Retrieved from: https://news.mst.edu/2020/12/20-million-grant-funds-effort-to-develop-ultra-high-strength-and-lightweight-steels-for-u-s-army/
5. Yunanda W.W., Gunadi G.I. and Kasim K. (2022). Metal as a Ballistic-Resistant Lightweight Protective Material in the Military Field. *International Journal of SocialScience Research and Review,* 5, 287-296. http://dx.doi.org/10.47814/ijssrr.v5i12.808
6. Ringer Nature Switzerland AG 2020R. Rana (ed.), High-Performance Ferrous Alloys, Chapter 6, Low-density steels. https://doi.org/10.1007/978-3-030-53825-5_6

7. Howell, R.A., Montgomery, J.S. and Van Aken, D.C. (2009). Advancements in Steel for Weight Reduction of P900 Armor Plate*, AIST, PR-PM0709-7*.
8. Sebek K. et al. (2018). High Mn, high Al steels for thick plate armor applications. *Ndia ground vehicle systems engineering and technology symposium materials & advance manufacturing (M&AM) technical session,* August 7-9, Nova, Michigan
9. Verzilov O.P., Voron M.M., Semenko A. Yu., Shemet V.Zh. (2021). The current state and the prospects for the development of high-plasticity ultrastrong Fe-Mn-Al-C steels. Communication 1. *Metal and Casting of Ukraine* (2), 101-109. https://doi.org/10.15407/steelcast2021.02.101
10. Voron M. M., Semenko A. Yu, Tymoshenko A. M., Shemet V. Zh. (2023). Structural and phase characteristics and mechanical properties of TWIP steel Fe-24Mn-11Al-1.4C. *Metal Science and Treatment of Metals* (4), 50-57. https://doi.org/10.15407/mom2023.04.050
11. Chemical composition of Ssab steels. Available from : https://www.ssab.com/en
12. MSK Ukraine. Retrieved from: https://mskukraine.com/uk/katalog-produkcziyi/bronestal-uk/
13. Kostin V. A., Poznyakov V. D. and others (2020). Influence of structural transformations on the mechanical properties of welded joints of armored steels. P*hysical and Chemical Mechanics of Materials* (4), 36-43.
14. Piston M., Bartlett L. et al. (2020). Microstructural Influence on Mechanical Properties of a Lightweight Ultrahigh Strength Fe-18Mn-10Al-0.9C-5Ni (wt.%) *Steel. Metals* (10), 1305. https://doi.org/10.3390/met10101305

Машинне навчання як ключовий інструмент оборонних кібероперацій: ефективність виявлення фішингових загроз

Machine learning as a key tool in defensive cyber operations: the effectiveness of phishing threat detection

Надія Бурова [A]
Corresponding author бакалавр, студент, e-mail: nadiia.burova.mKBUI.2023@lpnu.ua, ORCID: 0009-0008-6539-6743

Роман Оприск [A]
бакалавр, студент, e-mail: roman.oprysk.mKBUI.2023@lpnu.ua, ORCID: 0009-0009-5646-2718

Євгеній Курій [A]
доктор філософії, асистент, e-mail: yevhenii.o.kurii@lpnu.ua, ORCID: 0000-0002-3423-5655

Юрій Лах [A]
кандидат фізико-математичних наук, доцент, e-mail: yurii.v.lakh@lpnu.ua, ORCID: 0000-0003-4153-8125

Віталій Сусукайло [A]
доктор філософії, асистент, e-mail: vitalii.a.susukailo@lpnu.ua, ORCID: 0000-0003-4431-9964

Nadiia Burova [A]
Corresponding author Bachelor, Student, e-mail: nadiia.burova.mKBUI.2023@lpnu.ua, ORCID: 0009-0008-6539-6743

Roman Oprysk [A]
Bachelor, Student, e-mail: roman.oprysk.mKBUI.2023@lpnu.ua, ORCID: 0009-0009-5646-2718

Yevhenii Kurii [A]
Doctor of Philosophy, Assistant, e-mail: yevhenii.o.kurii@lpnu.ua, ORCID: 0000-0002-3423-5655

Yuriy Lakh [A]
Candidate of Physical and Mathematical Sciences, Associate Professor, e-mail: yurii.v.lakh@lpnu.ua, ORCID: 0000-0003-4153-8125

Vitalii Susukailo [A]
Doctor of Philosophy, Assistant, e-mail: vitalii.a.susukailo@lpnu.ua, ORCID: 0000-0003-4431-9964

[A] Національний університет Львівська політехніка, м. Львів, Україна
[A] Lviv Polytechnic National University, Lviv, Ukraine

Received: October 18, 2024 | Revised: October 28, 2024 | Accepted: October 31, 2024

DOI: 10.33445/sds.2024.14.5.11

Мета роботи: визначити ефективність використання алгоритмів машинного навчання для виявлення фішингових загроз у межах оборонних кібероперацій.

Метод дослідження: використання алгоритмів випадкових лісів, логістичної регресії та методу опорних векторів для автоматизованого аналізу URL-адрес. Програма реалізована на мові Python з використанням фреймворку Flask.

Результати дослідження: розроблене програмне рішення виявило високу ефективність у виявленні фішингових посилань, продемонструвавши точність аналізу при тестуванні на наборах реальних даних.

Практична цінність дослідження: запропонована система може бути впроваджена як частина оборонних кібероперацій для автоматизованого виявлення шкідливих посилань та підвищення кібербезпеки.

Тип статті: теоретичний, практичний.

Purpose: to determine the effectiveness of using machine learning algorithms for detecting phishing threats within the scope of defensive cyber operations.

Method: utilization of random forest algorithms, logistic regression, and supporting vector machines for automated URL analysis. The program is implemented in Python using the Flask framework.

Findings: the developed solution demonstrated high effectiveness in detecting phishing links, showcasing accuracy in analysis when tested on real data sets.

Practical implications: the proposed system can be implemented as part of defensive cyber operations for automated detection of malicious links and enhancement of cybersecurity.

Papertype: theoretical, practical.

Ключові слова: кібербезпека, машинне навчання, фішинг, оборонні операції, аналіз URL.

Key words: cybersecurity, machine learning, phishing, defensive operations, URL analysis.

Вступ

Кібербезпека стає однією з найважливіших складових сучасної глобальної безпеки, особливо в контексті збройних конфліктів. Кібероперації, спрямовані на дестабілізацію державної і приватної інфраструктури, перетворилися на невід'ємний елемент гібридної війни. Фішингові атаки, що використовують методи соціальної інженерії для обману користувачів і отримання несанкціонованого доступу до інформації, є однією з найпоширеніших форм таких кібератак. В умовах сучасного конфлікту між Україною та Росією ці атаки набули нового значення, ставши

одним із основних інструментів для впливу на критичні системи та підривання оборонних можливостей.

Використання алгоритмів машинного навчання в оборонних кібероперацiях пропонує нові можливості для протидії фішинговим загрозам. Завдяки здатності цих алгоритмів автоматизувати аналіз даних та оперативно виявляти потенційні загрози, його інтеграція у системи кіберзахисту забезпечує більш ефективну та проактивну оборону. У цій статті розглядаються методи використання машинного навчання для перевірки посилань з метою запобігання фішингових атак, а також описуються практичні аспекти впровадження оборонних кібероперацій для підвищення стійкості до таких загроз.

Теоретичні основи дослідження

Фішинг був і залишається однією з найбільш поширених та ефективних тактик для проведення кібератак. Ці атаки націлені на обман користувачів з метою викрадення їхніх облікових даних, отримання доступу до конфіденційної інформації або встановлення шкідливого програмного забезпечення на їхніх пристроях.

Кібератаки з використанням фішингу проти України активно застосовувалися ще до повномасштабного вторгнення Росії в 2022 році та залишаються важливою частиною її кіберкампаній (Mueller та інші, 2023). Наприклад, на початку вторгнення у лютому 2022 року хакери, пов'язані з російськими та білоруськими урядами, організували фішингові атаки, націлені на українських держслужбовців, військових і навіть міжнародні організації, які координували допомогу біженцям (Lewis, 2022). Одна з таких атак включала використання зламаних електронних поштових скриньок, що ускладнювало її виявлення та підвищувало ймовірність успіху (Security Insider, 2022).

Під час війни, окрім традиційного використання фішингу для збору облікових даних, атакуючі часто застосовують шкідливі програми типу “вайпера” (wiper), такі як HermeticWiper та IsaacWiper (Fendorf та інші, 2022). Ці програми були спеціально розроблені для знищення даних на українських урядових та корпоративних системах, що ускладнювало роботу державних органів і знижувало можливості ефективного управління кризовими ситуаціями (Freedberg, 2023). Використання фішингу для поширення таких програм стало однією з найбільш небезпечних форм кібератак, оскільки дозволяло швидко отримувати доступ до критичних систем і розгортати руйнівні дії.

Оборонні кібероперації відіграють важливу роль у протидії фішинговим атакам, особливо під час військових конфліктів, коли кіберпростір стає ключовим елементом бойових дій. Такі операції спрямовані на виявлення, пом’якшення наслідків та запобігання шкідливим активностям у кіберпросторі (Huskaj, 2023) (Daniel, 2022) . В Україні оборонні кібероперації стали важливим інструментом у відбитті російських кібератак. Оборонні кібероперації виконують важливі функції у контексті протидії фішинговим атакам. Вони забезпечують ефективне виявлення загроз, де машинне навчання та інші інструменти використовуються для аналізу даних про підозрілі URL-адреси, поведінкові патерни користувачів і активність у мережі. Це дає змогу виявляти фішингові атаки на ранніх етапах та запобігати їх поширенню (Porche та інші, 2011).

Машинне навчання є однією з ключових технологій, яка дозволяє значно підвищити ефективність оборонних кібероперацій. Завдяки здатності до автоматизації аналізу даних, алгоритми машинного навчання можуть ідентифікувати аномалії та виявляти загрози швидше та точніше, ніж традиційні методи. Це особливо важливо у протидії фішинговим атакам, де зловмисники використовують нові техніки для обходу стандартних засобів захисту. Переваги використання машинного навчання в кібербезпеці включають здатність алгоритмів адаптуватися до змін у тактиці атак та виявляти нові загрози, які раніше не були відомі.

Існує кілька типів алгоритмів машинного навчання, що можуть бути застосовані для аналізу URL-адрес, таких як класифікація, кластеризація та регресія. Класифікаційні алгоритми, як-от “випадкові ліси” та логістична регресія, дозволяють моделювати ймовірність того, що URL є фішинговим. Кластеризаційні алгоритми, такі як метод опорних векторів, допомагають групувати дані на основі схожих ознак, що може бути корисним для виявлення нових фішингових кампаній (Sarker, 2024).

Варто зазначити, що ефективність алгоритмів машинного навчання залежить від якості та кількості даних, використаних для навчання моделей. Використання наборів даних, які включають як фішингові, так і безпечні URL-адреси, дозволяє забезпечити високу точність моделей. У той же час, застосування додаткових ознак, таких як аналіз метаданих, оцінка довжини домену, кількість субдоменів і валідність SSL-сертифікатів, значно підвищує здатність алгоритмів розпізнавати шкідливі посилання (Kapan та інші,2023).

Крім того, варто враховувати складність сучасних фішингових атак, де кіберзлочинці використовують техніки соціальної інженерії та намагаються імітувати легітимні веб-сайти. Це робить традиційні методи захисту менш ефективними, а застосування алгоритмів машинного навчання – необхідністю. У такому випадку системи на базі ШІ можуть аналізувати не лише URL, але й вміст сторінки, що дозволяє виявляти фішингові сайти, навіть якщо вони використовують легітимний SSL-сертифікат або виглядають автентично.

Машинне навчання варто активно застосовувати для перевірки посилань на фішинг, що значно підвищить ефективність оборонних кібероперацій. Використання алгоритмів машинного навчання дозволить автоматизувати аналіз URL-адрес і виявляти потенційні загрози в режимі реального часу. Системи на основі алгоритмів машинного навчання можуть запобігати фішинговим атакам, аналізуючи URL на наявність фішингових ознак. Вони здатні виявляти навіть добре замасковані фішингові сайти, які використовують техніки соціальної інженерії для обману користувачів. Таким чином, машинне навчання стає критично важливим компонентом оборонних кібероперацій, який допомагає не тільки реагувати на кіберзагрози, але й запобігати їм, що забезпечує більш проактивний підхід до захисту в сучасному кіберпросторі.

Постановка проблеми

Сучасні кіберзагрози стають дедалі складнішими, і фішингові атаки відіграють важливу роль у здійсненні шкідливої діяльності в кіберпросторі. Традиційні методи захисту від фішингу часто виявляються недостатньо ефективними, оскільки зловмисники використовують новітні техніки соціальної інженерії та швидко адаптуються до наявних засобів захисту. У зв'язку з цим актуальною є розробка та впровадження інноваційних методів, таких як використання ШІ, для виявлення і запобігання фішинговим атакам на ранніх стадіях.

Методологія дослідження

У цій роботі використані такі методи дослідження:

1. Аналіз наукових джерел: Огляд літератури, наукових статей та доповідей, що стосуються оборонних кібероперацій, використання алгоритмів машинного навчання у кібербезпеці, а також фішингових атак, дозволить отримати загальне розуміння поточного стану досліджень у цій галузі.

2. Систематизація та узагальнення інформації: Класифікація існуючих методів боротьби з фішингом та застосування алгоритмів машинного навчання для аналізу URL-адрес дозволяє структурувати знання з цієї тематики та визначити ключові напрями подальших досліджень.

3. Аналіз випадків фішингових атак проти України: Розгляд реальних прикладів використання фішингу під час російсько-української війни для оцінки ефективності різних методів захисту та виявлення слабких місць в існуючих системах.

Результати та обговорення

Для ефективної реалізації оборонних кібероперацій пропонується застосування інноваційного підходу до виявлення фішингових загроз, який включає розробку програмного забезпечення на основі штучного інтелекту. Цей підхід забезпечує автоматизований аналіз URL-адрес для виявлення потенційно небезпечних посилань, дозволяючи оперативно реагувати на нові загрози. Використання алгоритмів машинного навчання у рамках оборонних операцій підвищує точність і швидкість аналізу, що сприяє зниженню ризику успішних фішингових атак та забезпеченню проактивного захисту критичних систем.

Підкреслюється необхідність глибокого та ретельного аналізу. В основу програмної реалізації входить використання мови програмування Python з закладеним в неї фреймворком Flask для розробки веб-додатку, а також необхідних бібліотек для реалізації аналізу URL за допомогою комплексу алгоритмів машинного навчання та додаткових інструментів.

Аналіз включає в себе використання:

- Алгоритму випадкових лісів;
- Алгоритму логістичної регресії;
- Алгоритму опорно-векторного кластерування на основі методу опорних векторів;

Одним із початкових кроків структури машинного навчання є безпосередньо тренування моделі. Для демонстрації працездатності роботи цілком достатньо невеликого набору даних.

У реалізації програми звертається увагу на те, що фішингові посилання можуть містити в назві IP-адресу, що з високою ймовірністю свідчить про небезпеку такого URL. Для цього випадку передбачається функція, яка за допомогою регулярних виразів аналізує назву URL-адреси та повертає значення “1”, якщо в її назві виявлено послідовність символів, які використовуються у IP-адресах (Рис. 1).

```
def has_ip(url):
    pattern = re.compile(r"(?:\d{1,3}\.){3}\d{1,3}")
    return 1 if pattern.search(url) else 0
```

Рисунок 1 – Функція для виявлення наявності IP-адреси в назві URL

Також загально відомо, що веб-сайти використовують HTTPS для безпеки з’єднання. Разом з розвитком безпеки веб-сайтів продовжує розвиватися й світ кіберзлочинців, які навчилися використовувати сертифікати SSL для фішингових сайтів з метою їх маскування під безпечні. На основі цього існує потреба в перевірці URL-адреси на валідність SSL-сертифікату. Для цього створюється функція, що аналізує посилання на наявність та валідність SSL-сертифікату (Рис. 2). Вона дозволяє більш ефективно оцінювати рівень загрози URL-адрес, що підкреслює точність програмної реалізації.

```python
def has_valid_ssl(url):
    try:
        parsed_url = urlparse(url)
        hostname = parsed_url.hostname if parsed_url.hostname else parsed_url.path

        context = ssl.create_default_context()
        with socket.create_connection((hostname, 443)) as sock:
            with context.wrap_socket(sock, server_hostname=hostname) as ssock:
                ssl_info = ssock.getpeercert()

        return 1
    except Exception as e:
        return 0
```

Рисунок 2 – Функція для перевірки валідності SSL-сертифікату

Не менш важливим кроком є повне покриття можливих варіантів аналізу посилань на фішингові ознаки. На сьогоднішній день у сфері інформаційних технологій існує багато хороших рішень, проте усі вони лише частково покривають перевірку URL-адрес.

У цьому випадку створюється функція, що допоможе усунути цю проблему. Вона буде вирізнятися кількістю параметрів, згідно, яких буде аналізуватися URL-адреса (Рис.3).

Сюди входять:

- Визначення кількості підозрілих символів в назві URL;
- Перевірка на наявність символів IP-адреси в назві URL;
- Перевірка наявності протоколу HTTPS;
- Перевірка на наявність підозрілого доменного імені та його довжина;
- Перевірка кількості суб-доменів;
- Перевірка валідності SSL-сертифікату;

```python
def extract_features(url):
    suspicious_symbols = ['@', '%', '&', '=']
    has_ip_addr = has_ip(url)
    suspicious_count = sum([url.count(symbol) for symbol in suspicious_symbols])
    uses_https = 1 if url.startswith('https') else 0
    domain_info = tldextract.extract(url)
    domain_length = len(domain_info.domain)
    subdomain_count = len(domain_info.subdomain.split('.')) if domain_info.subdomain else 0
    dangerous_word_count = 1 if has_dangerous_words(url) else 0
    valid_ssl = has_valid_ssl(url)

    return [has_ip_addr, suspicious_count, uses_https, domain_length, subdomain_count, dangerous_word_count, valid_ssl]
```

Рисунок 3 –Функція для перевірки URL-адреси за кількома параметрами

Головною ідеєю програмної реалізації є використання комплексу алгоритмів машинного навчання. Перед безпосередньою його реалізацією важливо підготувати набір даних для подальшого аналізу. Тут мається на увазі розбиття даних з вибірки на навчальні та тестові. Важливим тут є правильне їх розділення. Оскільки, початковий набір даних не є великим і складається з шести URL-адрес, дані рекомендується ділити наступним чином: чотири URL з набору даних входять у тестову вибірку (70%), а два URL у навчальну (30%) (Рис. 4).

```python
features = np.array([extract_features(url) for url in data])
X_train, X_test, y_train, y_test = train_test_split( *arrays: features, labels, test_size=0.3, random_state=42)
```

Рисунок 4 – Підготовка даних

У зв’язку з використанням невеликих наборів даних задаються оптимальні значення для кожного з алгоритмів, що входять в комплекс. Вони не затримують процес виконання програми і разом з тим зумовлюють точні результати аналізу (Рис. 5).

```
model_rf = RandomForestClassifier(n_estimators=100, random_state=42)
model_lr = LogisticRegression(random_state=42)
model_svc = SVC(probability=True, random_state=42)
```

Рисунок 5 – Створення моделей

Для створення комплексу алгоритмів машинного навчання їх потрібно об’єднати. В такому випадку порівняння отриманих результатів відбувається внаслідок виконання кожного алгоритму та автоматичний вибір оптимальної оцінки аналізу (Рис. 6).

```
ensemble_model = VotingClassifier(estimators=[
    ('rf', model_rf), ('lr', model_lr), ('svc', model_svc)
], voting='soft')
```

Рисунок 6 – Створення комплексу алгоритмів

Тренування комплексу алгоритмів машинного навчання відбувається зразу після його створення. Також використовується функція, яка видає кінцевий результат аналізу URL-адреси про те чи є посилання безпечним чи фішинговим в залежності від того, яке було отримане на вхід.

Для більш зручної роботи використовується створений веб-додаток з використанням фреймворку Flask. Його суттю є введення користувачем URL-адреси для аналізу та отримання результатів аналізу і звіту про усі введені посилання.

Звідси виникає логічне твердження, що вже існує схожий веб-додаток під назвою “PhishTank”. В такому разі на прикладі розглядається програмна реалізація аналізу URL-адрес на фішингові ознаки з використанням комплексу алгоритмів машинного навчання.

На початку, користувач бачить інтуїтивну сторінку з можливістю вводу URL-адреси для аналізу. Тут зразу варто зазначити, що інтуїтивність є однією з переваг даної програми у порівнянні з “PhishTank”.

Для порівняння: користувач вводить один безпечний (Рис. 7) та два фішингових сайти.

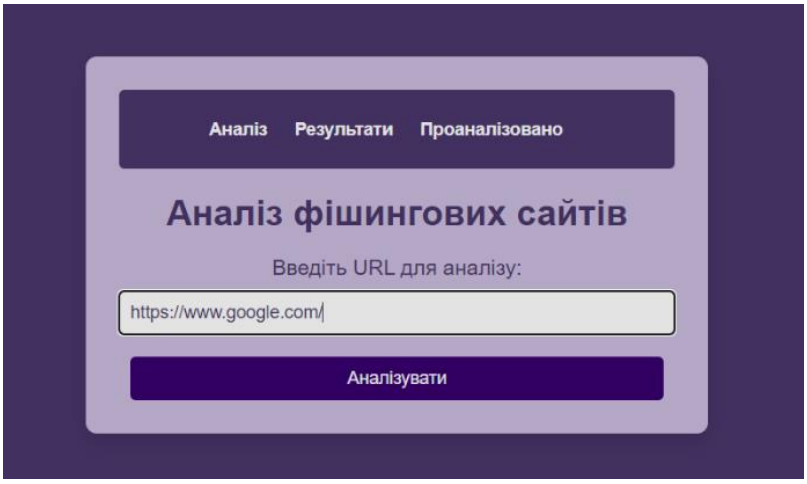


Рисунок 7 – Введення безпечного сайту для аналізу

Після підтвердження свого вибору одразу же можна побачити результат (Рис. 8).

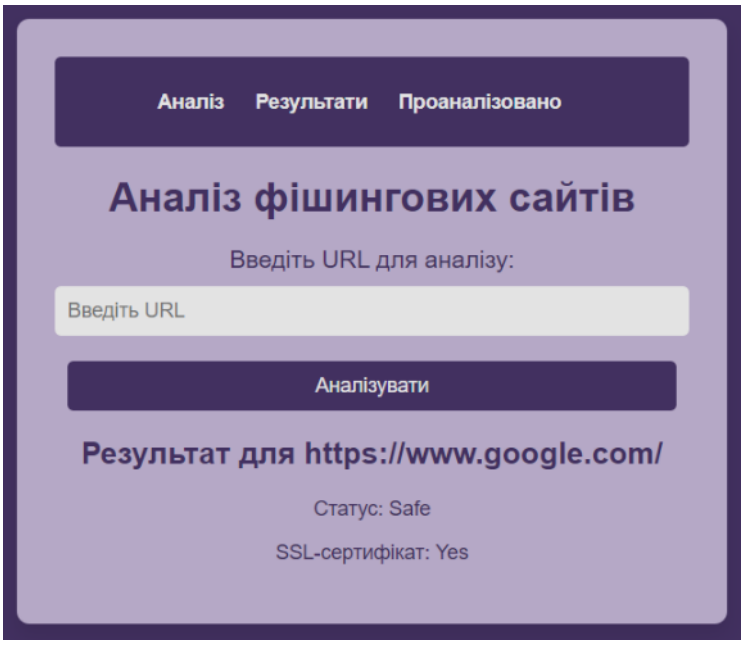


Рисунок 8 – Результат аналізу безпечного сайту

Тут підкреслюється швидкість виконання даної програми та актуальність перевірки на валідність SSL-сертифікату. “PhishTank” безумовно також має можливість вводу посилання для аналізу, проте отримання фінального результату займає тижні або місяці. Оскільки, усі посилання перевіряються людьми, то навіть за умови отримання кінцевого результату, він не є достатньо надійним, адже тут присутній людський фактор.

Така програмна реалізація також надає можливість користувачеві переглянути вже проаналізовані URL-адреси (Рис. 9). Як результат, очікувані результати роботи програми та наявні збігаються, адже було взято одну безпечну та дві фішингові URL-адреси.

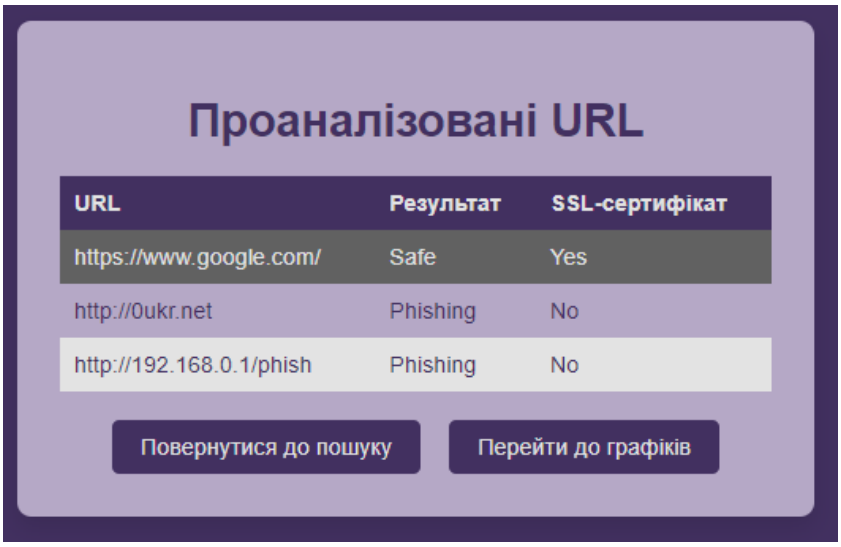


Рисунок 9 – Перегляд проаналізованих URL-адрес

Для вираження точності роботи програмної реалізації використовуються реальні фішингові адреси. Рекомендується використовувати підтверджений чорний список URL-адрес.

З нього обрано 20 фішингових посилань для проведення перевірки надійності результатів програмної реалізації (Рис. 10). Варто врахувати, що всі URL-адреси використовують протокол HTTPS, що ускладнює виявлення ознак фішингу.

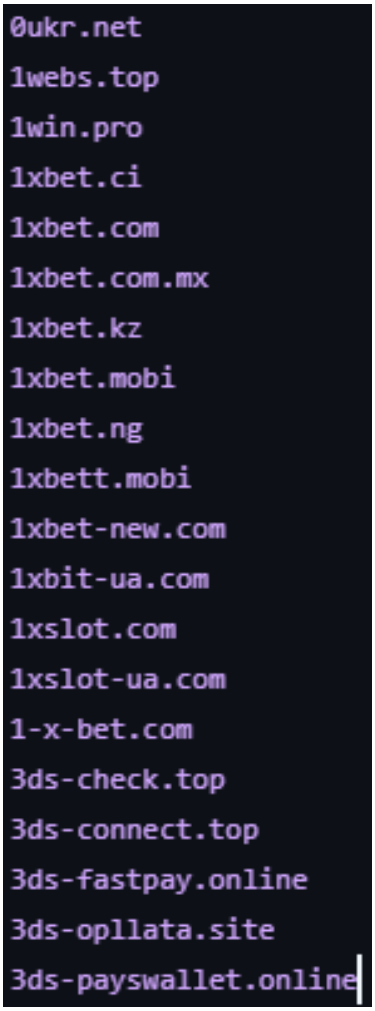


Рисунок 10 – Тестова вибірка чорного списку URL-адрес

Оскільки у програмній реалізації запобігання фішинговим атакам використовується функція перевірки SSL-сертифікату це тестування в свою чергу дає можливість показати її роботу.

Очкікується, що результатом програми, яка використовує комплекс алгоритмів машинного навчання будуть 20 URL-адрес з підтвердженням наявності фішингових ознак та невалідними SSL-сертифікатами.

Після введення усіх URL-адрес із чорного списку та їх перегляду після аналізу спостерігається, що усі посилання були позначені як фішингові, а перевірка SSL-сертифікатів показала, що вони не є валідними (Рис. 11). Таким чином, очікувані результати збігаються з наявними, що підкреслює точність роботи програмної реалізації аналізу URL-адрес на фішингові ознаки.

Проаналізовані URL

URL	Результат	SSL-сертифікат
https://0ukr.net	Phishing	No
https://1webs.top	Phishing	No
https://1win.pro	Phishing	No
https://1xbet.ci	Phishing	No
https://1xbet.com	Phishing	No
https://1xbet.com.mx	Phishing	No
https://1xbet.kz	Phishing	No
https://1xbet.mobi	Phishing	No
https://1xbet.ng	Phishing	No
https://1xbett.mobi	Phishing	No
https://1xbet-new.com	Phishing	No
https://1xbit-ua.com	Phishing	No
https://1xslot.com	Phishing	No
https://1xslot-ua.com	Phishing	No
https://1-x-bet.com	Phishing	No
https://3ds-check.top	Phishing	No
https://3ds-connect.top	Phishing	No
https://3ds-fastpay.online	Phishing	No
https://3ds-opllata.site	Phishing	No
https://3ds-payswallet.online	Phishing	No

Повернутися до пошуку | Перейти до графіків

Рисунок 11 – Демонстрація результатів

Після розгляду програми, можна порівняти її з “PhishTank” по швидкодії, точності та ефективності роботи (Рис. 12).

Програмна реалізація запобігання фішинговим атакам на основі комплексу алгоритмів машинного навчання суттєво виділяється на фоні “PhishTank”, адже ефективний аналіз URL-адрес не потребує великих часових затрат. Точність в свою чергу не залежить від людського фактору, а заснована безпосередньо на надійних алгоритмах машинного навчання, які працюючи в комплексі надають можливість ефективно запобігати фішинговим атакам.

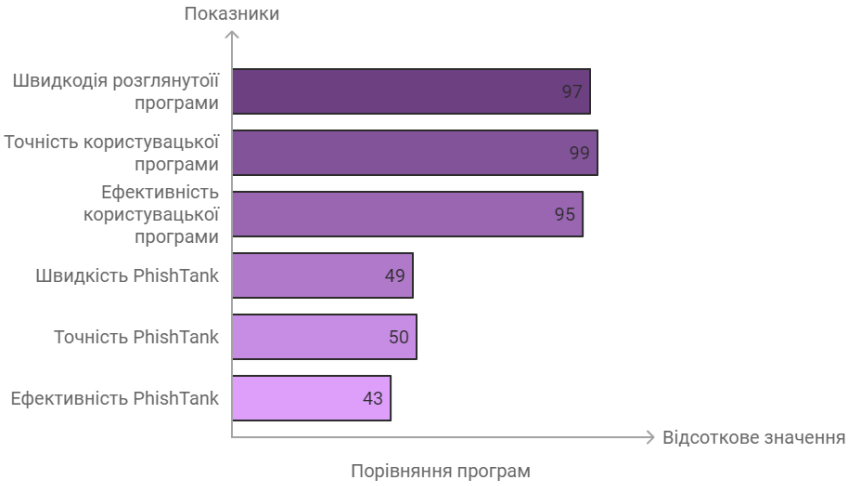


Рисунок 12 – Порівняльний графік

Висновки

Розробка і впровадження систем для автоматизованого виявлення фішингових атак є важливою складовою сучасних оборонних кібероперацій. Проведений аналіз показав, що застосування алгоритмів машинного навчання дозволяє підвищити ефективність захисту від фішингових загроз, забезпечуючи швидке та точне виявлення небезпечних URL-адрес. Використання таких алгоритмів, як випадкові ліси, логістична регресія та метод опорних векторів, дозволяє комплексно оцінювати ознаки фішингу, включаючи наявність IP-адрес у посиланні, валідність SSL-сертифікатів та кількість субдоменів.

Успішна реалізація запропонованого підходу підтверджується результатами тестування, де система виявила всі фішингові посилання із чорного списку. Це свідчить про високу точність програмного рішення, що ґрунтується на об'єднанні кількох алгоритмів машинного навчання. Додаткові переваги запропонованої системи включають її швидкодію та відсутність залежності від людського фактору, що є значним покращенням порівняно з існуючими рішеннями, такими як "PhishTank".

Подальший розвиток цієї програми передбачає збільшення набору даних для тренування моделей, а також впровадження нових методів аналізу, таких як глибоке навчання. Це дозволить адаптувати систему до змінних умов кіберзагроз та забезпечити її ефективність на довгострокову перспективу. Результати дослідження підтверджують, що інтеграція машинного навчання в оборонні кібероперації є перспективним напрямком для зміцнення кібербезпеки та протидії фішинговим атакам.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Mueller, G. B., Jensen, B., Valeriano, B., Maness, R. C., & Macias, J. M. (2023, 13 липня). *Cyber operations during the Russo-Ukrainian war*. Center for Strategic and International Studies. URL : https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war
2. Lewis, J. A. (2022, 16 червня). *Cyber war and Ukraine*. Center for Strategic and International Studies. https://www.csis.org/analysis/cyber-war-and-ukraine
3. Russia's cyberattack activity in the Ukraine / *Security Insider*. (2022). URL : https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/special-report-ukraine/
4. Freedberg Jr, S. J. (2023, 16 лютого). *Russian phishing attacks flooded Ukraine, tripled against NATO nations in 2022: Report – Breaking Defense*. Breaking Defense. URL : https://breakingdefense.com/2023/02/russian-phishing-attacks-flooded-ukraine-tripled-against-nato-nations-in-2022-report/
5. Fendorf, K., & Miller, J. (2022, 24 березня). *Tracking cyber operations and actors in the russia-ukraine war*. Council on Foreign Relations. URL : https://www.cfr.org/blog/tracking-cyber-operations-and-actors-russia-ukraine-war
6. Daniel, M. (2022). *Offensive cyber operations: Understanding intangible warfare*. Oxford University Press, Incorporated.
7. Huskaj, G. (2023). Offensive cyberspace operations for cyber security. *International Conference on Cyber Warfare and Security*, *18*(1), 476–479. https://doi.org/10.34190/iccws.18.1.1054

8. Porche, I. R., Sollinger, J. M., & McKay, S. (2011). *A cyberworm that knows no boundaries. RAND Corporation.* https://doi.org/10.7249/op342
9. Sarker, I. H. (2024). Learning technologies: Toward machine learning and deep learning for cybersecurity. У *AI-Driven cybersecurity and threat intelligence: Cyber automation, intelligent decision-making and explainability* (с. 43-59). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-54497-2_3
10. Kapan, S., & Sora Gunal, E. (2023). Improved phishing attack detection with machine learning: A comprehensive evaluation of classifiers and features. *Applied Sciences*, *13*(24). https://doi.org/10.3390/app132413269

References

1. Mueller, G. B., Jensen, B., Valeriano, B., Maness, R. C., & Macias, J. M. (2023, July 13). *Cyber operations during the Russo-Ukrainian war*. Center for Strategic and International Studies. Available from : https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war
2. Lewis, J. A. (2022, June 16). *Cyber war and Ukraine*. Center for Strategic and International Studies. https://www.csis.org/analysis/cyber-war-and-ukraine
3. Russia's cyberattack activity in the Ukraine | *Security Insider*. (2022). Available from : https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/special-report-ukraine/
4. Freedberg Jr, S. J. (2023, February 16). *Russian phishing attacks flooded Ukraine, tripled against NATO nations in 2022: Report – Breaking Defense*. Breaking Defense. Available from : https://breakingdefense.com/2023/02/russian-phishing-attacks-flooded-ukraine-tripled-against-nato-nations-in-2022-report/
5. Fendorf, K., & Miller, J. (2022, March 24). *Tracking cyber operations and actors in the russia-ukraine war*. Council on Foreign Relations. https://www.cfr.org/blog/tracking-cyber-operations-and-actors-russia-ukraine-war
6. Daniel, M. (2022). *Offensive cyber operations: Understanding intangible warfare*. Oxford University Press, Incorporated.
7. Huskaj, G. (2023). Offensive cyberspace operations for cyber security. *International Conference on Cyber Warfare and Security*, *18*(1), 476–479. https://doi.org/10.34190/iccws.18.1.1054
8. Porche, I. R., Sollinger, J. M., & McKay, S. (2011). *A cyberworm that knows no boundaries. RAND Corporation.* https://doi.org/10.7249/op342
9. Sarker, I. H. (2024). Learning technologies: Toward machine learning and deep learning for cybersecurity. У *AI-Driven cybersecurity and threat intelligence: Cyber automation, intelligent decision-making and explainability* (S. 43-59). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-54497-2_3
10. Kapan, S., & Sora Gunal, E. (2023). Improved phishing attack detection with machine learning: A comprehensive evaluation of classifiers and features. *Applied Sciences*, *13*(24). https://doi.org/10.3390/app132413269

Інновації та майбутнє автономних бойових літаків

Innovations and greatest autonomous combat limits

Олександр Сорочкін [A]
Corresponding author: старший викладач кафедри, e-mail: aozhnups@gmail.com, ORCID: 0000-0001-8336-9978
Михайло Сосулін [A]
старший викладач кафедри, e-mail: sosulin@ukr.net, ORCID: 0009-0003-0178-621X
Євген Матвєєв [A]
викладач кафедри, e-mail: gekamatvei11@gmail.com, ORCID: 0000-0002-1582-7591
Борис Головко [A]
доцент кафедри, e-mail: bo4ka18tonn@gmail.com, ORCID: 0000-0002-2669-9249

Oleksandr Sorochkin [A]
Corresponding author: Senior lecturer of the Department, e-mail: aozhnups@gmail.com, ORCID: 0000-0001-8336-9978
Mykhailo Sosulin [A]
Senior lecturer of the Department, e-mail: sosulin@ukr.net, ORCID: 0009-0003-0178-621X
Yevhen Matvieiev [A]
lecturer of the Department, e-mail: gekamatvei11@gmail.com, ORCID: 0000-0002-1582-7591
Borys Holovko [A]
Associate professor of the Department, e-mail: bo4ka18tonn@gmail.com, ORCID: 0000-0002-2669-9249

[A] Харківський національний університет Повітряних Сил імені Івана Кожедуба, м. Харків, Україна
[A] Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine

Received: October 4, 2024 | Revised: October 28, 2024 | Accepted: October 31, 2024

DOI: 10.33445/sds.2024.14.5.12

Мета роботи: є комплексний аналіз інновацій та перспектив розвитку автономних бойових літаків, включаючи вивчення наукових досліджень, патентних даних та практичних прикладів впровадження АБЛ, що дозволить визначити основні тенденції та пріоритетні напрямки розвитку військової авіації, а також окреслити ключові виклики та можливості, пов'язані з використанням автономних систем у бойових умовах.

Метод дослідження: якісні та кількісні методи дослідження.

Результати дослідження: Дослідження визначає ключові технологічні напрямки в розробці автономних бойових літаків, включаючи досягнення в області штучного інтелекту, передові матеріали, автономні системи управління та етичні міркування. Інновації в матеріалознавстві, такі як термопластичні еластомери та керамічні композити, виділяються за їхню роль у підвищенні довговічності та зменшенні ваги літака. Автономні системи керування на основі штучного інтелекту відомі своїми можливостями щодо прийняття рішень у реальному часі, обробки даних та адаптивністю до мінливих умов. Аналіз патентних даних виявляє перспективні технології, зокрема системи на основі штучного інтелекту та нові матеріали, які мають вирішальне значення для майбутніх розробок.

Теоретична цінність дослідження: Дослідження сприяє теоретичному розумінню інтеграції передових технологій, таких як ШІ та нових матеріалів, у військовій авіації. Хоча він явно не відкидає та не змінює існуючі теорії, він спирається на поточні знання в цій галузі, забезпечуючи всебічний аналіз стану та майбутніх перспектив автономних бойових літаків.

Практична цінність дослідження: Вивчення інтеграції ШІ у військові стратегії та тактику, зокрема в контексті динаміки бойових дій, що розвивається, наприклад переходу до позиційної війни та війни на виснаження. Аналіз потенційного впливу технологій ШІ між пілотованими та безпілотними літальними платформами у військовій авіації.

Майбутні дослідження: Покращення можливостей прийняття рішень систем ШІ для автономних бойових літаків, включаючи адаптацію в режимі реального часу.

Purpose: there is a comprehensive analysis of innovations and prospects for the development of autonomous combat aircraft, including the study of scientific research, patent data and practical examples of the implementation of ABL, which will allow to determine the main trends and priority directions of the development of military aviation, as well as to outline the key challenges and opportunities related to using autonomous systems in combat conditions.

Method: qualitative and quantitative research methods.

Research results: The study identifies key technological areas in the development of autonomous combat aircraft, including advances in artificial intelligence, advanced materials, autonomous control systems and ethical considerations. Innovations in materials science, such as thermoplastic elastomers and ceramic composites, are highlighted for their role in increasing durability and reducing aircraft weight. Autonomous AI-based control systems are known for their real-time decision-making capabilities, data processing, and adaptability to changing conditions. Analysis of patent data reveals promising technologies, including artificial intelligence-based systems and new materials, that are critical to future developments.

The theoretical value of the research: The research contributes to the theoretical understanding of the integration of advanced technologies such as AI and new materials in military aviation. While it does not explicitly reject or change existing theories, it builds on current knowledge in the field, providing a comprehensive analysis of the state and future prospects of autonomous combat aircraft.

The value of the research: Exploring the integration of AI into military strategies and tactics, particularly in the context of evolving warfare dynamics, such as the transition to positional warfare and warfare of attrition. Analysis of the potential impact of AI technologies between manned and unmanned aerial platforms in military aviation.

Future research: Improving the decision-making capabilities of AI systems for autonomous combat aircraft, including real-time adaptation. Increasing the reliability and safety of autonomous systems based on artificial intelligence, solving cyber security problems and system failures. Exploring the

Підвищення надійності та безпеки автономних систем на основі штучного інтелекту, вирішення проблем кібербезпеки та системних збоїв. Вивчення інтеграції розширених алгоритмів машинного навчання для таких завдань, як розпізнавання цілей, планування місії та автономна навігація.

Тип статті: Концептуальна.

Ключові слова: автономні бойові літаки, інновації, штучний інтелект, військова авіація, етичні аспекти.

integration of advanced machine learning algorithms for tasks such as target recognition, mission planning, and autonomous navigation.

Papertype: Conceptual.

Key words: autonomous combat aircraft, innovations, artificial intelligence, military aviation, ethical aspects.

Вступ

Актуальність теми обумовлена зростаючими вимогами до технічних характеристик бойових літаків, які використовуються у військових конфліктах та для захисту національної безпеки. Сучасні тенденції в розвитку автономних систем вказують на значний потенціал для вдосконалення військової авіації за рахунок інтеграції ШІ та новітніх матеріалів, що дозволяє знизити ризики для пілотів, підвищити точність та ефективність бойових місій, а також забезпечити адаптацію до швидкозмінних умов.

Теоретичні основи дослідження

Розвиток автономних бойових літаків та інновацій у військовій авіації активно досліджується в наукових колах. Робота [2] містить комплексний огляд сучасних технологічних трендів у військовій авіації, зокрема, в області безпілотних літальних апаратів та автономних систем управління. Автор звертає увагу на вплив штучного інтелекту та новітніх матеріалів на підвищення ефективності та довговічності бойових літаків. Аналізуються передові технології, які забезпечують поліпшення аеродинамічних характеристик, зниження ваги та підвищення паливної ефективності.

У роботі [7] розглядаються інновації у розробці безпілотних літаків, що працюють на сонячних батареях. Зокрема, аналізується діяльність провідних компаній, таких як SZ DJI Technology, яка спеціалізується на виробництві дронів для комерційного, сільськогосподарського та промислового секторів. Ці технології дозволяють збільшити тривалість польоту та покращити енергоефективність безпілотних літальних апаратів.

У роботі [4] представляє аналіз світових тенденцій у розвитку військової техніки, включаючи автономні бойові системи. Автори розглядають вплив новітніх технологій на зміну стратегій та тактик у військових операціях. Важливим аспектом є також аналіз етичних та правових питань, пов’язаних із застосуванням автономних систем у бойових умовах.

Андрощук Г. О. та Кваша Т. К. у своїй статті [1] досліджують патентні дані для визначення перспективних напрямків розвитку військових технологій. Виявлено, що значний акцент робиться на розробку автономних систем управління та інноваційних матеріалів, що підвищують ефективність бойових літаків.

Коритько О. І. та Підчибій Л. В. у своїй праці [3] аналізують останні розробки тактичних літаків. Автори зазначають, що впровадження автономних систем та новітніх матеріалів є ключовими факторами підвищення бойової ефективності та безпеки літаків. Важливим аспектом є також інтеграція ШІ у системи управління літаком, що дозволяє підвищити точність та швидкість прийняття рішень в бойових умовах.

Ці дослідження підкреслюють важливість інновацій у розвитку військової авіації та необхідність подальшого дослідження автономних бойових літаків з метою підвищення їх ефективності та безпеки.

Постановка проблеми

Завданням дослідження є визначення основних напрямків розвитку автономних бойових літаків, аналіз поточних наукових досліджень та інновацій у цій галузі, а також оцінка

перспектив використання АБЛ у військових операціях. Необхідно розглянути технічні, етичні та нормативно-правові аспекти впровадження автономних систем у військовій авіації.

Метою статті є комплексний аналіз інновацій та перспектив розвитку автономних бойових літаків, включаючи вивчення наукових досліджень, патентних даних та практичних прикладів впровадження АБЛ, що дозволить визначити основні тенденції та пріоритетні напрямки розвитку військової авіації, а також окреслити ключові виклики та можливості, пов'язані з використанням автономних систем у бойових умовах.

Результати

Комплексний бібліометричний аналіз бази даних Web of Science виявляє найперспективніші наукові тренди у військовій авіації, включаючи БПЛА, проектування літаків на базі ШІ та новітні матеріали для підвищення продуктивності та довговічності. Аналіз патентних даних, проведений за допомогою бази Derwent Innovation, ідентифікує пріоритетні та перспективні технології у військовій авіації, до найбільш значущих досягнень належать інновації у конструкції літаків, роторних літальних апаратів, компонентів БПЛА та передових матеріалів, і серед найвідоміших заявників на патенти у цій галузі є компанії KDDI, яка спеціалізується на розробці невеликих комерційних дронів, та SZ DJI Technology, яка виробляє комерційні дрони для споживчого, сільськогосподарського та промислового секторів.

Інновації в матеріалознавстві мають вирішальне значення для покращення характеристик автономних літаків, включаючи ламінати з термопластичних еластомерів, крильчатки відцентрових вентиляторів та керамічні матричні композити для турбін, що підвищують довговічність, зменшують вагу та покращують паливну ефективність. БПЛА продовжують бути в центрі інновацій з розробкою сонячних електричних літаків та вдосконалених систем управління, які дозволяють збільшити тривалість польоту, покращити маскувальні можливості та підвищити універсальність. Китайська компанія SZ DJI Technology подала найбільшу кількість патентів на технології запуску дронів, вона виробляє комерційні дрони для споживчого, сільськогосподарського та промислового секторів і спеціалізується на високоякісних камерах та інтеграції з програмним забезпеченням. Системи на базі ШІ для автономних літаків включають вдосконалені можливості навігації, розпізнавання цілей та планування місій, що дозволяє досягати більшої автономії та точності у бойових операціях. Понад 180 інновацій формуватимуть майбутнє аерокосмічної та оборонної промисловості за даними GlobalData Technology Foresights [2].

Майбутнє автономних бойових літаків визначатиметься поточними дослідженнями та розробками провідних аерокосмічних та оборонних компаній, таких як Boeing, Lockheed Martin та Airbus, які активно інвестують у ШІ, передові матеріали та безпілотні системи для підтримання технологічної переваги. Звіти провідних оборонних компаній та дослідницьких організацій надають цінну інформацію щодо майбутніх напрямів розвитку технологій військової авіації, підкреслюючи потенціал для подальших досягнень в автономних бойових літаках, включаючи вдосконалені можливості ШІ, покращені матеріали та інтегровані системи. Штучний інтелект та машинне навчання дозволяють автономним бойовим літакам обробляти великі обсяги даних, приймати рішення та адаптуватися до змінних умов у реальному часі, а застосування ШІ в АБЛ включає можливість самонавчання та вдосконалення стратегій на основі отриманих даних [7]. Алгоритми машинного навчання можуть аналізувати польотні дані, щоб покращувати точність і ефективність бойових місій. Оснащені високоточними сенсорами, АБЛ можуть ефективніше виявляти та реагувати на загрози, а сенсори включають радіолокаційні системи, інфрачервоні камери, системи нічного бачення та інші датчики, які дозволяють літаку виявляти об'єкти в різних умовах видимості та погоди. Вдосконалені сенсори забезпечують точність і надійність виконання місій, зменшуючи ризик помилок та

підвищуючи оперативну ефективність. Безпечні та надійні системи зв'язку забезпечують можливість АБЛ діяти у тандемі з пілотованими літаками та наземними контрольними пунктами, дозволяючи передавати дані в реальному часі, координувати дії між різними одиницями та забезпечувати безперебійний зв’язок навіть у складних умовах [4].

АБЛ можуть збирати розвідувальні дані без ризику для людських життів, моніторити ворожі позиції, оцінювати пошкодження та збирати інформацію в реальному часі, дозволяючи військовим керівникам приймати обґрунтовані рішення. АБЛ можуть виконувати точні удари, зменшуючи побічні втрати, оснащуючись різноманітними видами озброєння, включаючи ракети та бомби, і атакувати стратегічно важливі об’єкти з мінімальним ризиком для людських життів. АБЛ можуть використовуватися для доставки вантажів та медичної евакуації в умовах ворожого середовища, включаючи доставку боєприпасів, медикаментів та інших матеріалів у важкодоступні зони, а також евакуацію поранених з поля бою, що підвищує оперативні можливості, економію коштів та зменшення ризиків для пілотів. Вони можуть виконувати місії в умовах, які є занадто небезпечними для пілотованих літаків, забезпечуючи при цьому високий рівень ефективності та надійності [1].

Технічні питання включають надійність систем ШІ та кібербезпеку, а забезпечення стабільної роботи ШІ в умовах бойових дій є критично важливим, тому захист від кібератак є необхідною умовою для збереження функціональності та безпеки АБЛ. Використання автономної зброї піднімає значні етичні питання щодо відповідальності та можливих непередбачуваних наслідків, тому існує необхідність у розробці міжнародних стандартів та регулювань для забезпечення етичного використання автономних бойових систем. Забезпечення безперебійної інтеграції з існуючими військовими системами та стратегіями може бути складним завданням, оскільки важливо враховувати взаємодію між різними компонентами військової інфраструктури та забезпечити їхню сумісність з АБЛ.

Сполучені Штати розробили X-47B, який демонструє значний прогрес у технології АБЛ, включаючи можливості автономного дозаправлення у повітрі та виконання точних ударів, а Китай розробив CH-5, який розширює автономні повітряні можливості країни, зосереджуючись на довготривалому спостереженні та бойових місіях. Ці приклади надають цінні інсайти щодо практичного застосування та ефективності АБЛ, демонструючи їхню здатність виконувати складні бойові завдання з високим рівнем ефективності [3].

Майбутнє АБЛ виглядає перспективно, з поточними дослідженнями, спрямованими на підвищення можливостей ШІ, поліпшення технології невидимості та розробку більш надійних автономних систем, а інновації, такі як технологія роєвих систем, де кілька АБЛ діють у координації, очікується, що революціонізують військові стратегії.

Розгортання АБЛ вимагає наявності міцної нормативно-правової бази для вирішення таких питань: відповідність міжнародному праву, забезпечення того, щоб використання АБЛ відповідало міжнародному гуманітарному праву, дотримання принципів пропорційності та необхідності у військових діях, запобігання невибірковим атакам, а етичне використання передбачає встановлення керівних принципів для запобігання зловживанням та забезпечення відповідальності в автономних операціях, тому важливо розробити етичні стандарти для використання АБЛ, які враховують питання відповідальності та гуманності у військових діях.

Поточна динаміка російсько-українського конфлікту вказує на перехід до етапів позиційної війни та війни вичерпання, що вимагає перегляду стратегій та концепцій захисту України. Особлива увага приділяється потребі технологічної переваги на полі бою та забезпеченню достатніх виробничих можливостей для постійного поповнення запасів сучасного озброєння та військової техніки.

Досвід військових дій підкреслює необхідність зміни пріоритетів у сфері виробництва озброєнь, з акцентом на системи, які забезпечують так звану «асиметричну» технологічну перевагу. Важливими є автономні безпілотні системи, безекіпажні бойові та розвідувальні

морські платформи для діяльності в Чорному морі, далекобійні системи точного ураження, крилаті ракети, оперативно-тактичні ракетні комплекси, системи радіоелектронної боротьби та системи протиповітряної та протиракетної оборони.

Генерал Валерій Залужний, Головнокомандувач ЗСУ (2021–2024), зазначає, що для досягнення успіху війська мають мати перевагу в повітрі, здатність до глибокого прориву мінних полів, ефективні засоби для контрбатарейної боротьби, а також інструменти для радіоелектронної боротьби та розвідки. Він підкреслює, що ключ до отримання цих бойових спроможностей полягає не в звичних методах XX століття, а в новітніх технологіях, які можуть забезпечити значний прорив і вийти з пастки позиційної війни [9].

З огляду на розвиток ситуації та глобальні умови, підходи, описані генералом Залужним, залишатимуться важливими на тривалий час, вказуючи на середньострокову та довгострокову орієнтацію розвиткових програм військового озброєння та технологій на зазначені технологічні напрями.

14 листопада 2024 року Європейська оборонна агенція прийняла 22 Європейські пріоритети розвитку оборонних здібностей – 2023, що сприятиме модернізації армій країн ЄС [8]. Як вказав голова EDA і Високий представник ЄС у закордонних справах Жозеп Боррель, «ці пріоритети забезпечать ефективний формат для координації оборонного планування і ініціатив у ЄС» [5]. Пріоритети базуються на оновленому Плані розвитку можливостей ЄС (Capability Development Plan, CDP) і враховують зміни в стратегічному середовищі ЄС та уроки війни Росії проти України. Відповідно до цих пріоритетів будуть оновлені Координований щорічний огляд оборони (CARD), проекти Постійної структурованої співпраці (PESCO), робота Європейського оборонного фонду (EDF) та інші інструменти оборони ЄС.

22 пріоритети об'єднані за ключовими напрямками, включаючи сухопутні, повітряні та морські сили, космос, кіберпростір, стратегічні системи забезпечення та розширення військових можливостей. Вони спрямовані на стимулювання спільних оборонно-промислових проектів у ЄС, що раніше стикалися з браком фінансування та мотивації для досягнення спільних оборонних цілей Європи. Серед ключових викликів залишається модернізація повітряних сил Європи з використанням перспективних багатофункціональних бойових літаків 5-6 поколінь. Незважаючи на те, що розробка таких платформ тривала багато років без особливого прогресу, США вдалося здійснити експансію свого F-35 Joint Strike Fighter на європейському ринку, де до 2030 року очікується базування до 550 таких літаків. В Європі зараз реалізуються два основних проекти в цій сфері: Франція, Німеччина та Іспанія розпочали проект SCAF, а Великобританія, Італія та Японія – проект GCAP. Параметри та перспективи обох проектів залишаються неясними, що викликає занепокоєння щодо їх майбутнього успіху [6].

Уроки війни між Росією та Україною показали, що розвиток безпілотних технологій відбувається з надзвичайною швидкістю, оскільки ці системи виконують все більше функцій на полі бою. Водночас пілотована авіація продовжує грати вирішальну роль у військових операціях, хоча баланс між пілотованими та безпілотними системами може зміщуватися на користь останніх. Штучний інтелект вже активно використовується для аналізу та пріоритизації тактичної інформації в рамках безпілотних систем, і передбачається, що до 2035-2040 років актуальність традиційних бойових авіаційних платформ може змінитися на користь гібридних або повністю безпілотних проектів.

Фрагментація зусиль європейських країн у цій сфері надає перевагу новітнім модифікаціям F-35 у порівнянні з європейськими ініціативами, такими як GCAP та SCAF. Оскільки рамки і результати цих проектів залишаються невизначеними до 2035-2040 років, участь України в них видається малоймовірною. Більш реалістичним є взаємодія України з Європейською оборонною агенцією, яка може бути модернізована для підтримки потреб ЗСУ. Кроком до зміцнення співпраці стало проведення в Києві у вересні 2023 року першого Міжнародного форуму оборонних індустрій (DFNC1) з участю 252 компаній з 30 країн, який

зосереджувався на створенні практичних проектів для виробництва озброєнь. Планується, що подібні форуми Україна-ЄС сприятимуть подальшій оборонно-промисловій співпраці між українськими та європейськими компаніями. Таким чином, в контексті сучасної воєнно-політичної обстановки Україна повинна переглянути свої оборонні стратегії, звертаючи увагу на необхідність технологічної переваги та забезпечення військових потреб ЗСУ передовими озброєннями та технологіями.

Висновки

У результаті проведеного дослідження встановлено, що автономні бойові літаки є важливим напрямком розвитку сучасної військової авіації, який значно впливає на ефективність та безпеку бойових операцій. Інновації в галузі штучного інтелекту та новітніх матеріалів забезпечують можливість підвищення автономності, точності та ефективності бойових місій. Зокрема, використання термопластичних еластомерів та керамічних матричних композитів підвищує довговічність, зменшує вагу та покращує паливну ефективність літаків. Автономні системи управління, основані на ШІ, дозволяють обробляти великі обсяги даних, приймати рішення в реальному часі та адаптуватися до змінних умов, що підвищує ефективність та безпеку виконання бойових завдань.

Разом з тим, використання автономної зброї піднімає значні етичні питання щодо відповідальності та можливих непередбачуваних наслідків. Тому необхідно розробити міжнародні стандарти та регулювання для забезпечення етичного використання автономних бойових систем. Важливим аспектом є також міжнародна співпраця, яка включає обмін технологіями, спільні дослідження та розробки, а також координацію нормативно-правової бази. Майбутнє автономних бойових літаків виглядає перспективним з огляду на поточні дослідження та інновації у галузі ШІ, новітніх матеріалів та автономних систем управління, однак для успішного впровадження цих технологій необхідно враховувати етичні та нормативно-правові аспекти, а також сприяти міжнародній співпраці у сфері військової авіації.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Андрощук Г.О., Кваша Т.К. Патентний ландшафт як інструмент прогнозування світових технологічних трендів: сфера озброєння та військової техніки. Наука, технології, інновації. 2019. № 4 (12). С. 28-40. https://doi.org/10.35668/2520-6524-2019-4-04.
2. Богомазова В.М. Світові технологічні тренди у сфері “Військова авіація”: монографія / В.М. Богомазова. – К.: УкрІНТЕІ, 2023. – 244 с.
3. Коритько О.І., Підчибій Л.В. Сучасні тенденції розвитку проєктів тактичних літаків світу / О.І. Коритько, Л.В. Підчибій // Державний науково-дослідний інститут авіації, Київ. 2021. URL: https://znp.dndia.org.ua/index.php/znp/article/view/4/2.
4. Писаренко Т.В. Аналіз світових технологічних трендів у військовій сфері: монографія [Електронний ресурс] / Т. Писаренко, Т. Кваша, Т. Гаврис та ін., за заг. редакцією Т.В. Писаренко. – К.: УкрІНТЕІ, 2021. – 110 с.

5. EU Defence Ministers agree to prioritise 22 military capabilities to bolster European armed forces. URL: https://eda.europa.eu/news-and-events/news/2023/11/14/eu-defence-ministers-agree-to-prioritise-22-military-capabilities-to-bolster-european-armed-forces.
6. How the F-35 swept Europe, and the competition it could soon face. URL: https://www.defensenews.com/global/europe/2022/09/04/how-the-f-35-swept-europe-and-the-competition-it-could-soon-face/.
7. Innovation in drones: Leading companies in solar-powered electric aircraft. URL: https://www.airforce-technology.com/data-insights/innovators-drones-solarpowered-electric-aircraft-aerospace-defence/?utm_source=lgp1&utm_medium=6-229074&utm_campaign=recommended-articles-pi.
8. The 2023 EU Capability Development Priorities. URL: https://eda.europa.eu/docs/default-source/brochures/qu-03-23-421-en-n-web.pdf.
9. The commander-in-chief of Ukraine's armed forces on how to win the war. URL: https://www.economist.com/by-invitation/2023/11/01/the-commander-in-chief-of-ukraines-armed-forces-on-how-to-win-the-war.

References

1. Androschuk G. O., Kvasha T. K. (2019). Patent landscape as a tool for forecasting global technological trends: the sphere of armaments and military equipment. *Science, technology, innovation*. 2019. № 4 (12). P. 28-40. https://doi.org/10.35668/2520-6524-2019-4-04.
2. Bogomazova V.M. World technological trends in the field of "Military Aviation": monograph. – Kyiv: UkrINTEI, 2023. – 244 p.
3. Korytko O.I., Pidchibiy L.V. (2021). Modern trends in the development of tactical aircraft projects of the world. *State Research Institute of Aviation*, Kyiv. 2021. Available from : https://znp.dndia.org.ua/index.php/znp/article/view/4/2.
4. Pisarenko T. V. Analysis of global technological trends in the military sphere: monograph [Electronic resource] / T. Pisarenko, T. Kvasha, T. Havrys, etc., according to the general edited by T.V. Pisarenko – Kyiv: UkrINTEI, 2021. – 110 p.
5. EU Defence Ministers agree to prioritise 22 military capabilities to bolster European armed forces. Available from : https://eda.europa.eu/news-and-events/news/2023/11/14/eu-defence-ministers-agree-to-prioritise-22-military-capabilities-to-bolster-european-armed-forces.
6. How the F-35 swept Europe, and the competition it could soon face. Available from : https://www.defensenews.com/global/europe/2022/09/04/how-the-f-35-swept-europe-and-the-competition-it-could-soon-face/.
7. Innovation in drones: Leading companies in solar-powered electric aircraft. Available from : https://www.airforce-technology.com/data-insights/innovators-drones-solarpowered-electric-aircraft-aerospace-defence/?utm_source=lgp1&utm_medium=6-229074&utm_campaign=recommended-articles-pi.
8. The 2023 EU Capability Development Priorities. Available from : https://eda.europa.eu/docs/default-source/brochures/qu-03-23-421-en-n-web.pdf.
9. The commander-in-chief of Ukraine's armed forces on how to win the war. Available from : https://www.economist.com/by-invitation/2023/11/01/the-commander-in-chief-of-ukraines-armed-forces-on-how-to-win-the-war.

Стратегічне управління банком в сучасних умовах

Bank strategic management under modern conditions

Віолетта Харабара [A]

Corresponding author: к. екон. н., доцент, доцент кафедри фінансів та кредиту, e-mail: v.kharabara@chnu.edu.ua, ORCID: 0000-0002-8555-6440

Роман Грешко [A]

к. екон. н., доцент, доцент кафедри фінансів та кредиту, e-mail: r.greshko@chnu.edu.ua, ORCID: 0000-0003-3054-356X

Іван Ткач [B]

д. екон. н., професор, e-mail: tim68@ukr.net, ORCID: 0000-0001-5547-6303

Володимир Харабара [B]

к. в. н, доцент, професор кафедри керівництва військами (силами) в мирний час, e-mail: ivanovuth@ukr.net, ORCID: 0000-0001-7912-6578

Violetta Kharabara [A]

Corresponding author: PhD in Economics, Associate Professor, Associate Professor of the Department of Finance and Credit, e-mail: v.kharabara@chnu.edu.ua, ORCID: 0000-0002-8555-6440

Roman Greshko [B]

PhD in Economics, Associate Professor, Associate Professor of the Department of Finance and Credit, e-mail: r.greshko@chnu.edu.ua, ORCID: 0000-0003-3054-356X

Ivan Tkach [B]

Doctor of Economic Sciences, Professor, e-mail: tim68@ukr.net, ORCID: 0000-0001-5547-6303

Volodymyr Kharabara [B]

PhD in Military Science, Professor of the Department of Command and Control of Troops (Forces) in Peacetime, e-mail: ivanovuth@ukr.net, ORCID: 0000-0001-7912-6578

[A] Чернівецький національний університет імені Юрія Федьковича, м. Чернівці, Україна

[A] Yuriy Fedkovych Chernivtsi National University, Chernivtsi, Ukraine

[B] Національний університет оборони, м. Київ, Україна

[B] National University of Defense of Ukraine, Kyiv, Ukraine

Received: October 2, 2024 | Revised: October 20, 2024 | Accepted: October 31, 2024

JEL Classification: G0; G21

DOI: 10.33445/sds.2024.14.5.13

Мета роботи: полягає в узагальнені понять "стратегія", "стратегічне управління" та дослідження його ролі у формуванні та розвитку банківської системи України.

Метод дослідження: основними методами дослідження є: теоретично-емпіричний, формації та оцінювання матеріалу.

Результати дослідження полягає у донесені до широкого кола науковців специфіки вибору стратегій щодо управління у банківській сфері.

Теоретична цінність дослідження: теоретична цінність дослідження визначена у науковому обґрунтовані стратегії як фундаменту успішного стратегічного управління банком та сучасних умовах функціонування банківської системи, основною вимогою є постійний пошук нових підходів до формування та реалізації стратегій.

Практична цінність дослідження: практичне значення одержаних результатів полягає в тому, що практичні рекомендації у комплексі формують підґрунтя для підвищення ефективності функціонування суб'єктів банківської системи у контексті забезпечення стратегічного управління.

Майбутні дослідження: майбутні дослідження будуть сконцентровані на аналізі підходів щодо стратегічного управління, оцінки та тестуванні в реальних умовах, щодо застосування стратегічного управління.

Тип статті: теоретичний, описовий.

Purpose: is to generalize the concepts of "strategy", "strategic management" and research its role in the formation and development of the banking system of Ukraine.

Method: the main methods of research are: theoretical and empirical, formation and evaluation of material.

Findings: consist in conveying to a wide range of scientists the specifics of the choice of management strategies in the banking sector.

Theoretical implications: the theoretical value of the research is defined in a scientifically based strategy as the foundation of successful strategic management of the bank and modern conditions of the functioning of the banking system, the main requirement is the constant search for new approaches to the formation and implementation of strategies.

Practical implications: the practical significance of the obtained results is that the practical recommendations as a whole form the basis for increasing the efficiency of the functioning of the subjects of the banking system in the context of ensuring strategic management.

Future research: future research will focus on the analysis of approaches to strategic management, evaluation and testing in real conditions, regarding the application of strategic management.

Papertype: theoretical, descriptive.

Ключові слова: управління, банк, стратегія, валюта.

Key words: management, bank, strategy, currency.

Вступ

Банки відіграють вирішальну роль в економіці будь-якої країни. У період кризи, такої як пандемія та гібридна війна, їхня роль стає ще важливішою. Війна зробила економічну ситуацію

вкрай нестабільною. Непередбачуваність військових дій може призвести до різких змін на ринках, курсах валют та фінансовій стабільності в окремих регіонах та по всій Україні. Банки повинні бути в змозі швидко та ефективно реагувати на ці виклики, щоб зберегти свої позиції на ринку. Стратегічне управління дозволяє банкам передбачати потенційні проблеми та розробляти плани на випадок непередбачених обставин, щоб підтримувати роботу під час кризи. Одним із ключових аспектів стратегічного управління є розвиток гнучкості та адаптативності в бізнес-процесах банків. Це відображає не лише здатність швидко реагувати на зміни, але й запобігати потенційним проблемам, які можуть виникнути в умовах нестабільності. Інвестиції в сучасні технології, такі як аналітика даних і автоматизація, можуть значно підвищити ефективність банківських операцій.

Теоретичні основи дослідження

Військова економіка вимагає зосередженості на підтримці національних інтересів. Мова йде про фінансування ініціатив, спрямованих на підтримку підприємств, важливих для розвитку оборонного сектору та самозабезпечення країни. Стратегічний підхід гарантує, що ресурси банку спрямовані на підтримку цих критичних сфер, зберігаючи при цьому фінансову стабільність. Вторгнення російської федерації може вплинути на валютну стабільність країни та спричинити значний інфляційний тиск. Стратегічне управління потрібне для вирішення цих макроекономічних проблем, ефективного управління ризиками та адаптації до регуляторних змін, запроваджених для стабілізації економіки.

Аналіз останніх досліджень і публікацій. Дослідженнями у цій сфері займалися такі автори, як Васильєва Т. А.[2], Кузнєцова Л., Онопрієнко Ю. Ю.[3], Яцкевич І. В. [10].

Постановка проблеми

Метою статті є дослідження суті стратегічного управління та його вплив на розвиток банківської системи України.

Результати

Реалізація чіткої стратегії в нестабільному та мінімальному середовищі є досить складним завданням, яке вимагає від керівництва банку максимум зусиль. Керівництво банківських фінансових установ має вибрати оптимальний напрямок розвитку, обґрунтовано оцінити вплив ринкової кон'юнктури та зовнішніх факторів, сформувати оптимальні стратегії розвитку. Важливою складовою управління банком є стратегічне планування, яке базується на постановці довгострокових цілей і визначені поточні плани, спрямовані на досягнення цих цілей. У реалізації процесу різноманітних стратегій мають бути чітко визначені завдання, які використовують постійне вдосконалення та відповідають основним цілям стратегічного управління.

Ефективне управління банком передбачає не лише прагнення до максимального прибутку та зміцнення ринкових позицій. Банк, як невід'ємна частина фінансового сектору, має також забезпечувати фінансування реальної економіки. Саме тому діяльність банківських установ регулюється Національним банком України, який визначає загальні напрями розвитку банківської системи та проводить монетарну і валютну політику. Стратегічне управління банками має враховувати ці вимоги та поєднувати комерційні інтереси з соціальною відповідальністю.

Досліджуючи зміст терміну «стратегія», доцільно звернути увагу на його походження. Грецьке слово "strategia" ("stratos" – військо, "ago" – веду) пов'язане із військовим мистецтвом, що вивчає закономірності, детальне планування, підготовку та проведення

військових операцій. В економічній сфері цей термін вперше був використаний у 1962 р. А. Чендлером-молодшим. Він розглядав “стратегію”, як “визначення основних довгострокових цілей разом з відповідним планом дій та розподілом ресурсів для їх досягнення” [8]. Саме з того часу почалося використання стратегічного планування на підприємствах в умовах ринкової економіки.

Сучасний процес стратегічного управління характеризується новими фокусами об’єктів управління. Одним із прикладів є поняття “блакитний океан” – ринковий простір, вільний від конкуренції. У “блакитних океанах” не існує конкуренції, не встановлені правила поведінки на ринку, там повинна використовуватися нетрадиційна, модерністська маркетингова стратегія. Блакитні океани означають нові ділянки ринку, що вимагають творчих підходів і дають можливість зростання та високих прибутків [8]. Це посилює роль маркетингу, що стає центром стратегії будь-якого підприємства, особливо це стосується банківських установ.

Стратегічне управління банку – це діяльність, направлена на досягнення якісних та кількісних цільових орієнтирів розвитку банку, шляхом здійснення своєчасних змін в організації бізнес-процесів у відповідь на виклики зовнішнього та внутрішнього середовища з урахуванням його ресурсного потенціалу. Основною метою стратегічного управління банками є створення системи управління діяльністю банку [7]. Ця система має дозволяти сформулювати місію та цілі фінансової установи, розробляти та вдосконалювати стратегію розвитку для вдосконалення економічних та соціальних результатів, враховуючи внутрішнє і зовнішнє середовище [7].

Ефективність стратегічного управління банківськими установами залежить від якості процесу формування та реалізації стратегії. Як показано на рис.1, першим критичним кроком є проведення комплексного аналізу. Цей аналіз має охоплювати як зовнішнє середовище (ринкові тренди, регуляторні зміни, конкурентне середовище), так і внутрішнє середовище банку (фінансові показники, ресурси, технології, репутація). Наступним етапом є визначення стратегічних цілей на основі отриманих в результаті аналізу даних. Ці цілі повинні бути вимірюваними, досяжними і відповідати загальній візії банку. Важливо, щоб усі учасники процесу розуміли свої ролі в досягненні цих цілей, що сприятиме формуванню командного духу та спрямованості зусиль. Відтак, реалізація стратегії вимагає розробки чіткої операційної структури, де будуть визначені конкретні дії, терміни їх виконання та відповідальні особи. Успішне втілення стратегії також пов’язане із забезпеченням ресурсами, включаючи фінансові, людські та технологічні. Це дозволяє банку швидко реагувати на зміни у зовнішньому середовищі та адаптуватися до нових викликів.

Також рекомендуємо звернути увагу на існуючі загрози та можливості. Це пояснюється тим, що перші можуть значно погіршити становище компанії, а другі можуть бути використані для досягнення стратегічних цілей розвитку. З аналізом зовнішнього середовища, компанія може виявити критичні фактори, які впливають на її діяльність. Ідентифікація загроз, таких як зміни в законодавстві, конкурентний тиск або коливання ринкових умов, дозволяє своєчасно реагувати на потенційні виклики. Водночас, виявлення можливостей, як-от нові технологічні тренди або зміна споживчих уподобань, може слугувати основою для інновацій та оптимізації бізнес-процесів.

Забезпечивши належний моніторинг цих аспектів, компанія може адаптувати свою стратегію, зменшуючи ризики та максимізуючи вигоди. Наступним кроком є розробка плану дій, що враховує виявлені загрози й можливості. Це включає формування стратегічних ініціатив, які сприятимуть зміцненню позицій на ринку та підвищенню конкурентоспроможності. Зокрема, важливо підтримувати відкриту комунікацію з усіма зацікавленими сторонами, аби забезпечити інформаційний обмін та виділити ключові області для росту. Активне управління ризиками і використання можливостей має стати невід’ємною частиною

організаційної культури, що в свою чергу сприятиме формуванню стійкого бізнесу, готового до змін.

Рисунок 1 – Алгоритм забезпечення ефективності стратегічного управління банківською установою

Джерело: складено автором на основі [6; 7; 10; 3; 1]

Своєчасне застосування інструментів ризик-менеджменту може мінімізувати можливий негативний вплив загрози на ринкову позицію банку, тоді як можливість часто є точкою зростання, впливати на яку за допомогою фінансових, управлінських, інтелектуальних та інших ресурсів, що знаходяться в них, може забезпечити прогрес, змінити існуючий бізнес-модель, або хоча б збільшити кількість та якісні показники діяльності.

Пізніше, в процесі розробки стратегії, банки будують прогнозні документи, які відображають зміни в компанії без зміни внутрішніх параметрів. Таким чином, цей прогноз демонструє майбутню зупинку і не активує інтелектуальний та управлінський потенціал для зміни поточних умов ринку та розвитку фінансових компаній, а враховує об'єктивне зовнішнє середовище, яке створює можливості та обмеження для подальшого розвитку. У разі обрання стратегії розвитку, управлінці вплинуть на різні параметри корпоративного середовища банка з метою покращення якості та кількості показників його діяльності. Це може включати

оптимізацію процесів, підвищення ефективності управління, поліпшення інтелектуального потенціалу команди та адаптацію до поточних ринкових умов. Важливо також враховувати об'єктивні зовнішні фактори, такі як можливості та обмеження, які можуть вплинути на реалізацію стратегії та подальший розвиток банку.

На ранніх етапах формування стратегії корпоративного розвитку визначаються цілі такого процесу. Звичайно, найважливіше – це бачення власника, який розраховує на певну віддачу від вкладеного капіталу. Однак інтереси різних груп зацікавлених сторін також повинні бути прийняті до уваги, оскільки роль банку є більш важливою, ніж роль інших фінансових установ. Це може стосуватися уряду, споживачів, громадськості. Таким чином, розробка стратегії корпоративного розвитку повинна бути комплексною і враховувати інтереси усіх зацікавлених сторін. Власникам слід звернути увагу на те, як їх рішення можуть вплинути на репутацію банку, його соціальну відповідальність та довгострокову стійкість. Наприклад, зростання інтересу до екологічних питань вимагає від банку не лише дотримання стандартів, але й активного впровадження сталих практик у свою діяльність. Відкритість до діалогу з місцевими громадами може допомогти в уникненні конфліктів та створенні позитивного іміджу, що в свою чергу вплине на фінансові результати. Урядові регуляції також можуть суттєво змінити рамки, в яких відбувається корпоративний розвиток. Аналітики погоджуються, що в умовах сучасної економіки адаптація до змін у законодавстві та активна взаємодія з державними органами стають ключовими для забезпечення стабільності і розвитку бізнесу. Отже, визначення чітких цілей стратегії корпоративного розвитку має стати основою для формування всієї подальшої діяльності підприємства, яке прагне не лише до фінансового успіху, але й до відповідального ведення бізнесу в сучасному світі.

Щоб розробити ефективну корпоративну стратегію, варто скористатися методом бенчмаркінгу. Це процес детального вивчення найкращих практик компаній-лідерів у вашій галузі. Аналізуючи їх стратегії, рішення та досягнення, ви можете виявити нові можливості для власного бізнесу. Особливо актуальним бенчмаркінг є для компаній, що діють на конкурентному ринку з кількома великими гравцями. Завдяки бенчмаркінгу ви зможете зрозуміти, які саме прийоми та підходи допомогли лідерам досягти успіху, і адаптувати їх до потреб вашої компанії.

Після чіткого визначення свого місця на ринку, місії та цілей компанія має обрати одну з кількох стратегій розвитку:

- стабільність: зберегти статус-кво, не вносячи суттєвих змін до бізнес-моделі;
- внутрішнє зростання: розвиватись за рахунок збільшення обсягів виробництва, розширення асортименту продукції або послуг, проникнення на нові сегменти ринку;
- зовнішнє зростання: зростати шляхом злиття або поглинання інших компаній, стратегічних альянсів або франчайзингу;
- скорочення: зменшити масштаби бізнесу, вийти з неефективних сегментів ринку, продати некорові активи;
- інтернаціоналізація: вийти на міжнародні ринки з метою збільшення продажів і диверсифікації ризиків.

Впровадження системи ключових показників ефективності (КПЕ) є потужним інструментом для мотивації управлінців. Тісно пов'язавши рівень їхнього фінансового стимулювання з конкретними результатами роботи компанії, ми створюємо прямий інтерес до досягнення стратегічних цілей. Іншими словами, чим успішнішою буде компанія, тим більшу винагороду отримають її керівники. Такий підхід стимулює управлінців до більш активної роботи над підвищенням прибутковості, зниження витрат та впровадження інновацій.

На завершення зауважимо, що подробиці процесу будуть розкриті на кожному етапі. Сюди входить чітке вивчення зовнішнього середовища, проведення аналізу можливостей

організації, проведення стратегічного аналізу, прогнозування діяльності компанії без урахування змін, місії, цілей і пріоритетів подальшої діяльності. Як статичний аналіз, так і методи планування є важливими методами в таких процесах. Ці етапи дозволяють організації не лише адаптуватися до змін в середовищі, а й проактивно впливати на них. Важливою частиною цього процесу є розробка системи індикаторів, які дозволятимуть оцінювати ефективність реалізації стратегії. Керівництво повинно періодично аналізувати отримані результати, вносячи корективи в стратегію на основі нових даних та тенденцій.

Наступним кроком є формування планів дій, що спрямовані на досягнення визначених цілей. Ці плани повинні бути чіткими, з розподілом обов'язків та з установленням термінів виконання. Успішна реалізація стратегії багато в чому залежить від здатності команди зосередитися на пріоритетах і злагоджено працювати в напрямку спільних цілей.

Не менш важливим є моніторинг змін у зовнішньому середовищі, оскільки це дозволяє своєчасно реагувати на нові виклики та можливості. Зокрема, організація має стежити за конкурентами, ринковими тенденціями і змінами в потребах споживачів. Це створює умови для своєчасної адаптації і вдосконалення стратегічного підходу.

Крім того, важливо наголосити на культурі інновацій та навчання в організації. Підтримка атмосфери, де співробітники заохочуються генерувати нові ідеї та ділитися ними, сприяє постійному розвитку і підвищенню конкурентоспроможності. Залучення всіх рівнів персоналу до стратегічного планування зміцнює командний дух і відповідальність за результати.

Висновки

Описаний процес стратегічного управління банку має певні обмеження. Зокрема, він не враховує динамічність зовнішнього середовища і не передбачає постійної адаптації стратегії до змін. Прогнозування без урахування непередбачуваних факторів може призвести до неточності прогнозів і, як наслідок, до неефективної стратегії.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Бей Г. В., Шперчук А. О., Думанська А. О. Можливості застосування технологій в системі стратегічного управління розвитком банківської установи. *Економіка та суспільство*. 2022. № 44. С. 1–10. URL: https://economyandsociety.in.ua/index.php/journal/article/view/1827 (дата перегляду: 9 вересня 2024)
2. Васильєва Т. А., Гончаренко Т. П., Мордань Є. Ю., Теоретико-методичний базис визначення векторів розвитку стратегічного управління банків та формування їх бізнес-моделей. Вісник Сумського державного університету. Серія Економіка. 2022. № 3. С. 17-30. URL: https://essuir.sumdu.edu.ua/handle/123456789/89043 (дата перегляду: 9 вересня 2024)
3. Кузнєцова Л., Артеменко Д., Стратегічне управління взаємодією банків з клієнтами в умовах цифровізації. Modern problems in science. 2020. С. 80-84. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=pprbsu_2014_40_19 (дата перегляду: 9 вересня 2024)

4. Міщенко В. І., Стратегічне управління процесами цифрової трансформації економіки. Економіка України. 2022. №1. С.67-81.
5. Онопрієнко Ю. Ю., Обод О. М. Аналіз функціонування банківської системи та вплив факторів невизначеності на стратегічне управління фінансами банків. Механізм регулювання економіки. 2020. № 2. С. 74-85. URL: http://mer-journal.sumy.ua/index.php/journal/article/view/159 (дата перегляду: 12 вересня 2024).
6. Харченко Т. О. Стратегічне управління банківською структурою в умовах трансформації банківської системи. 2020. URL: http://baltijapublishing.lv/omp/index.php/bp/catalog/download/59/1174/2549 (дата перегляду: 12 вересня 2024).
7. Харченко Т. О. Формування технологій стратегічного управління в банківській системі. Сучасні детермінанти розвитку бізнес процесів в Україні. 2019. С. 235-238. URL: http://www.economy.nayka.com.ua/?op=1&z=6852 (дата перегляду: 12 вересня 2024).
8. Черкасова М. В. Теоретичні засади стратегії та стратегічного управління у банківській сфері. *Вісник соціально-економічних досліджень: зб. наук. праць* Одеса : Одеський національний економічний університет. 2021. № 3-4(78-79). Сс. 132-141. URL: http://vsed.oneu.edu.ua/collections/2021/78-79/pdf/132-141.pdf (дата перегляду: 14 вересня 2024).
9. Шевцова О. Й., Стратегія управління фінансовою безпекою банку. Науковий вісник. 2022. №1. С.65-69. URL: https://eprints.oa.edu.ua/id/eprint/8793/1/Tezy_fin_systema_2022.pdf (дата перегляду: 15 вересня 2024).
10. Яворська О., Ткачук Н. М., Стратегічне управління банківським бізнесом. Сучасні гроші, банківські послуги та фінансові інновації в цифровій економіці. 2021. С. 115-117. URL: https://journals.uran.ua/vsed_oneu/article/view/260728/257154 (дата перегляду: 14 вересня 2024).

References

1. Bey, G.V., Shperchuk, A.O. and Dumanska A.O. (2022). Possibilities of using technologies in the system of strategic management of the development of a banking institution. Economy and society. Vol. 44. Pp. 1–10. Available from : https://economyandsociety.in.ua/index.php/journal/article/view/1827 (accessed September 9, 2024)
2. Vasilieva, T.A., Goncharenko, T.P. and Mordan, E.Y. (2022). Theoretical and methodological basis for determining the vectors of development of strategic management of banks and the formation of their business models. Bulletin of Sumy State University. Series Economics. Vol. 3. Pp. 17-30. Available from : https://essuir.sumdu.edu.ua/handle/123456789/89043 (accessed September 9, 2024)
3. Kuznetsova, L. and Artemenko, D. (2020). Strategic management of banks' interaction with clients in the conditions of digitalization. Modern problems in science. Pp. 80-84. Available from : http://www.irbis-nbuv.gov.ua/cgibin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=pprbsu_2014_40_19 (accessed September 9, 2024)
4. Mishchenko, V. I. (2022). Strategic management of digital transformation of the economy. *Economy of Ukraine.* Vol.1. Pp.67-81.
5. Onoprienko, Y.Y. and Obod, O.M. (2020). Analysis of the functioning of the banking system and the impact of uncertainty factors on the strategic management of banks' finances. *Mechanism of regulation of the economy.* Vol. 2. Pp. 74-85. Available from : http://mer-journal.sumy.ua/index.php/journal/article/view/159 (accessed September 12, 2024)

6. Kharchenko, T. O. (2020). Strategic management of the banking structure in the conditions of transformation of the banking system. *Access mode.* Available from : http://baltijapublishing.lv/omp/index.php/bp/catalog/download/59/1174/2549 (accessed September 12, 2024)
7. Kharchenko, T. O. (2019). Formation of strategic management technologies in the banking system. *Modern determinants of business processes development in Ukraine*. Pp. 235-238. Available from : http://www.economy.nayka.com.ua/?op=1&z=6852 (accessed September 12, 2024)
8. Cherkasova, M. V. (2021). Theoretical foundations of strategy and strategic management in the banking sector. *Bulletin of Socio-Economic Research: a collection of scientific papers.* Odesa: Odesa National Economic University. Vol. 3-4(78-79). Pp. 132-141. Available from : http://vsed.oneu.edu.ua/collections/2021/78-79/pdf/132-141.pdf (accessed September 14, 2024)
9. Shevtsova, O. Y. (2022). Strategy of managing the financial security of the bank. *Scientific Bulletin.* Vol.1. Pp. 65-69. Available from : https://eprints.oa.edu.ua/id/eprint/8793/1/Tezy_fin_systema_2022.pdf (accessed September 15, 2024)
10. Yavorska, O. and Tkachuk, N.M. (2021). Strategic management of the banking business. *Modern money, banking services and financial innovations in the digital economy.* Pp. 115-117. Available from : https://journals.uran.ua/vsed_oneu/article/view/260728/257154 (accessed September 14, 2024).

Актуальність використання сучасних навчально-тренувальних засобів для навчання громадян України, які проходять військову підготовку за програмою підготовки офіцерів запасу з вогневої підготовки

Relevance of using modern educational and training tools for training citizens of Ukraine undergoing military training under the training program for reserve officers in fire training

Ігор Волков [A]

Corresponding author: к. військ.н., старший дослідник, заступник начальника Науково-дослідного центру ракетних військ і артилерії, e-mail: volkov_01.77@ukr.net, ORCID: 0000-0001-6332-7586

Руслан Черевко [B]

д. філософ., доцент кафедри, e-mail: cherepruslan2017@gmail.com, ORCID: 0000-0003-0414-0695

Сергій Князєв [B]

д. філософ., провідний науковий співробітник кафедри, e-mail: knazich@ukr.net, ORCID: 0000-0002-9746-704X

Оксана Ключак [B]

д. філософ., старший науковий співробітник кафедри, e-mail: ksyuschechka@gmail.com, ORCID: 0000-0003-3422-3379

Igor Volkov [A]

Corresponding author: Candidate of Military Sciences, Senior researcher, Deputy Head of Scientific Research Center of Missile Troops and Artillery, e-mail: volkov_01.77@ukr.net, ORCID ID 0000-0001-6332-7586

Ruslan Cherevko [B]

Doctor of Philosophy, Associate professor of the department, e-mail: cherepruslan2017@gmail.com, ORCID: 0000-0003-0414-0695

Sergey Knyazev [B]

Doctor of Philosophy, leading researcher of the department, e-mail: knazich@ukr.net, ORCID: 0000-0002-9746-704X

Oksana Kliuchak [B]

Senior researcher of the department, e-mail: ksyuschechka@gmail.com, ORCID: 0000-0003-3422-3379

[A] Науково-дослідний центр ракетних військ і артилерії, м. Суми, Україна

[B] Національний університет оборони, м. Київ, Україна

[A] Research Center of Missile Troops and Artillery, Sumy, Ukraine

[B] National University of Defense of Ukraine, Kyiv, Ukraine

Received: October 2, 2024 | Revised: October 20, 2024 | Accepted: October 31, 2024

DOI: 10.33445/sds.2024.14.5.14

Мета роботи: Дослідження переваг та недоліків використання сучасних навчально-тренувальних засобів у процесі підготовки громадян України, які проходять військову підготовку за програмою підготовки офіцерів запасу з вогневої підготовки.

Метод дослідження: аналіз, синтез, порівняння.

Результати дослідження: проведено аналіз використання сучасних навчально-тренувальних засобів з вогневої підготовки для підготовки громадян України, які проходять військову підготовку за програмою підготовки офіцерів запасу.

Теоретична цінність дослідження: дослідження допоможе покращити систему підготовки громадян України, які проходять військову підготовку за програмою підготовки офіцерів запасу з вогневої підготовки, що, в свою чергу, вплине на підвищення підготовленості сил оборони України в цілому.

Цінність дослідження: полягає у підвищенні ефективності підготовки громадян України які проходять військову підготовку за програмою підготовки офіцерів запасу з вогневої підготовки.

Майбутні дослідження: проведення детальних досліджень, які порівнюють ефективність традиційних методів навчання з новітніми технологіями, такими як віртуальна реальність або симулятори, в контексті вогневої підготовки.

Тип статті: теоретична.

Ключові слова: громадянин України, офіцер запасу, організація підготовки, навчально-тренувальні засоби, вогнева підготовка.

Purpose: Study of the advantages and disadvantages of using modern educational and training tools in the process of training citizens of Ukraine who are undergoing military training under the program of training reserve officers in fire training.

Method: analysis, synthesis, comparison.

Findings: an analysis of the use of modern educational and training tools for fire training for the training of citizens of Ukraine undergoing military training under the reserve officer training program was carried out.

Theoretical value of research: the research will help to improve the system of training of Ukrainian citizens who undergo military training under the reserve officer training program for fire training, which, in turn, will affect the improvement of the readiness of the defense forces of Ukraine as a whole.

Value of research: consists in increasing the effectiveness of the training of citizens of Ukraine undergoing military training under the reserve officer training program for fire training.

Future research: conducting detailed studies that compare the effectiveness of traditional training methods with the latest technologies, such as virtual reality or simulators, in the context of fire training.

Type of article: theoretical.

Key words: citizen of Ukraine, reserve officer, organization of training, educational and training equipment, fire training.

Вступ

В умовах відбиття збройної агресії російської федерації проти України сили безпеки та оборони України мають потребу у якісно підготовлених офіцерах запасу, зокрема з вогневої підготовки. Для успішного виконання вогневих завдань в сучасному бою необхідний високий рівень знань та навичок поводження з усіма видами стрілецької зброї та озброєння бойових машин, яке є на озброєнні механізованих підрозділів. Досягти потрібного рівня готовності до виконання вогневих завдань в бою можливо лише шляхом постійних тренувань в умовах, наближених до бойових, із використанням сучасних навчально-тренувальних засобів. У статті проведено аналіз останніх досліджень і публікацій дослідників стосовно впровадження сучасних навчально-тренувальних засобів з вогневої підготовки у процес підготовки громадян України, які проходять військову підготовку за програмою підготовки офіцерів запасу. Проаналізовано переваги та недоліки використання сучасних навчально-тренувальних засобів з вогневої підготовки, таких як комплексного тренажеру екіпажу БМП-2 та мультимедійного (електронного, лазерного) тиру у процесі підготовки громадян України, які проходять військову підготовку за програмою підготовки офіцерів запасу з вогневої підготовки. Розглянуто форми і методи проведення занять з вогневої підготовки на базі навчально-тренувальних засобах. Запропоновано шляхи підвищення ефективності проведення занять з вогневої підготовки з використанням сучасних навчально-тренувальних засобах.

Теоретичні основи дослідження

Аналіз останніх досліджень і публікацій з використання навчально-тренувальних засобів під час підготовки військовослужбовців, а також досвід застосування підрозділів у воєнних конфліктах останніх [1,2] десятиліть показує, що провідні вчені світу у галузі розробки та виробництва навчально-тренувальних засобів (далі - НТЗ) неодноразово та обґрунтовано доводили необхідність проведення невідкладних заходів стосовно впровадження новітніх навчально-тренувальних технологій у процес підготовки військовослужбовців, у тому числі і громадян України, які навчаються за програмою підготовки офіцерів запасу з подальшим її інтегруванням у єдину систему навчання. Останнім часом у провідних країнах світу погляди на роль і місце тренажерної підготовки в загальній системі навчання військових фахівців суттєво змінилося. В арміях країн-членів НАТО на початковому етапі навчання військовослужбовців відводиться 40-70% для занять на НТЗ, а екіпажів бойових машин не допускаються до експлуатації бойової техніки без попереднього навчання і підготовки на НТЗ.

Також, в країнах-членах НАТО діє жорсткий закон: постачання озброєння та військової техніки повинно здійснюватись лише безпосередньо в комплекті із відповідним тренажерним та системним обладнанням. Використання НТЗ у збройних силах цих країн є невід'ємною складовою частиною навчального процесу [3, 4].

У роботі [5] розглянуті проблемні питання існуючого стану та перспектив розвитку НТЗ для підготовки екіпажів машин механізованих і танкових підрозділів, визначено загальні напрямки розвитку перспективних зразків на найближчі роки. Базовою основою стратегії модернізації, розроблення та впровадження в систему професійної підготовки особового складу танкових і механізованих підрозділів і частин сучасних НТЗ повинні стати комп'ютерні технології, тренажерно-моделювальні комплекси та системи [5, 6-8]. В указаних роботах основна увага акцентована на тому, що підготовка військовослужбовців із використанням тренажерів стає основним з атрибутів в професійній підготовці майже всіх категорій військових спеціалістів.

У роботі [9] розглядався підхід щодо оцінювання рівня забезпечення заходів вогневої підготовки навчально-тренувальними засобами. У статті [10] проведений аналіз наявності,

ефективності використання навчально-матеріальної бази для проведення занять з вогневої підготовки з військовослужбовцями Національної гвардії України.

Постановка проблеми

Згідно з вимогами Концепції трансформації системи військової освіти одним із завданням спрямованим на розв'язання проблеми трансформації системи військової освіти є організація освітнього процесу з використанням нових, сучасних зразків озброєння і військової техніки, тренажерів, навчально-тренувальних систем, комплексів, лабораторій, центрів моделювання. Сучасну вогневу підготовку важко уявити без інновацій, які допомагають сформувати стійкі знання та практичні навички у застосуванні стрілецької зброї та озброєння бойових машин при виконанні вогневих завдань, як під час тренувань так і в бою. Але в умовах сьогодення існують окремі питання щодо застосування сучасних навчально-тренувальних засобів з вогневої підготовки під час навчання громадян України, які навчаються за програмою підготовки офіцерів запасу.

Результати

Готовність громадян України, які проходять військову підготовку за програмою підготовки офіцерів запасу виконувати вогневі завдання в сучасному бою обумовлена їх професійною підготовкою та знаннями передових військових технологій. Тільки завдяки цим факторам вони зможуть ефективно виконувати завдання та враховувати сучасні бойові умови. Водночас випускники кафедр військової підготовки під час вступу до лав Збройних Сил України часто відчувають недостатні практичні навички у впевненому володінні стрілецькою зброєю та озброєнням бойових машин. Зокрема тому, що сучасний навчальний процес на кафедрах військової підготовки перевантажений вивченням теоретичних питань, відсутності достатньої кількості боєприпасів, сучасних зразків стрілецької зброї та НТЗ.

Успішне навчання громадян України, які проходять військову підготовку за програмою підготовки офіцерів запасу умінню користуватися стрілецькою зброєю і бойовою технікою неможливе без наявності сучасних НТЗ.

Пріоритетним напрямком підготовки громадян України, які проходять військову підготовку за програмою підготовки офіцерів запасу в системі вогневої підготовки, є впровадження в навчальний процес сучасних НТЗ та вдосконалення форм і методів навчання з їх використанням.

Аналіз використання під час проведення занять з вогневої підготовки сучасних НТЗ у військових навчальних підрозділах закладів вищої освіти або у вищих військових навчальних закладах, які здійснюють підготовку громадян України, які проходять військову підготовку за програмою підготовки офіцерів запасу свідчить, що громадяни України активно виявляють інтерес до них, і це дозволяє як істотно підвищити, так і стабілізувати їх результати незалежно від рівня їх вогневої виучки. Застосування сучасних НТЗ під час проведення занять з вогневої підготовки дозволить підвищити рівень ефективності навчання та підготовки громадян України, забезпечити їм можливість навчатися в умовах, які максимально наближені до реальних бойових дій, сприяти швидшій адаптації до складних ситуацій та підвищити їхню компетентність і військову майстерність.

Водночас повна відмова від традиційних підходів до проведення занять з вогневої підготовки з переходом на новітні технології може виявитися важкою через велику кількість факторів, включаючи фінансові, освітні та технічні аспекти. Рекомендується поступове впровадження сучасних НТЗ, забезпечуючи сталий процес навчання та підтримуючи здоровий баланс між традиційними та інноваційними підходами.

Сучасні НТЗ забезпечують можливість більш наочно і доступно проводити заняттям з особовим складом, здійснювати контроль за діями тих, кого навчаються, у ході занять, вчасно виявляти помилки, що допускають, та їх причини, одночасно навчати більшу кількість тих, кого навчають, ніж на бойовій техніці, проводити тренування в польових умовах і в навчальних класах.

До НТЗ з вогневої підготовки належить наступне військово-навчальне майно: імітаційні засоби (ураження (MILES, LASERTAG в т.ч. вид інженерних засобів (вибуху, пострілу), комплекти пейнтбольного та страйкбольного обладнання, індивідуальні тренажери (мультимедійні комплекси) ОВТ, комплексні тренажери (мультимедійні комплекси) ОВТ, мультимедійні тири, електронні тири, бойові тири, макети озброєння, навчальне озброєння, навчальні боєприпаси, навчально-тренувальні та навчально-імітаційні ручні гранати, засоби для холостої стрільби, пристосування для навчання стрільби (вкладні стволи, ПУС-7, ПУС-9, командирські ящики), полігонне обладнання та мішені багаторазового використання (гонги, 3D мішені); навчальне програмне забезпечення тощо.

По своєму застосуванню НТЗ діляться на класні та польові (мобільні). Класні НТЗ застосовуються для навчання стрільбі на скороченій та умовній дальності, як правило, без витрати боєприпасів. Польові (мобільні) НТЗ дозволяють проводити навчання стрільбі по цілям, розташованим на дійсних відстанях, в умовах, наближених до реальних, як без витрати боєприпасів, так і зі стрільбою замінниками штатних боєприпасів. У свою чергу класні та польові НТЗ по обсягу завдань, що розв'язуються, можуть бути спеціалізовані (дозволяють навчати окремим, найбільш складним елементам дій при озброєнні) і комплексні (дозволяють виробляти та удосконалювати увесь комплекс навичок, необхідних для успішного рішення вогневих завдань у бою). Крім того, НТЗ можуть бути індивідуальні, призначені для підготовки одного того, кого навчають (фахівця), та колективні, призначені для підготовки і бойового залагодження екіпажу або розрахунку (відділення, взводу– комплексний тренажер екіпажу БМП-2 чи система "MILES"). Уніфіковані (комбіновані) НТЗ дозволяють проводити навчання стрільбі з декількох різних видів зброї або бойової, травматичної, пневматичної зброї, різноманітних лазерних імітаторів ("LASERTAG","SKIF", тощо).

Новітні НТЗ, крім того:

- обладнані модулем контролю теоретичних знань та допуску навчання на НТЗ;
- дозволяють без витрат боєприпасів підготувати фахівців до виконання вправ з озброєння за короткий час з великою економічною ефективністю (в дватри рази збільшують пропускну спроможність; в три – чотири рази зменшують кількість сил і засобів, що залучаються до навчання);
- дають можливість застосовувати штатну зброю, що не потребує ніяких модернізацій або змін;
- дозволяють відпрацьовувати вправи Курсу стрільб і нормативи зі збірників нормативів з бойової підготовки;
- моделюють, відтворюють та імітують звуковий супровід пострілу (вибуху), вогневе ураження, появу цілі (роботу вузлів, агрегатів та систем БМ), односторонній чи двосторонній бій, бойову обстановку або зовнішні умови (ніч, день, сутінки) в реальному масштабі часу;
- забезпечують зв'язок між тими, хто навчаються, та інструктором;
- обладнані апаратними засобами та спеціальними програмами для адекватного реагування інструктора на невірні дії тих, хто навчаються;
- автоматично фіксують та оцінюють результати стрільб (дій), зберігають та надають інформацію для здійснення аналізу проведених дій.

Заняття на НТЗ засобах проводяться як у планові годинники занять, так і під час самостійної підготовки. Перш ніж приступитися до навчання на НТЗ громадяни України, які проходять військову підготовку за програмою підготовки офіцерів запасу вивчають

матеріальну частину зброї (озброєння), правила стрільби, знайомляться із загальною будовою тренажерів та заходами безпеки при роботі на них.

Сучасний комплексний тренажер екіпажу БМП-2 (схожа модифікація модульний комплексний тренажер екіпажу БМП-2 тощо) призначений для навчання та тренування екіпажів бойової машини піхоти (далі – БМП-2) у складі командира, оператора-навідника (далі - навідника) і механіка-водія діям при озброєнні, стрільбі та водінні в різних погодних умовах, порі року та доби, без витрачання боєприпасів, моторесурсів машини і паливно-мастильних матеріалів в умовах навчального класу. Тренажер КТЕ (МКТЕ) БМП-2 включає: автоматизоване робоче місце керівника заняття (інструктора), імітатор бойового відділення на динамічній платформі, імітатор відділення управління на динамічній платформі (в МКТЕ – відповідно по 3 од. імітаторів).

КТЕ БМП-2, у залежності від потреби, може використовуватися для виконання тренувань як у складі повного екіпажу БМП-2 (командир, навідникоператор, механік-водій), так і в скороченому складі. Вправи можуть виконуватися тільки вогневі (навідником, командиром і навідником), або тільки з водіння (одним механіком-водієм). КТЕ БМП-2 максимально повно імітує відділення управління та башту БМП-2, включаючи систему управління, приціли, всі перемикачі, рукоятки, пускову установку та імітатор ПТКР. За допомогою тренажера, програмних модулів і ПЗ можливе створення комп'ютерних моделей реальних ділянок місцевості. При цьому забезпечується моделювання ландшафту, цілей, шумів і ефектів стрільби і пусків ПТКР, необхідних для гарантування навчання екіпажів Використання комплексного тренажера дозволяє вирішувати наступні завдання:

- відпрацьовування та закріплення навичок у використанні всього штатного озброєння БМП-2 (ПТКР, гармати та кулемета, системи запуску димових гранат);
- початкове навчання та вдосконалення навичок водіння БМП-2 на різній місцевості, в умовах різної видимості і метеорологічних умовах;
- гарантовану підтримку на високому рівні навичок у стрільбі екіпажів БМП-2;
- об’єктивну оцінку дій тих, хто навчаються;
- моделювання у вправах таких умов реального бою, які недосяжні іншими методами в мирних умовах бойової підготовки;
- злагодження членів екіпажу БМП-2 в умовах, максимально наближених до реальних бойових умов [11].

Мультимедійний інтерактивний лазерний тренажерний комплекс “Тренажер Т1” призначений для навчання, тренування та оцінки рівня підготовки особового складу прийомам та правилам стрільби зі стрілецької зброї та засобів ближнього бою, застосовується як для індивідуальної та групової підготовки та дозволяє відпрацьовувати навчальні вправи у відповідності до чинного Курсу стрільб [12].

Цілі та задачі які виконуються при занятті на тренажері Т1:

- ознайомлення з технічними особливостями різних видів зброї;
- підготовка особового складу для отримання первинних навичок зі стрільби;
- відпрацювання та вдосконалення навичок вже досвідчених бійців;
- відпрацьовування одиночних та групових вправ зі стрільби;
- покращення швидкості оцінки ситуації та прийняття рішення;
- покращення результативності стрільби, як по рухомим так і по стаціонарним цілям;
- відпрацьовування вправ з урахуванням: дистанції, сили та напрямку вітру;
- виживання військовослужбовця в бою [13].

Мультимедійні тири дозволяють науково-педагогічним працівникам тренувати громадян України, які проходять військову підготовку за програмою підготовки офіцерів запасу з метою вироблення практичних навичок прицільної стрільби по нерухомих і рухомих цілях, насамперед відпрацювати тактичну стрілецьку стійку та правильне тримання зброї,

швидке та точне прицілювання, плавний спуск курка, техніку швидкісної прицільної стрільби та переносу точки прицілювання, тактичної заміни магазину тощо. Мультимедійні тири у процесі підготовки громадян України, які проходять військову підготовку за програмою підготовки офіцерів запасу дозволяють сформувати навички стрільби по цілі з використанням периферичного зору, тренувати координацію рухів і “м’язову пам'ять” для швидкісної прицільної стрільби та стрільби під час руху.

Процес навчання громадян України, які проходять військову підготовку за програмою підготовки офіцерів запасу ефективному застосуванню стрілецької зброї та правильному поводженню з нею передбачає педагогічний вплив на них з метою формування стійких навичок стрільби. Формування стійких навичок стрільби має супроводжуватися фізіологічною та психологічною підготовкою до негативних чинників, це допомагає забезпечити правильну реакцію та контроль у стресових ситуаціях.

Але існуючі тренажери, поряд з багатьма перевагами, мають деякі недоліки, що властиві всім лазерним засобам та пристроями – не враховують вплив зовнішніх умов, таких як температура повітря, рух цілі на “політ кулі”, а найголовніше – вони не враховують траєкторію польоту кулі в просторі. Як показує досвід, всі початкові та підготовчі вправи під час проведення занять з вогневої підготовки необхідно виконувати спочатку на тренажерах (це скорочує час на проведення занять, заощаджує ресурси і виключає серйозні наслідки чи травмування, до яких може призвести порушення вимог заходів безпеки). Після виконання вправ на тренажерах доцільно проводити заняття та тренування на бойовій техніці, виконуючи навчальні та контрольні стрільби.

Таким чином, громадяни України, які проходять військову підготовку за програмою підготовки офіцерів запасу, перш ніж виконати стрільбу з озброєння бойової машини, зобов’язані відпрацювати свої дії на тренажері, набуваючи вміння (повне засвоєння дій) і навички (виконання дії з високим рівнем майстерності, доведеним до автоматизму) в безпечних аудиторних умовах. Використання сучасних НТЗ та технологій в процесі вогневої підготовки дозволяють отримати наступні результати: збільшення кількості навчених громадян України, які проходять військову підготовку за програмою підготовки офіцерів запасу; скорочення термінів навчання і підвищення якості підготовки; досягнення високого рівня готовності до виконання вогневих завдань в бою.

При цьому забезпечується: максимальна об’єктивність контролю рівня підготовки громадяни України, які проходять військову підготовку за програмою підготовки офіцерів запасу; комплексна підготовка екіпажів (розрахунків) з використанням сучасних комп'ютерних технологій в комплексі з застосуванням традиційних форм і методів навчання; ефективна підготовка громадяни України, які проходять військову підготовку за програмою підготовки офіцерів запасу до бойових дій в складних умовах місцевості, в містах і населених пунктах; підвищення морально-психологічної стійкості особового складу в умовах обстановки, близької до реальної.

Таким чином, за рахунок гнучкого застосування оновлених форм і методів навчання з використанням сучасних НТЗ можливо значно покращити ефективність ведення вогню зі стрілецької зброї та озброєння бойових машин.

Використання сучасних НТЗ з вогневої підготовки може мати як переваги, так і недоліки.

Перевагами використання сучасних НТЗ з вогневої підготовки є:

безпека: використання тренажерів дає змогу проводити тренування безпечним способом, що дозволяє уникнути ризику поранення чи втрати життя під час навчання;

ефективність: сучасні технології дозволяють проводити реалістичні тренування з використанням віртуальних сценаріїв, що допомагає підвищити ефективність вогневої підготовки громадян України, які навчаються за програмою підготовки офіцерів запасу;

економія коштів: використання тренажерів може бути економічно вигіднішим порівняно з реальними тренуваннями, що потребують витрат на паливо, боєприпаси тощо.

Недоліками використання сучасних НТЗ з вогневої підготовки є:

недостатність реалізму: віртуальні тренажери можуть не передати повністю реалістичні умови бойових дій, через що підготовка громадян України, які навчаються за програмою підготовки офіцерів запасу до справжніх воєнних умов не буде здійснена повною мірою.

потреба у постійному оновленні технічного забезпечення для забезпечення актуальності навчально-тренувальних програм.

відсутність фізичного навантаження: використання віртуальних тренажерів може не забезпечити достатнього фізичного навантаження, що є необхідним для підготовки до реальних бойових дій.

потреба в реальних тренуваннях: незважаючи на всі переваги тренажерів, реальні тренування в умовах бойових дій є необхідними для підготовки громадян України, які навчаються за програмою підготовки офіцерів запасу до реальних умов війни. Вони дозволяють підвищити рівень підготовки, відточити навички та побудувати командний дух, що є важливим в умовах війни.

вплив технологій на психологію: використання симуляторів та віртуальних тренажерів може мати вплив на психологію особового складу, зокрема, сприяти створенню фальшивого відчуття безпеки та знижувати рівень їхньої готовності до реальних бойових дій.

Висновки

Таким чином, розвиток і впровадження сучасних НТЗ з вогневої підготовки має стимулювати науково-педагогічних працівників до вдосконалення навичок у використанні новітнього обладнання та програмного забезпечення, що створює основу для підвищення методичного рівня проведення занять та тренувань із вогневої підготовки. За рахунок гнучкого застосування оновлених форм і методів навчання з використанням сучасних НТЗ можливо значно покращити ефективність ведення вогню зі стрілецької зброї та озброєння бойових машин.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. McMaster H.R. Learning from Contemporary Conflicts to Prepare for Future War. Orbis. 2017. Vol. 61, N 3. pp. 303– 321. https://doi.org/10.1016/j.orbis.2017.05.006.
2. Betz D., Cormack A. Iraq, Afghanistan and British Strategy. *Orbis*. 2009. Vol. 53. No. 2. pp. 319-336.
3. Руснак І.С. Проблеми модернізації та створення тренажерно-моделювальних військових комплексів. Наука і оборона. 2016. №3. С. 32-34.
4. Ткач В. Иллюзия боя. Обзор тренажерных средств общевойсковой подготовки частей и подразделений. Defense express. 2017. № 10. С. 37-45. URl : http://www.defense-express.ua.com.
5. Русіло П.О. Проблемні питання щодо стану та перспектив розвитку навчально-тренажерних засобів для механізованих і танкових підрозділів. Системи озброєння і військової техніки. № 2(22). Х: ХУПС, 2010. С. 61-64.

6. Матвієвський О. Методичний підхід до обґрунтування характеристик тренажерних засобів і систем. Наука і оборона. 2005. – № 1. С. 58-62.
7. Красник Я.В., Римар О. В., Попович Т. Д. Обґрунтування ефективності створення навчально-тренувальних засобів для підготовки особового складу збройних сил на основі максимального використання комп'ютерних технологій. Військово-технічний збірник. – № 1(4). Львів: АСВ. 2011. С.183-187.
8. Василенко О. В. Основні світові тенденції розвитку озброєння та військової техніки для ведення війн у майбутньому. Наука і оборона. 2009. №4. С. 18-23.
9. Георгадзе О. А., Петров В.А. Часткова методика оцінювання рівня організації вогневої підготовки офіцерів запасу. Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України. 2023. № 1 (77). С. 112–119.
10. Самсонов Ю.В., Мудрик В.Г. Актуальність використання сучасної навчально-матеріальної бази для навчання військовослужбовців Національної гвардії України під час занять з вогневої підготовки. Молодий вчений. 2019. № 2 (66). С. 171-174. https://doi.org/10.32839/2304-5809/2019-2-66-38.
11. Методика підготовки та проведення занять з вогневої підготовки // Навчально-методичний посібник. Житомир: Центр оперативних стандартів і методики підготовки Збройних Сил України спільно з національною академією Сухопутних військ імені гетьмана Петра Сагайдачного, 2020. 212 с.
12. Курс стрільб зі стрілецької зброї і бойових машин : затв. наказом ГШ ЗС України від 17.04.2018 № 160. 292 с.
13. Патент "Тренажер Інтерактивний лазерний для тренування стрільби зі стрілецької зброї (Тренажер Т1)", 4 с., №126776 від 10.07.2018 Винахідники: Алексєєв В.Ю., Бобарчук О.А., Соловйова Н.А., Яременко В. А., Яременко С. В.

References

1. McMaster H.R. Learning from Contemporary Conflicts to Prepare for Future War. Orbis. 2017. Vol. 61, N 3. pp. 303– 321. https://doi.org/10.1016/j.orbis.2017.05.006.
2. Betz D., Cormack A. Iraq, Afghanistan and British Strategy // Orbis. 2009. Vol. 53. No. 2. pp. 319-336.
3. Rusnak I.S. Problems of modernization and creation of training and simulation military complexes. Science and defense. 2016. No 3. P. 32-34.
4. Tkach V. Illusion of combat. Review of training equipment for combined arms training of units and subdivisions. Defense express. 2017. No. 10. P. 37-45. Available from : http://www.defense-express.ua.com.
5. Rusilo P.O. Problematic questions regarding the state and prospects for the development of training equipment for mechanized and tank units. Systems of weapons and military equipment. No. 2(22). Kh: KhAFU, 2010. P. 61-64.
6. Matvievskyi O. (2005). A methodical approach to justifying the characteristics of exercise equipment and systems. *Science and defense*. No. 1. P. 58-62.
7. Krasnyk, Ya.V., Rymar, O.V., Popovych, T.D. Justification of the effectiveness of the creation of educational and training tools for the training of personnel of the armed forces based on the maximum use of computer technologies. *Village technical collection*. No. 1(4). Lviv: ASV. 2011. P.183-187.
8. Vasylenko O.V. (2009). The main global trends in the development of weapons and military equipment for waging wars in the future. *Science and defense*. No. 4. P. 18-23.
9. Georgadze O. A., Petrov V. A. Partial method of assessing the level of organization of fire training of reserve officers. Collection of scientific works of the Center for Military and Strategic

Research of the National Defense University of Ukraine. 2023. No. 1 (77). P. 112–119.
10. Samsonov, Yu.V., Mudryk, V.H. The relevance of using a modern educational and material base for training servicemen of the National Guard of Ukraine during fire training classes. Young scientist, 2 (66), 171-174. https://doi.org/10.32839/2304-5809/2019-2-66-38.
11. Methodology of preparation and conduct of classes on fire training // Educational and methodological manual. Zhytomyr: Center for operational standards and training methods of the Armed Forces of Ukraine together with the National Academy of Land Forces named after Hetman Petro Sagaidachny, 2020. 212 p.
12. Shooting course with small arms and combat vehicles: approved. by order of the General Staff of the Armed Forces of Ukraine dated April 17, 2018 No. 160. 292 p.
13. Patent “Interactive laser simulator for small arms training (T1 simulator)”, 4 c., No. 126776 dated 07.10.2018 Inventors: V.Yu. Alekseev, O.A. Bobarchuk, N.A. Solovyova, V.A. Yaremenko, S.V. Yaremenko.

Еволюція підходів до кадрового менеджменту в Збройних Силах України в умовах воєнного стану

Evolution of approaches to personnel management Ukrainian army under the conditions of the state of martial

Олег Маслій [A]

Corresponding author: д. пед. н., професор, заступник начальника академії з навчальної роботи, e-mail: mon2369@ukr.net, ORCID: 0000-0003-2809-2763

Віктор Олехнович [A]

начальник кафедри продовольчого та речового забезпечення, e-mail: ovd-odessa@ukr.net, ORCID: 0000-0001-6114-8154

[A] Військова академія, м. Одеса, Україна

Oleg Maslii [A]

Corresponding author: Dr. of Pedagogical Sciences, Deputy Head of the Academy for Educational Work, e-mail: mon2369@ukr.net, ORCID: 0000-0003-2809-2763

Viktor Olekhnovych [A]

Head of the Departament, e-mail: ovd-odessa@ukr.net, ORCID: 0000-0001-6114-8154

[A] Military academy, Odesa, Ukraine

Received: October 2, 2024 | Revised: October 20, 2024 | Accepted: October 31, 2024

DOI: 10.33445/sds.2024.14.5.15

Мета роботи: аналіз підходів до кадрової політики, які застосовуються у державному секторі країн світу і, зокрема, у Збройних Силах України, її напрямів, форм та методологічних засад.

Метод дослідження: компаративний.

Результати дослідження: виділено основні типи кадрової політики, серед них – державного рівня, активного спрямування, закрита і конкурентноорієнтована. Визначено, що поширена у довоєнний період (до 2014 року) концепція щодо більшої ефективності залучення цивільних спеціалістів для виконання завдань у Збройних Силах не виправдовує своїх очікувань у воєнний час. Це пов'язано зі специфікою завдань, що виконуються. Проаналізовані складові кадрової політики, визначено місце і роль освітнього компонента у стратегічних концепціях кадрового менеджменту. Одним з ключових завдань кадрового менеджменту, зокрема, в галузі логістичного забезпечення, на всіх рівнях є передусім питання формування професійних військових шляхом якісної підготовки військових спеціалістів, їхнього просування по кар'єрним сходам і максимально ефективного використання людського ресурсу для вирішення поставлених перед Збройними Силами завдань.

Цінність дослідження: визначення стратегічних концепцій кадрового менеджменту в умовах воєнного стану дозволить досягти оптимального рівня ефективності у питаннях використання людського ресурсу для вирішення поставлених перед Збройними Силами завдань.

Тип статті: теоретична.

Ключові слова: кадровий менеджмент, логістичне забезпечення, кадрова політика Збройні Сили України.

Purpose: analysis of approaches to personnel policy, which are used in the public sector of the countries of the world and, in particular, in the Armed Forces of Ukraine, its directions, forms and methodological principles.

Method: comparative.

Findings: the main types of personnel policy are highlighted, among them - state-level, active direction, closed and competitively oriented. It was determined that the pre-war concept (until 2014) regarding the greater effectiveness of engaging civilian specialists to perform tasks in the Armed Forces does not live up to its expectations in wartime. This is related to the specifics of the tasks being performed. The components of personnel policy are analyzed, the place and role of the educational component in the strategic concepts of personnel management is determined. One of the key tasks of personnel management, in particular, in the field of logistics support, at all levels is primarily the issue of the formation of a professional military through high-quality training of military specialists, their promotion along the career ladder and the most effective use of human resources to solve the tasks set before the Armed Forces.

Value of research: the definition of strategic concepts of personnel management in the conditions of martial law will allow to achieve the optimal level of efficiency in the use of human resources to solve the tasks set before the Armed Forces.

Type of article: theoretical.

Key words: personnel management, logistical support, personnel policy of the Armed Forces of Ukraine.

Вступ

Сьогодні, в умовах відбиття російської збройної агресії, все частіше обговорюється питання так званого "кадрового голоду", який став проблемою Збройних Сил України. З огляду на це, видається доцільним проаналізувати принципи кадрового менеджменту, а також місце і роль військових навчальних закладів у забезпеченні кадрами Збройних Сил. Кадрова політика державного рівня являє собою складну багатоступеневу систему різного роду заходів

правового, організаційного, управлінського характеру, які направлені на забезпечення потреб у спеціалістах певного спрямування. Іншими словами, державна кадрова політика має на меті укомплектування належними спеціалістами тих державних структур, які забезпечують виконання державницьких функцій [1]. Якщо екстраполювати дану тезу на принципи забезпечення особовим складом Збройних Сил України, це означає, що кадрова політика ЗСУ направлена на пошук і підготовку спеціалістів, які якнайкраще підходять для виконання поставлених перед Збройними Силами завдань [2].

Теоретичні основи дослідження

Засадничими елементами кадрової політики ЗСУ є вимоги, принципи та ідеї, які визначаються основоположними для окреслення напрямів, форм та методологічних засад функціонування забезпечення Збройних Сил кваліфікованими спеціалістами [3]. Завдання забезпечення національної безпеки України потребує виваженого підходу до формування стратегії комплектування Збройних Сил підготовленими людськими ресурсами, здатними повною мірою виконувати завдання мирного та військового часу.

Різноманітні аспекти кадрового забезпечення аналізувала плеяда українських дослідників. Зокрема, напрямки розвитку кадрової політики, в тому числі – у Збройних Силах України, висвітлювалися в роботах О. Клименка. О. Бранчук-Петросова зосереджувала увагу на першочергових завдання удосконалення елементів кадрової політики у Збройних Силах. Проблеми взаємозв'язку управління кадровим потенціалом та стратегії організації, побудованій на конкурентній моделі, організації, висвітлювалися в роботах І. Павленко та В Гонтюк, тощо. Разом з тим, ряд питань кадрового забезпечення, зокрема, у Збройних Силах, потребують теоретичного осмислення.

Постановка проблеми

Серед основних завдань, яке стоїть перед системою управління людськими ресурсами, є підготовка і пошук відповідних кадрів, а також цілеспрямоване формування людей з належним рівнем теоретичної та практичної підготовки, морально-психологічний склад яких відповідає потребам оборони Української держави [4].

У західній парадигмі прийнято виділяти наступні типи кадрової політики [5]:

- кадрова політика державного рівня, яка формується на підставі загальнодержавних стратегічних цілей формування, еволюції та грамотного використання людського потенціалу, яким володіє держава. Визначення необхідної кількості фахівців з тої чи іншої спеціальності з певним рівнем компетенції відбувається у точній відповідності до державних потреб;
- кадрова політика активного спрямування. Керівництво повинно мати об'єктивні прогнози щодо кадрових потреб та певних засобів впливу на наявні кадри. В рамках даного підходу виявляється доцільним проведення моніторингу еволюції наукових напрямків, промислового комплексу, аграрної сфери, нововведень в галузі освіти тощо, тобто всього, що так чи інакше може призвести до зміни кадрових запитів в рамках одного організму, а також на державному рівні [6];
- кадрова політика закритого типу, яка передбачає можливість отримання підвищення тільки нижчим персоналом. Такий підхід до кадрової політики відзначається орієнтацією на імплементацію нових людських ресурсів, з наданням їм всебічних можливостей кар'єрного зростання. Весь спектр заміщень та посадових призначень, відповідно до даного типу кадрової політики, можливий виключно всередині організації [7]. Такий підхід відповідає специфіці кадрової політики, яка притаманна Збройним Силам;
- кадрова політика конкурентного типу формується на підставі конкуренції організмів (наприклад, підприємств) на ринку праці. Згідно з даним підходом, до військової служби

будуть залучені найбільш підготовлені фахівці, які отримали належний рівень кваліфікації у навчальних закладах військового або цивільного спрямування [8]. Це можуть бути випускники ВНЗ або працівники, які мають певний досвід роботи в інших сферах господарства.

Метою даної роботи є аналіз підходів до кадрової політики, які застосовуються у державному секторі країн світу і, зокрема, у Збройних Силах України. Розуміння теоретичних засад кадрового менеджменту дозволить оптимізувати процеси забезпечення Збройних Сил висококласними професіоналами різних спеціалізацій шляхом забезпечення якісної підготовки військових спеціалістів і максимально ефективного використання у ЗС України людського ресурсу.

Результати

Одним з найбільш важливих понять, які визначають підходи до формування кадрової політики в Збройних Силах, є «конкуренція». Сутність цього поняття включає в себе такі аспекти, як вартість підготовки фахівця в системі вищої військової освіти у порівнянні з залученням цивільного спеціаліста, який має досвід роботи за спеціальністю.

До повномасштабного вторгнення російської федерації більшість дослідників у галузі кадрової політики схилялися до того, що залучення цивільних спеціалістів для виконання завдань у Збройних Силах є більш раціональним рішенням, ніж підготовка кваліфікованого фахівця у системі вищої військової освіти розгорнутого типу [9]. Разом з тим, бойовий досвід протидії російській агресії наочно демонструє необхідність отримання повного курсу військової освіти особам, які залучені до служби в Збройних Силах у зв'язку зі специфікою умов служби та бойових завдань, які покладаються на спеціалістів [10].

У західній парадигмі прийнято виокремлювати наступні складові кадрової політики:

- організаційні заходи, направлені на підготовку та перепідготовку фахівців, на підвищення їхнього рівня кваліфікації;
- організаційні заходи, направлені на створення кадрового резерву;
- належна підготовка та призначення на відповідні посади кадрового складу;
- організаційні заходи, направлені на проходження стажування спеціалістів;
- організаційні заходи з контролю за темпами на напрямком укомплектування структурних елементів системи військової освіти, підбору кадрів та проходження навчання;
- грамотна організація розподілу випускників;
- грамотна побудова системи кадрового менеджменту в підпорядкованих структурах;
- аналіз та поширення позитивних елементів досвіду в системі кадрового менеджменту [11].

З огляду на те, наскільки велика увага приділяється питанням, так чи інакше пов'язаним з освітнім компонентом, доцільним буде говорити про те, що, відповідно до західної концепції підходів до кадрової політики, освітянська діяльність та освітня галузь є чи не ключовим елементом кадрової політики загалом [12]. Таким чином, належна підготовка особового складу, і в подальшому їхня належна професійна діяльність базується передусім на якісному впровадженні освітніх стандартів. Відповідно до того, завдання якого рівня стоять перед органом, що займається питаннями кадрової політики, вони вирішуються різними кадровими структурами.

Кадровою політикою стратегічного рівня займається Міністерство Оборони. Ним як органом, який здійснює державне управління, визначаються політичні аспекти кадрового забезпечення, а також заходи, направлені на контроль щодо застосування Збройних Сил. На цьому рівні визначається структура, чисельний склад, методи та критерії управління наявними кадровими ресурсами. Крім того, Міністерством Оборони визначаються напрям та характер

зовнішніх зв'язків, а також специфіка співпраці з громадськістю та іншими органами державного управління [13]. На Міністерство оборони в галузі кадрової політики покладаються наступні функції:

- окреслення загальної структури Збройних Сил, кількості військових формувань, в тому числі – резервного типу у короткій, середній та далекій перспективі;
- обґрунтування наукових підходів до вибраних засад кадрової політики, способів подолання найбільш типових проблем, принципів та засад проходження служби у Збройних Силах, розробка загальних підстав проходження служби, звільнення в запас тощо;
- розробка пропозицій щодо нагальних заходів, направлених на всебічне забезпечення окреслених теоретичних аспектів кадрової політики і надання їх до відповідних органів державної влади;
- процедура забезпечення кваліфікаційної відповідності посад, які обіймають особи з офіцерським званням, і держслужбовців, які зайняті в управлінському апараті на цивільних посадах. Також в рамках даного аспекту кадрової політики здійснюється аргументація та визначення розмірів посадових окладів, розробляються загальні принципи пенсійного забезпечення;
- робота у сфері розробки та вибору оптимальних рішень щодо набуття необхідних освітніх кваліфікацій та комплектування військ як елементу кадрової політики, розробка системи заохочень та матеріального забезпечення, ведення атестаційних справ, контроль за загальними питаннями, які так чи інакше пов'язані з проблемами кар'єрного зростання та планування кар'єри;
- проведення різного роду практичних заходів стратегічного рівня. До таких належать: присвоєння чергових звань, які належать до вищого рівня, нагородження, функціонування апеляційної системи адміністративного типу, перманентна співпраця з фінансовими органами державного підпорядкування, підтримка співпраці з громадськістю [14].

Кадрова політика функціонального рівня реалізовується на рівні Генерального штабу, а також в органах управління персоналом за видами Збройних Сил. Так, Генеральним штабом здійснюється керівництво оперативно-стратегічного рівня, яке включає в себе заходи підготовчого характеру в органах, які здійснюють управління військами, а також бойову підготовку Збройних Сил, комплектування кадровими офіцерами та персоналом у сфері призначення, перепризначення та звільнення, присвоєння військових звань, нагородження тощо [15]. У зону відповідальності Генерального Штабу входить також контроль за неухильним виконанням принципів, норм і завдань, які були визначені на стратегічному (державному) рівні.

У сфері кадрової політики генеральний штаб здійснює наступні функції:

- планування майбутнього розподілу осіб з офіцерським званням, а також здійснення контролю за тим, як відбувається реалізація прийнятих у галузі кадрового менеджменту рішень;
- визначення способів та шляхів практичної реалізації нормативно-правових актів, які так чи інакше стосуються кадрових рішень, умов контрактів, надання рекомендацій щодо опрацювання особових справ;
- детальна розробка заходів з практичної реалізації рішень у галузі кадрової політики;
- робота над питаннями управлінського характеру, розробка алгоритмів роботи з кожною конкретною справою;
- заходи, які забезпечують дотримання вимог публічності та гласності;
- заходи, направлені на планування та здійснення навчання безпосередньо у центрах підготовки, на спеціалізованих курсах, тощо;
- розробка інноваційних алгоритмів у галузі управління кар'єрою, включно з розробкою схеми просування кар'єрними сходами;

- різнопланові аспекти управлінської діяльності [16].

Кадровий менеджмент службового рівня передбачає роботу з особовим складом в напрямку максимальної відповідності штатного складу та фактичної облікової наявності. Крім того, на рівні з'єднань здійснюється:

- реалізація нормативно-правових документів, роз'яснення отриманих з вищих органів управління настанов та інструкцій;
- тренінги щодо практичного використання розроблених процедур;
- консультація офіцерів щодо подальшого кар'єрного просування, управління діяльністю центрів, які здійснюють набір персоналу;
- заходи, направлені на те, щоби зробити військову службу максимально безпечною (наскільки це можливо в умовах ведення бойових дій);
- процедури, які передбачають комплексне управління системою військової освіти початкового рівня, який включає в себе школи, спеціалізовані курси, навчальні центри;
- планова робота у сфері кадрового менеджменту, яка включає в себе призначення та перепризначення на посади, співбесіди, формування єдиного реєстру з даними тощо [17].

Кадрова робота на тактичному рівні (у військових частинах) полягає у наступних заходах:

- окреслення актуальних вимог до кандидата відповідно до посади;
- надання зацікавленим особам потрібної інформації щодо кадрових пропозицій та можливостей кар'єрного зростання;
- реалізація розроблених вищими органами постанов та процедур з метою актуального розподілу прав та обов'язків між зацікавленими особами;
- визначення необхідного устаткування матеріально-технічного характеру, які потрібні для реалізації підготовки кадрів належної якості;
- практичні заходи, направлені на відбір кандидатів з числа молодих військовослужбовців та їх кар'єрного зростання [18].

Висновки

Таким чином, одним з ключових завдань кадрового менеджменту, зокрема, в галузі логістичного забезпечення, на всіх рівнях є передусім питання формування професійних військових шляхом якісної підготовки військових спеціалістів, їхнього просування по кар'єрним сходам і максимально ефективного використання людського ресурсу для вирішення поставлених перед Збройними Силами завдань.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Клименко, О. В. (2015) Кадрова політика в Україні: напрям розвитку та шляхи реалізації. *Економіка та держава.* № 12. С. 84-88. URL : http://www.economy.in.ua/pdf/12_2015/23.pdf
2. Клименко О. В. Актуальні питання кадрової політики в Україні. *Економіка та держава*. (2017). № 1. С. 76–81. URL : http://www.economy.in.ua/pdf/1_2017/19.pdf

3. Клименко, Володимир (2006). Проблеми військово-соціального управління: кадрова політика у Збройних Силах України. №6. С. 82-88. URL : https://ipiend.gov.ua/wp-content/uploads/2018/07/klymenko_problemy.pdf
4. Банчук-Петросова О. В. (2014). Про першочергові завдання з удосконалення кадрової політики збройних сил України. *Економіка та держава.* № 8. С. 114–116. URL : http://www.investplan.com.ua/pdf/18_2014/44.pdf
5. Концепція кадрової політики у Збройних Силах України на період до 2017 року: затвержена наказом Міністерства оборони України від 04.12.2013 № 843.
6. Gontiuk V. (2013). The conceptual aspects of human resource evaluation. *Management theory and studies for rural business and infrastructure development.* Vol. 35, №. 4. P. 522–528.
7. Gontiuk V. (2014). Structural and logical model of human resource development in the company. *Journal L'Association 1901 «SEPIKE».* Ed. 6. P. 78–81.
8. Павленко І. І., Гонтюк В. А. (2015). Взаємозв'язок стратегічного плану управління кадровим потенціалом та конкурентної стратегії організації. *Глобальні та національні проблеми економіки.* Вип. 3. С. 376–379. URL : http://www.global-national.in.ua/issue-3-2015
9. Obeidat B. (2012). The Relationship between Human Resource Information System (HRIS) Functions and Human Resource Management (HRM) Functionalities. *The IUP Journal of Management Research.* Vol. 4, No. 4. P. 192–210. https://doi.org/10.5296/jmr.v4i4.2262.
10. Sienkiewicz L. (2014). Competency-based human resources management. The lifelong learning perspective. Warsaw. 264 p. https://doi.org/10.1111/ijn.12936
11. Klett F., Wang M. (2013). Editorial: The War for Talent Technologies and solutions toward competency and skills development and talent ident ification. *Knowledge Management & E-Learning.* № 5 (1). P. 1–9. https://doi.org/10.34105/j.kmel.2013.05.001
12. Gontiuk Viktoriia. (2014). Structural and logical model of human resource development in the company. L'Association 1901 «SEPIKE». Ed. 6. P. 78–81.
13. Galperin L. Bella, Lituchy R. Terri. (2014). Human Resource Development in Service Firms Across Cultures. *Human Resource Development Review.* Vol. 13. P. 336–368. https://doi.org/10.1177/1534484313511971
14. Bhatawdekar S. (2015). Competency Management (Competency Matrix and Competencies). *CreateSpace Independent Publishing Platform.* 128 p. 164.
15. Сидорова А. В., Глущенко А. М. Статистичне забезпечення управління змінами на підприємствах великого бізнесу: монографія. Вінниця : ДонНУ імені Василя Стуса, 2017. 169 с.
16. Сидорова А. В., Гонтюк В. А. (2019). Оцінювання кадрового потенціалу підприємств на основі компетентнісного підходу. *Економіка і організація управління*. № 2 (34). С. 37–45. https://doi.org/10.29038/2786-4618-2023-01-80-89
17. Розвиток професійної компетентності управлінського персоналу : монографія / Дороніна М. С., Литовченко І. В., Михайленко Д. Г., Полубєдова А. О. Х.: ВД «ІНЖЕК». (2014). 368 с. URL : http://repository.hneu.edu.ua/handle/123456789/7258.
18. Nils Malzahn, Sabrina Ziebarth, H. Ulrich Hoppe. (2013). Semi-automatic creation and exploitation of competence ontologies for trend aware profiling, matching and planning. *Knowledge Management & E-Learning.* № 5 (1). P.84-103. Vol 5, No 1. https://doi.org/10.34105/j.kmel.2013.05.007.

References

1. Klymenko, O. V. (2015). Personnel policy in Ukraine: direction of development and ways of implementation. *Economy and the state*. №12. P. 84-88. Available from : http://www.economy.in.ua/pdf/12_2015/23.pdf

2. Klymenko, O. V. (2017). Current issues of personnel policy in Ukraine. *Economy and the state*. № 1. С. 76–81. Available from : http://www.economy.in.ua/pdf/1_2017/19.pdf
3. Klymenko, Volodymyr (2006). Problems of military social management: personnel policy in the Armed Forces of Ukraine. №6. P. 82-88. Available from : https://ipiend.gov.ua/wp-content/uploads/2018/07/klymenko_problemy.pdf
4. Banchuk-Petrosova O. V. (2014). About the priority tasks for improving the personnel policy of the armed forces of Ukraine. *Economy and the state.* № 8. С. 114–116. Available from : http://www.investplan.com.ua/pdf/18_2014/44.pdf
5. The concept of personnel policy in the Armed Forces of Ukraine for the period until 2017: approved by the order of the Ministry of Defense of Ukraine from 04.12.2013 № 843.
6. Gontiuk V. (2013). The conceptual aspects of human resource evaluation. *Management theory and studies for rural business and infrastructure development.* Vol. 35, №. 4. P. 522–528.
7. Gontiuk V. (2014). Structural and logical model of human resource development in the company. *Journal L'Association 1901 «SEPIKE».* Ed. 6. P. 78–81.
8. Pavlenko, I. I., Hontyuk, V. A. (2015). The relationship between the strategic plan of personnel management and the organization's competitive strategy. Global and national economic problems. Vol. 3. С. 376–379. Available from : http://www.global-national.in.ua/issue-3-2015
9. Obeidat B. (2012). The Relationship between Human Resource Information System (HRIS) Functions and Human Resource Management (HRM) Functionalities. *The IUP Journal of Management Research.* Vol. 4, No. 4. P. 192–210. https://doi.org/10.5296/jmr.v4i4.2262.
10. Sienkiewicz L. (2014). Competency-based human resources management. The lifelong learning perspective. Warsaw. 264 p. https://doi.org/10.1111/ijn.12936
11. Klett F., Wang M. (2013). Editorial: The War for Talent Technologies and solutions toward competency and skills development and talent identification. *Knowledge Management & E-Learning.* № 5 (1). P. 1–9. https://doi.org/10.34105/j.kmel.2013.05.001
12. Gontiuk Viktoriia. (2014). Structural and logical model of human resource development in the company. L'Association 1901 «SEPIKE». Ed. 6. P. 78–81.
13. Galperin L. Bella, Lituchy R. Terri. (2014). Human Resource Development in Service Firms Across Cultures. *Human Resource Development Review.* Vol. 13. P. 336–368. https://doi.org/10.1177/1534484313511971
14. Bhatawdekar S. (2015). Competency Management (Competency Matrix and Competencies). *CreateSpace Independent Publishing Platform.* 128 p. 164.
15. Sydorova A. V., Glushchenko A. M. Statistical support of change management at large business enterprises: monograph. Vinnytsia: DonNU named after Vasyl Stus, 2017. 169 p.
16. Сидорова А. В., Гонтюк В. А. (2019). Оцінювання кадрового потенціалу підприємств на основі компетентнісного підходу. *Економіка і організація управління*. № 2 (34). С. 37–45. https://doi.org/10.29038/2786-4618-2023-01-80-89
17. Development of professional competence of management personnel: monograph / Doronina M. S., Lytovchenko I. V., Mykhaylenko D. G., Polubedova A. O. Kharkiv. (2014). 368 p. http://repository.hneu.edu.ua/handle/123456789/7258.
18. Nils Malzahn, Sabrina Ziebarth, H. Ulrich Hoppe. (2013). Semi-automatic creation and exploitation of competence ontologies for trend aware profiling, matching and planning. *Knowledge Management & E-Learning.* № 5 (1). P.84-103. Vol 5, No 1. https://doi.org/10.34105/j.kmel.2013.05.007.

Обґрунтування показників та критеріїв для удосконалення методики оцінювання ефективності управління забезпеченням економічної безпеки агрофірм

Justification of indicators and criteria for improving the method of assessing the efficiency of management of ensuring the economic security of agricultural firms

Вікторія Генчевська [A]
e-mail: vikavorobyova2@ukr.net, ORCID: 0000-0002-6305-8782
[A] ВНЗ «Університет економіки та права «КРОК», м. Київ, Україна

Viktoriia Henchevska [A]
e-mail: vikavorobyova2@ukr.net, ORCID: 0000-0002-6305-8782
[A] KROK University, Kyiv, Ukraine

Received: October 5, 2024 | Revised: October 20, 2024 | Accepted: October 31, 2024

DOI: 10.33445/sds.2024.14.5.16

Мета роботи: вибір та обґрунтування показників і критеріїв щодо управління забезпеченням економічної безпеки агрофірм у складних умовах російсько-української війни та на їх основі удосконалення методики адекватного оцінювання ефективності управління забезпеченням економічної безпеки агрофірм в умовах російсько-української війни (кризових ситуаціях).

Метод: методи аналізу та синтезу, метод системного підходу, методи експертного оцінювання та групування, графічний та абстрактно-логічний методи.

Практична цінність дослідження: проаналізовано існуючі показники економічної безпеки аграрних підприємств (агрофірм) та підходи до оцінювання рівня ефективності цього процесу; обґрунтовано показники та критерії щодо управління забезпеченням економічної безпеки агрофірм в складних умовах російсько-української війни та на їх основі удосконалено методику адекватного оцінювання ефективності управління забезпеченням економічної безпеки агрофірм в умовах російсько-української війни (кризових ситуаціях).

Цінність дослідження: удосконалена методика оцінювання ефективності управління забезпеченням економічної безпеки агрофірм за визначеними показниками та критеріями, які враховують всі складові економічної безпеки агрофірми та визначено зони економічної безпеки агрофірми, що дозволяє розробити комплекс заходів щодо забезпечення належного рівня економічної безпеки, підвищити ступінь економічної обґрунтованості прийняття рішення стосовно пріоритетності реакції агрофірми щодо самозбереження, стабілізації, формування конкурентної, інноваційної позицій або позиції забезпечення довгострокового потенціалу в межах забезпечення економічної безпеки агрофірми.

Тип статті: теоретичний; практичний.

Ключові слова: управління; забезпечення економічної безпеки; рівень економічної безпеки; зона економічної безпеки; агрофірма; підприємство; аграрне підприємство; показники; критерії; індикатори; методика; етап; алгоритм; оцінювання; ефективність; російсько-українська війна.

Purpose: the selection and justification of indicators and criteria for managing the economic security of an agricultural company in the conditions of the Russian-Ukrainian war and, based on them, improving the methodology for adequately assessing the effectiveness of managing the economic security of an agricultural company in the conditions of the Russian-Ukrainian war (crisis situations).

Method: methods of analysis and synthesis, method of system approach, methods of expert evaluation and grouping, graphical and abstract logical methods.

Practical implications: the existing indicators of the economic security of agricultural enterprises (agrofirms) and approaches to evaluating the level of efficiency of this process are analyzed. The indicators and criteria for managing the economic security of agricultural firms in the difficult conditions of the Russian-Ukrainian war are substantiated, and based on them, the methodology for adequately evaluating the effectiveness of managing the economic security of agricultural firms in the conditions of the Russian-Ukrainian war (crisis situations) is improved.

Value: an improved methodology for evaluating the effectiveness of managing the economic security of agrofirms according to the specified indicators and criteria that take into account all components of the economic security of an agrofirm; the zones of economic security of an agricultural firm are determined, which allows to develop a set of measures to ensure the proper level of economic security, to increase the degree of economic validity of decision-making regarding the priority of the reaction of an agricultural firm regarding self-preservation, stabilization, the formation of a competitive, innovative position or the position of ensuring long-term potential within the limits of ensuring the economic security of an agricultural firm.

Paper type: theoretical; practical.

Key words: management; ensuring economic security; level of economic security; zone of economic security; agricultural firm; enterprise; agricultural enterprise; indicators; criteria; indicators; method; stage; algorithm; assessment; efficiency; Russian-Ukrainian war.

Вступ

Для проведення подальшого дослідження щодо обґрунтування теоретичних положень та розробки практичних рекомендацій щодо удосконалення процесу управління забезпеченням економічної безпеки агрофірм проведемо вибір та обґрунтування показників і критеріїв щодо оцінювання ефективності управління забезпеченням економічної безпеки агрофірм.

Тому досить доречно виконати це завдання, у подальшому для удосконалення методики адекватного оцінювання ефективності управління забезпеченням економічної безпеки агрофірм, що і є актуальним завданням даної статті.

Теоретичні основи дослідження

Вітчизняні й зарубіжні економісти зробили безліч спроб кількісної оцінки рівня економічної безпеки підприємств. Виходячи з цих результатів, у сучасній економічній літературі можна виділити декілька підходів до оцінки рівня економічної безпеки. Досить відомий індикаторний підхід у роботах науковців Шило Ж. С., Кречко М. Ю. [1], Алькема В. Г., Літвін Н. М., Кириченко О. С. [2], Варічевої Р. В. [3], при якому рівень економічної безпеки визначається за допомогою так званих індикаторів. Автором Коптєвою Г. М. [4] запропонований інтегральний підхід до оцінки економічної безпеки підприємств. Згідно з ресурсно-функціональним підходом, який пропонується у працях авторів Сосновської О. О., Житар М. О. [5], Васильців Т. Г., Микитюк Р. М. [6], Дідик А. М. [7], оцінка рівня економічної безпеки підприємства здійснюється на основі оцінки стану використання корпоративних ресурсів за спеціальними критеріями. Ці всі спроби оцінки рівня економічної безпеки носять розрізнений та не системний характер, що частіше дає змогу використовувати вищезазначені підходи спеціалістам досить високого рівня. У разі некваліфікованого визначення рівня економічної безпеки підприємств та пов`язаних з цим некоректних управлінських рішень цілком можливе виникнення украй негативних наслідків для підприємства.

Проведений сучасними науковцями аналіз існуючих на сьогодні найбільш розповсюджених методик оцінки економічної безпеки аграрного підприємства встановив, що кожна з них має певні недоліки та обмеження, а тому існує необхідність у вдосконаленні існуючих підходів до вирішення поставленої проблеми. Додатково підсилює необхідність у цьому також виявлена потреба в обов’язковому врахуванні галузевих аспектів та особливостей діяльності аграрного підприємства, зокрема агрофірми.

Виходячи з визначення поняття управління економічною безпекою підприємства (агрофірми), що приведене в роботі автора Ружицького А. В. [8], яке полягає у протидії загрозам як сигналам, що негативно впливають на результати його роботи. Причому виникнення загроз обумовлене різноманітністю факторів, які по-різному впливають на стан економічної безпеки підприємства (агрофірми). Слід зазначити, що загрозами для підприємства (агрофірми) є сукупність умов, процесів, факторів, які здійснюють негативний вплив на реалізацію їх економічних інтересів. Їх можна кваліфікувати за різними ознаками. Серед них можна виділити, такі як – катастрофічні, що пов’язані з кризовими ситуаціями, що виникають в умовах російсько-української війни, інформаційні, конкурентні, пов’язані з некомпетентністю власника в правових, виробничо-фінансових і організаційних питаннях та інші.

Тому назріла об`єктивна необхідність у розробці системи показників, що мають характеризувати стан функціональних складових економічної безпеки агрофірм, у тому числі й з урахуванням негативних впливів російсько-української війни та інших кризових ситуацій. Окрім того, виникає потреба у вирішенні завдання щодо удосконалення існуючих методик оцінювання ефективності управління забезпеченням економічної безпеки агрофірм.

Постановка проблеми

Метою статті є вибір та обґрунтування показників і критеріїв щодо управління забезпеченням економічної безпеки агрофірм в складних умовах російсько-української війни та на їх основі удосконалення методики адекватного оцінювання ефективності управління забезпеченням економічної безпеки агрофірм в умовах російсько-української війни (кризових ситуаціях).

Для досягнення мети досить доречно проаналізувати існуючі показники економічної безпеки підприємств та підходи до оцінювання рівня ефективності цього процесу, шляхом адаптації та застосування існуючих показників, критеріїв, моделей та методів оцінювання ефективності цього процесу за допомогою розширення їх можливостей у сучасних складних умовах.

Результати

Методика оцінки рівня економічної безпеки аграрного підприємства (агрофірми) на сучасному етапі повинна поєднувати в собі не тільки теоретичну, але й практичну цінність. Тобто вона повинна бути такою, щоб її використання, проведення розрахунків та формулювання висновків могли бути реалізовані управлінцями в межах аграрного підприємства (агрофірми), а не потребували залучення додаткових консультантів та виконавців, а також додаткових капіталовкладень на програмне забезпечення, тощо [9].

У зв’язку з цим, методика оцінки економічної безпеки аграрного підприємства (агрофірми) має бути побудована на основі використання таких раніше виявлених методик, як:

- оцінювання економічної безпеки підприємства на основі показників прибутку;
- формування інтегрального показника економічної безпеки за ресурсно-функціональним підходом [10-11].

Саме зазначені методики дозволять врахувати як принципову важливість для будь-якого підприємства отримання прибутку, так і той факт, що економічна безпека підприємства поняття комплексне, а тому оцінювання потребують усі головні аспекти, що спричиняють свій вплив на неї.

Виходячи із вже існуючих методів та методик оцінювання рівня управління забезпеченням економічної безпеки агрофірм пропонуємо наступний порядок (алгоритм) реалізації удосконаленої методики оцінювання ефективності управління забезпеченням економічної безпеки агрофірм за визначеними показниками та критеріями (рис. 1):

1) визначення знаходження агрофірми в стані економічної безпеки за рівнем чистого прибутку, тобто за принципом достатності його для реалізації простого та розширеного відтворення з врахування фактору інфляції;

2) визначення інтегрального показника економічної безпеки на основі оцінювання складових, що мають місце в діяльності агрофірм за галузевим принципом;

3) узгодження першого та другого етапів оцінювання, визначення зон економічної безпеки агрофірм;

4) врахування несприятливих факторів пов’язаних з російсько-українською війною (кризовими ситуаціями), що виражається у виборі і обґрунтуванні відповідних показників.

Встановлено, що агрофірма перебуває в стані економічної безпеки лише у тому випадку, коли вона отримує прибуток, а розмірів чистого прибутку достатньо для покриття витрат на просте відтворення з врахуванням фактору інфляції. Стан агрофірми тим безпечніший, чим більше чистий прибуток перевищує розміри скорегованих на рівень інфляції амортизаційних відрахувань. На основі цього твердження можна сформулювати порядок отримання висновків про “перший рівень економічної безпеки агрофірми”.

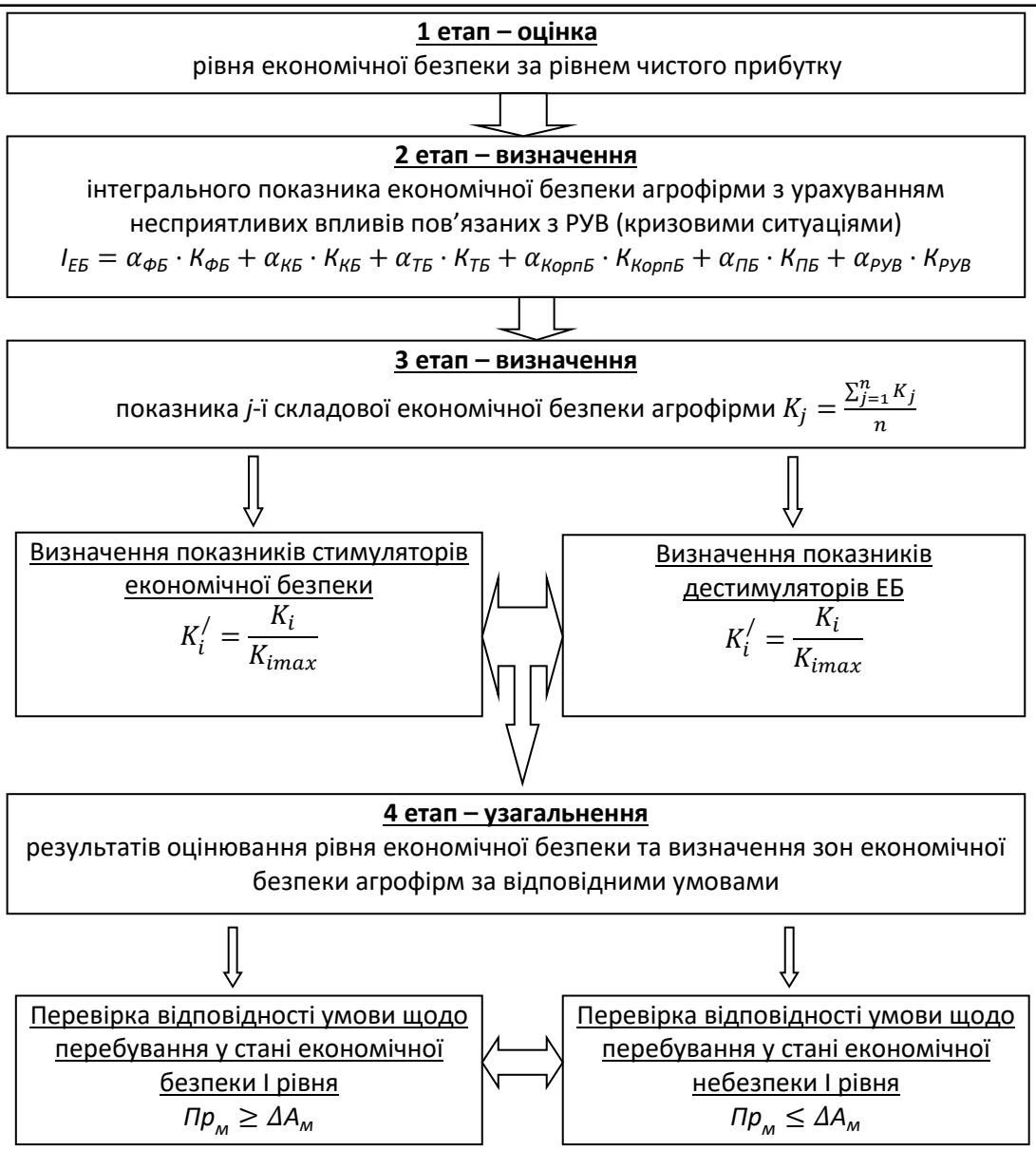


Рисунок 1. – Порядок (алгоритм) реалізації удосконаленої методики оцінювання ефективності управління забезпеченням економічної безпеки агрофірм за визначеними показниками та критеріями

Джерело: розроблено автором

Таким чином перший етап оцінювання рівня економічної безпеки пропонуємо здійснювати в такій послідовності:

1) визначення розмірів нарахованих в аналізованому році амортизаційних відрахувань за основними виробничими фондами агрофірми та проведення їх корегування на рівень інфляції:

$$A_м^{інф} = A_м \cdot (1 + \frac{T_{інф}}{100}), \quad (1)$$

де $A_м$ – амортизація основних засобів;

$T_{інф}$ – темпи інфляції в аналізованому періоді.

2) визначається різниця між нарахованою амортизацією та амортизацією з врахуванням інфляції:

$$\Delta A_м = A_м^{інф} - A_м, \quad (2)$$

Розмір нестачі коштів для простого відтворення, відшкодованих за рахунок амортизаційних відрахувань, які повинні бути покриті за рахунок реінвестованого прибутку.

3) визначається розмір прибутку, що залишився у розпорядженні агрофірми;

4) визначається частка прибутку, що реінвестується, після чого різниця між нарахованою та скорегованою амортизацією ($\Delta A_м$) порівнюється з рівнем прибутку, що спрямоване на реінвестування ($\Delta A_м$). Якщо, $Пр_м \geq \Delta A_м$ то агрофірма перебуває в стані економічної безпеки першого рівня. Якщо $Пр_м \leq \Delta A_м$, агрофірма в стані економічної небезпеки першого рівня.

Другий етап оцінки економічної безпеки полягає у визначенні рівня інтегрального показника, який оцінює кожну з складових з врахуванням вагомості їх впливу на кінцевий рівень економічної безпеки агрофірм [12 – 13]. Тому необхідним є визначення показників, що мають бути оцінені в межах кожної складової.

Інтегральний показник рівня економічної безпеки агрофірми пропонуємо визначати відповідно до ресурсно-функціонального підходу:

$$I_{ЕБ} = \sum_6^{j=1} K_j \cdot \alpha_j, \quad (3)$$

де K_j – показник *j*-ї складової економічної безпеки агрофірми;
α_j – показник вагомості *j*-ї складової економічної безпеки агрофірми.

Якщо розписати вираз (3), то отримаємо:

$$\mathrm{I_{ЕБ}} = \alpha_{\mathrm{ФБ}} \cdot \mathrm{К_{ФБ}} + \alpha_{\mathrm{КБ}} \cdot \mathrm{К_{КБ}} + \alpha_{\mathrm{ТБ}} \cdot \mathrm{К_{ТБ}} + \alpha_{\mathrm{КорпБ}} \cdot \mathrm{К_{КорпБ}} + \alpha_{\mathrm{ПБ}} \cdot \mathrm{К_{ПБ}} + \alpha_{\mathrm{РУВ}} \cdot \mathrm{К_{РУВ}}, \quad (4)$$

де $K_{\mathrm{ФБ}}$ – показник фінансової безпеки агрофірми;
$K_{\mathrm{КБ}}$ – показник кадрової безпеки агрофірми;
$K_{\mathrm{ТБ}}$ – показник технологічної безпеки агрофірми;
$K_{\mathrm{КорпБ}}$ – показник корпоративної безпеки агрофірми;
$K_{\mathrm{ПБ}}$ – показник правової безпеки агрофірми;
$K_{\mathrm{РУВ}}$ – показник стійкості безпеки агрофірми з урахуванням негативних впливів російсько-української війни та інших кризових ситуацій;
$\alpha_{\mathrm{ФБ}}$ – показник вагомості фінансової безпеки агрофірми;
$\alpha_{\mathrm{КБ}}$ – показник вагомості кадрової безпеки агрофірми;
$\alpha_{\mathrm{ТБ}}$ – показник вагомості технологічної безпеки агрофірми;
$\alpha_{\mathrm{КорпБ}}$ – показник вагомості корпоративної безпеки агрофірми;
$\alpha_{\mathrm{ПБ}}$ – показник вагомості правової безпеки агрофірми;
$\alpha_{\mathrm{РУВ}}$ – показник вагомості стійкості безпеки агрофірми з урахуванням негативних впливів російсько-української війни та інших кризових ситуацій.

Під час формування інтегрального показника слід врахувати, що кількість показників для різних складових економічної безпеки є не однаковою, що може здійснити суттєвий вплив на об'єктивність отриманих результатів, тому показник *j*-ї складової економічної безпеки агрофірми пропонуємо визначати наступним чином:

$$K_j = \frac{\sum_{j=1}^{n} K_j}{n}, \quad (5)$$

де n – кількість показників в *j*-й складовій економічної безпеки агрофірми.

Для кожної складової економічної безпеки агрофірми визначається показник, що оцінює негативні тенденції, що спричиняють вплив на загальний рівень економічної безпеки, з єдиним діапазоном вимірювання від 0 до 1 [14].

Розрахунок ключових показників кожної складової економічної безпеки підприємства доцільно проводити наступним чином:

для показників стимуляторів:

$$K_i^{/} = \frac{K_i}{K_{imax}}, \quad (6)$$

для показників дестимуляторів:

$$K_i^{/} = \frac{K_i}{K_{imax}}, \quad (7)$$

де $K_i^{/}$ – скорегований показник дії *i*-ї кількості стимуляторів (де стимуляторів) в *j*-й складовій економічної безпеки агрофірми;

K_{i} – значення *i*-го показника в *j*-й складовій економічної безпеки агрофірми;

K_{imax} – максимальне або нормативне значення *i*-го показника в *j*-й складовій економічної безпеки агрофірми.

Система показників складових економічної безпеки аграрного підприємства (агрофірми), на основі яких доцільно визначати рівень економічної безпеки представлено в табл.1.

Таблиця 1 – Система показників оцінювання рівня економічної безпеки агрофірми

Складова економічної безпеки	Характер показника	Показник
Фінансова безпека	Стимулятор	- коефіцієнт незалежності;
	Стимулятор	- коефіцієнт покриття;
	Стимулятор	- коефіцієнт абсолютної ліквідності;
	Стимулятор	- коефіцієнт прибутковості;
	Стимулятор	- коефіцієнт оборотності оборотних коштів;
	Дестимулятор	- коефіцієнт, який враховує зниження фінансової безпеки в умовах російсько-української війни (кризових ситуацій).
Кадрова безпека	Стимулятор	- рівень заробітної плати у порівнянні з середнім рівнем по регіону;
	Стимулятор	- темпи зростання продуктивності праці у порівнянні з темпами зростання заробітної плати в середньому по підприємству;
	Стимулятор	- рівень трудової дисципліни, який є надзвичайно важливим для будь-якого підприємства, діяльність яких пов’язана з постійно присутніми ризиками і відповідальністю за життя та здоров’я пасажирів та інших учасників руху, а також зі збереженням вантажів;
	Стимулятор	- плинність кадрів, яка є реальним показником задоволеності персоналу умовами праці та рівнем заробітної плати;
	Дестимулятор	- коефіцієнт, який враховує зниження кадрового потенціалу в умовах російсько-української війни (кризових ситуацій)

Складова економічної безпеки	Характер показника	Показник
Технологічна безпека	Дестимулятор	- рівень фізичного зносу основних фондів підприємства;
	Дестимулятор	- аварійність та надзвичайні випадки з вини невідповідного технічного стану обладнання;
	Дестимулятор	- коефіцієнт, який враховує зниження технологічної безпеки в умовах російсько-української війни (кризових ситуацій)
	Стимулятор	- процеси оновлення та приросту основних виробничих фондів
Правова безпека	Стимулятор	- юридична грамотність складання документів на підприємстві;
	Стимулятор	- частка судових справ, по яких були отримані задовільні результати під супроводом юридичного відділу підприємства;
	Стимулятор	- економічна ефективність витрат на утримання юридичного відділу;
	Дестимулятор	- коефіцієнт, який враховує зниження правової безпеки в умовах російсько-української війни (кризових ситуацій)
Корпоративна безпека	Стимулятор	- кількість мажоритарний акціонерів та їх вагомість;
	Стимулятор	- співвідношення пакетів у мажоритарних акціонерів;
	Стимулятор	- співвідношення пакетів акцій у мажоритарних та міноритарних акціонерів;
	Дестимулятор	- коефіцієнт, який враховує зниження корпоративної безпеки в умовах російсько-української війни (кризових ситуацій)
Стабілізаційна безпека в умовах російсько-української війни (кризових ситуацій)	Дестимулятор	- збільшення кількості агрофірм через несприятливі фактори пов’язані з російсько-українською війною (кризовими ситуаціями);
	Дестимулятор	- обмеження можливостей стабільності управління економічної безпеки агрофірм через фактор війни;
	Дестимулятор	- деструктивний вплив на всі складові у системі управління безпекою економічної безпеки агрофірм

Джерело: доповнено автором на основі [9].

Важливим кроком в оцінюванні рівня економічної безпеки аграрного підприємства, зокрема агрофірми, є визначення вагових коефіцієнтів, що мають відобразити внесок кожної складової економічної безпеки агрофірми в загальний її рівень.

Визначення таких коефіцієнтів може бути проведене за допомогою методу аналізу ієрархій, що добре зарекомендував себе під час проведення аналогічних досліджень і, на відміну від загально вживаного ранжування за експертним методом, дозволяє отримати більш об’єктивні та достовірні результати [15].

Сутність методу полягає у ієрархічному представленні елементів, які характеризують певну проблему. Реалізація методу полягає у декомпозиції аналізованої проблеми на прості елементи та подальшому аналізі суджень про них шляхом проведення попарного порівняння, в результаті якого можуть бути отримані дані про пріоритетність одних елементів перед іншими [15].

Слід зазначити, що інтегральний показник управління забезпеченням економічної безпеки агрофірми ($I_{ЕБ}$) може приймати значення в діапазоні від 0 до 1. При цьому наближення значення до 1 свідчить про зменшення ймовірності негативних змін в агрофірмі, та, відповідно, про збільшення рівня економічної безпеки, наближення значення до 0 – про

зменшення рівня економічної безпеки підприємства. Таку оберненість показників слід врахувати у шкалі оцінювання, бо шкали оцінювання ефективності управління забезпеченням економічної безпеки агрофірми, що наведені авторами основані на зворотному, тобто вони сформовані за принципом: чим вищий показник, тим вищий рівень економічної безпеки підприємства [14].

Інтегральний показник ефективності управління забезпеченням економічної безпеки агрофірми може приймати наступні значення [13]:

- від 0 до 0,29 – ймовірність негативних змін висока;
- від 0,3 до 0,49 – негативні зміни ймовірні;
- від 0,5 до 1 – ймовірність негативних змін низька.

Аналізуючи наведену шкалу для оцінювання значень інтегрального показника ефективності управління забезпеченням економічної безпеки агрофірми, можна відмітити, що, фактично, негативними для неї є в стратегічному плані значення менше за 0,5. Тому саме це значення є тією критичною точкою, що має бути врахована під час поєднання результатів оцінювання ефективності управління забезпеченням економічної безпеки агрофірми.

Узагальнення результатів оцінювання ефективності управління забезпеченням економічної безпеки агрофірми за двома етапами дозволяє визначити зони економічної безпеки агрофірми (табл. 2).

Таблиця 2 – Характеристика зон економічної безпеки агрофірми

Зони економічної безпеки агрофірми	Показники першого етапу	Показники другого етапу	Значення	Зміст
Зона I	$Пр_м \geq \Delta A_м$	[0,50; 1,00]	Економічна безпека	Економічна безпека агрофірми
Зона II		[0,30; 0,49]	Економічна безпека I-го рівня	Поточна економічна безпека агрофірми
Зона III	$Пр_м \leq \Delta A_м$	[0,30; 0,49]	Економічна безпека II-го рівня	Стратегічна економічна безпека агрофірми
Зона IV		[0; 0,29]	Економічна небезпека	Абсолютна економічна небезпека агрофірми

Джерело: сформовано автором.

Зона I представляє собою зону абсолютної економічної безпеки як з поточної, так і зі стратегічної точки зору. Потрапляння агрофірми до цієї зони свідчить про економічну стабільність та ефективне управління ресурсами, наслідком яких є отримання прибутку, достатнього для відтворення, та низька ймовірність суттєвих змін в стані агрофірми під впливом негативних факторів внутрішнього або зовнішнього середовища. Метою управління забезпеченням економічної безпеки агрофірми в цій зоні є утримання та розвиток усіх існуючих переваг.

Зона II є зоною поточної економічної безпеки, в межах якої агрофірмі вистачає отриманого прибутку для відтворення, однак його функціонування є нестабільним та чутливим до негативних змін середовища, значна мінливість якого може призвести до потрапляння підприємства в зону IV, тобто в зону абсолютної економічної небезпеки. Метою управління забезпеченням економічної безпеки агрофірми в зоні II є підвищення ефективності використання та управління ресурсами з метою забезпечення довгострокової економічної безпеки.

Зона III є певною перехідною зоною між станами економічної безпеки та небезпеки. Потрапляння до цієї зони свідчить про наявність у агрофірми можливості до стабільного функціонування в стратегічній перспективі завдяки досить ефективному управлінню ресурсами та наявності значного потенціалу для подальшого розширення позитивних тенденцій. Метою управління забезпеченням економічної безпеки є підтримання та розширення усіх наявних переваг з метою отримання прибутку, достатнього для забезпечення процесів відтворення.

Зона IV є зоною абсолютної економічної небезпеки агрофірми. Потрапляння до цієї зони свідчить про нестабільність та значні негативні тенденції в розвитку підприємства, неефективність управління наявними ресурсами, що вже в короткостроковій перспективі призведе підприємство до скорочення виробничих можливостей через неможливість забезпечення навіть простого відтворення та банкрутства в довгостроковій перспективі. Метою управління забезпеченням економічної безпеки агрофірми в зоні IV є розробка та впровадження негайних заходів для виведення агрофірми з кризи.

Приведені вище міркування дозволять в подальшому дослідити вплив прийняття раціональних управлінських рішень на рівень загальної економічної безпеки агрофірм.

Висновки

Таким чином, удосконалена методика оцінювання ефективності управління забезпеченням економічної безпеки агрофірм за визначеними показниками та критеріями, які враховують всі складові економічної безпеки агрофірми. Застосування зазначеної методики оцінювання дозволить визначити зону економічної безпеки, в якій знаходиться агрофірма, розробити комплекс заходів щодо забезпечення належного рівня економічної безпеки, підвищити ступінь економічної обґрунтованості прийняття рішення стосовно пріоритетності реакції агрофірми щодо самозбереження, стабілізації, формування конкурентної, інноваційної позицій або позиції забезпечення довгострокового потенціалу в межах забезпечення економічної безпеки агрофірми. Окрім того, в алгоритмі реалізації запропонованої методики враховується забезпечення стійкості економічної безпеки агрофірми з урахуванням негативних впливів російсько-української війни та інших кризових ситуацій, за рахунок використання показників стабільності і вагомості.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Шило Ж. С., Кречко М. Ю. Методи оцінки рівня економічної безпеки підприємства: підходи до оцінювання та забезпечення економічної безпеки. Вісник НУВГП. Економічні науки: зб. наук. праць. Рівне: НУВГП. 2022. Вип. 2 (98). С. 278–288. URL : http://ep3.nuwm.edu.ua/id/eprint/24406
2. Алькема В. Г., Літвін Н. М., Кириченко О. С. Економічна безпека інноваційного підприємства: навчальний посібник. К. : ВНЗ «Університет економіки та права «КРОК», 2015. 320 с.
3. Варічева Р. В. Методичні підходи до оцінки якості економічної безпеки підприємства: облікове забезпечення. Вісник Хмельницького національного університету. Економічні науки. 2016. № 3(1). С. 88–93. URL : http://nbuv.gov.ua/UJRN/Vchnu_ekon_2016_3%281%29__20

4. Коптєва Г. М. Класифікація підходів до оцінки економічної безпеки підприємства. Східна Європа: Економіка, бізнес та управління. 2020. Вип. 2(25). С. 221–229. URL : https://www.easterneurope-ebm.in.ua/journal/25_2020/34.pdf
5. Сосновська О. О., Житар М. О. Аналіз методів оцінки рівня економічної безпеки підприємств. Бізнес Інформ. 2019. № 1. С. 21–26. URL : https://elibrary.kubg.edu.ua/id/eprint/28836/1/%D0%9E_Sosnovska_M_Zhytar_BI_1_FITU_UDFSU.pdf
6. Васильців Т. Г., Микитюк Р. М. Удосконалення методики оцінювання економічної безпеки підприємства. Науковий вісник НЛТУ України. 2012. Вип. 22.14. С. 181–188. URL : http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=nvnltu_2012_22.14_33
7. Дідик А. М. Економічна безпека підприємства : підручник. Львів : Львівська політехніка, 2019. 624 с.
8. Ружицький А. В. Показники економічної безпеки підприємств. Сучасні проблеми економіки та підприємство. № 8, 2011. С. 116–120. URL : http://sb-keip.kpi.ua/article/view/50571
9. Толстова А. В., Хоменко К. В. Методика оцінювання рівня економічної безпеки підприємства. Економіка підприємства. № 63, 2018. С. 187–195. URL : http://lib.kart.edu.ua/bitstream/123456789/1660/1/Tolstova.pdf
10. Близнюк А. О. Аналіз методик оцінювання економічної безпеки підприємства. Вчені пр.: Вищ. навч. закл. "Університет економіки та права "КРОК". К., 2013. Вип. 34. С. 240–247.
11. Близнюк А. О. Методичні основи оцінювання економічної безпеки підприємства. Економічний простір : зб. наук. праць. Вип. 55. Дніпро: ПДАБА, 2011. С. 188–194.
12. Пілецька С. Т., Коритько Т. Ю., Ткаченко Є. В. Модель інтегральної оцінки економічної безпеки підприємства. Економічний вісник Донбасу. 2021. № 3 (65). С. 56–65. URL : http://dspace.nbuv.gov.ua/handle/123456789/181846
13. Сисоліна Н. П. Економічна безпека підприємства: навч. посіб. Кропивницький: ЦУНТУ, 2014. 226 с.
14. Козаченко Г. В., Пономарьов В. П., Ляшенко О. М. Економічна безпека підприємства: сутність та механізм забезпечення: монографія. К.: Лібра, 2003. 280 с.
15. Усикова О. М. Метод аналізу ієрархій у системі прийняття рішень на підприємстві. Економічний вісник Дніпровського державного технічного університету. 2023. № 1(6). С. 86–91. https://doi.org/10.31319/2709-2879.2023iss1(6).283000pp86-91

References

1. Shylo Zh. S., Krechko M. Yu. Methods of assessing the level of economic security of an enterprise: approaches to assessing and ensuring economic security. Bulletin of the NUWEE. Economic sciences: coll. of science works. Rivne: NUWEE. 2022. Issue 2 (98). P. 278–288. Available from : http://ep3.nuwm.edu.ua/id/eprint/24406
2. Alkema V. G., Litvin N. M., Kyrychenko O. S. Economic security of an innovative enterprise: a study guide. K.: KROK University of Economics and Law, 2015. 320 p.
3. Varycheva R. V. Methodical approaches to the assessment of the quality of economic security of the enterprise: accounting support. *Bulletin of the Khmelnytskyi National University. Economic sciences*. 2016. No. 3(1). P. 88–93. Available from : http://nbuv.gov.ua/UJRN/Vchnu_ekon_2016_3%281%29__20
4. Kopteva H. M. Classification of approaches to the assessment of the economic security of the enterprise. Eastern Europe: Economics, Business and Management. 2020. Issue 2(25). P. 221–

229. Available from : https://www.easterneurope-ebm.in.ua/journal/25_2020/34.pdf
5. Sosnovska O. O., Zhitar M. O. Analysis of methods for assessing the level of economic security of enterprises. *Business Inform*. 2019. No. 1. C. 21–26. Available from : https://elibrary.kubg.edu.ua/id/eprint/28836/1/%D0%9E_Sosnovska_M_Zhytar_BI_1_FITU_UDFSU.pdf
6. Vasyltsiv T. G., Mykytyuk R. M. Improvement of the method of assessing the economic security of the enterprise. *Scientific bulletin of UNFU of Ukraine*. 2012. Issue 22.14. P. 181–188. Available from : http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=nvnltu_2012_22.14_33
7. Didyk A. M. Economic security of the enterprise: textbook. Lviv: Lviv Polytechnic, 2019. 624 p.
8. Ruzhytskyi A. V. Indicators of economic security of enterprises. Modern problems of economy and enterprise. No. 8, 2011. P. 116–120. Available from : http://sb-keip.kpi.ua/article/view/50571
9. Tolstova A. V., Khomenko K. V. Methodology for assessing the level of economic security of an enterprise. *Enterprise economy*. No. 63, 2018. P. 187–195. Available from : http://lib.kart.edu.ua/bitstream/123456789/1660/1/Tolstova.pdf
10. Blyznyuk A.O. Analysis of methods for assessing the economic security of an enterprise. Academic notes: Higher educational institution. KROK University of Economics and Law. Kyiv, 2013. Issue 34. P. 240-247.
11. Blyznyuk A.O. Methodological basis for assessing the economic security of an enterprise. Economic space: coll. of science works Vol. 55. Dnipro: PSACEA, 2011. P. 188–194.
12. Piletska S.T., Korytko T.Yu., Tkachenko E.V. Model of integrated assessment of economic security of the enterprise. *Economic Herald of Donbass*. 2021. No. 3 (65). P. 56–65. Available from : http://dspace.nbuv.gov.ua/handle/123456789/181846
13. Sysolina N. P. Economic security of the enterprise: study guide. Kropyvnytskyi: CUNTU, 2014. 226 p.
14. Kozachenko G. V., Ponomaryev V. P., Lyashenko O. M. Economic security of the enterprise: essence and mechanism of provision: monograph. Kyiv: Libra, 2003. 280 p.
15. Usykova O. M. The method of analyzing hierarchies in the decision-making system at the enterprise. *Economic Bulletin of the Dnipro State Technical University*. 2023. No. 1(6). P. 86–91. https://doi.org/10.31319/2709-2879.2023iss1(6).283000pp86-91

Математична модель оцінювання ризиків функціонування об’єктів критичної інфраструктури на основі теорії нечіткої логіки

Mathematical model of risk assessment of the operation of critical infrastructure objects based on the theory of fuzzy logic

Рустам Мурасов [A]
Corresponding author: кан. техн. наук, професор кафедри, e-mail: rustamm@ukr.net, ORCID:0000-0003-0800-2062
Анатолій Нікітін [A]
Доктор філософії, професор кафедри, e-mail: tolik-nikitin@ukr.net, ORCID: 0000-0003-1487-0616
Іван Мещеряков [A]
Доктор філософії, доцент кафедри, e-mail: shulyk3004@ukr.net, ORCID: 0000-0001-5797-0735

Rustam Murasov [A]
Corresponding author: Candidate of Technology Sciences, Professor of the Department, e-mail: rustamm@ukr.net, ORCID: 0000-0003-0800-206
Anatolii Nikitin [A]
Doctor of Philosophy, Professor of the Department, e-mail: tolik-nikitin@ukr.net, ORCID: 0000-0003-1487-0616
Ivan Meshcheriakov [A]
Doctor of Philosophy, associate professor of the department, e-mail: shulyk3004@ukr.net, ORCID: 0000-0001-5797-0735

[A] Національний університет оборони України, м. Київ, Україна
[A]National Defense University of Ukraine, Kyiv, Ukraine

Received: October 4, 2024 | Revised: October 20, 2024 | Accepted: October 31, 2024

DOI: 10.33445/sds.2024.14.5.17

Мета роботи: розробка математичної моделі оцінювання ризиків функціонування об’єктів критичної інфраструктури на основі теорії нечіткої логіки.
Метод: теорія ймовірності, теорія нечіткої логіки, метод центру ваги, моделювання.
Результати дослідження: розроблена математична модель оцінювання ризиків функціонування об’єктів критичної інфраструктури на основі теорії нечіткої логіки. На практичному прикладі обчислення нечітких та невизначених даних перевірена її адекватність.
Теоретична цінність дослідження: процес оцінювання ризиків в наслідок ударів противника став більш адаптивним і точним для подальших досліджень.
Тип статті: дослідницька.

Purpose: development of a mathematical model for assessing the risks of the operation of critical infrastructure objects based on the theory of fuzzy logic
Method: theory of probability, fuzzy logic theory, center of gravity method, modeling.
Findings: a mathematical model was developed for assessing the risks of the operation of critical infrastructure objects based on fuzzy logic theory. Its adequacy is verified on a practical example of calculating fuzzy and uncertain data.
Theoretical implications: the process of assessing risks as a result of enemy strikes has become more adaptive and accurate for further research.
Papertype: research.

Ключові слова: критична інфраструктура, надзвичайна ситуація, нечітка логіка, ймовірність, загроза, захист, ризик.

Key words: critical infrastructure, emergency, fuzzy logic, probability, threat, protection, risk.

Вступ

Оцінювання ризиків функціонування об’єктів критичної інфраструктури є ключовим елементом забезпечення національної безпеки, оскільки дозволяє ідентифікувати можливі загрози та приймати рішення щодо їхнього усунення чи мінімізації. Традиційні методи оцінювання ризиків часто виявляються недостатньо ефективними через високу невизначеність і складність даних, що надходять з існуючих систем захисту критичної інфраструктури. В умовах постійно змінюваних загроз, таких як природні катаклізми, техногенні аварії або цілеспрямовані ракетно-дронові атаки рф, особливо актуальним є використання методів, які дозволяють працювати з нечіткими, неповними або непередбачуваними даними.

Використання теорії нечіткої логіки є одним із найбільш перспективних підходів для ідентифікації можливих загроз та оцінювання відповідних ризиків їх реалізації, оскільки вона дозволяє працювати з інформацією, яка не може бути точно виміряною або яка має значну невизначеність. Відповідно, застосування нечітких множин дозволяє ефективніше

моделювати реалізацію загроз для об’єктів критичної інфраструктури та оцінювати ризик їх функціонуванню на основі змінних, що не мають чітких границь або однозначних значень.

Сучасні виклики, зокрема пов’язані з військовими загрозами, кібератаками, природними катастрофами, потребують створення математичних моделей, здатних швидко реагувати на зміни та враховувати комплексність процесів. Особливо це актуально в умовах агресивних ракетно-дронових атак на об’єкти критичної інфраструктури, що може призвести до каскадних деструктивних наслідків. Знищення ключових об’єктів атомної енергетики, гідросистем, водопостачання, зв’язку чи транспорту може викликати великомасштабні аварії, що впливають на економіку, екологію та населення.

Теоретичні основи дослідження

Аналіз останніх публікацій [1-4] стосовно підходів до ідентифікації загроз і оцінювання ризиків на основі теорії нечіткої логіки свідчить, що застосування нечіткої логіки для оцінювання ризиків функціонування критичної інфраструктури є актуальним напрямком дослідження через високу невизначеність даних і складність системи. Методи, які запропоновані у попередніх дослідженнях, демонструють, що нечітка логіка є ефективним інструментом для моделювання надзвичайних ситуацій та ідентифікації загроз і оцінювання ризиків.

На думку багатьох провідних фахівців [5-12], які досліджували питання захисту об’єктів критичної інфраструктури (ОКІ), на сьогодні не існує загальноприйнятої методики для ідентифікації загроз і оцінювання ризиків функціонування ОКІ, особливо в умовах ракетно-дронових атак. Існують тільки часткові рішення для окремих об'єктів або конкретних надзвичайних ситуацій. Основним пріоритетом ставиться мінімізація наслідків надзвичайних ситуацій на ОКІ. Крім того, підходи до оцінювання ризиків функціонування ОКІ здебільшого фокусуються на проведенні аварійно-рятувальних заходів, спрямованих на усунення наслідків, а не на проактивні стратегії попередження можливих загроз. В умовах сучасних викликів, таких як масовані ракетно-дронові атаки рф, ці методи залишаються недостатньо ефективними. Існуючі методики не враховують комплексний характер взаємодії різних типів загроз і обмежуються аналізом ризиків на локальному рівні, не забезпечуючи системного підходу до управління ризиками. Світовий досвід також вказує на те, що основна увага зосереджується на відновленні після події, але не на попередженні або мінімізації реалізації загрози.

Загалом, аналіз зазначених джерел свідчить про активне використання нечіткої логіки та інших математичних методів для оцінювання ризиків функціонування ОКІ. Ці методи дозволяють працювати з невизначеністю та складністю таких систем, що робить їх незамінними інструментами для ідентифікації загроз і оцінювання ризиків функціонування ОКІ під час виникнення надзвичайних ситуацій та в разі вчинення терористичних актів.

Постановка проблеми

Зважаючи на важливість захисту об’єктів критичної інфраструктури, розробка математичних моделей для оцінювання ризиків функціонування ОКІ на основі нечіткої логіки стає вкрай необхідною. Такі моделі дозволяють формалізувати взаємозв’язки між ймовірністю реалізації загроз, ступенем їх впливу на функціонування ОКІ та ефективністю засобів захисту ОКІ. Вони також дають змогу враховувати широкий спектр можливих сценаріїв, роблячи процес оцінювання ризиків більш адаптивним і точним.

Таким чином, метою цієї роботи є розробка математичної моделі оцінювання ризиків функціонування ОКІ на основі теорії нечіткої логіки, яка дозволить працювати з невизначеними даними та забезпечить точнішу оцінку можливих загроз.

Результати

Актуальні виклики сьогодення, такі як військові загрози, вторинні деструктивні впливи та природні катаклізми, потребують створення математичних моделей, здатних швидко адаптуватися до змін і враховувати багатофакторність процесів. Це особливо актуально при захисті від ракетно-дронових атак на ОКІ, оскільки вони можуть спровокувати ланцюгові руйнівні аварії та катастрофи, що матимуть значний вплив на економічний стан країни, стан довкілля та добробут населення.

Із найперспективніших підходів до вирішення цієї проблеми є теорія нечіткої логіки, яка дає можливість аналізувати інформацію, яка не піддається точному вимірюванню або має значний рівень невизначеності. Застосування нечітких множин забезпечує більш ефективну ідентифікацію і моделювання загроз для функціонування ОКІ та дозволяє оцінювати ризик на основі даних, які не мають чітких меж.

Тому виникає необхідність, щодо розробки та опису математичної моделі оцінювання ризиків функціонування ОКІ на основі теорії нечіткої логіки яка представлена на рис. 1.

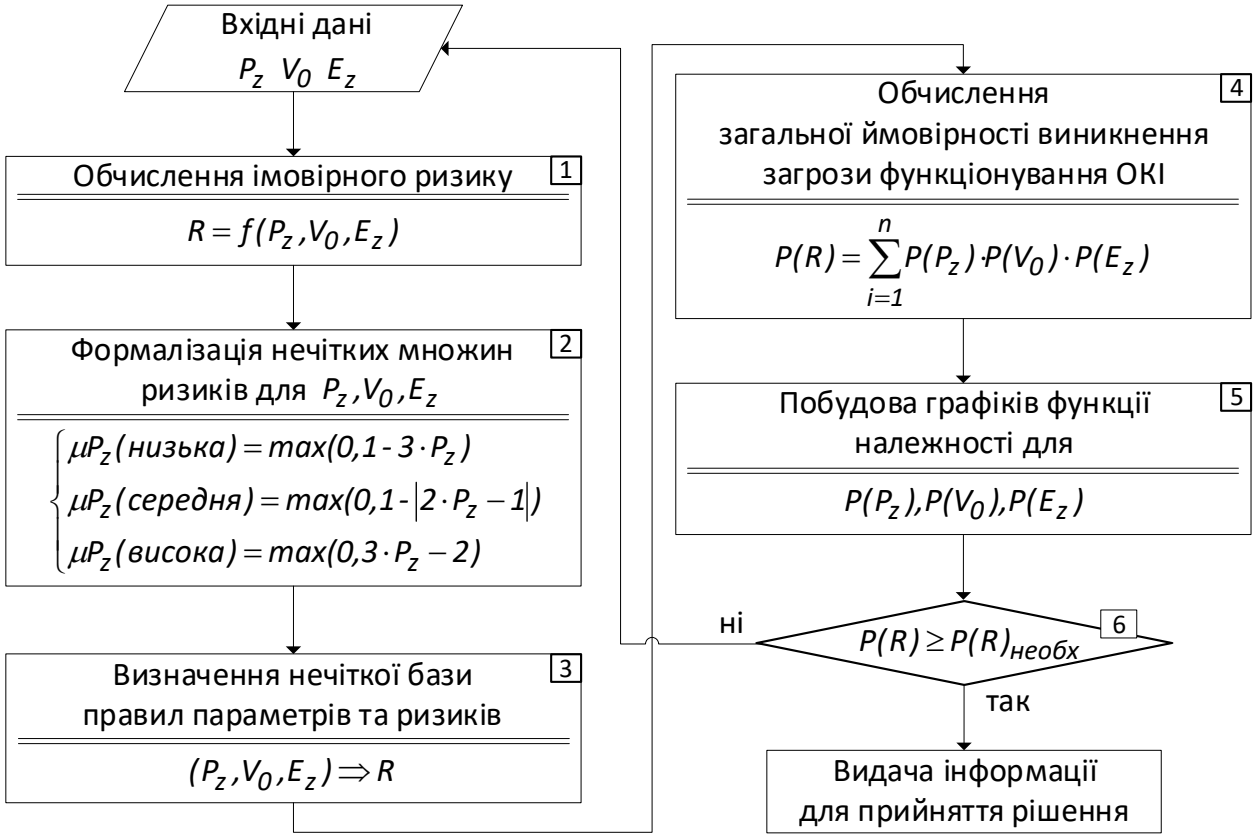


Рисунок 1 – Структурно-логічна схема математичної моделі оцінювання ризиків критичної інфраструктури на основі теорії нечіткої логіки

Блок 1. Обчислення імовірного ризику.

Метою є оцінювання ризику функціонування ОКІ з урахуванням таких основних параметрів:

P_z – ймовірність виникнення загрози;

V_0 – рівень впливу загрози на об’єкт;

E_z – ефективність засобів захисту.

Рівень ризику R розраховується на основі трьох змінних і визначається як:

$$R = f(P_z, V_0, E_z). \quad (1)$$

Кожен із цих параметрів є нечітким, тому їх необхідно моделювати за допомогою функцій належності.

Блок 2. Формалізація нечітких множин.

Для кожної змінної ми використовуємо три рівні належності: “низька”, “середня”, “висока”. Ці рівні задаються трикутними функціями належності.

Функції належності для ймовірності виникнення загрози P_z визначаються таким чином:

$$\begin{cases} \mu P_z(низька) = max(0,1\text{-}3 \cdot P_z) \\ \mu P_z(середня) = max(0,1\text{-}|2 \cdot P_z - 1|), \\ \mu P_z(висока) = max(0,3 \cdot P_z - 2) \end{cases} \quad (2)$$

де, μP_z – функція належності для параметра P_z.

Функції належності для рівня впливу загрози на об’єкт V_0 визначаються таким чином:

$$\begin{cases} \mu V_0(низький) = max(\,0,1 - 3 \cdot V_0) \\ \mu V_0(середній) = max(\,0,1 - |2 \cdot V_0 - 1|). \\ \mu V_0(високий) = max(\,0,3 \cdot V_0 - 2) \end{cases} \quad (3)$$

Функції належності для ефективності засобів захисту E_z визначаються таким чином:

$$\begin{cases} \mu E_z(низький) = max(\,0,1\text{-}3 \cdot E_z) \\ \mu E_z(середній) = max(\,0,1\text{-}|2 \cdot E_z - 1|). \\ \mu E_z(високий) = max(\,0,3 \cdot E_z - 2) \end{cases} \quad (4)$$

Блок 3. Визначення нечіткої бази правил параметрів та ризику

Правила в нечіткій базі знань мають вигляд умов “якщо-то”, які визначають взаємозв’язок між параметрами P_z, V_0, E_z та ризиком R.

$$(P_z, V_0, E_z) \Rightarrow R. \quad (5)$$

Показник між параметрами та ризиком визначається за табл. 1.

Таблиця 1 – Нечітка база правил

Правило	P_z	V_0	E_z	R
1	Низька	Низький	Високий	Низький
2	Низька	Високий	Низький	Середній
3	Середня	Середній	Середній	Середній
4	Висока	Високий	Низький	Високий
5	Середня	Високий	Високий	Низький
6	Висока	Низький	Середній	Високий

Блок 4. Обчислення загальної ймовірності виникнення загрози функціонування ОКІ.

Для обчислення загальної ймовірності ризику ми можемо скористатися комбінованою оцінкою, яка враховує ймовірності різних загроз, їх впливу та ефективності захисту. Нехай $P(P_z), P(V_0), P(E_z)$ – ймовірності значень відповідних параметрів.

Сукупний рівень ризику можна виразити так:

$$P(R) = \sum_{i=1}^{n} P(P_z) \cdot P(V_0) \cdot P(E_z) \quad (6)$$

Блок 5. Побудова графіків функції належності.

Для кращого розуміння, як функції належності описують кожен параметр, побудуємо графіки для $P(P_z), P(V_0), P(E_z)$.

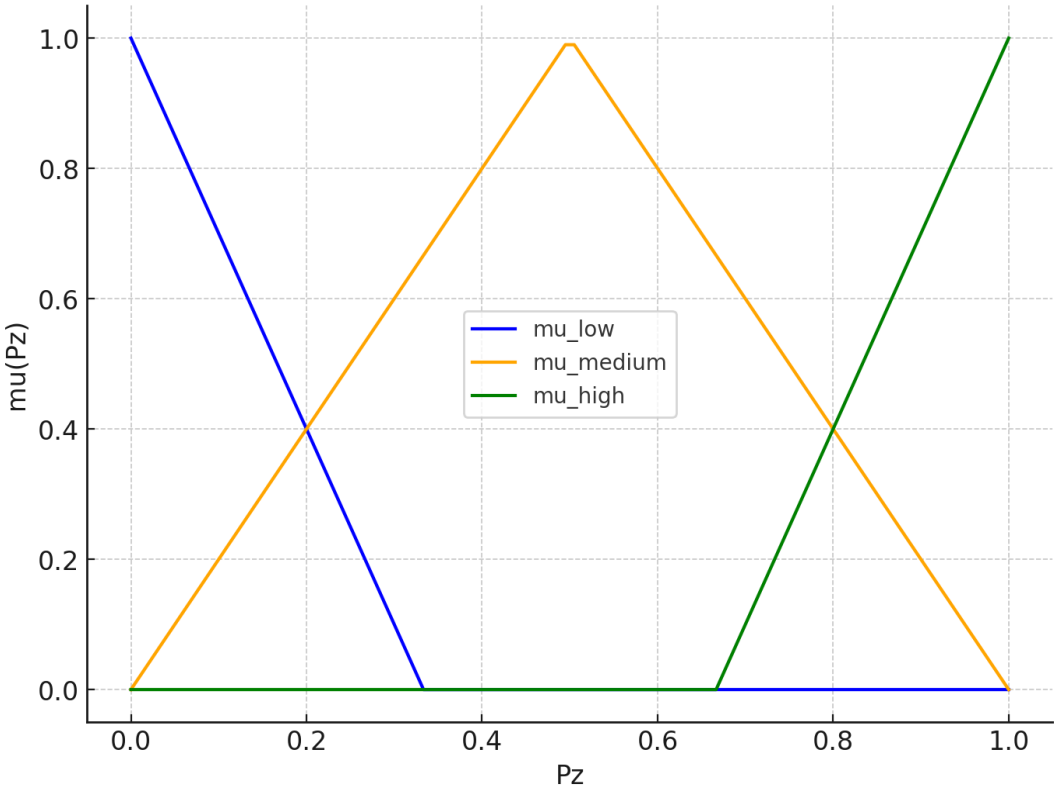


Рисунок 2 – Функція належності для параметра P_z

З цього графіка можна зрозуміти, як змінюються функції належності для різних значень параметра P_z. Він показує три функції належності – “низький”, “середній” і “високий” рівні значень P_z, які мають наступні властивості:

Низький рівень (mu_low) — функція належності має найбільші значення при малих значеннях P_z. Вона починається з максимальної належності (1) при P_z = 0 і лінійно зменшується до нуля при P_z=0,33.

Середній рівень (mu_medium) — ця функція має найбільшу належність при середніх значеннях P_z (близько 0,5). Вона є симетричною і досягає 1 при P_z = 0,5, а потім плавно зменшується до нуля при дуже малих або великих значеннях P_z.

Високий рівень (mu_high) — функція належності для високих значень P_z. Вона починається з нуля при P_z = 0,67, а потім лінійно зростає до 1 при P_z = 1.

Цей графік демонструє, що параметр P_z може належати до різних категорій (низький, середній, високий) з різним ступенем впевненості в залежності від свого значення.

Блок 6. Перевірка умов визначення показника ефективності запобігання реалізації ризику.

Для визначення показника ефективності пропонується використовувати наступний

критерій:

$$P(R) \geq P(R)_{\text{необх}} \quad (7)$$

Адекватність описано моделі оцінювання ризиків критичної інфраструктури на основі теорії нечіткої логіки перевіримо на практичному прикладі обчислення нечітких та невизначених даних.

Припустимо, що значення параметрів такі:

P_z = 0,6 – ймовірність виникнення загрози,

V_0 = 0,8 – рівень впливу загрози на об'єкт,

E_z = 0,4 – ефективність засобів захисту.

Для кожного параметра визначаємо відповідні значення функцій належності: "низька", "середня", "висока". Ці рівні задаються трикутними функціями належності.

Функції належності для параметра P_z:

низька: $\mu P_z(низька) = max(0,1 - 3P_z)$ для P_z = 0,6: $\mu P_z(низька) = max(0,1 - 3 \cdot 0,6) = 0$;

середня: $\mu P_z(середня) = max(0,1 - |2P_z - 1|)$ для P_z = 0,6: $\mu P_z(середня) = max(0,1 - |2 \cdot 0,6 - 1|) = 0,8$;

висока: $\mu P_z(висока) = max(0,3P_z - 2)$ для P_z = 0,6: $\mu P_z(висока) = max(0,3 \cdot 0,6 - 2) = 0,8$.

Функції належності для параметра V_0:

низька: $\mu V_0(низька) = max(0,1 - 3V_0)$ для V_0 = 0,8: $\mu V_0(низька) = max(0,1 - 3 \cdot 0,8) = 0$;

середня: $\mu V_0(середня) = max(0,1 - |2V_0 - 1|)$ для V_0 = 0,8: $\mu V_0(середня) = max(0,1 - |2 \cdot 0,8 - 1|) = 0,4$;

висока: $\mu V_0(висока) = max(0,3V_0 - 2)$ для V_0 = 0,8: $\mu V_0(висока) = 1$.

Функції належності для параметра E_z:

низька: $\mu E_z(низька) = max(0,1 - 3E_z)$ для E_z = 0,4: $\mu E_z(низька) = max(0,1 - 3 \cdot 0,4) = 0,8$;

середня: $\mu E_z(середня) = max(0,1 - |2E_z - 1|)$ для E_z = 0,4: $\mu E_z(середня) = 0,6$;

висока: $\mu E_z(висока) = max(0,3E_z - 2)$ для E_z = 0,4: $\mu E_z(висока) = 0$.

Згідно з нечітким правилом: "якщо P_z середня, V_0 середній, а E_z середня, то ризик середній", мінімальне значення належності для цього правила:

$$\mu R = min(\mu P_z(середня); \mu V_0(середня); \mu E_z(середня)) = min(0,8;0,4;0,6) = 0,4$$

Сукупний рівень ризику визначається за комбінованою оцінкою ймовірностей різних загроз, їх впливу та ефективності захисту:

$$P(R) = P(P_z) \cdot P(V_0) \cdot P(E_z) = 0,8 \cdot 0,4 \cdot 0,6 = 0,192.$$

Отже, сукупний рівень ризику становить $P(R)$ = 0,192.

Процес дефазифікації (розширений опис) дозволяє перетворити нечітке значення ризику R на чітке значення ризику R_{crips}. Для цього використовується метод центру ваги. Він визначає чітке значення R_{crips} на основі інтегралів площі функцій належності вихідної змінної.

Якщо нечітка множина для вихідного ризику описується функціями належності, побудованими для низького, середнього та високого ризиків, тоді формула виглядає так:

$$R_{crips} = \frac{\int_x \mu R(x) x dx}{\int_x \mu R(x) dx}. \quad (8)$$

Для нашого прикладу, після обчислення інтегралів ризик складає приблизно: $R_{\text{crips}} \approx 0{,}55$.

Висновки

У статті розроблена математична модель оцінювання ризиків функціонування ОКІ на основі теорії нечіткої логіки, яка є ефективним інструментом для обробки нечітких та невизначених даних з можливістю отримати чітке значення результату. Розроблена математична модель дозволяє:

використовувати невизначену інформацію для оцінки ризиків, що робить її придатною для застосування в умовах неповних даних;

побудувати нечітку базу правил, яка відображає складні взаємозв'язки між загрозами, рівнем впливу та ефективністю захисту;

включати в розрахунки ймовірнісні оцінки, що дозволяє більш точно прогнозувати ризики.

Застосування методів дефазифікації, зокрема методу центру ваги, дозволяє отримати чітке значення ризику, що є важливим для прийняття рішень в умовах реальних загроз. Модель є гнучкою і може бути адаптована для інших областей, таких як техногенна безпека та екологічний моніторинг.

Ми отримали змогу враховувати широкий спектр можливих сценаріїв, роблячи процес оцінювання ризиків більш адаптивним і точним для подальших досліджень.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Amini, A., Jamil, N., Ahmad, A.R. & Sulaiman, H. (2017). Підхід до оцінки ризиків на основі нечіткої логіки для оцінки та визначення пріоритетів ризиків у середовищі хмарних обчислень. – Recent Trends in Information and Communication Technology Lecture Notes on Data Engineering and Communications Technologies, 650-659. https://doi.org/10.1007/978-3-319-59427-9_67 [Дата звернення 1.10.2024].
2. Wang, Y.M., & Elhag, T.M.S. (2006). Метод нечіткої TOPSIS на основі наборів альфа-рівнів із застосуванням для поєднання оцінки ризику. – Expert Systems with Applications, 31(2), 309-319. https://doi.org/10.1016/j.eswa.2005.09.040 [Дата звернення 1.10.2024].
3. Haimes, Y.Y. (2004). Моделювання, оцінка та управління ризиками. – John Wiley & Sons. URL: https://onlinelibrary.wiley.com/doi/book/10.1002/0471723908 [Дата звернення 1.10.2024].
4. Фадєєва І.Г., Гринюк О.І. (2017). Нечітке моделювання в оцінці ризиків діяльності нафтогазовидобувних підприємств. – Балтійський журнал економічних досліджень, 3 (4), 256–264. https://doi.org/10.30525/2256-0742/2017-3-4-256-264 [Дата звернення 1.10.2024].
5. Мурасов Р., Нікітін А., Мещеряков І., Підгородецький М., Поплавець С. (2024). Удосконалення науково-методичного апарату для розрахунку ризиків виникнення та

аналізу сценаріїв надзвичайних ситуацій на об'єктах критичної інфраструктури. *Social Development and Security*, 14 (1), 205-217. https://doi.org/10.33445/sds.2024.14.1.17 [Дата звернення 1.10.2024].

6. Мурасов Р., Нікітін А., Мещеряков І., Підгородецький М., Поплавець С. (2024). Методика оцінювання загроз і ризиків для об'єктів критичної інфраструктури за сценаріями розвитку надзвичайних ситуацій. – Сучасні інформаційні технології у сфері безпеки та оборони, 3(48), 35-43. https://doi.org/10.33099/2311-7249/2023-48-3-35-43 [Дата звернення 1.10.2024].
7. Мурасов, Р., & Мещеряков, І. (2023). Інформаційно-технічний метод попередження надзвичайних ситуацій терористичного характеру шляхом оцінки можливості ступеневого росту деструктивних подій викликаних каскадними наслідками первинного терористичного впливу. *Social Development and Security*, *13*(5), 180-191. https://doi.org/10.33445/sds.2023.13.5.17 [Дата звернення 1.10.2024].
8. Фурсенко О.М., Чумаченко С.М. та Кармазин С.В. (2015) Експертна оцінка загроз для об'єктів критичної інфраструктури газотранспортної системи України з використанням методу аналізу ієрархій. – Техногенно-екологічна безпека та цивільний захист, 9, 68-77. URL: http://tes.igns.gov.ua/wp-content/uploads/2018/02/V9.pdf [Дата звернення 1.10.2024].
9. Wolbers J., Groenewegen P., Mollee J., & Bím J. (2013). Включення динаміки часу в аналіз соціальних мереж в управлінні надзвичайними ситуаціями. – Journal of Homeland Security and Emergency Management, 10(2), 555-585. https://doi.org/10.1515/jhsem-2013-0019 [Дата звернення 1.10.2024].
10. Яременко О.І., Страхніцький Я.О. (2022). Визначення та управління загрозами у структурі державної політики захисту критичної інфраструктури. – Університетські наукові записки, 3 (87), 73-82. https://doi.org/10.37491/UNZ.87.6 [Дата звернення 1.10.2024].
11. Ruban, I., Khudov, H., Makoveichuk, O., Khizhnyak, I., Khudov, V., Podlipaiev, V., Shumeiko, V., Atrasevych, O., Nikitin, A., & Khudov, R. (2019). Segmentation of opticalelectronic images from on-board systems of remote sensing of the earth by the artificial bee colony method. – Eastern-European Journal of Enterprise Technologies, 2 (9-98), 37-45. https://doi: 10.15587/1729-4061.2019.161860 [Дата звернення 1.10.2024].
12. Trysnyuk, V., Trysnyuk, T., Nikitin, A., Kurylo, A., & Demydenko, O. (2021). Geomodels of space monitoring of water bodies. – E3S Web of Conferences, 280, art. no. 09016. https://doi: 10.1051/e3sconf/202128009016 [Дата звернення 1.10.2024].

References

1 Amini, A., Jamil, N., Ahmad, A.R. & Sulaiman, H. (2017). A Fuzzy Logic Based Risk Assessment Approach for Evaluating and Prioritizing Risks in Cloud Computing Environment. *Recent Trends in Information and Communication Technology Lecture Notes on Data Engineering and Communications Technologies*, 650-659. https://doi.org/10.1007/978-3-319-59427-9_67 [Accessed date 1.10.2024].

2. Wang, Y.M., & Elhag, T.M.S. (2006). Fuzzy TOPSIS method based on alpha level sets with an application to bridge risk assessment. *Expert Systems with Applications*, 31(2), 309-319. https://doi.org/10.1016/j.eswa.2005.09.040 [Accessed date 1.10.2024].
3. Haimes, Y.Y. (2004). Risk modeling, assessment, and management. – John Wiley & Sons. URL: https://onlinelibrary.wiley.com/doi/book/10.1002/0471723908 [Accessed date 1.10.2024].
4. Fadyeyeva, I., & Gryniuk, O. (2017). Fuzzy modelling in risk assessment of oil and gas production enterprises' activity. *Baltic Journal of Economic Studies*, 3 (4), 256–264. https://doi.org/10.30525/2256-0742/2017-3-4-256-264 [Accessed date 1.10.2024].
5. Murasov, R., Nikitin, A., Meshcheriakov, I., Pidhorodetskyi, M., & Poplavets, S. (2024).

Improvement of the scientific and methodological apparatus for calculating the risks of occurrence and analyzing scenarios of emergency situations at critical infrastructure facilities. *Social Development and Security*, 14(1), 205-217. https://doi.org/10.33445/sds.2024.14.1.17 [Accessed date 1.10.2024].

6. Murasov, R., Nikitin, A., Meshcheriakov, I., Pidhorodetskyi, M., & Poplavets, S. (2024). Methodology for assessing threats and risks for critical infrastructure objects under emergency development scenarios. *Modern Information Technologies in the Sphere of Security and Defence*, 3(48), 35-43. https://doi.org/10.33099/2311-7249/2023-48-3-35-43 [Accessed date 1.10.2024].
7. Murasov, R., & Meshcheriakov, I. (2023). The information and technical method of preventing emergency situations of a terrorist nature by assessing the possibility of gradual growth of destructive events caused by the cascading consequences of the primary terrorist impact. *Social Development and Security*, 13(5), 180-191. https://doi.org/10.33445/sds.2023.13.5.17 [Accessed date 1.10.2024].
8. Fursenko, O.M., Chumachenko, S.M., & Karmazyn, S.V. (2015). Expert assessment of threats to objects of critical infrastructure of the gas transportation system of Ukraine using the method of analysis of hierarchies. *Technogenic and ecological safety and civil protection*, 9, 68-77. Available from: http://tes.igns.gov.ua/wp-content/uploads/2018/02/V9.pdf [Accessed date 1.10.2024].
9. Wolbers J., Groenewegen P., Mollee J., & Bím J. (2013). Incorporating Time Dynamics in the Analysis of Social Networks in Emergency Management. *Journal of Homeland Security and Emergency Management*, 10(2), 555-585. https://doi.org/10.1515/jhsem-2013-0019 [Accessed date 1.10.2024].
10. Yaremenko, O., & Strahnitskyi, Y. (2022). Detection and Management of Threats in the Structure of State Policy for Critical Infrastructure Protection. *University Scientific Notes*, 3 (87), 73-82. https://doi.org/10.37491/UNZ.87.6 [Accessed date 1.10.2024].
11. Ruban, I., Khudov, H., Makoveichuk, O., Khizhnyak, I., Khudov, V., Podlipaiev, V., Shumeiko, V., Atrasevych, O., Nikitin, A., & Khudov, R. (2019). Segmentation of opticalelectronic images from on-board systems of remote sensing of the earth by the artificial bee colony method. *Eastern-European Journal of Enterprise Technologies*, 2 (9-98), 37-45. https://doi: 10.15587/1729-4061.2019.161860 [Accessed date 1.10.2024].
12. Trysnyuk, V., Trysnyuk, T., Nikitin, A., Kurylo, A., & Demydenko, O. (2021). Geomodels of space monitoring of water bodies. *E3S Web of Conferences*, 280, art. no. 09016. https://doi: 10.1051/e3sconf/202128009016 [Accessed date 1.10.2024].

Розробка математичної моделі підвищення ефективності проведення аварійно-рятувальних робіт в умовах можливого бойового ураження

The Development of a mathematical model for increasing the efficiency of emergency rescue operations in conditions of possible combat damage

Віктор Стрілець [A]
Corresponding author: д.т.н., професор, доцент кафедри, e-mail: vstrelec1956@ukr.net, ORCID: 0000-0001-5992-1195

Ігор Маловик [B]
головний інспектор відділу нормативної та ліцензійної роботи управління пожежної безпеки Департаменту запобігання надзвичайним ситуаціям апарату ДСНС, e-mail: ivmal132@gmail.com, ORCID: 0009-0009-2319-9730

Сергій Степанчук [C]
старший викладач кафедри піротехнічних та спеціальних робіт, e-mail: stepanchukdsns@gmail.com, ORCID: 0000-0002-6618-4119

Валерій Стрілець [D]
к.т.н., Supervisor EORE, e-mail: v.strelec.brand@gmail.com, ORCID: 0000-0003-1913-7878

Андрій Хижняк [E]
PhD, e-mail: poltava@dsns.gov.ua, ORCID: 0009-0005-1745-0432

Олександр Вальченко [F]
к.в.н., доцент, доцент кафедри, e-mail: valchenko@gmail.com, ORCID: 0000-0002-9635-9418

Viktor Strelets [A]
Corresponding author: Dr of Sciences, Professor, Docent, e-mail: vstrelec1956@ukr.net, ORCID: 0000-0001-5992-1195

Ighor Malovyk [B]
Chief Inspector of the Department of Regulatory and Licensing Work of the fire Safety Department of the Emergency Prevention Department of the State Emergency Service, e-mail: ivmal132@gmail.com, ORCID: 0009-0009-2319-9730

Serhii Stepanchuk [C]
Senior teacher of the Department of Pyrotechnics and Special Works, e-mail: stepanchukdsns@gmail.com, ORSID: 0000-0002-6618-4119

Valery Strelec [D]
PhD, Supervisor EORE, e-mail: v.strelec.brand@gmail.com, ORCID: 0000-0003-1913-7878

Andrii Khyzhniak [E]
PhD, e-mail: poltava@dsns.gov.ua, ORCID: 0009-0005-1745-0432

Oleksander Valchenko [F]
PhD, Associate Professor, Associate Professor of the Department, e-mail: valchenko@gmail.com, ORCID: 0000-0002-9635-9418

[A] Інститут державного управління та наукових досліджень з цивільного захисту, м. Київ, Україна
[B] Державна служба України з надзвичайних ситуацій, м. Київ, Україна
[C] Національний університет цивільного захисту України, м. Харків, Україна
[D] Гуманітарна міжнародна організація "The Halo Trust", м. Київ, Україна
[E] ГУ ДСНС України в Полтавській області, м. Полтава, Україна
[F] Національний авіаційний університет, м. Київ, Україна

[A] Institute of Public Administration and Scientific Research on Civil Protection, Kyiv, Ukraine
[B] State Emergency Service of Ukraine, Kyiv, Ukraine
[C] National University of Civil Defence of Ukraine, Kharkiv, Ukraine
[D] International humanitarian organization "The Halo Trust", Kyiv, Ukraine
[E] State Emergency Service of Ukraine in Poltava region, Poltava, Ukraine
[F] National Aviation University, Kyiv, Ukraine

Received: July 22, 2024 | Revised: October 10, 2024 | Accepted: October 31, 2024

DOI: 10.33445/sds.2024.14.5.18

Мета роботи: розробка математичної моделі підвищення ефективності проведення аварійно-рятувальних робіт в умовах можливого бойового ураження.
Метод дослідження: застосування теорії множин.
Результати дослідження: вперше розроблено математичну модель підвищення ефективності проведення аварійно-рятувальних робіт в умовах можливого бойового ураження.
Теоретична цінність дослідження: обґрунтована можливість отримання закономірностей діяльності рятувальників не тільки безпосередньо в ході проведення аварійно-рятувальних робіт, але й під час їх навчання та тренування, у тому разі на спеціалізованих тренажерних (навчально-тренувальних) комплексах або за допомогою імітаційних систем, які повністю реалізуються на ЕОМ.
Практична цінність дослідження: розроблена математична модель має стати науковим підґрунтям методики скорочення часу

Purpose: development of a mathematical model for increasing the efficiency of emergency rescue operations in conditions of possible combat damage.
Method: application of set theory.
Findings: for the first time, a mathematical model for increasing the efficiency of emergency rescue operations in conditions of possible combat damage was developed.
Theoretical implications: a well-founded possibility of obtaining patterns of rescuers' activity not only directly during emergency rescue operations, but also during their training and training, in that case at specialized training (educational and training) complexes or with the help of simulation systems that are fully implemented on a computer.
Practical value of the research: the developed mathematical model should become the scientific basis of the methodology for reducing the time of emergency rescue work by rescuers of

проведення аварійно-рятувальних робіт рятувальниками ДСНС в умовах можливого бойового ураження.

Оригінальність/Цінність дослідження: визначення функціональної структури процесу розкриття закономірностей проведення аварійно-рятувальних робіт в умовах можливого бойового ураження у вигляді відповідної множини функцій розкриття закономірностей діяльності рятувальників надає можливість проводити аналіз функцій системи «рятувальник – засоби захисту та забезпечення аварійно-рятувальних робіт – надзвичайна ситуація з можливістю бойового ураження» незалежно від рівня її складності.

Обмеження дослідження/Майбутні дослідження: необхідність проведення багаточисельних експериментальних досліджень для підтвердження достовірності розробленої математичної моделі та ефективності методики скорочення часу аварійно-рятувальних робіт в умовах можливого бойового ураження на її основі.

Тип статті: аналітичний.

Ключові слова: аварійно-рятувальні роботи, бойове ураження, математична модель, ефективність.

the State Emergency Service in conditions of possible combat damage.

Originality/Value of the research: the definition of the functional structure of the process of revealing the patterns of emergency and rescue operations in the conditions of possible combat damage in the form of a corresponding set of functions of revealing the patterns of the activities of rescuers provides an opportunity to analyze the functions of the system "rescuer - means of protection and provision of emergency and rescue operations - an emergency situation with the possibility of combat damage" regardless of the level of its complexity.

Research Limitations/Future Research: the need to conduct numerous experimental studies to confirm the reliability of the developed mathematical model and the effectiveness of the methodology for reducing the time of emergency and rescue operations in conditions of possible combat damage based on it.

Paper type: analytical.

Key words: emergency and rescue operations, combat damage, mathematical model, efficiency.

Вступ

В умовах сьогодення, коли рашисти використовують підлу тактику нанесення подвійних ударів по цивільним об’єктам, націлюючись на рятувальників, які прибувають для проведення аварійно-рятувальних робіт, особовий склад Оперативно-рятувальної служби кожен день здійснює близько 200 виїздів на ліквідацію наслідків ураження ворогом населених пунктів та об’єктів інфраструктури [1].

Все це свідчить про актуальність проблеми підвищення ефективності проведення аварійно-рятувальних робіт в умовах можливого бойового ураження рятувальників.

Теоретичні основи дослідження

Проблема підвищення ефективності особового складу оперативно-рятувальних підрозділів під час проведення аварійно-рятувальних робіт розглядалась з різних сторін: з позицій загальної теорії недопущення надзвичайних ситуацій [2, 3], відповідності тому, як розвиваються надзвичайні ситуації [4, 5], організації робіт в рятувальних підрозділах [6, 7]. В усіх цих роботах у якості недоліку та напрямку, у відповідності до якого треба проводити наукові дослідження, відзначалась відсутність математичних моделей. Саме останні повинні бути основою відповідних науково-обґрунтованих рекомендацій.

Це ж зазначено і в [8], де показано, що саме детальний аналіз складних інцидентів, які доцільно розглядати у вигляді моделі, яка відображає функціонування системи “людина – техніка – середовище”, дозволить розробити рекомендації щодо підвищення ефективності функціонування цієї системи. З урахуванням цього в [9] була розроблена модель навчання служб швидкого реагування на основі великомасштабних тактико-спеціальних навчань. Але до недоліків зробленого можна відзначити, що з самого початку перед конкретними підрозділами керівництво навчання на ставило цілі, які б було можливим конкретизувати у вигляді, який можна представити у якості вихідних даних моделі. Аналогічний недолік має місце і в [10], де рекомендації розробляються за результатами аналізу реальних вихідних даних, які були отримані під час стихійних лих.

Все це підкреслює необхідність дослідження причинно-наслідкових зв’язків під час функціонування системи “людина – техніка – середовище” [11, 12]. Проте, при цьому ніде не показано, що аналіз функціональної структури процесу функціонування такої системи може надати можливість отримати всі необхідні для оцінки показники її ефективності за допомогою відповідних імітаційних моделей (як тих, що відтворюються на ЕОМ, так і фізичних).

В той же час аналіз наявних імітаційних моделей, які відтворюють проведення аварійно-рятувальних робіт [13, 14, 15] показує на проблему визначення узагальнених інтегральних характеристик, оскільки розробці оперативно-технічних рекомендацій за їх допомогою має передувати визначення тих цілей, яких має досягнути система “рятувальник – засоби забезпечення аварійно-рятувальних робіт – надзвичайна ситуація”.

В загальному випадку підхід до визначення цих цілей було зроблено в [16], де була підкреслена проблема обґрунтування обмежень як під час розрахунку як показників ефективності системи, що розглядається, так і під час визначення нормативних показників ефективності. А в умовах можливого бойового ураження це ускладнюється тим, що рятувальники використовують не тільки, загальноприйняті засоби індивідуального захисту, але й засоби противибухового захисту [17], використання яких несе як додаткове навантаження (більше 10 кг), так і обмежує рух.

Тим більше, що наявні експериментальні дослідження проведення аварійно-рятувальних робіт в умовах можливого бойового ураження і стосовно бойового розгортання пожежно-рятувальних автомобілів [18], і стосовно роботи газодимозахисників [19] в засобах бронезахисту, а також гуманітарного розмінування в радіаційно-забрудненій місцевості [20] підтвердили те, що розглянуті показники діяльності рятувальників мають суттєві (на рівні 0,05) відмінності.

Постановка проблеми

Таким чином, важливою та нерозв’язаною частиною проблеми підвищення ефективності проведення аварійно-рятувальних робіт в умовах можливого бойового ураження без зниження рівня безпеки рятувальників є відсутність узагальненої математичної моделі, яка б враховувала функціональну структуру процесу розкриття закономірностей відповідної діяльності рятувальників, завдавала властивості системи «рятувальник – засоби захисту та забезпечення аварійно-рятувальних робіт – надзвичайна ситуація з можливістю бойового ураження» у вигляді узагальнених інтегральних характеристик, а також визначала цілі імітаційної оцінки такої системи з урахуванням обмежень, пов’язаних з можливістю бойового ураження.

Методологія дослідження

Метою статті є розробка математичної моделі підвищення ефективності проведення аварійно-рятувальних робіт в умовах можливого бойового ураження.

Для її досягнення потребують вирішення наступні завдання:

- визначення функціональної структури процесу розкриття закономірностей проведення аварійно-рятувальних робіт в умовах можливого бойового ураження;
- завдання властивостей системи «рятувальник – засоби захисту та забезпечення аварійно-рятувальних робіт – надзвичайна ситуація з можливістю бойового ураження» у вигляді узагальнених інтегральних характеристик;
- визначення цілей імітаційної оцінки системи ««рятувальник – засоби захисту та забезпечення аварійно-рятувальних робіт – надзвичайна ситуація з можливістю бойового ураження;
- представлення шуканої математичної моделі у вигляді системи рівнянь.

Результати

1. Визначення функціональної структури процесу розкриття закономірностей проведення аварійно-рятувальних робіт в умовах можливого бойового ураження

Функціональна структура процесу розкриття закономірностей проведення аварійно-рятувальних робіт в умовах можливого бойового ураження може бути представлена у вигляді якісного складу функцій, їх кількості і відносини між ними. Для виконання функцій може використовуватися безліч наборів різноманітних засобів. При цьому вони повинні мати область значень у вигляді множини наборів вихідних характеристик модельованого процесу проведення аварійно-рятувальних робіт (АРР) рятувальниками.

Позначимо у вигляді $X_{НС} = \{x_{нс}\}$ множину наборів різноманітних НС у відповідності до [1], а $X_{APO}^{HC} = \{x_{apo}^{нс}\}$ – множину існуючого та такого, що створюється, можливого аварійно-рятувального обладнання.

Тоді

$$(x_{нс}, x_{apo}^{нс}) \in A_1, A_1 \subset X_{НС} \times X_{APO}^{HC}, \quad (1)$$

де $X_{\text{НС}} \times \text{X}_{\text{APO}}^{\text{HC}}$ – множина упорядкованих пар $(x_{\text{нс}}, \text{x}_{\text{apo}}^{\text{нс}})$;

A_1 – відношення, яке відображає процес отримання набору вихідних характеристик $\text{x}_{\text{apo}}^{\text{нс}}$ з у відповідності до набору $x_{\text{нс}}$ різноманітних НС.

Областю визначення відношення A_1 функціональної структури вибору аварійно-рятувального обладнання, яке є необхідним для проведення аварійно-рятувальних робіт під час ліквідації НС є множина перших координат

$$D_1(A_1) \subset X_{НС}. \quad (2)$$

Областю значень (результатів) відношення A_1 є множина других координат

$$D_2(A_1) \subset X_{APO}^{HC}. \quad (3)$$

Тобто, якщо $x_{нс_i} \in X_{НС}$, то перетин по x_i відношення A_1 є множина $x_{apo}^{нс} \in X_{APO}^{HC}$ таких, що $A_{1_i} = (x_{нс_i}, x_{apo}^{нс}) \in A_1$. Звідси видно, що для фіксованого варіанту можливої НС $x_{нс_i}$ можна встановити набір можливого аварійно-рятувального обладнання, використання якого забезпечить процес ліквідації НС.

Розмірковуючи аналогічно, позначимо $X_{APP}^{HC} = \{x_{app}^{нс}\}$ – множину аварійно-рятувальних робіт, які можуть бути виконані під час ліквідації НС. Тоді

$$(x_{нс}, x_{app}^{нс}) \in A_2, A_2 \subset X_{НС} \times X_{APP}^{HC}, \quad (4)$$

де $X_{НС} \times X_{APP}^{HC}$ – множина упорядкованих пар $(x_{нс}, x_{app}^{нс})$;

A_2 – відношення, яке відображає процес отримання набору вихідних характеристик $x_{app}^{нс}$ з у відповідності до набору $x_{нс}$ різноманітних НС.

Областю визначення відношення A_2 функціональної структури розкриття закономірностей під час ліквідації НС є множина перших координат

$$D_1(A_2) \subset X_{НС}. \quad (5)$$

Областю значень (результатів) відношення A_2 є множина других координат

$$D_2(A_2) \subset X_{APP}^{HC}. \quad (6)$$

Тобто, якщо $x_{нс_i} \in X_{НС}$, то перетин по x_i відношення A_2 є множина $x_{app}^{нс} \in X_{APP}^{НС}$ таких, що $A_{1_i} = (x_{нс_i}, x_{apo}^{нс}) \in A_2$. Звідси видно, що для фіксованого варіанту можливої НС $x_{нс_i}$ можна встановити можливий набір аварійно-рятувальних робіт, виконання яких забезпечить ліквідацію НС.

Якщо у випадку дій в умовах можливого бойового ураження множину їх різноманітних видів представити у вигляді $X_y = \{x_y\}$, а рятувальне обладнання, яке використовується для забезпечення безпеки особового складу, у вигляді $X_{33}^y = \{x_{зз}^y\}$, то

$$(x_y, x_{зз}^y) \in A_3, A_3 \subset X_y \times X_{33}^y, \quad (7)$$

де $X_y \times X_{33}^y$ – множина упорядкованих пар $(x_y, x_{зз}^y)$;

A_3 – відношення, яке відображає процес отримання набору вихідних характеристик $x_{зз}^y$ засобів захисту у відповідності до набору x_y різноманітних видів можливого бойового ураження.

Областю визначення відношення A_3 функціональної структури вибору існуючих засобів захисту, яке забезпечить безпеку рятувальників від впливу небезпечних чинників можливого бойового ураження, є множина перших координат

$$D_1(A_3) \subset X_y. \quad (8)$$

Областю значень (результатів вибору) відношення A_3 є множина других координат

$$D_2(A_3) \subset X_{33}^y. \quad (9)$$

Тобто, якщо $x_{y_i} \in X_y$, то перетин по x_{y_i} відношення A_3 є множина $x_{зз}^y \in X_{33}^y$ таких, що $A_{3_i} = (x_{y_i}, x_{зз}^y) \in A_3$. Звідси видно, що для фіксованого варіанту можливого бойового ураження x_{y_i} можна встановити набір можливих засобів захисту, використання якого забезпечить безпеку від впливу небезпечних чинників можливого бойового ураження.

Якщо ж $X_P^y = \{x_p^y\}$ множина заходів, які повинні здійснити рятувальники для забезпечення своєї безпеки в умовах можливого бойового ураження, то

$$(x_y, x_p^y) \in A_4, A_4 \subset X_y \times X_P^y, \quad (10)$$

де $X_y \times X_p^y$ – множина упорядкованих пар (x_y, x_p^y);

A_4 – відношення, яке відображає процес отримання набору вихідних характеристик x_p^y тих заходів, які рятувальники повинні здійснити у відповідності до набору x_y різноманітних видів можливого бойового ураження.

Областю визначення відношення A_4 функціональної структури розкриття закономірностей дій рятувальників щодо забезпечення свої безпеки в умовах можливого бойового ураження, є множина перших координат

$$D_1(A_4) \subset X_y. \quad (11)$$

Областю значень (результатів вибору відповідних дій щодо забезпечення безпеки рятувальників) відношення A_4 є множина других координат

$$D_2(A_4) \subset X_P^y. \quad (12)$$

Тобто, якщо $x_{y_i} \in X_y$, то перетин по x_{y_i} відношення A_4 є множина $x_p^y \in X_P^y$ таких, що $A_{4_i} = (x_{y_i}, x_p^y) \in A_4$. Звідси видно, що для фіксованого варіанту можливого бойового ураження x_{y_i} можна встановити набір дій, виконання яких забезпечить безпеку рятувальників у відповідних умовах.

Проте треба враховувати, що для забезпечення аварійно-рятувальних робіт в умовах можливого бойового ураження (АРР УБУ) треба одночасно використовувати як аварійно-рятувальне обладнання (множина $X_{APO}^{HC} = \{x_{apo}^{нс}\}$), так і відповідні засоби захисту (множина $X_{ЗЗ}^y = \{x_{зз}^y\}$), тобто має місце множина $X_{APO}^{HC+y} = X_{APO}^{HC} \times X_{ЗЗ}^y$ упорядкованих пар $(x_{apo}^{нс}, x_{зз}^y)$. Це вимагає від рятувальників вміння одночасно виконувати як дії, що пов'язанні з ліквідацією НС (множина $X_{APP}^{HC} = \{x_{app}^{нс}\}$), так і дії, що пов'язані із забезпеченням безпеки від можливого бойового ураження (множина $X_P^y = \{x_p^y\}$). Тобто має місце множина $X_{APP}^{HC+y} = X_{APP}^{HC} \times X_P^y$ упорядкованих пар $(x_{app}^{нс}, x_{зз}^y)$.

Тоді

$$(x_{apo}^{нс+y}, x_{app}^{нс+y}) \in A_5, A_5 \subset X_{APO}^{HC+y} \times X_{APP}^{HC+y}, \quad (13)$$

де $X_{APO}^{HC+y} \times X_{APP}^{HC+y}$ – множина упорядкованих пар $(x_{apo}^{нс+y}, x_{app}^{нс+y})$;

A_5 – відношення, яке відображає розкриття закономірностей діяльності рятувальників у вигляді процесу отримання набору показників $\{x_{app}^{нс+y}\}$, що характеризують дії особового складу під час проведення аварійно-рятувальних робіт без зниження рівня безпеки у відповідності до набору $\{x_{apo}^{нс+y}\}$ того обладнання, яке необхідне для проведення аварійно-рятувальних робіт, та засобів захисту від небезпечних чинників можливого бойового ураження.

Областю визначення відношення A_5 функціональної структури вибору тих аварійно-рятувальних робіт, які особовий склад повинен виконати із дотриманням умов забезпечення безпеки від впливу небезпечних чинників можливого бойового ураження під час ліквідації НС, є множина перших координат

$$D_1(A_5) \subset X_{APO}^{HC+y}. \quad (14)$$

Областю значень (результатів) відношення A_5 є множина других координат

$$D_2(A_5) \subset X_{APP}^{HC+y}. \quad (15)$$

Тобто, якщо $x_{apo}^{нс+y}{}_i \in X_{APO}^{HC+y}$, то перетин по x_i відношення A_5 є множина $x_{app}^{нс+y} \in X_{APP}^{HC+y}$ таких, що $A_{5_i} = (x_{apo}^{нс+y}{}_i, x_{app}^{нс+y}) \in A_5$. Звідси видно, що для фіксованого набору $\{x_{apo}^{нс+y}\}$ аварійно-рятувального обладнання, включаючи засоби захисту, яке є необхідним для ліквідації НС в умовах можливого бойового ураження, можна встановити набір $\{x_{app}^{нс+y}\}$ показників, які

характеризують дії проведення аварійно-рятувальних робіт рятувальниками без зниження рівня безпеки рятувальників.

Множина A_{5_i} всіх перетинів відношення A_5, що викликають зацікавленість фахівців, з одного боку представляє собою множину функцій *F* розкриття закономірностей (РЗ) проведення аварійно-рятувальних робіт під час ліквідації НС в умовах можливого бойового ураження, а з іншого – утворює фактор-множину $X_{APP}^{HC+У}$ по відношенню A_5, тобто

$$F = X_{APP}^{HC+У}/A_5 = \bigcup_{i=1}^{n} A_{5_i}, \quad (16)$$

де $X_{APP}^{HC+У}/A_5$ – фактор-множина $X_{APP}^{HC+У}$ по відношенню A_5;

n – кількість перетинів, які відповідають доцільним варіантам розкриття діяльності рятувальників під час проведення АРР УБУ із застосуванням існуючого або перспективного комплексу аварійно-рятувального обладнання та засобів захисту від можливих небезпечних чинників.

При цьому множина функцій F розкриття закономірностей проведення АРР УБУ може складатись з двох підмножин

$$F = \Omega\{\theta_j\} \cup M\{m_k\}, \quad (17)$$

де $\Omega\{\theta_j\}$ – підмножина функцій РЗ тих видів діяльності рятувальників, які здійснюються безпосередньо в процесі проведення АРР УБУ;

$M\{m_k\}$ – підмножина функцій РЗ, які виконуються за допомогою імітаційної системи.

Заміщення функцій РЗ безпосередньо в процесі проведення АРР УБУ результатами імітаційного моделювання (у тому разі у вигляді фізичного моделювання операцій і процесів, які здійснюють рятувальники) системи “рятувальник – засоби захисту та забезпечення аварійно-рятувальних робіт – надзвичайна ситуація з можливістю бойового ураження” (СРЗЗНСУ) є операцією γ переводу елементів підмножини Ω в елементи множини *M*, яка уявляє собою підмодель власне імітаційної системи $M_{APP}^{HC+У}$ проведення АРР УБУ як моделі функціонування системи СРЗЗНСУ.

Множина операцій переводу $P = \{\gamma(j)\}$ утворюється на множині всіх пар

$$P = \Omega \times M_{APP}^{HC+У}. \quad (18)$$

Тобто, множина Ω може бути повністю заміщеною множиною *M*, в результаті чого всі вихідні характеристики СРЗЗНСУ можуть бути отримані імітаційним шляхом, а сама функціональна структура процесу РЗ проведення АРР УБУ розглядатися як імітаційна система. В результаті закономірності проведення таких аварійно-рятувальних робіт можуть бути знайдені незалежно від рівня складності даної СРЗЗНСУ.

Множина результатів операції γ збігається з безліччю $S = \{s\}$ станів СРЗЗНС, перехід в які визначається діяльністю рятувальників. За аналогією з (10) та з урахуванням (11) і (12) отримаємо

$$F = M_{APP}^{HC+У}/B = \bigcup_{j=1}^{s} B_j, \quad (19)$$

де $M_{\text{APP}}^{\text{НС+У}}/B$ – фактор-множина $M_{\text{APP}}^{\text{НС+У}}$ по відношенню В;
$B_j = (\theta_j, m) \in B$ – множина всіх перетинів по θ_j відношення B, що викликають у фахівців зацікавленість, у тому разу пов'язану з, наприклад, здійсненням процесу імітації проведення аварійно-рятувальних робіт в умовах можливого бойового ураження.

Таким чином, визначення функціональної структури процесу розкриття закономірностей проведення аварійно-рятувальних робіт в умовах можливого бойового ураження у вигляді відповідної множини функцій розкриття закономірностей діяльності рятувальників надає можливість проводити аналіз функцій системи «рятувальник – засоби захисту та забезпечення аварійно-рятувальних робіт – надзвичайна ситуація з можливістю бойового ураження» незалежно від рівня її складності, оскільки дозволяє по мірі зростання складності системи процесу ліквідації надзвичайної ситуації перейти від оцінки закономірностей виконання типових операцій або процесів безпосередньо в ході проведення аварійно-рятувальних робіт перейти до їх отримання під час навчання та тренування, у тому разі на спеціалізованих тренажерних (навчально-тренувальних) комплексах, або повністю реалізувати процес оцінювання закономірностей діяльності за допомогою імітаційних систем, які повністю реалізуються на ЕОМ.

2. Завдання властивостей системи "рятувальник – засоби захисту та забезпечення аварійно-рятувальних робіт – надзвичайна ситуація з можливістю бойового ураження" у вигляді узагальнених інтегральних характеристик

Стосовно моделей функціонування СРЗЗНСУ незалежні перемінні компонентів системи є характеристиками системи, а вхідні перемінні – моделями цих характеристик. Завдання властивостей СРЗЗНСУ є необхідною, але недостатньою умовою розв'язання задач оцінки цієї системи. Ці властивості повинні бути об'єднані у визначені сукупності або виражатися у вигляді узагальнених інтегральних характеристик. Такими узагальненими характеристиками виступають показники якості СРЗЗНСУ, тобто така сукупність її властивостей, яка виражає ступінь корисності системи для зовнішнього середовища на виході імітаційної системи.

В цьому випадку показник якості СРЗЗНСУ в цілому представляє собою невпорядковану безліч

$$Q_{APP}^{НС+У} = \left\langle \left\{ Q_{APP}^{НС+У}{}_i \right\}; i = 1,2,\ldots, n_{Q_{APP}^{НС+У}} \right\rangle, \tag{20}$$

де $Q_{\text{APP}}^{\text{НС+У}}{}_i$ – *i*-ий показник якості СРЗЗНСУ;
$n_{Q_{\text{APP}}^{\text{НС+У}}}$ – кількість показників якості.

Оскільки досягнення мети системою повинно дозволити виділення її основних формальних властивостей, вона повинна бути формалізована, тобто приведена до виду, який допускає кількісну оцінку. Тоді кожен показник якості $Q_{APP}^{НС+У}$ повинен являти собою впорядковану безліч

$$Q_{APP}^{НС+У}{}_i = \left\langle \begin{matrix} \left\{ Q_{APP}^{НС+У}{}_{i_j} \right\}; j = 1,2,\ldots, n_{Q_i}; \\ Q_{APP}^{НС+У}{}_{i_1} < Q_{APP}^{НС+У}{}_{i_2} < \ldots < Q_{APP}^{НС+У}{}_{i_{n_{Q_i}}} \end{matrix} \right\rangle, \tag{21}$$

де $Q_{\text{APP}}^{\text{НС+У}}{}_{i_j}$ – *j*-е значення *i*-ого показника якості.

При цьому показники Q_i визначені за допомогою множини функцій *F* розкриття закономірностей проведення аварійно-рятувальних робіт під час ліквідації НС в умовах можливого бойового ураження на безлічі $\{x_{apo}^{нс+у}\}$ безпосередньо самої системи або ж, у відповідності до (19), на вході моделі $M_{APP}^{НС+У}$ власне імітаційної системи. Виходячи з цього, показник якості для моделі $M_{APP}^{НС+У}$ з урахуванням правил організації СРЗЗНСУ є вже часткова впорядкована безліч

$$Q_{APP}^{НС+У} = \left\langle \begin{matrix} \{Q_{APP}^{НС+У}{}_k\}; k = 1,2,\dots,n_{Q^\Sigma}; \\ Q_{APP}^{НС+У}{}_1 < Q_{APP}^{НС+У}{}_2 < \dots < Q_{APP}^{НС+У}{}_{n_{Q^\Sigma}} \end{matrix} \right\rangle = \left\langle \begin{matrix} \{Q_{APP}^{НС+У}{}_k\}; k = 1,2,\dots,n_{Q^\Sigma}; \phi \\ \varphi: K \times X_{APP}^{НС+У} \to Q_{APP}^{НС+У} \end{matrix} \right\rangle, \quad (22)$$

де $Q_{\text{APP}}^{\text{НС+У}}{}_k$ – *k*-ий показник якості СРЗЗНСУ;

$K \times X_{\text{APP}}^{\text{НС+У}}$ – декартовий твір;

K – безліч, яка впорядковує та відображає правила організації СРЗЗНСУ;

φ – відображення $K \times X_{\text{APP}}^{\text{НС+У}}$ в безліч $Q_{\text{APP}}^{\text{НС+У}}$.

Оскільки проведення аварійно-рятувальних робіт на інтервалі *T* має причинно-наслідковий характер, то в моделях СРЗЗНСУ, що розглядаються, наслідком, результатом причин, що діють на систему, буде ефект СРЗЗНСУ, тобто впорядкована безліч

$$Y_{APP}^{НС+У} = \left\langle \begin{matrix} \{Y_{APP}^{НС+У}{}_l\}; l = 1,2,\dots,n_Y; \phi \\ \varphi_1: Z \times Q_{APP}^{НС+У} \times T \to Y_{APP}^{НС+У} \end{matrix} \right\rangle, \quad (23)$$

де $Y_{\text{APP}}^{\text{НС+У}}{}_l$ – *l*-е значення ефекту на інтервалі *T*;

n_Y – кількість значень ефекту;

Z – безліч, що впорядковує, яка уявляє собою безліч закономірностей функціонування СРЗЗНСУ зі встановленими зв'язками між показниками якості системи і результатами її функціонування;

φ_1 – відображення $Z \times Q_{\text{APP}}^{\text{НС+У}} \times T$ в безліч $Y_{\text{APP}}^{\text{НС+У}}$.

Відображення φ_1 фактично уявляє собою процес визначення ефектів від реалізації конкретних складових обраного варіанту проведення АРР УБУ. Такі ефекти можуть бути отримані як після натурних досліджень, і тоді реалізація Z_l уявляє собою методику отримання емпіричних даних на інтервалі *T*, так і в результаті використання попередньо визначених функціональних залежностей

$$Y_{APP}^{НС+У}{}_l = F_l(X_{APP}^{НС+У}, T), \quad (24)$$

які фактично є закономірностями проведення аварійно-рятувальних робіт в умовах можливого бойового ураження.

Таким чином, у якості закономірності проведення аварійно-рятувальних робіт в умовах можливого бойового ураження може розглядатись функціональна залежність, яка відображає функціонування системи "рятувальник – засоби захисту та забезпечення аварійно-рятувальних робіт – надзвичайна ситуація з можливістю бойового ураження, встановлюючи об'єктивний, повторюваний за певних умов зв'язок між показниками якості системи і властивими їй ефектами функціонування в часі.

3. Визначення цілей імітаційної оцінки системи "рятувальник – засоби захисту та забезпечення аварійно-рятувальних робіт – надзвичайна ситуація з можливістю бойового ураження"

Якщо окремі властивості СРЗЗНСУ є частковими характеристиками системи, то ефективність системи є нормований до витрат ресурсів результат функціонування системи на певному інтервалі часу, тобто ефективність СРЗЗНСУ представляє собою впорядковану безліч

$$E = \left\langle \begin{matrix} \{E_m\}; m = 1,2,\ldots,n_E; E_1 < E_2 < \ldots < E_{n_E}; \\ \varphi_2 : H \times X_{APP}^{HC+У} \times Y_{APP}^{HC+У} \to E \end{matrix} \right\rangle, \quad (25)$$

де E_m – m-е значення ефективності системи, $E_m \in E$;

$X_{APP}^{HC+У}$ – витрачений ресурс, який представляє собою набір $\{x_{apo}^{нс+у}\}$ того обладнання, яке необхідне для проведення аварійно-рятувальних робіт, та $\{x_{зз}^{нс+у}\}$ засобів захисту від небезпечних чинників можливого бойового ураження;

H – безліч, яка встановлює зв'язок між витраченим ресурсом, отриманим ефектом і показниками ефективності СРЗЗНСУ;

φ_2 – відображення $H \times X_{APP}^{HC+У} \times Y_{APP}^{HC+У}$ в безліч E.

СРЗЗНСУ мають внутрішньосистемні і зовнішні (надсистемні) критерії ефективності [21]. При цьому зовнішній критерій ефективності системи повинен бути [22] величиною, яка має фізичний вимір. Це дозволяє функціонування СРЗЗНСУ розглядати у вигляді нормативної діяльності, яка передбачає забезпечення ефективності системи не нижче заданої. В цьому випадку зовнішній критерій ефективності може розглядатися як

$$E(T) \geq E^*(T) | t = T\,, \quad (26)$$

де $\mathrm{E(T)}$ – значення ефективності системи в момент часу $t = T$;

$\mathrm{E^*(T)}$ – нормативне значення ефективності системи в момент часу $t = T$.

Внутрішньосистемні критерії ефективності базуються на можливості отримання кількісної оцінки ступеня досягнення мети за допомогою безлічі формалізованих властивостей СРЗЗНСУ та, відповідно, безлічі критеріїв якості діяльності системи. Безліч показників якості діяльності організації визначає безліч критеріїв ефективності СРЗЗНСУ. Різні підходи [23,24] до отримання кількісних оцінок ефективності систем по безлічі критеріїв в кінцевому підсумку зводяться до вибору виду залежності F показника E узагальненої ефективності СРЗЗНСУ від показника її узагальненої ефективності, викликаного показниками якості, властивими системі,

$$E(T) = [Y_{APP}^{HC+У}] \quad , \quad (27)$$
$$X_{APP}^{HC+У} \leq (X_{APO}^{HC+У})^*$$
$$T \leq T^*$$

де $Y_{\mathrm{APP}}^{\mathrm{HC+У}} = \left[\left\{Y_{\mathrm{APP}}^{\mathrm{HC+У}}{}_k\right\}\right]_{Q_k \geq Q_k{}^*}$ – безліч ефектів, притаманних СРЗЗНСУ;

$Q_k{}^*, \left(\mathrm{X_{APP}^{HC+У}}\right)^*, T^*$ – відповідно, необхідні значення k-го показника якості системи, ресурсів та часу.

Тоді при виконанні умов

$$\begin{cases} Q \quad \geq Q^*, \\ X_{APP}^{HC+У} \leq \left(X_{APP}^{HC+У}\right)^*, \\ T \leq T^* \end{cases} \tag{28}$$

необхідно досягнути

$$E(T) = [Y_{APP}^{HC+У}]_{\substack{X_{APP}^{HC+У} \leq \left(X_{APP}^{HC+У}\right)^* \\ T \leq T^* \\ Q \quad \geq Q^*}} \geq E(T)^*. \tag{29}$$

Таким чином, визначення цілей оцінки системи “рятувальник – засоби захисту та забезпечення аварійно-рятувальних робіт – надзвичайна ситуація з можливістю бойового ураження” полягає у визначенні таких закономірностей функціонування цієї системи, реалізація яких за обмежень, пов’язаних з часом та якістю проведення аварійно-рятувальних робіт в умовах можливого бойового ураження, а також наявним ресурсом, який є необхідним як для здійснення визначеного комплексу робіт, так і забезпечення безпеки рятувальників, дозволить перевищити нормативне значення ефективності системи.

4. Представлення шуканої математичної моделі у вигляді системи рівнянь

Аналіз функціональної структури процесу розкриття закономірностей проведення аварійно-рятувальних робіт в умовах можливого бойового ураження (19)

$$F = M_{APP}^{HC+У}/B = \bigcup_{j=1}^{s} B_j,$$

де $M_{\text{APP}}^{\text{HC+У}}/B$ – фактор-множина $\text{M}_{\text{APP}}^{\text{HC+У}}$ по відношенню В;

$B_j = \left(\theta_j, m\right) \in B$ – множина всіх перетинів по θ_j відношення B, що викликають у фахівців зацікавленість, у тому разу пов’язану з, наприклад, здійсненням процесу імітації проведення аварійно-рятувальних робіт в умовах можливого бойового ураження;

дозволяє знайти обмеження, пов’язані із забезпеченням безпеки рятувальників під час проведення аварійно-рятувальних робіт в умовах можливого бойового ураження, та здійснити перехід до визначення закономірностей відповідної діяльності рятувальників за допомогою імітаційних систем, як таких, що реалізуються на спеціалізованих тренажерних (навчально-тренувальних) комплексах, так і таких, які реалізуються на ЕОМ.

У якості закономірності проведення АРР УБУ може розглядатись (24)

$$Y_{APP}^{HC+У} = F(X_{APP}^{HC+У}, T),$$

де $X_{\text{APP}}^{\text{HC+У}}$ – множина показників, які характеризують дії рятувальників без зниження рівня їх безпеки під час проведення аварійно-рятувальних робіт в умовах можливого бойового ураження на протязі визначеного часу *T*;

оскільки відображає функціонування системи “рятувальник – засоби захисту та забезпечення аварійно-рятувальних робіт – надзвичайна ситуація з можливістю бойового ураження”, встановлюючи об’єктивний, повторюваний за певних умов зв’язок між показниками якості системи і властивими їй ефектами функціонування.

Тоді ціллю оцінки системи “рятувальник – засоби захисту та забезпечення аварійно-рятувальних робіт – надзвичайна ситуація з можливістю бойового ураження” буде визначення таких закономірностей діяльності рятувальників $Y_{APP}^{HC+У}$, реалізація яких за обмежень,

пов'язаних з часом $T \le T^*$ та якістю $Q \le Q^*$ проведення аварійно-рятувальних робіт в умовах можливого бойового ураження, а також наявним ресурсом, який є необхідним $X_{APP}^{HC+У} \le \left(X_{APP}^{HC+У}\right)^*$ як для здійснення визначеного комплексу робіт, так і забезпечення безпеки рятувальників, дозволить (29)

$$E(T) = [Y_{APP}^{HC+У}]_{\begin{cases} X_{APP}^{HC+У} \le \left(X_{APP}^{HC+У}\right)^* \\ T \le T^* \\ Q \ge Q^* \end{cases}} \ge E(T)^*$$

отриманому значенню ефективності системи $E(T)$ перевищити його нормативне $E(T)^*$ значення.

Об'єднуючи вирази (19), (24) та (29) в систему рівнянь, отримаємо шукану математичну модель

$$\begin{cases} F = M_{APP}^{HC+У}/B = \bigcup_{j=1}^{s} B_j\,; \\ Y_{APP}^{HC+У} = F(X_{APP}^{HC+У}, T); \\ E(T) = [Y_{APP}^{HC+У}]_{\begin{cases} X_{APP}^{HC+У} \le \left(X_{APP}^{HC+У}\right)^* \\ T \le T^* \\ Q \ge Q^* \end{cases}} \ge E(T)^*. \end{cases} \quad (30)$$

Таким чином, математична модель підвищення ефективності проведення аварійно-рятувальних робіт в умовах можливого бойового ураження уявляє систему з трьох аналітичних залежностей. Перша – функціонал, який описує процес визначення обмежень, які пов'язані із забезпеченням безпеки рятувальників під час проведення аварійно-рятувальних робіт в умовах можливого бойового ураження, та закономірностей відповідної діяльності рятувальників. Друга – функціонал, який уявляє собою закономірність, що відображає функціонування системи "рятувальник – засоби захисту та забезпечення аварійно-рятувальних робіт – надзвичайна ситуація з можливістю бойового ураження", встановлюючи зв'язок між показниками якості системи і властивими їй ефектами функціонування в часі. Третя – функціонал уточнення на основі отриманих закономірностей таких правил організації системи, реалізація яких за існуючих обмежень, пов'язаних з часом, якістю проведення аварійно-рятувальних робіт в умовах можливого бойового ураження та наявним ресурсом, дозволить перевищити нормативне значення ефективності системи.

Висновки

1. Важливою та нерозв'язаною частиною проблеми підвищення ефективності проведення аварійно-рятувальних робіт в умовах можливого бойового ураження є відсутність відповідної узагальненої математичної моделі.

2. Визначення функціональної структури процесу розкриття закономірностей проведення аварійно-рятувальних робіт в умовах можливого бойового ураження у вигляді відповідної множини функцій розкриття закономірностей діяльності рятувальників надає можливість проводити аналіз функцій системи "рятувальник – засоби захисту та забезпечення аварійно-рятувальних робіт – надзвичайна ситуація з можливістю бойового ураження" незалежно від рівня її складності, оскільки дозволяє по мірі зростання складності системи процесу ліквідації надзвичайної ситуації перейти від оцінки закономірностей виконання типових операцій або процесів безпосередньо в ході проведення аварійно-рятувальних робіт перейти до їх отримання під час навчання та тренування, у тому разі на спеціалізованих

тренажерних (навчально-тренувальних) комплексах, або повністю реалізувати процес оцінювання закономірностей діяльності за допомогою імітаційних систем, які повністю реалізуються на ЕОМ.

3. У якості закономірності проведення аварійно-рятувальних робіт в умовах можливого бойового ураження може розглядатись функціональна залежність, яка відображає функціонування системи “рятувальник – засоби захисту та забезпечення аварійно-рятувальних робіт – надзвичайна ситуація з можливістю бойового ураження”, встановлюючи об'єктивний, повторюваний за певних умов зв’язок між показниками якості системи і властивими їй ефектами функціонування в часі.

4. Визначення цілей оцінки системи “рятувальник – засоби захисту та забезпечення аварійно-рятувальних робіт – надзвичайна ситуація з можливістю бойового ураження” полягає у визначенні таких закономірностей функціонування цієї системи, реалізація яких за обмежень, пов’язаних з часом та якістю проведення аварійно-рятувальних робіт в умовах можливого бойового ураження, а також наявним ресурсом, який є необхідним як для здійснення визначеного комплексу робіт, так і забезпечення безпеки рятувальників, дозволить перевищити нормативне значення ефективності системи.

Математична модель підвищення ефективності проведення аварійно-рятувальних робіт в умовах можливого бойового ураження уявляє систему з трьох аналітичних залежностей. Перша – функціонал, який описує процес визначення обмежень, які пов’язані із забезпеченням безпеки рятувальників під час проведення аварійно-рятувальних робіт в умовах можливого бойового ураження, та закономірностей відповідної діяльності рятувальників. Друга – функціонал, який уявляє собою закономірність, що відображає функціонування системи ««рятувальник – засоби захисту та забезпечення аварійно-рятувальних робіт – надзвичайна ситуація з можливістю бойового ураження», встановлюючи зв'язок між показниками якості системи і властивими їй ефектами функціонування в часі. Третя – функціонал уточнення на основі отриманих закономірностей таких правил організації системи, реалізація яких за існуючих обмежень, пов’язаних з часом, якістю проведення аварійно-рятувальних робіт в умовах можливого бойового ураження та наявним ресурсом, дозволить перевищити нормативне значення ефективності системи.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Державна служба України з надзвичайних ситуацій. URL: https://dsns.gov.ua/
2. Gibson, T.D. and Scott, N. (2019). Views from the Frontline and Frontline methodology: critical reflection on theory and practice. *Disaster Prevention and Management*, Vol. 28 No. 1, pp. 6-19. https://doi.org/10.1108/DPM-07-2018-0214
3. Garnier, E. (2019). Lessons learned from the past for a better resilience to contemporary risks. *Disaster Prevention and Management*, Vol. 28 No. 6, pp. 786-803. https://doi.org/10.1108/DPM-09-2019-0303
4. Olasunkanmi Habeeb Okunola (2019). Spatial analysis of disaster statistics in selected cities of Nigeria. *International Journal of Emergency Management*, 2019 Vol.15 No.4, pp.299 – 315. https://doi.org/10.1504/IJEM.2019.104195

5. Ralf Josef Johanna Beerens (2019). Does the means achieve an end? A document analysis providing an overview of emergency and crisis management evaluation practice in the Netherland. *International Journal of Emergency Management*, 2019 Vol.15 No.3, pp.221 – 254. https://doi.org/10.1504/IJEM.2019.102310
6. Kayvan Yousefi Mojir; Sofie Pilemalm (2016). Actor-centred emergency response systems: a framework for needs analysis and information systems development. *International Journal of Emergency Management* (IJEM), Vol. 12, No. 4, 2016, pp.435 – 456. https://doi.org/10.1504/ IJEM.2016.079844
7. Willem Treurniet; Kees Boersma; Peter Groenewegen (2019). Configuring emergency response networks. *International Journal of Emergency Management*, 2019 Vol.15 No.4, pp.316 – 333. https://doi.org/10.1504/IJEM.2019.104200
8. David E. Verbitsky (2018). Quantitative analysis and assessment of intrinsic and extrinsic factors in human-in-the-loop incidents and prevalent early failures. *International Journal of Human Factors Modelling and Simulation*, 2018, 6:2-3, 228-248. https://doi.org/10.1504/IJHFMS.2018.093208
9. David Sjoberg and Miguel Inzunza (2022). Improving emergency preparedness with a live collaboration exercise model for first responders. *International Journal of Emergency Management*, 2022, 17:3-4, 195-216. https://doi.org/10.1504/IJEM.2022.125152
10. Marjan Malešič (2021). Institutional and emergent improvisation in response to disasters in Slovenia. *International Journal of Emergency Management*, 2021, 17:2, 138-153. https://doi.org/10.1504/IJEM.2021.122932
11. Akhilesh Barve, Ram Naresh Prasad, and Devendra K. Yadav (2020). Investigating causal relationship of disaster risk reduction activities in the Indian context. *International Journal of Emergency Management*, 2020, 16:1, 1-21. https://doi.org/10.1504/IJEM.2020.110105
12. Liane Okdinawati, Made Irma Dwiputranti, and Raden Adriyani Oktora (2019). The role and multi parties interaction and coordination mechanism on disaster management. *International Journal of Emergency Management*, 2019, 15:2, 187-204. https://doi.org/10.1504/IJEM.2019.099380
13. Стрелец В. М. Многофакторная оценка пожарно-спасательных работ на станциях метрополитена. Проблемы пожарной безопасности. 2004. №.15. С. 208 -214.
14. Васильев М. В., Стрелец В. М., Тригуб В. В. Анализ многофакторной модели функционирования системы “спасатель – средства защиты и ликвидации аварии – чрезвычайная ситуация с выбросом опасного химического вещества”. Проблеми надзвичайних ситуацій. 2013. № 18. С. 22-33. URL: https://nuczu.edu.ua/sciencearchive/ProblemsOfEmergencies/vol18/Pns_2013_18_6.pdf
15. Соловйов І. І., Стрілець В. М., Львовін Д. А. Багатофакторна модель підйому водолазом-сапером вибухонебезпечного предмету. Проблеми надзвичайних ситуацій. 2021. № 34. С. 272-294. https://doi.org/10.52363/2524-0226-2021-34-20
16. Львовін Д.А., Савельєв І.В., Стрілець В.М. Формування комплексу цілей імітаційної оцінки системи “рятувальник – засоби захисту та забезпечення аварійно-рятувальних робіт – надзвичайна ситуація”. Комунальне господарство міст. 2022. № 6(173). https://doi.org/10.33042/2522-1809-2022-6-173-148-153
17. Стрілець В., Скоробогатько Т., Пруський А., Маловик І. Обґрунтування нормативів для оцінювання рівня підготовленості рятувальників до одягання захисного спорядження в комплекті із засобами бронезахисту. Надзвичайні ситуації: попередження та ліквідація, 2024, випуск 1 (8). С.101-112. https://doi.org/10.31731/2524.2636.2024.8.1.101.112
18. Белюченко Д. Ю., Стрілець В. М., Луценко Т. О., Корчагін П. О., Маловик І. В., Ребров О. В. Обґрунтування нормативів для оцінювання оперативних розгортань в засобах

бронезахисту. Проблеми надзвичайних ситуацій, 2023, випуск 2 (38). – С.25-39. https://doi.org/10.52363/2524-0226-2024-39-2

19. Скоробагатько Т.М., Пруський А.В.1, Маловик І.В.., Прокоф'єв М.І., Якіменко М.Л., Середа Д.В. Особливості діяльності газодимозахисників в умовах можливого бойового ураження. Науковий вісник: Цивільний захист та пожежна безпека. 2024. № 1(17). – С. 15-28. https://doi.org/10.33269/nvcz.2024.1.15-28
20. Степанчук С.О., Стрілець В.М., Макаров Є.О., Стрілець В.В. Порівняльний кількісний аналіз особливостей гуманітарного розмінування в радіаційно-забрудненій місцевості. Проблеми надзвичайних ситуацій, 2023, випуск 2 (38). – С. 208-223. https://doi.org/10.52363/2524-0226-2023-38-14
21. Multicultural Health and Safety Research. Final Report – Fire 20/20. – 2007. – 314 p. URL: http://fire2020.org/oldsite/MHSRPReportOnline/Frames/images/MHSRP_Report_FINALv2.3.3.pdf
22. Дружинин В.В., Конторов Д.С. Проблемы системологии. – Сов. радио, 1976. – 296 с.
23. Подиковский В.В., Гаврилов В.М. Оптимизация по последовательно применяемым критериям. – Сов. радио, 1975. – 216 с.
24. Кузьмин И.В. Оценка эффективности и оптимизации АСКУ. – Сов. радио, 1971. – 324 с.

References

1 State Service of Ukraine for Emergency Situations. Available at: https://dsns.gov.ua/

2. Gibson, T.D. and Scott, N. (2019). Views from the Frontline and Frontline methodology: critical reflection on theory and practice. *Disaster Prevention and Management*, Vol. 28 No. 1, pp. 6-19. https://doi.org/10.1108/DPM-07-2018-0214
3. Garnier, E. (2019). Lessons learned from the past for a better resilience to contemporary risks. *Disaster Prevention and Management*, Vol. 28 No. 6, pp. 786-803. https://doi.org/10.1108/DPM-09-2019-0303
4. Olasunkanmi Habeeb Okunola (2019). Spatial analysis of disaster statistics in selected cities of Nigeria. *International Journal of Emergency Management*, 2019 Vol.15 No.4, pp.299 – 315. https://doi.org/10.1504/IJEM.2019.104195
5. Ralf Josef Johanna Beerens (2019). Does the means achieve an end? A document analysis providing an overview of emergency and crisis management evaluation practice in the Netherland. *International Journal of Emergency Management*, 2019 Vol.15 No.3, pp.221 – 254. https://doi.org/10.1504/IJEM.2019.102310
6. Kayvan Yousefi Mojir; Sofie Pilemalm (2016). Actor-centred emergency response systems: a framework for needs analysis and information systems development. *International Journal of Emergency Management* (IJEM), Vol. 12, No. 4, 2016, pp. 435 – 456. https://doi.org/10.1504/ IJEM.2016.079844
7. Willem Treurniet; Kees Boersma; Peter Groenewegen (2019). Configuring emergency response networks. *International Journal of Emergency Management*, 2019 Vol.15 No.4, pp.316 – 333. https://doi.org/10.1504/IJEM.2019.104200
8. David E. Verbitsky (2018). Quantitative analysis and assessment of intrinsic and extrinsic factors in human-in-the-loop incidents and prevalent early failures. *International Journal of Human Factors Modelling and Simulation*, 2018, 6:2-3, 228-248. https://doi.org/10.1504/IJHFMS.2018.093208
9. David Sjoberg and Miguel Inzunza (2022). Improving emergency preparedness with a live collaboration exercise model for first responders. *International Journal of Emergency Management*, 2022, 17:3-4, 195-216. https://doi.org/10.1504/IJEM.2022.125152

10. Marjan Malešič (2021). Institutional and emergent improvisation in response to disasters in Slovenia. *International Journal of Emergency Management*, 2021, 17:2, 138-153. https://doi.org/10.1504/IJEM.2021.122932
11. Akhilesh Barve, Ram Naresh Prasad, and Devendra K. Yadav (2020). Investigating causal relationship of disaster risk reduction activities in the Indian context. *International Journal of Emergency Management*, 2020, 16:1, 1-21. https://doi.org/10.1504/IJEM.2020.110105
12. Liane Okdinawati, Made Irma Dwiputranti, and Raden Adriyani Oktora (2019). The role and multi parties interaction and coordination mechanism on disaster management. *International Journal of Emergency Management*, 2019, 15:2, 187-204. https://doi.org/10.1504/IJEM.2019.099380
13. Strelets, V.M. (2004). Multifactorial assessment of fire and rescue operations at metro stations. Problemy pozhezhnoi bezpeky, pp. (208 -214). Kharkiv: NUTsZU [in Ukrainian].
14. Vasyliev, M.V., Strelets, V.M., Tryhub, V.V. (2013). Analysis of a multifactorial model of the functioning of the system "rescuer – means of protection and liquidation of an accident – emergency situation with the release of a hazardous chemical substance". *Problemy nadzvychainykh sytuatsii* (pp. 22-33). Kharkiv: NUTsZU [in Ukrainian]. Available at: https://nuczu.edu.ua/sciencearchive/ProblemsOfEmergencies/vol18/Pns_2013_18_6.pdf
15. Soloviov, I. I., Strilets, V. M., Lovin, D. A. (2021). A multifactorial model of lifting an explosive object by a diver-sapper. *Problemy nadzvychainykh sytuatsii* (pp. 22-33). Kharkiv: NUTsZU [in Ukrainian]. https://doi.org/10.52363/2524-0226-2021-34-20
16. Lovin, D.A., Saveliev, I.V., Strilets, V.M. (2022). Formation of a set of goals for the simulated assessment of the system "rescuer – means of protection and provision of emergency and rescue work – emergency". *Komunalne hospodarstvo mist*, 6(173), 148-153. https://doi.org/10.33042/2522-1809-2022-6-173-148-153
17. Strilets, V., Skorobohatko, T., Pruskyi, A., Malovyk, I. (2024). Justification of standards for assessing the level of readiness of rescuers to wear protective equipment complete with body armor. Nadzvychaini sytuatsii: poperedzhennia ta likvidatsiia, 101-112. Cherkasy: ChIPB NUTsZU [in Ukrainian]. https://doi.org/10.31731/2524.2636.2024.8.1.101.112
18. Beliuchenko, D. Yu., Strilets, V. M., Lutsenko, T. O., Korchahin, P. O., Malovyk, I. V., Rebrov, O. V. (2023). Justification of standards for evaluating operational deployments in means of armor protection. *Problemy nadzvychainykh sytuatsii*, 2(38), 25-39. Kharkiv: NUTsZU [in Ukrainian]. https://doi.org/10.52363/2524-0226-2024-39-2
19. Skorobahatko, T.M., Pruskyi, A.V., Malovyk, I.V.., Prokofiev, M.I., Yakimenko, M.L., Sereda, D.V. (2024). Peculiarities of the activity of gas and smoke detectors in the conditions of a possible combat damage. Naukovyi visnyk: Tsyvilnyi zakhyst ta pozhezhna bezpeka, 1(17), 15-28. Kyiv: UNDICZ [in Ukrainian]. https://doi.org/10.33269/nvcz.2024.1.15-28
20. Stepanchuk, S. O., Strilets, V. M., Makarov, Ye. O., Strilets, V. V. (2023). Comparative analysis of the regulations of humanitarian demining in a radiation-contaminated area. *Problemy nadzvychainykh sytuatsii*, 2(38), 208-223. https://doi.org/10.52363/2524-0226-2023-38-14 [in Ukrainian].
21. Multicultural Health and Safety Research. Final Report – Fire 20/20. – 2007. 14 p. Available at: http://fire2020.org/oldsite/MHSRPReportOnline/Frames/images/MHSRP_Report_FINALv2.3.3.pdf
22. Druzhynyn,V.V., Kontorov, D.S. (1976). Problems of systemology. *Sov. Radyo*: [in Russian].
23. Podykovskyi, V.V., Havrylov, V.M. (1975). Optimization based on consistently applied criteria. *Sov. Radyo*: [in Russian].
24. Kuzmyn, I.V. (1971). Assessing the effectiveness and optimization of automated control systems. *Sov. Radyo*: [in Russian].

Системні передумови оцінювання загроз для об'єктів критичної енергетичної інфраструктури в умовах збройного протистояння в Україні

Systemic prerequisites for assessing threats to critical energy infrastructure facilities in the context of armed conflict in Ukraine

Микола Хомік [A]
Corresponding author: д.т.н., професор, головний науковий співробітник науково-дослідного управління, e-mail: nkhomik@ukr.net, ORCID: 0000-0002-1201-7702

Петро Мацько [B]
начальник управління підготовки, e-mail: petiamm79.@gmail.com

[A] Національний університет оборони України, м. Київ, Україна
[B] Командування Сил підтримки Збройних Сил України, м. Київ, Україна

Mykola Khomik [A]
Corresponding author: Dr of Sciences, Professor,, Chief Researcher of the Scientific Research Department, e-mail: nkhomik@ukr.net, ORCID: 0000-0002-1201-7702

Petro Matsko [B]
Chief of Training Directorate, e-mail: petiamm79.@gmail.com

[A] The National Defense University of Ukraine, Kyiv, Ukraine
[B] Command of the Support Forces of the Armed Forces of Ukraine, Kyiv, Ukraine

Received: October 14, 2024 | Revised: October 27, 2024 | Accepted: October 31, 2024

DOI: 10.33445/sds.2024.14.5.19

Мета роботи: полягає у розробці підходів до системного оцінювання загроз і ризиків для об'єктів критичної енергетичної інфраструктури в умовах збройного конфлікту в Україні.

Метод дослідження: використовується теорія стохастичних процесів і системний аналіз.

Практична цінність дослідження: Запропонований підхід щодо системного оцінювання загроз і ризиків для об'єктів критичної енергетичної інфраструктури в умовах збройного конфлікту. Зазначений підхід передбачає розглядати воєнно-техногенну безпеку системи критичної енергетичної інфраструктури як стохастичну систему, яка може перебувати в трьох станах. Користуючись графом "станів і переходів" було складено систему диференційних рівнянь (Колмогорова) для темпів («швидкості у часі") зміни імовірностей станів при зміні станів з відомими темпами переходів. Вирішення цієї системи рівнянь з врахуванням умов "стаціонарності» процесу переходів та "повноти" даної множини станів для їх імовірності, дозволило отримати імовірності перебування системи в кожному зі станів, математичне сподівання відвернених системою воєнно-техногенної безпеки збитків і нанесених системі збитків, тобто – потенціальний та реальний "ризик»..

Майбутні дослідження: подальші дослідження слід спрямувати на системні дослідження оцінювання загроз і ризиків системі критичної енергетичної інфраструктури в аспекті воєнно-техногенної безпеки сил оборони України.

Тип статті: теоретичний.

Ключові слова: воєнна безпека держави, воєнно-техногенна безпека, система критичної енергетичної інфраструктури, об'єкти критичної енергетичної інфраструктури, структурно-функціональна модель, оцінювання, загроза, ризик.

Purpose: is to develop approaches to the systematic assessment of threats and risks for objects of critical energy infrastructure in the conditions of the armed conflict in Ukraine.

Method: the theory of stochastic processes and system analysis is used.

Practical value of the research: The proposed approach to the systematic assessment of threats and risks for critical energy infrastructure facilities in conditions of armed conflict. This approach involves considering the military-technological security of the critical energy infrastructure system as a stochastic system that can be in three states. Using the "states and transitions" graph, a system of differential equations (Kolmogorov) was compiled for the rates ("speed in time") of changing state probabilities when changing states with known rates of transitions. Solving this system of equations, taking into account the conditions of "stationarity" of the process of transitions and the "completeness" of a given set of states for their probability, made it possible to obtain the probabilities of the system being in each of the states, the mathematical expectation of the losses averted by the military-technological security system and the losses caused to the system, that is, the potential and real "risk".

Future Research: further research should be directed to systematic studies of the assessment of threats and risks to the system of critical energy infrastructure in the aspect of military-technological security of the defense forces of Ukraine.

Paper type: theoretical.

Key words: military security of the state, military-technological security, critical energy infrastructure system, critical energy infrastructure objects, structural-functional model, assessment, threat, risk.

Вступ

Потужна і надійна енергетика країні є головною умовою функціонування усіх її сфер діяльності, а тому, в умовах збройної агресії російської федерації проти України, стає найважливішою системою стратегічних об'єктів "відповідальності" для сфери воєнної безпеки держави і її складової – воєнно-техногенної безпеки.

З початком бойових дій на Сході України, а особливо під час широкомасштабної збройної агресії російської федерації проти України утворилося нове явище – техногенна безпека суспільства в ході війни.

І зрозуміло, виникла нова парадигма, яка полягає в необхідності захисту не тільки населення, території, об'єктів від наслідків надзвичайних ситуацій, а сил оборони України. Причому, на перше місце виходить захист від надзвичайних ситуацій воєнного характеру.

В зв'язку з зазначеним, автори роблять спробу ввести нову дефініцію – воєнно-техногенна безпека сил оборони України.

На думку авторів, воєнно-техногенна безпека сил оборони України (складова воєнної безпеки держави) – стан захищеності сил оборони України від надзвичайних ситуацій воєнного характеру.

Враховуючи той факт, що на сьогоднішній день забезпечення безпеки критичної енергетичної інфраструктури є одним із ключових елементів забезпечення національної безпеки і обороноздатності виникає необхідність визначення комплексу заходів і раціонального розподілу сил для забезпечення захисту критичної енергетичної інфраструктури.

Це породжує завдання системного оцінювання загроз і ризиків в умовах швидкої зміни оперативної та воєнно-політичної обстановки при відбитті збройної агресії рф.

Теоретичні основи дослідження

Аналіз публікацій щодо рішень РНБО України [1, 2] показав, що на сьогоднішній день питання захисту критичної енергетичної інфраструктури є надзвичайно важливими для забезпечення функціонування єдиного комплексу заходів з виживання українського суспільства під час війни. Публікації Червоного Хреста підкреслюють важливість цих питань з точки зору гуманітарного вирішення захисту цивільного населення під час ударів по об'єктах енергетики, в тому числі й атомної [3, 4].

В наукових публікаціях Національного інституту стратегічних досліджень розглядаються як фундаментальні питання захисту критичної інфраструктури [5, 6] так і обґрунтування наукових підходів до оцінювання загроз і ризиків для об'єктів енергетичної інфраструктури [7].

Крім того, проблемі захисту об'єктів критичної інфраструктури, у тому числі, в аспекті накладання її на воєнно-техногенну безпеку сил оборони України присвячено низьку робіт таких вчених: М. Дівізінюк, І. Романенко, С. Чумаченко, М. Хомік, В. Коцюруба, Р. Мурасов.

Однак по сьогоднішній день немає єдиного підходу щодо вирішення завдання обґрунтування наукових підходів до оцінювання загроз і ризиків для об'єктів енергетичної інфраструктури, особливо в умовах воєнного стану.

Наведене підтверджує актуальність та перспективність обраного дослідження.

Постановка проблеми

Мета статті полягає у розробці підходів до системного оцінювання загроз і ризиків для об'єктів критичної енергетичної інфраструктури в умовах збройного конфлікту в Україні.

Результати

1. Загальний аналіз воєнно-техногенної безпеки системи критичної енергетичної інфраструктури.

З точки зору системного підходу до системи критичної енергетичної інфраструктури (СКЕІ), як сукупності взаємопов'язаних об'єктів, які забезпечують стан захищеності національних інтересів у енергетичній сфері, належать (рис. 1):

- система забезпечення енергоносіями (СЗЕН);
- система забезпечення електроенергією (СЗЕЕ);
- система теплоенергетики (СТЕ).

Система забезпечення енергоносіями включає:

- критичну інфраструктуру об'єктів добичі енергоносіїв природного походження чи інших об'єктів – джерел енергетичної сировини (вугілля, нафта, газ, уранові руди, хімічна сировина для неорганічних енергоносіїв, тощо);

- критичну інфраструктуру об'єктів їх переробки на гірничо-збагачувальних та гірничо-переробних підприємствах (у нафтопродукти, ракетне паливо, рідкий газ, активні елементи для ядерних реакторів);

- критичну інфраструктуру об'єктів постачання перероблених енергоносіїв (транспортування, накопичення, зберігання та розподіл).

Систему забезпечення електроенергією утворює інфраструктура об'єктів запасів (сховищ) енергоносіїв, об'єктів "генерування" електроенергії (теплові, атомні та гідроелектростанції) та об'єктів її постачання (лінії електропередач ЛЕП, трансформаторні підстанції (ТП) розподілу електроенергії).

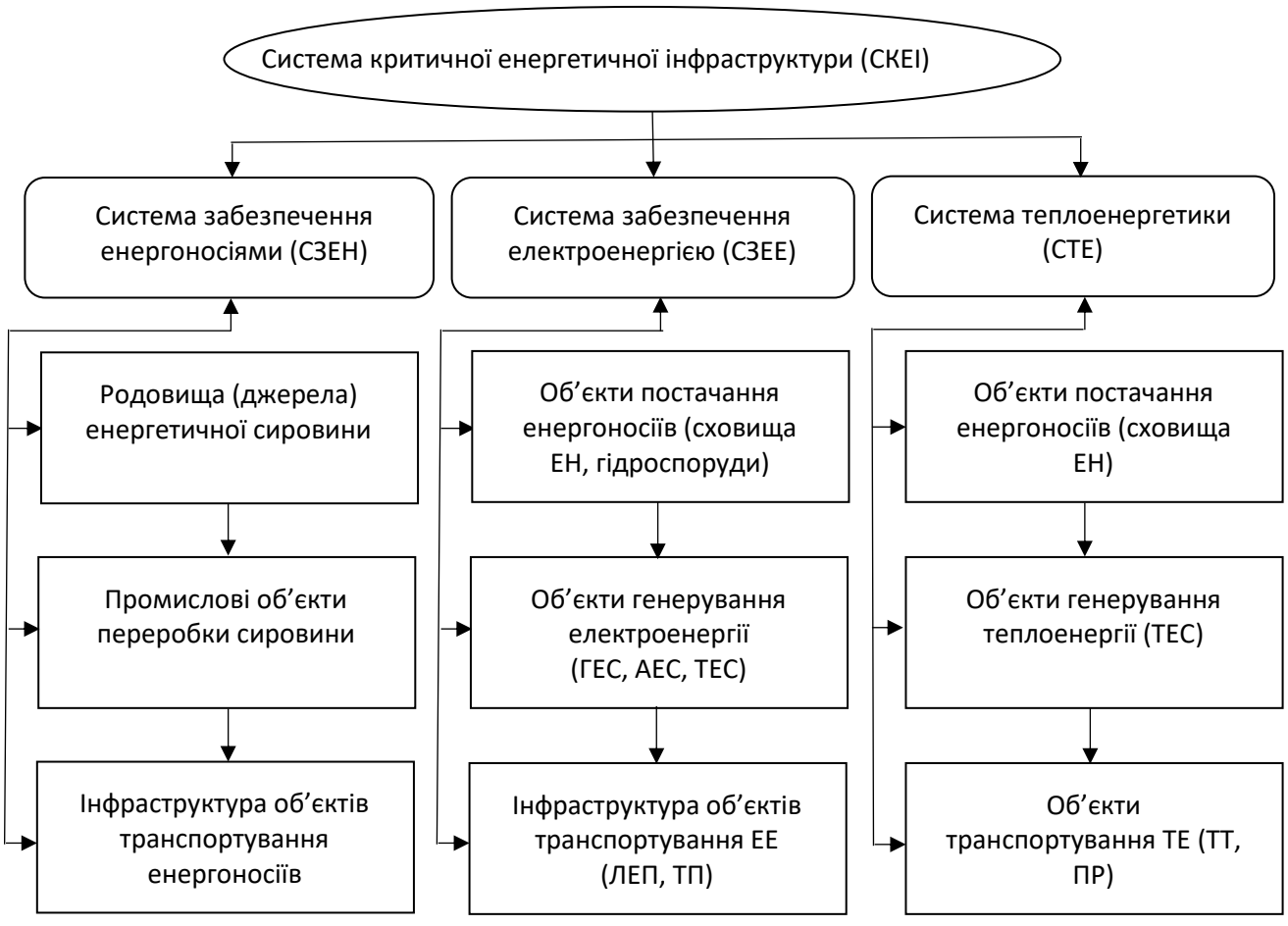


Рисунок 1 – Структурно-функціональна модель системи критичної енергетичної інфраструктури

Систему теплоенергетики утворює інфраструктура об'єктів накопичення (постачання) енергоносіїв (ЕН), об'єктів вироблення ("генерування") теплової енергії (теплоцентралі) та об'єктів її постачання (теплотраси ТТ та пункти розподілу – ПР теплоносіїв).

СКЕІ є однією із основних складових забезпечення необхідного рівня воєнно-економічного потенціалу країни, що визначає її обороноздатність. З іншого боку, сили оборони України для СКЕІ України є також одним з основних споживачів, оскільки енергоносії, електроенергія та теплова енергія в цілому є головним джерелом боєздатності ЗС.

В Сухопутних Військах споживачами великих об'ємів пального, електро- та теплової енергії є механізовані, аеромобільні й танкові частини, армійська авіація, ракетні війська і артилерія, армійська ППО, війська (сили) бойового та матеріально-технічного забезпечення.

В Повітряних Силах споживачами різнорідного пального, електро- та теплової енергії є тактична та транспортна авіація, зенітно-ракетні і радіотехнічні війська та авіація протиповітряної оборони (ППО), сили бойового та матеріально-технічного забезпечення.

У Військово-Морських Силах споживачами різнорідного пального, електро- та теплової енергії є кораблі бойового складу та складу сил забезпечення, військово-морські бази, війська (сили) берегової оборони.

Крім Збройних Сил України, споживачами значного обсягу зазначених ресурсів є Державна служба спеціального зв'язку та захисту інформації України, Державна спеціальна служба транспорту, інші військові формування, правоохоронні та розвідувальні органи.

Пальне для військ (сил) у мирний час накопичується у сховищах пально-мастильних матеріалів (ПММ) на об'єктах споживання. Під час бойових дій постачання пального військам (силам) здійснюється як "танкерними" системами (залізничний, водний та автомобільний транспорт), так і "трубопровідними" системами (стаціонарними і тимчасовими, які розгортаються на території країни у воєнний час).

Окремими об'єктами системи енергоносіїв є сховища компонентів ракетного палива. Дані компоненти (гептил й меланж) будуть знову потрібні у випадку створення балістичних ракет й авіаційно-космічних комплексів з повітряним стартом важких ракет-носіїв орбітальних об'єктів воєнного призначення (розвідки, попередження, навігації, зв'язку, управління, ударних) в інтересах оборони країни.

У мирний час Збройні Сили використовують державні системи енергетики, під час бойових дій для систем зброї і військової техніки застосовуються накопичені запаси ЕН, штатні автономні системи електро- та теплоенергетики.

Об'єкти СКЕІ завжди відносять до об'єктів захисту ("відповідальності") найбільшої оперативно-стратегічної важливості, які є для противника одними з "першочергових" об'єктів знищення або захоплення і, нажаль, мають високий ступень уразливості. Фахівцями США досліджено, що диверсійна група з 7 осіб може паралізувати мільйонне місто своїми діями саме по об'єктах СКЕІ, звичайно результати такої диверсії можуть впливати і на рівень енергетичної забезпеченості Сил оборони України.

СЗЕН мають у складі в основному стаціонарні об'єкти здобичі сировини (чи термінали зовнішніх джерел), об'єкти переробки сировини (нафтоперегінні і нафтогазові підприємства) та об'єкти транспортування ЕН (інфраструктура об'єктів "танкерного" водного, залізничного, авіаційного і автомобільного транспорту та стаціонарних об'єктів трубопровідних магістралей). Комплекси об'єктів ЕН мають масштабне у просторі розташування та значну уразливість щодо деструктивного впливу. У випадку ураження даних об'єктів можливі масштабні руйнівні та шкідливі екологічні наслідки, які пов'язані зі значними витратами сил, засобів і часу на їх ліквідацію.

СЗЕЕ мають у складі стаціонарні об'єкти накопичення ЕН (сховища пального, гідротехнічні споруди ГЕС), об'єкти генерування ЕЕ (ТЕС, ГЕС, АЕС) та об'єкти транспортування й розподілу ЕЕ. Об'єкти накопичення ЕН мають значну уразливість щодо деструктивного

впливу. Найбільш небезпечними щодо ураження об'єктами генерування ЕЕ є енергоблоки з ядерними реакторами АЕС. Наземні лінії електропередач, як об'єкти транспортування ЕЕ, найбільш уразливі щодо виведення їх з ладу та небезпечні для військ і населення при їх руйнуванні через виникнення масштабних пожеж при "короткому" замиканні в електромережах та ураження високою напругою. Кабельні лінії електропередач менш уразливі щодо руйнування, але застосовуються лише на невеликих відстанях передачі ЕЕ.

СТЕ мають у складі стаціонарні об'єкти ЕН (сховища пального), об'єкти генерування ТЕ (ТЕЦ) та об'єкти транспортування й розподілу ТЕ. Об'єкти накопичення ЕН мають значну уразливість щодо деструктивного впливу, у випадку ураження цих об'єктів можливі масштабні руйнівні та шкідливі екологічні наслідки, які пов'язані зі значними трудовитратами сил і нарядами засобів на їх ліквідацію. Об'єкти генерування та транспортування ТЕ також мають уразливість щодо деструктивного впливу, але насідки їх руйнування менш небезпечні.

Трубопровідні магістралі (ТМ) військового призначення в останній час набули поширення у збройних силах розвинутих країн. Вони розгортаються під час воєнного стану для постачання військам (силам) основних енергоносіїв (пального) для військової техніки та інших оперативно-стратегічних об'єктів.

Станції (пункти) забору (завантаження) енергоносіїв ТМ розгортаються на нафтопереробних підприємствах країни та сховищах ЕН.

Станції розподілу енергоносіїв розгортаються на об'єктах :

- аеродроми тактичної та транспортної авіації ПС;
- пункти заправки рухомої військової техніки;
- військово-морські бази ВМС;
- об'єкти військово-промислового (оборонного) комплексу;
- об'єкти критичної інфраструктури оперативно-стратегічного значення.

Кожна "нитка" ТМ від станції забору до стацій розподілу представляє собою збірний трубопровід, секція якого має діаметр навколо 12,5 см і довжину до декількох десятків метрів. Секції з'єднуються гнучким герметичним манжетом та укладаються спеціальною технікою на глибину до 0.5 м в ґрунт (до 0,5 км за годину) чи на поверхню ґрунту (до 5 км за годину). Для підтримання потрібної продуктивності транспортування енергоносіїв вздовж "нитки" ТМ через кожні приблизно 50 км розташовуються компресорні станції, пункти управління та забезпечення відповідними ресурсами. Під час транспортування трубопровід завантажується енергоносієм об'ємом приблизно 10 $м^3$ продукту на 1 погонний км, швидкість транспортування – до 25 км/год. ТМ визнана значно більш ефективним засобом постачання енергоносіїв в порівнянні з "танкерним" транспортуванням, тому буде й в майбутньому головним засобом постачання енергоносіїв військам (силам) під час проведення операцій. Але ТМ, через стаціонарне розташування своїх елементів системи на значній площі, нажаль, має підвищену уразливість як саме "ниток" трубопроводів, так і станцій забору, компресорних станцій, станцій розподілу та пунктів управління їх забезпеченням.

Таким чином, усі об'єкти СКЕІ у воєнний час безумовно можуть бути об'єктами вогневого ураження для ударної авіації і ракетних комплексів, а також об'єктами диверсійних дій з боку противника. Виведення з ладу СКЕІ противником пов'язане, по-перше, зі зривом забезпечення енергією об'єктів воєнно-економічного (оборонного) потенціалу, об'єктів усіх інших сфер діяльності країни та бойових дій угруповань військ (сил) в операціях, і, по-друге, з нанесенням величезних економічних втрат, виникненням небезпечних екологічних наслідків для об'єктів критичної інфраструктури (ОКІ), населення, навколишнього природного середовища (НПС) і безумовно, Сил оборони України. Небезпека для об'єктів енергетики стає надзвичайно великою саме через максимально високу концентрацію джерел хімічної енергії безпосередньо у енергоносіїв, так і механічної, електричної та теплової енергії на об'єктах її генерування, яка вивільняється при техногенних аваріях і катастрофах. Тому вже є багато

прикладів НС із загибеллю людей та багатомільярдними збитками через знищення ОКІ і витратами на ліквідацію наслідків катастроф – пожежі та вибухи через аварії на вугільних шахтах, нафтопереробних підприємствах і сховищах пально-мастильних матеріалів, трубопровідних магістралях, техногенні катастрофи через руйнування АЕС із радіоактивним забрудненням НПС (Чорнобиль, Фукусіма).

Існує також величезний ризик техногенних катастроф на об'єктах зберігання великих об'ємів агресивних компонент ракетного палива (гептил та меланж). Все це є наслідками низького рівня «живучості» об'єктів СКЕІ через неефективність заходів попередження і запобігання НС на них.

2. Підхід щодо системного оцінювання загроз і ризиків для об'єктів критичної енергетичної інфраструктури в умовах збройного конфлікту.

Практика експлуатації СКЕІ показує, що функції всебічної воєнно-техногенної безпеки ОКІ не можуть покладатися на персонал, який має основну функцію експлуатації СКЕІ за призначенням, і потребують створення "системи (служби) воєнно-техногенної безпеки", як підсистеми "забезпечення", з відповідними специфічними функціями.

"Живучість" об'єкта СКЕІ є здатність збереження саме його "системної функції" при "деструктивному" на нього впливі. Проблема "живучості" систем підвищеного ризику щодо виникнення воєнно-техногенної небезпеки в умовах "загроз" вимагає докладного розгляду окремих положень теорії воєнно-техногенної безпеки на ґрунті "системного підходу».

Вже існують нібито науково "канонізовані" погляди [8, 9] на визначення понять в галузі безпеки, але вони, нажаль, є евристичними і не мають підґрунтя саме системного підходу щодо аналізу безпеки "складних" систем.

"Загроза" є джерелом "небезпеки", але не її синонімом. Функціональною "загрозою" для складної системи даного призначення є виникнення умови переходу системи в стан "небезпеки", коли вона не спроможна відвернути власними силами неприйнятні (для її "існування") збитки через дію деструктивних факторів. Якщо на поточний момент часу не існує реальна можливість виникнення неприйнятних збитків, то загроза є потенціальною, якщо існує – то реальною. Це надає додаткову ознаку стану "небезпеки" системи – "потенційна небезпека" чи "реальна небезпека". Потенційна загроза пов'язана з "відкладеним" у часі ризиком, реальна – з наявним.

Так, виведення з ладу ОКІ можливим деструктивним впливом при відсутності підсистеми "попередження, запобігання й захисту" є реальною загрозою, яка усувається створенням даної підсистеми [10]. Недосконалість підсистеми "запобігання й захисту" СКЕІ (можлива її "відмова") при реальному деструктивному впливі є потенційною загрозою, яка усувається її вдосконаленням (максимізацією ефективності підсистеми).

Досягнення системою у стані небезпеки спроможності відвернути неприйнятні збитки є усуненням загрози, коли виникає умова переходу системи у стан "безпеки"

Таким чином, якщо система воєнно-техногенної безпеки СКЕІ спроможна відвернути неприйнятні збитки, то над-система "СКЕІ" знаходиться у стані "безпеки", тобто "відсутності загрози». Очевидно, стани "безпеки" та "небезпеки" складають "повну групу" станів системи СКЕІ щодо подій "наявності" чи "відсутності" загроз.

Розглянемо воєнно-техногенну безпеку СКЕІ як стохастичну систему.

Очікувані збитки при "небезпеці" (виникненні загроз) для СКЕІ поділяються на "воєнні", "матеріальні" та "екологічні". "Воєнні" збитки вимірюються зниженням "о.-с. важливості" (об'єму продукції) СКЕІ при вогневому ураженні або захопленні ОКІ противником. "Матеріальні" збитки вимірюються втратами основного ресурсу технологічної системи (персоналу й обладнання) на об'єктах СКЕІ при аваріях (катастрофах) техногенного походження. "Екологічні" збитки СКЕІ вимірюються екологічними наслідками вогневого ураження чи надзвичайних ситуацій техногенного походження на об'єктах СКЕІ.

"О.-с. важливість" для СКЕІ багатьма розвиненими країнами розуміється як "вартість" об'єктів системи (при їх втраті) чи вартість їх відновлення (при руйнуванні). Воєнний аспект "О.-с. важливості" припускає її оцінку кількісною мірою "впливу" СКЕІ на утримання стану воєнної безпеки силами оборони України, тому "О.-с. важливість" доцільно вимірювати безрозмірним показником ($0 \le C \le 100$), значення якого є, як правило, експертною оцінкою.

СКЕІ щодо її воєнно-техногенної безпеки розглядається як "стохастична система", яка може перебувати в наступних станах (рис. 2):

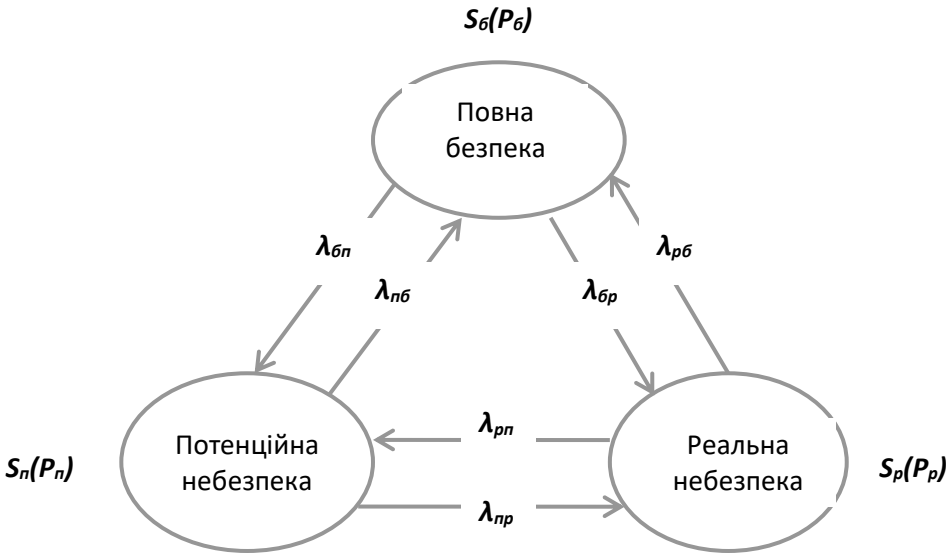


Рисунок 2 – Граф станів й переходів стохастичної системи СКЕІ

де $S_б$ – стан, коли СКЕІ здатна відвернути неприпустимі для її існування збитки власним ресурсом (ознака стану – "повна безпека");

$S_п$ – стан, коли СКЕІ не здатна відвернути неприпустимі для її існування потенційні збитки власним ресурсом (ознака стану – "потенційна небезпека");

$S_р$ – стан, коли СКЕІ не здатна відвернути неприпустимі для її існування реальні збитки власним ресурсом (ознака стану – "реальна небезпека").

Множина даних станів складає так звану "повну групу", для якої сума ймовірностей перебування СКЕІ в кожному відповідному стані $(P_б, P_п, P_р)$ дорівнює одиниці.

У поточному часі СКЕІ знаходиться в одному з перелічених станів, змінюючи їх випадковим чином як по "напрямку", так і по "моменту часу", за дією впливів випадкових подій:

"виникнення реальної загрози" з темпом у часі $\lambda_{бп}$;

"усунення реальної загрози" з темпом у часі $\lambda_{рб}$;

"виникнення потенційної загрози" з темпом у часі $\lambda_{бп}$;

"усунення потенційної загрози" з темпом у часі $\lambda_{пб}$;

"перетворення потенційної загрози в реальну" з темпом у часі $\lambda_{пр}$;

"перетворення реальної загрози в потенційну" з темпом у часі $\lambda_{рп}$.

Впливи подій із "загрозами" вважаються "пуассонівськими", причому інтенсивності подій "виникнення (чи збільшення) загрози" визначаються зовнішніми факторами, а подій "усунення (чи зменшення) загрози" – внутрішніми факторами, пов'язаними з "можливостями" системи щодо "середніх" витрат часу τ на усунення реальної (чи потенційної) загрози –

$$\lambda_{рб} = (1/\tau_{рб}); \ \lambda_{пб} = (1/\tau_{пб}); \ \lambda_{рп} = (1/\tau_{рп}). \quad (1)$$

Тому СКЕІ з розглянутим внутрішнім процесом зміни “станів” типу “неперервний ланцюг Маркова” слід вважати “стохастичною системою” щодо її функціональної сталості. Проаналізуємо дану стохастичну систему .

Користуючись графом “станів і переходів” (рис. 2), складемо систему диференційних рівнянь (Колмогорова) для темпів (“швидкості у часі”) зміни імовірностей станів *($S_б$, $S_п$, $S_р$)* при зміні станів з відомими темпами переходів (λ) для системи –

$$\begin{aligned}
\frac{dp_б}{dt} &= -(\lambda_{бп} + \lambda_{бр}) \cdot p_б(t) + \lambda_{пб} \cdot p_п(t) + \lambda_{рб} \cdot p_р(t) \\
\frac{dp_п}{dt} &= \lambda_{бп} \cdot p_б(t) - (\lambda_{пб} + \lambda_{пр}) \cdot p_п(t) + \lambda_{рп} \cdot p_р(t) \\
\frac{dp_п}{dt} &= \lambda_{бр} \cdot p_б(t) + \lambda_{пр} \cdot p_п(t) - (\lambda_{рб} + \lambda_{рп}) \cdot p_р(t).
\end{aligned} \tag{2}$$

Запишемо умову “стаціонарності” процесу переходів (для $t \to \infty$), коли похідні за часом обертаються в нуль і поточні ймовірності станів досягають відповідних асимптотичних значень ($P_б$, $P_п$, $P_р$); тобто –

$$\begin{aligned}
-(\lambda_{бп} + \lambda_{бр})P_б + \lambda_{пб}P_п + \lambda_{рб}P_р &= 0 \\
\lambda_{бп}P_б - (\lambda_{пб} + \lambda_{пр})P_п + \lambda_{рп}P_р &= 0 \\
\lambda_{бр}P_б + \lambda_{пр}P_п - (\lambda_{рб} + \lambda_{рп})P_р &= 0.
\end{aligned} \tag{3}$$

Дана система лінійних рівнянь є “лінійно залежною”, бо сума будь-яких двох з них дорівнює третьому. Тому виключимо з даної системи, наприклад, останнє (третє), замість якого додамо рівняння умови “повноти” даної множини станів для їх імовірності; одержимо

$$\begin{aligned}
-(\lambda_{бп} + \lambda_{бр})P_б + \lambda_{пб}P_п + \lambda_{рб}P_р &= 0 \\
\lambda_{бп}P_б - (\lambda_{пб} + \lambda_{пр})P_п + \lambda_{рп}P_р &= 0 \\
P_б + P_п + P_р &= 1.
\end{aligned} \tag{4}$$

Вирішимо дану систему рівнянь (наприклад, методом Крамера).

Детермінант системи –

$$\Delta = \begin{Vmatrix} -(\lambda_{бп} + \lambda_{бр}) & \lambda_{пб} & \lambda_{рб} \\ \lambda_{бп} & -(\lambda_{пб} + \lambda_{пр}) & \lambda_{рп} \\ 1 & 1 & 1 \end{Vmatrix}, \tag{5}$$

часткові детермінанти (для стовпчика “вільних” членів системи рівнянь) відповідно –

$$\Delta_б = \begin{Vmatrix} 0 & \lambda_{пб} & \lambda_{рб} \\ 0 & -(\lambda_{пб} + \lambda_{пр}) & \lambda_{рп} \\ 1 & 1 & 1 \end{Vmatrix}, \tag{6}$$

$$\Delta_n = \begin{Vmatrix} -(\lambda_{бп} + \lambda_{бр}) & 0 & \lambda_{рб} \\ \lambda_{бп} & 0 & \lambda_{рп} \\ 1 & 1 & 1 \end{Vmatrix}, \quad (7)$$

$$\Delta_p = \begin{Vmatrix} -(\lambda_{бп} + \lambda_{бр}) & \lambda_{пб} & 0 \\ \lambda_{бп} & -(\lambda_{пб} + \lambda_{пр}) & 0 \\ 1 & 1 & 1 \end{Vmatrix}. \quad (8)$$

Остаточно рішенням даної системи рівнянь є “асимптотичні” значення імовірності перебування системи в кожному стані –

$$P_б = (\Delta_б / \Delta), \; P_п = (\Delta_п / \Delta), \; P_р = (\Delta_б / \Delta). \quad (9)$$

Саме значення імовірності $P_б$ слід вважати оцінкою “живучості”, а значення $P_р$ – оцінкою “вразливості” системи.

Якщо дана система енергетики має оперативно-стратегічну важливість *AS*, то завдяки “повноті групи подій” (станів “безпеки” та “небезпеки” СКЕІ) математичне сподівання відвернених системою воєнно-техногенної безпеки збитків –

$$VS = P_б \times AS, \quad (10)$$

і математичне сподівання нанесених системі збитків (потенціальний та реальний “ризик”) –

$$WS_п = P_п \times AS; \; WS_р = P_р \times AS. \quad (11)$$

Висновки

В ході проведеного дослідження:

1. Проведений аналіз воєнно-техногенної безпеки системи критичної енергетичної інфраструктури. На основі цього аналізу була узагальнена структурно-функціональна модель системи критичної енергетичної інфраструктури з точки зору воєнно-техногенної безпеки сил оборони України.

2. Запропонований підхід щодо системного оцінювання загроз і ризиків для об’єктів критичної енергетичної інфраструктури в умовах збройного конфлікту. Зазначений підхід передбачає розглядати воєнно-техногенну безпеку системи критичної енергетичної інфраструктури як стохастичну систему, яка може перебувати в трьох станах: “повна безпека”; “потенційна небезпека”; “реальна небезпека”.

3. Користуючись графом “станів і переходів” було складено систему диференційних рівнянь (Колмогорова) для темпів (“швидкості у часі”) зміни імовірностей станів при зміні станів з відомими темпами переходів.

Вирішення цієї системи рівнянь з врахуванням умов “стаціонарності” процесу переходів та “повноти” даної множини станів для їх імовірності дозволило отримати імовірності перебування системи в кожному зі станів, математичне сподівання відвернених системою воєнно-техногенної безпеки збитків та математичне сподівання нанесених системі збитків, тобто – потенціальний та реальний “ризик”.

4. Запропоновано створення системи (служби) воєнно-техногенної безпеки, як підсистеми забезпечення захисту критичної енергетичної інфраструктури в умовах ведення бойових дій з відповідними специфічними функціями запобігання, попередження і ліквідації надзвичайних ситуацій воєнного характеру.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Олександр Литвиненко: Важливо максимально підсилити рівень організації інженерного захисту об'єктів критичної інфраструктури. URL: https://www.ukrinform.ua/rubric-economy/3854309-zahist-kriticnoi-infrastrukturi-sekretar-rnbo-proviv-naradu.html.
2. Про організацію захисту та забезпечення безпеки функціонування об'єктів критичної інфраструктури та енергетики України в умовах ведення воєнних дій: Рішення Ради Національної Безпеки і Оборони України від 17 жовтня 2023 року. Введено в дію Указом Президента України від 17 жовтня 2023 року № 695/2023. URL: https://zakon.rada.gov.ua/laws/show/n0040525-23#Text.
3. Коли гасне світло: Захист енергетичної інфраструктури в умовах збройного конфлікту. URL: https://blogs.icrc.org/ua/2023/07/203/6217/.
4. Еббі Зейт та Ейріні Гіоргу, Небезпечні сили: захист атомних електростанцій в умовах збройного конфлікту, 18 жовтня 2022 року. URL: https://blogs.icrc.org/law-and-policy/2022/10/18/protection-nuclear-power-plants-armed-conflict/.
5. Суходоля О. М. Захист енергетичної інфраструктури: аналіз української законодавчої бази. Аналітична записка. URL: http://www.niss.gov.ua/articles/1568/.
6. Бірюков Д. С., Кондратов С. І. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні. Аналітична доповідь. – К.: НІСД, 2012. – 57 с.
7. Оцінка загрози ядерного тероризму: проектна загроза: Науково-методологічний посібник / С. І. Кондратов, Ю. М. Скалецький, В. І. Кравцов та ін.; за заг. ред. В. П. Горбуліна. – К.: ДП «НВЦ «Євроатлантикінформ», 2006. – 76 с.
8. Качинський А. Безпека, загрози і ризик: наукові концепції та математичні методи. – К.: "Поліграфконсалтинг", 2004. – 472 с.
9. Машков О. А, Іващенко Т. Г., Мухін Є. А., Мухіна К. Є., Триснюк В. М., Чумаченко С. М. Системний підхід в екологічних науках: системний аналіз та синтез управлінських екологічних рішень. – Монографія. — Дніпро: Адверта, Середняк Т.К., 2023. – 674 с. – ISBN 978-617-8245-31-3.
10. Потій О. Україна починає будувати систему захисту критичної інфраструктури відповідно до найкращих світових практик та чинних вимог європейського законодавства. URL: https://cip.gov.ua/ua/news/ukrayina-pochinaye-buduvati-sistemu-zakhistu-kritichnoyi-infrastrukturi-vidpovidno-do-naikrashikh-svitovikh-praktik-ta-chinnikh-vimog-yevropeiskogo-zakonodavstva.

References

1 Oleksandr Lytvynenko: It is important to maximize the level of organization of engineering protection of critical infrastructure facilities. Available from : https://www.ukrinform.ua/rubric-economy/3854309-zahist-kriticnoi-infrastrukturi-sekretar-rnbo-proviv-naradu.html.
2. On the organization of protection and ensuring the safety of the functioning of critical infrastructure and energy facilities of Ukraine in the conditions of hostilities: Decision of the National Security and Defense Council of Ukraine of October 17, 2023. Enacted by the Decree

of the President of Ukraine of October 17, 2023 No. 695/2023. Available from : https://zakon.rada.gov.ua/laws/show/n0040525-23#Text.
3. When the lights go out: Protection of energy infrastructure in the context of armed conflict. Available from : https://blogs.icrc.org/ua/2023/07/203/6217/.
4. Ebbi Zeit, Eirini Hiorhu, Dangerous Forces: Protecting Nuclear Power Plants in Armed Conflict, October 18, 2022. Available from : https://blogs.icrc.org/law-and-policy/2022/10/18/protection-nuclear-power-plants-armed-conflict/.
5. Sukhodolia O. M. Protection of Energy Infrastructure: Analysis of the Ukrainian Legislative Framework. Analytical note. Available from : http://www.niss.gov.ua/articles/1568/.
6. Biriukov D. S., Kondratov S. I. Critical Infrastructure Protection: Problems and Prospects for Implementation in Ukraine. Analytical report. – Kyiv: NISR, 2012. – 57 p.
7. Nuclear Terrorism Threat Assessment: Projected Threat: A scientific and methodological guide / S. I. Kondratov, Yu. M. Skaletskyi, V. I. Kravtsov та and others; under the general editorship V. P. Horbulina. – Kyiv: State-owned enterprise «Scientific and publishing center «Yevroatlantykinform», 2006. – 76 p.
8. Kachynskyi A. Security, threats and risk: scientific concepts and mathematical methods. – K.: "Polihrafkonsaltynh", 2004. – 472 p.
9. Mashkov O. A, Ivashchenko T. H., Mukhin Ye. A., Mukhina K. Ie., Trysniuk V. M., Chumachenko S. M. Systems approach in environmental sciences: system analysis and synthesis of environmental management decisions. – Monograph. – Dnipro: Adverta, 2023. – 674 p. – ISBN 978-617-8245-31-3.
10. Potii O. Ukraine begins to build a critical infrastructure protection system in accordance with the best international practices and current requirements of European legislation. Available from : https://cip.gov.ua/ua/news/ukrayina-pochinaye-buduvati-sistemu-zakhistu-kritichnoyi-infrastrukturi-vidpovidno-do-naikrashikh-svitovikh-praktik-ta-chinnikh-vimog-yevropeiskogo-zakonodavstva.

Оцінювання оборонних спроможностей за скороченою процедурою

Capabilities based assessment under a shortened procedure

Віктор Корендович [A]
Corresponding author: кан. техн. наук, доцент, професор кафедри, e-mail: vkorendovych@gmail.com, ORCID: 0000-0003-2949-1870

Сергій Ясенко [A]
кан. техн. наук, доцент, e-mail: gm1serhiiyasenko@gmail.com, ORCID: 0000-0003-1918-9459

Микола Ткач [A]
д. економ. наук, доцент, e-mail: nyck1985@ukr.net, ORCID: 0000-0002-8832-1268

Максим Кіріакіді [B]
Здобувач наукового ступеня, начальник Інституту, e-mail: nyck1985@ukr.net, ORCID: 0000-0003-4050-3377

Олег Візенкін [C]
начальник управління планування спроможностей Головного управління оборонного планування, e-mail: nyck1985@ukr.net

Віктор Дерев'янко [A]
кан. техн. наук, e-mail: derevianko.trainer@gmail.com, ORCID: 0009-0002-4568-4461

Victor Korendovych [A]
Corresponding author: Candidate of Technology Sciences, Associate Professor, Professor of the Department, e-mail: vkorendovych@gmail.com, ORCID: 0000-0003-2949-1870

Sergiy Yasenko [A]
Candidate of Technology Sciences, Associate Professor, e-mail: gm1serhiiyasenko@gmail.com, ORCID: 0000-0003-1918-9459

Mykola Tkach [A]
Dr Sciences, Associate Professor, e-mail: nyck1985@ukr.net, ORCID: 0000-0002-8832-1268

Maksym Kiriakidi [B]
PhD student, Head of the Institute, e-mail: nyck1985@ukr.net, ORCID: 0000-0003-4050-3377

Oleg Vizenkin [C]
Head of the Capability Planning Department of the Main Directorate of Defense Planning, e-mail: nyck1985@ukr.net

Victor Derevianko [A]
Candidate of Technology Sciences, e-mail: derevianko.trainer@gmail.com, ORCID: 0009-0002-4568-4461

[A] Національний університет оборони України, м. Київ, Україна
[B] Інституту Військово-Морських Сил Національного університету "Одеська Морська Академія", м. Одеса, Україна
[C] Генеральний штаб ЗС України, м. Київ, Україна

[A] National Defense University of Ukraine, Kyiv, Ukraine
[B] Institute of Naval Forces of the National University "Odesa Maritime Academy", Odesa, Ukraine
[C] General Staff of the Armed Forces of Ukraine, Kyiv, Ukraine

Received: October 4, 2024 | Revised: October 20, 2024 | Accepted: October 31, 2024

DOI: 10.33445/sds.2024.14.5.20

Мета роботи: опис методики оцінювання оборонних спроможностей за скороченою процедурою.
Метод: аналітичний та експертний методи оцінювання оборонних спроможностей.
Результати дослідження: методика оцінювання оборонних спроможностей за скороченою процедурою, яка відповідає принципам оцінювання оборонних спроможностей, які прийняті в провідних країнах НАТО.
Теоретична цінність дослідження: теоретичний та практичний механізм оцінювання оборонних спроможностей, що базується на принципах НАТО.
Тип статті: описовий, методичний.

Purpose: to describe the methodology for assessing defense capabilities using a shortened procedure.
Method: analytical and expert methods of assessing defense capabilities.
Research results: a methodology for assessing defense capabilities using a shortened procedure that meets the principles of defense capability assessment adopted by leading NATO countries.
Theoretical value of the study: a theoretical and practical mechanism for assessing defense capabilities based on NATO principles.
Type of article: descriptive, methodological.

Ключові слова: спроможності Збройних Сил України, методика оцінювання спроможностей, оцінювання спроможностей за скороченою процедурою.

Key words: capabilities of the Armed Forces of Ukraine, methodology of capabilities assessment, assessment of capabilities by the shortened procedure.

Вступ

В системі заходів оборонного планування оцінюванню спроможності (ОС) належить особливе місце. ОС присутнє в заходах довгострокового планування (його результати використовуються при огляді спроможностей); в рамках середньострокового планування результати ОС використовують в ході розробки програмних документів розвитку спроможностей; в короткостроковому плануванні – в ході розробки планів утримання та розвитку ЗС. Крім зазначеного, результати ОС є вихідними даним для проектної діяльності та вирішення інших практичних завдань розвитку спроможностей.

Методика ОС визначена військовим стандартом [1]. Проведені в період 2017-2021 рр.

оцінювання низки спроможностей довели коректність методики. Водночас тривала агресія рф обумовила нові вимоги до методики: бути придатною до використання в умовах правового режиму воєнного стану у стислих часових рамках (чинний стандарт передбачає значну тривалість оцінювання) та меншим за чисельністю персоналом, який безпосередньо проводить ОС; оперативно враховувати досвід реалізації спроможності в ході війни; забезпечувати оцінювання комплексних спроможностей (більшість оперативних спроможностей є саме такі); бути основою для проведення оглядів спроможностей; надавати об'єктивні дані для пріоритезації спроможностей.

Теоретичні основи дослідження

Система оборонного планування перебуває в процесі постійного вдосконалення. Це стосується і процедур оцінювання спроможностей. Досить системно процес ОС представлений у документах США. Теоретичні та практичні аспекти функціонування системи управління розвитком спроможностей у Збройних Силах США, і оцінювання спроможностей зокрема, регулярно оновлюються та викладаються у відкритих виданнях, зокрема [2, 3, 4]. У [5] представлено методичний підхід до оцінювання спроможностей міжвидового угруповання військ в інтересах оборонного планування. Практичні питаннях розвитку спроможностей наведені у низці робіт, які опубліковані після 2022 року. У [6] розглянуто питання оцінювання та прогнозування приросту рівня спроможностей Збройних Сил. Актуальні питання автоматизації оцінювання оборонних спроможностей за рахунок використання профільного програмного забезпечення наведено в [7].

Водночас питання методики та процедур оцінювання спроможностей в умовах дії правового режиму воєнного стану (коли цей процес має враховувати досвід реалізації спроможностей на полі бою) та здійснюватися у стислих часових рамках у вітчизняних дослідженнях не наводиться.

Постановка проблеми

Наведене вище свідчить про існування проблеми невідповідності методології, процедур та часових рамок оцінювання оборонних спроможностей, які визначені чинним військовим стандартом, вимогам обґрунтування рекомендацій щодо розвитку спроможностей в умовах правового режиму воєнного стану в Україні. Розробка методики оцінювання спроможностей, що задовольняє зазначеним вимогам, є актуальним науковим та практичним заданням.

Методологія дослідження

Пропонується для розробки методики оцінювання спроможностей ЗС України в умовах правового режиму воєнного стану в Україні, з врахуванням наведених вище вимог, застосувати підхід щодо полягає у проведенні ОС за скороченою процедурою. При цьому доцільно зберегти принципи ОС, які визначені нормативними документами Міністерства оборони та чинним військовим стандартом [1, 8, 9], а саме: самокорегованість (гнучкість) процесу; об'єктивність та неупередженість; використання методології аналітичного дослідження; зосередженість на спроможностях, які ЗС потребуватимуть у майбутньому.

Досягнення балансу між вимогами до ОС за скороченою процедурою та збереженням існуючих принципових засад ОС дозволяє визначити такі напрями вирішення проблеми:

А) *скорочення часових рамок ОС шляхом*: запровадження інформаційних технологій щодо автоматизації виконання окремих завдань; використання результатів аналізу досвіду реалізації спроможностей в період бойових дій; позбавлення від надлишкових та часо-витратних процедур;

B) *зменшення кількості фахівців*, які безпосередньо проводять оцінювання, шляхом створення умов та процедур, які дозволяють експертам брати участь в ОС дистанційно;

C) *забезпеченням наочності процесу* оцінювання на всіх його етапах шляхом гармонізації процедур оцінювання та їх відображення в єдиному доступному для всіх учасників документі та форматі, який можна опрацьовувати одночасно багатьма виконавцями;

D) *розроблення процедур оцінювання комплексних спроможностей,* які реалізують війська (сили), що належать до різних видів, родів військ (сил) шляхом декомпозиції спроможності з наступним узагальнення результатів.

Структурно-логічна схема ОС за скороченою процедурою за наведеними вище напрямами наведена на рис. 1.

Процес ОС включає 4 етапи [1]:

I етап – підготовчий (ініціювання ОС);

II етап – аналіз вимог;

III етап – аналіз недоліків (прогалин);

IV етап – аналіз рішень, в рамках якого розроблюють рекомендації щодо розвитку спроможності.

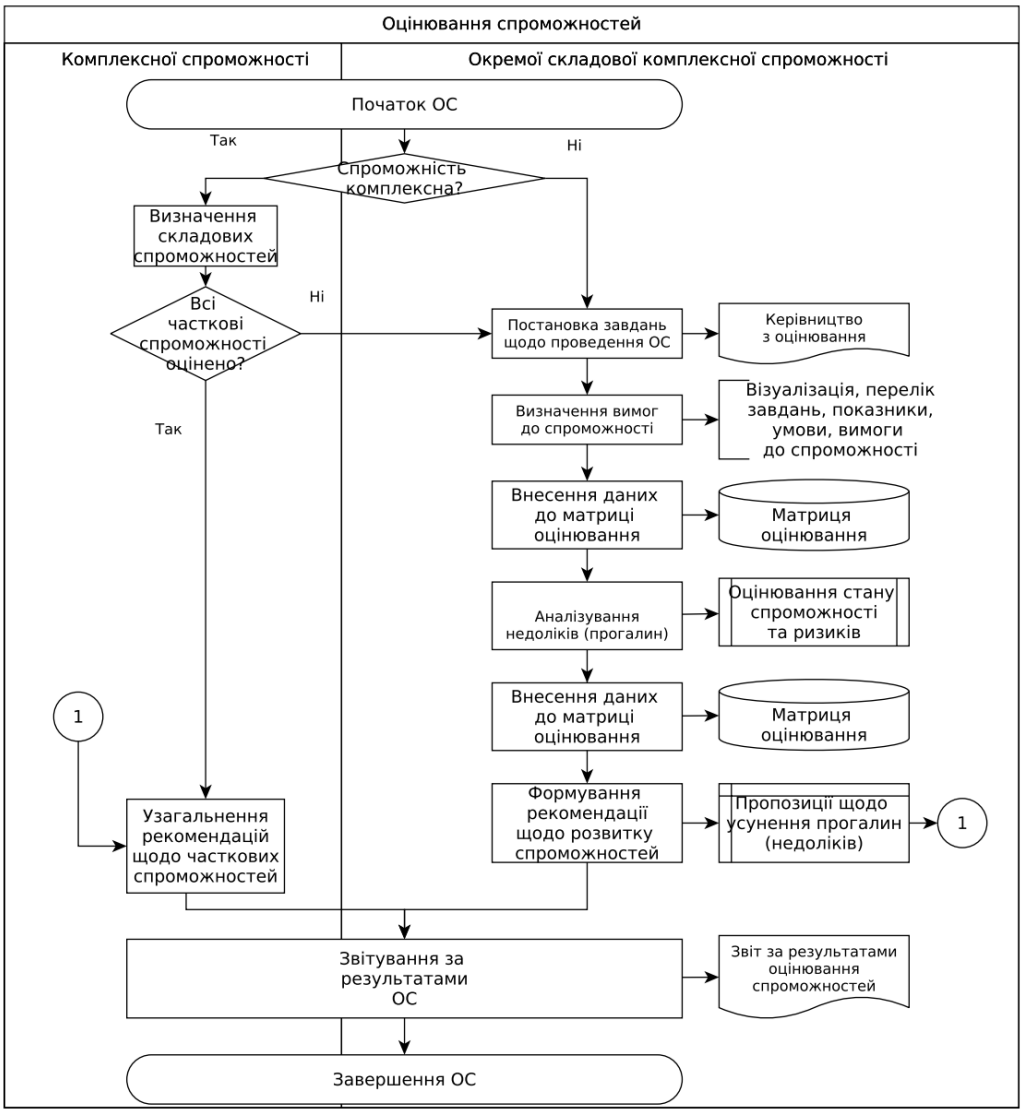


Рисунок 1 – Структурно-логічна схема оцінювання спроможності за скороченою процедурою

Перший етап охоплює заходи з організації проведення ОС. До них належать: ініціювання ОС; формування робочої групи (РГ); визначення порядку, умов та методології проведення ОС; розробка Керівництва з проведення ОС (за скороченою процедурою). Склад РГ має бути мінімально достатнім для проведення оцінювання в стислих часових рамках із залученням необхідних фахівців (експертів) в режимі on-line.

Другий, третій та четвертий етапи реалізують за підтримки матриці оцінювання спроможностей (далі матриця оцінювання), яка виконана у форматі електронних таблиць, наприклад Excel.

Використання електронних таблиць забезпечує наочність процедур кожного етапу, використання математичного апарату для проведення розрахунків щодо підтримки рекомендацій, залучення експертів для ОС в режимі on-line. Матриця оцінювання також в перспективі має забезпечити обмін результатами ОС в процедурах архітектури оборонних та безпекових інституцій [10].

Матриця оцінювання (її структура наведена в табл.1) побудована на декількох аркушах електронних таблиць Excel: “1 – оцінювання спроможності”; “2 – аналіз недоліків”; “3 – рекомендації”; “4 – план реалізації”; “5 – графік реалізації”; “6 – комплексна спроможність”.

В межах етапу аналізу вимог РГ на основі аналізу часткового сценарію (варіанту) виникнення та розвитку ситуації воєнного характеру (далі – сценарій) здійснює візуалізацію спроможності та визначає завдання та під-завдання, які мають бути виконані при реалізації спроможності. При цьому також враховують вимоги Єдиного переліку (каталогу) спроможностей [11], Перелік типових завдань [12]. Перелік завдань і під-завдань формують та зазначають в матриці оцінювання (табл.1, стовпчик 2). Залучення експертів в режимі on-line проводиться з використанням програмних засобів та технологій “розробки на основі єдиної бази”, “групової роботи” тощо. Прикладом можуть бути: Google Docs, Microsoft SharePoint, DocBook, програмні засоби на основі різних рішень реляційних баз даних тощо. Це дозволяє заносити дані до матриці оцінювання членами РГ одночасно.

Робоча група також визначає мету (очікуваний ефект) завдань та під-завдань; умови їх виконання; показники оцінювання рівня успішності досягнення ефекту (кінцевого результату) стосовно завдань; формулює вимоги до спроможності щодо виконання завдань (під-завдань). Вимога має визначати результат/ефект та кінцевий вплив, який має бути досягнутий виконанням під-завдання (завдання, якщо воно не складається з під-завдань) у визначених умовах і який вимірюється відповідним показником. Також вимога має зазначати носії спроможності (структури, підрозділи), які досягають визначений ефект. Дані заносять у стовпчики 3, 4, 5, 6 табл.1.

Сформовані робочою групою вимоги до спроможності дозволяють залучити інших експертів до участі в ОС на наступних етапах. Для цього матриця оцінювання (аркуші “1 – оцінювання спроможності”, “2 – аналіз недоліків”, “3 – рекомендації”) розсилається визначеним експертам. Водночас для забезпечення узгодженої роботи членів РГ та експертів останнім надається пояснення щодо аналізу недоліків, аналізу рішень та занесення даних до матриці оцінювання.

В межах етапу аналізу недоліків РГ використовує метод експертних оцінок (використання аналітичних методів аналізу також доцільне). При цьому оцінюють важливість та успішність виконання кожного *j*-го під-завдання з присвоєнням відповідних балів. Це дозволить отримати кількісну оцінку стану спроможності та ефективності її реалізації.

Рівень важливості *j*-го під-завдання визначають балом важливості $БВ_j$, якому присвоюється значення: 3 (завдання критичне); 2 (завдання дуже важливе); 1 (завдання важливе) відповідно. Рівень успішності виконання під-завдань (на основі аналізу досвіду їх виконання) – балом успішності $БУ_j$, якому присвоюється значення: 3 (успішність висока); 2

(успішність достатня); 1 (успішність низька); 0 (успішність мінімальна). Значення $БВ_j$, $БУ_j$ заносять у стовпчики 7, 8 (матриці оцінювання).

Бал успішності $БУ_i$ виконання *i*-го завдання визначають за балами важливості та успішності під-завдань за формулою (1), яка занесена в алгоритм матриці:

$$\text{БУ}_i = \frac{\sum_j^{k_i} \text{БУ}_j \text{БВ}_j}{\sum_j^{k} \text{БВ}_j}, \quad (1)$$

де k_i – кількість під-завдань *i*-го завдання (i=1..N_m),
N_m – кількість завдань *m*-ї стадії (m=1..4).

Аналогічно визначають бал успішності виконання всіх завдань m-*ї* стадії БУст_m (m = 1..4) за формулою

$$\text{БУст}_m = \sum_i^{N_m} \text{БУ}_\text{i}\, \text{БВ}_i / \sum_i^{N_m} \text{БВ}_i, \quad \text{(m=1..4)}. \quad (2)$$

Передбачається, що спроможність як правило реалізується на чотирьох стадіях (планування, підготовка, виконання, оцінювання результатів).

Бал успішності виконання всіх завдань БУсум, які виконують на всіх стадіях реалізації спроможності, визначають за формулою (3). Він автоматично наводиться в нижній частині стовпчика 9.

$$\text{БУсум} = \sum_m^4 \text{БУст}_m \text{Кст}_m \quad \text{(m=1..4)}, \quad (3)$$

де, Кст_m — коефіцієнт важливості завдань *m*-ї стадії, визначається РГ, при цьому $\sum_{m=1}^{4} \text{Кст}_m = 1$.

Бал важливості всіх завдань визначають за формулами аналогічними (2, 3). Він автоматично наводиться в нижній частині стовпчика 7.

Наведений підхід дозволяє визначити важливість всіх завдань при реалізації спроможності та успішність їх виконання. Ці дані необхідні при оцінювання стану спроможності, а також при огляді всіх спроможностей. При цьому рівень успішності виконання *i*-го завдання визначають критеріями успішності: *висока успішність* ($БУ_i \geq 2{,}5$); *достатня успішність* ($2{,}5 \geq БУ_i \geq 1{,}6$); *низька успішність* ($1{,}6 > БУ_i > 0{,}6$); *мінімальна успішність* ($0{,}6 \geq БУ_i$). Рівень важливості завдань – відповідно: завдання *критичне* ($БВ_i > 2{,}5$); завдання *дуже важливе* ($2{,}5 \geq БВ_i \geq 1{,}6$); завдання *важливе* ($1{,}6 > БВ_i$).

Недоліки спроможності щодо виконання кожного під-завдання РГ визначає на основі аналізу досвіду реалізації спроможності в ході операцій (бойових дій) та наводить у стовпчику 10 матриці оцінювання. При цьому зазначається базовий компонент (-ти) спроможності, з яким пов'язаний недолік. Причини недоліків залежать від стану спроможності, який в свою чергу залежить від низки чинників, і його доцільно оцінювати через стан базових компонентів DOTMLPFI [1, 2] та їх вплив на спроможність.

Рівень стану *l*-го базового компоненту PC_l та його впливу на ефективність виконання завдання PB_l визначають експертним методом з присвоєнням відповідних балів: 3 (рівень стану *високий/* рівень впливу *високий*); 2 (рівень стану *достатній /* рівень впливу *значний*), 1 (рівень стану *мінімальний /* рівень впливу *мінімальний*), 0 – рівень стану *незадовільний* (для PB_l – компонент невластивий спроможності щодо виконання завдання). РГ заносить бали PC_l та PB_l у відповідні стовпчики 11-18 матриці оцінювання.

Рівень стану спроможності стосовно виконання *j*-го під-завдання за всіма DOTMLPFI визначають її балом ($БС_j$) за формулою.

$$\text{БС}_j = \frac{\sum_l^8 \text{PC}_l \text{PB}_l}{\sum_l^8 \text{PB}_l}. \quad (4)$$

Таблиця 1. Матриця оцінювання спроможності за скороченою процедурою (назва та код спроможності)

Військова проблема спроможності: ….Мета: …Шляхи: …

Стадії функціонування спроможності	II. Вимоги до спроможності					III. Аналіз недоліків				
	Завдання (заходи)	Мета (очікуваний ефект)	Умови виконання завдання	Показник оцінювання завдання	Вимоги до спроможності щодо виконання завдання	Оцінювання важливості завдань та успішності їх виконання			Зазначте основні недоліки (пов'язані з компоненти DOTMLPFI) щодо виконання під-завдань
						Визначте рівень важливості під-завдань	Зазначте успішність виконання під-завдань	Рівень успішності виконання завдання	
1	2	3	4	5	6	7	8	9	10
1.Планування	Завдання 1.1		Умови 1.1					1,6	
	Під-завдання 1.1.1	Мета 1.1.1		Показник 1.1.1	Вимоги 1.1.1	2	1		Недолік… (D)
	Під-завдання 1.1.2	Мета 1.1.2		Показник 1.1.2	Вимогаи1.1.2	3	2		Недолік …(M,T,I)
	…							..	
	Завдання 1.N_1		Умови 1.N_1 4					1,8	
	..		..					..	
2. Підготовка	Завдання 2.1		Умови 2.1					2,1	
	Під-завдання 2.1.1	Мета 2.1.1		Показник 2.1.1	Вимоги 2.1.1	2	2		Недолік (O, F,I)
	…							..	
	Завдання 2.N_2		Умови 2.N_2					1,9	
3.Виконання	Завдання 3.1		Умови 3.1					1,9	
	…							..	
	Завдання 3.N_3		Умови 3.N_3					2,1	
4.Оцінкова	Завдання 4.1		Умови 4.1					2,0	
	…							..	
	Завдання 4.N_4		Умови 4.N_4					2.3	
						Важливість всіх завдань -**1,8** (низька)		Успішність всіх завдань – **1,3** (мінімальна)	

Аркуші:

1.Оцінювання спроможності	2.Аналіз недоліків	3.Рекомендації	4.План реалізації	5 Графік реалізації	6 Комплексна спроможність

Продовження таблиці 1

III. Аналіз недоліків																				IV Аналіз рішень	
Стадії функціонування спроможності	Завдання (заходи)	Визначте: рівень стану спроможності за компонентами DOTMLPFI (PC) та рівень впливу базового компонента на її стан (PB)						Стан спроможності (щодо виконання i-го завдання $БС_i$); стан матеріальн. компоненту БСМі		Необхідність уваги до спроможності	Напрями усунення недоліків	Визначте основні ризики	Визначте ймовірності виникнення	Визначте рівень ризику (I) в	Індекс ризику IR та рішення щодо нього	Рішення щодо ризику	Відповідальний за розвиток спроможності	Визначте рекомендації щодо усунення недоліків (за DOTMLPFI)		
		PC_0	PB_0	...	PC_i	PB_i		БС$_i$	БСМ$_i$											
1	2	11			18			19	20	21	22	23	24	25	26	27	29	28		
1.Планування	Завдання 1.1							1,9	1,3	*	**	Ризик1.1	1	4	4				A	Рішення (I)
	Під-завдання 1.1.1	2	1		1	2		1,4	1	*	**								C	Рішення (D)
	Під-завдання 1.1.2	3	2		2	3		1,8	2	*	**									
	...																		B	Рішення (M)
	Завдання 1.N_1							2,1	1,8	*	**	Ризик 1.N_1	2	3	6					
2. Підготовка	Завдання 2.1								1,5	*	**		1	4	4					
	Під-завдання 2.1.1	1	3		1	3		2,2	1	*	**								O	Рішення (F)
	...																			
	Завдання 2. N_2							1,5	1,6	*	**	Ризик 2.N_2	2	2	4				P	Рішення (O)
3.Виконання	Завдання 3.1							2,2	2,1	*	**	Ризик	2	3	6					
	...																			
	Завдання 3. N_3							1,3	2,2	*	**	Ризик 3.N_3	4	1	4				X	Рішення (F)
4.Оцінювання	Завдання 4.1							2,4	1,9	*	**	Ризик 4.1	2	1	2				E	Рішення (D)
	...																			
	Завдання 4. N_4							1,3	1,5	*	**	Ризик 4.N_4	1	3	3				K	Рішення (O)

Рівень стану спроможності БСС(s)	Рівень стану матеріального базового компоненту
1,4	1,2

IR для спроможності	Рішення щодо ризику
4,4	

* - (увага потрібна/ увага не потрібна/ .. /потрібна значна увага

** - (зміни не потрібні/.../невідкладні заходи щодо усунення недоліків)

Рівень стану спроможності стосовно виконання *i*-го завдання БСЗ$_i$ (*i*=1..N_m) має враховувати рівень її стану стосовно всіх під-завдань, а також рівень успішності *БУ$_j$ (j=1.. k$_i$)*, і визначають за формулою:

$$\text{БСЗ}_i = \frac{\sum_j^{k_i} \text{БС}_j \text{БУ}_j}{\sum_j^m \text{БУ}_j}, \quad (5)$$

Загальну оцінку стану спроможності щодо виконання всіх завдань *m*-ї стадії БСС$_m$ визначимо за формулою:

$$\text{БСС}_m = \sum_{i=1}^{N_m} \text{БСЗ}_\text{i}\, \text{БУ}_\text{i} / \sum_{i=1}^{N_m} \text{БУ}_i. \quad (6)$$

Загальна оцінка стану спроможності щодо виконання завдань на всіх стадіях її реалізації має враховувати відповідні оцінки стану щодо виконання всіх завдань. Бал загальної оцінки спроможності БСС$^{(S)}$ визначають за формулою

$$\text{БСС}^{(s)} = \sum_{m=1}^{4} K\text{ст}_m \text{БСС}_m. \quad (7)$$

Застосовуючи аналогічний підхід, визначений формулами (4) – (7), отримують бал оцінок стану матеріального базового компонента спроможності стосовно окремих завдань, всіх завдань стадії та всіх стадій. Рівні стану спроможності БСС$^{(s)}$ та її матеріального базового компоненту автоматично наводяться в нижній частині матриці оцінювання (табл. 1, стовпчики 19 і 20 відповідно).

Оцінки стану спроможності щодо виконання всіх завдань з урахуванням стану всіх компонентів DOTMLPFI, і матеріального (M) зокрема, дозволяють визначити причини недоліків та сформулювати напрями усунення недоліків за алгоритмом, який наведено в табл. 2 та реалізований в алгоритмі матриці оцінювання. Рекомендації щодо цих напрямів РГ наводить у відповідних строчках стовпчиках 21 і 22 матриці оцінювання.

Таблиця 2. Вибір напрямів усунення недоліків спроможності

	Рівень стану спроможності			
	Достатній (БСЗ$_i$≥2,5)	Задовільний (2,49≥ БСЗ$_i$ >1,6)	Мінімальний (1,59≥БСЗ$_i$ >0,6)	Потребує відновлення (0,59≥БСЗ$_i$)
Рівень успішності виконання завдань	Необхідність уваги до розвитку спроможності. Напрями усунення недоліків			
Високий (БУ$_i$ ≥ 2,5)	Увага не потрібна Зміни не потрібні	Увага потрібна Підтримання стану спроможності	Увага потрібна Розвиток спроможності	Потрібна значна увага. Системні заходи щодо усунення недоліків
Достатній (2,49≥ БУ$_i$>1,6)	Увага потрібна Підтримання стану спроможності	Увага потрібна Розвиток спроможності	Увага потрібна Системні заходи щодо усунення недоліків	Потрібна значна увага. Невідкладні заходи щодо усунення недоліків
Низький (1,59≥БУ$_i$>0,6)	Увага потрібна Розвиток спроможності	Увага потрібна Системні заходи щодо усунення недоліків	Увага потрібна Невідкладні заходи щодо усунення недоліків	Потрібна значна увага. Невідкладні заходи щодо усунення недоліків
Мінімальний (0,59≥БУ*i*)	Потрібна значна увага Системні заходи щодо усунення недоліків	Потрібна значна увага Невідкладні заходи щодо усунення недоліків	Потрібна значна увага Формування (відновлення) спроможності	Потрібна значна увага. Формування (відновлення) спроможності

Виявлені причини недоліків щодо виконання завдань (під-завдань) є також загрозами, що створюють певні ризики для спроможності. Рівні ризиків (загроз та їх наслідків) мають бути враховані в процесі визначення рекомендацій щодо усунення причин недоліків. Для цього визначають стратегію та методи реагування на ризик через визначення його індексу *IR,* який враховує ймовірності виникнення ризику (*P*) та рівень впливу ризику (*I*) на виконання завдання з використанням відомого підходу оцінювання ризику [13]. Матриця оцінювання запропонує стратегію (рішення) щодо зменшення ризику: прийняти ризик (при 4≥IR_i); пом'якшити або розподілити ризик (12 ≥IR_i >4); запобігти або уникнути (IR_i >12).

При ОС нас цікавить показник індексу ризику стосовно всієї спроможності IR_i. Його визначають для всіх завдань *m*-ї стадії $IRcm_m$ через індекс ризику IR_i стосовно *i*-го завдання за формулою

$$IR\text{ст}_m = \sum_i^{N_m} IR_i/N_m. \quad (8)$$

Індекс ризику стосовно спроможності IR_Σ визначають за формулою (9), який наводиться в нижній частині стовпчика 26.

$$IR_\Sigma = \sum_{m=1}^{4} IR\text{ст}_m \text{ Кст}_m. \quad (9)$$

Аналіз всіх недоліків проводять на аркуші "2-аналіз недоліків", табл.1. При цьому завдання, вимоги до них та недоліки з аркуша 1 (стовпчики 2, 6, 10) автоматично переносяться на аркуш 2, на якому проводять попередню декомпозицію недоліків за їх відношенням до базових компонентів DOTMLPFI.

Члени РГ, а також експерти, які працюють on-line, аналізують недоліки за компонентами DOTMLPFI стосовно кожного під-завдання на кожній стадії та в цілому за всі стадії, проводять їх узагальнення та формулюють недоліки спроможності. При цьому недоліки мають бути: пов'язаними із завданням та показниками їх виміру; специфічними (визначати окремі носії спроможностей, інструменти, політики, які є недостатніми або відсутні, і впливають на виконання завдання, особливо у певних умовах обстановки); сфокусованими (стосуватися декількох завдань, одночасно).

Отже в ході аналізу недоліків РГ оцінює важливість завдань та успішність їх виконання, визначає основні недоліки спроможності щодо виконання завдань, рівень стану спроможності за базовими компонентами DOTMLPFI, напрями усунення недоліків, ризики та стратегію щодо їх зниження. Зазначені оцінки є основою для обґрунтованого формування рекомендацій щодо усунення недоліків.

Четвертий етап (аналіз рішень) передбачає визначення нематеріальних, матеріальних або комбінації нематеріальних і матеріальних рекомендацій, які спрямовані на усунення недоліків (прогалин) у спроможностях або зменшать їх вплив.

Рекомендації щодо усунення недоліків повинні мати системний характер, бути сфокусованими на усунення конкретних недоліків (прогалин), або зменшенні їх впливу, чітко визначати орган військового управління, який відповідатиме за їх реалізацію. Водночас рекомендації мають відповідати наступним вимогам: бути придатними **(**мінімізувати/усувати недолік); бути реалістичними (їх можливо реалізувати); бути прийнятними (задовольняти всі зацікавлені сторони); містити терміни реалізації рішень та орієнтовну потребу у ресурсах, які можливо виділити для їх реалізації. Рекомендації щодо кожного під-завдання члени РГ та експерти заносять в матрицю оцінювання, аркуш 1, стовпчик 28.

Аналіз рішень щодо усунення недоліків проводять з використанням аркуша "3 Рекомендації" матриці оцінювання. При цьому завдання, недоліки та рекомендації з аркуша 1 (стовпчики 2, 10, 28) автоматично переносяться на аркуш "3 Рекомендації" матриці оцінювання, де проводиться їх декомпозиція за компонентами DOTMLPFI.

Нематеріальні підходи (щодо змін у нематеріальних базових компонентах DOTLPF) вживають у випадку виявлення недоліків у спроможностях, рівень яких не перевищує прийнятний (стан спроможності задовільний і вище, при цьому індекс ризику є прийнятним). Матеріальні підходи (впровадження вдосконаленої інформаційної системи, удосконалення компонентів їх життєвого циклу; модернізація або заміна ОВТ на те, що значно підвищує спроможності) вживають у випадку, коли неприйнятний рівень ризику залишається після застосування нематеріальних підходів.

Рекомендації опрацьовують щодо кожного під-завдання. Проводять їх аналіз та узагальнення за базовими компонентами стосовно всіх завдань (оскільки рекомендації можуть бути схожими щодо окремих під-завдань/завдань).

Отримані пропозиції потребують подальшої систематизації на предмет визначення їх взаємозв'язків, послідовності та термінів виконання. Для цього розробляють "План імплементації", в якому визначають: основні рекомендації; завдання/заходи щодо реалізації рекомендацій; тривалість виконання заходів; дати початку та завершення; взаємозалежність заходів; головного виконавця та співвиконавців; орієнтовну потребу у фінансових ресурсах; інші ресурси. Цю роботу проводять на аркуші "4 План реалізації".

В плані також наводять взаємозв'язок заходів. Тому він остаточно має бути уточнений за допомогою план-графіку імплементації, який опрацьовують на аркуші "5 Графік реалізації", в якому наводиться уточна потреба у ресурсах. Для кожного заходу плану додають коментар, який деталізує або пояснює зміст заходу.

План-графік реалізації рішень за результатами оцінювання опрацьовують відповідно до прийнятої практики. Одним з дієвих рішень є формування плану-графіка за допомогою програми Microsoft Project у виді діаграми Ганта [14], для цього дані зі аркуша "4 План реалізації" експортують з Excel в Microsoft Project, який забезпечує узгодженість всіх рекомендацій за часом та відповідальними виконавцями. Проводиться аналіз взаємозв'язків заходів, часових рамок тощо. Опрацьований в Microsoft Project план-графік переносять на аркуш "5 Графік реалізації".

Підсумковий документ за результатами ОС за скороченою процедурою опрацьовують одночасно з підготовкою рекомендацій щодо усунення виявлених недоліків (прогалин). Він має містити:

передмову;

опис військової проблеми (оперативна обстановка, основні недоліки існуючої спроможності);

опис операцій (бойових дій), на які впливає спроможність; ймовірні ризики, що можуть становити загрозу з огляду на потточний стан спроможності;

рекомендації щодо розвитку спроможності (нематеріальні та матеріальні рішення), які сформовані на аркуші "Рекомендації";

орієнтовний план реалізації рекомендацій з розвитку спроможностей (який сформований на аркуші "4 План реалізації") та План-графік реалізації рішень (який наведений на аркуші 5).

До підсумкового документу додаються:

Положення з проведення оцінювання спроможностей за скороченою процедурою, концептуальне бачення;

Матриця оцінювання спроможності, яка опрацьована РГ в ході ОС;

Положення наведеної методики оцінювання спроможності за скороченою процедурою опрацьовані у виді додатку до чинного військового стандарту [1].

Оцінювання комплексних спроможностей, які реалізують війська (сили), що належать до різних видів, родів військ (сил) здійснюється з використання матриці оцінювання за

наведеною вище методикою шляхом декомпозиції спроможності з наступним узагальнення результатів. Результати оцінювання наводять на аркуші “6. Комплексна спроможність“.

Результати

Апробація наведеної методики оцінювання спроможності за скороченою процедурою була проведена для оцінювання основних спроможностей одного з родів військ. Для цього була створена РГ із ключових фахівців. За її результатами зроблено висновок щодо придатності методики та доцільності її впровадження в системі оборонного планування для оцінювання спроможностей.

При цьому була досягнута повна наочність всього процесу, його відображення на сторінка електронних таблиць матриці оцінювання, отримані оцінки (у тому числі і кількісні) спроможності з урахуванням досвіду війни. Показники ОС та залучення персоналу були такими: час оцінювання був в 5-6 разів меншим за той, який був би необхідний при проведенні ОС у формі аналітичного дослідження; до проведення ОС були безпосередньо залучені тільки 10 осіб, а також окремі експерти на заключному етапі оцінювання.

Висновки

Наведена методика забезпечує проведення оцінювання оборонних спроможностей за скороченою процедурою у досить стислі терміни, незначною кількістю безпосередньо залученого персоналу, при цьому забезпечуються принципи, які визначені відповідним військовим стандартом. Отримані результати оцінювання дозволяють їх використовувати у всіх видах оборонного планування, програмуванні та у проєктній діяльності.

Застосування електронних таблиць (Excel) дозволяє залучати в режимі on-line необхідну кількість фахівців, забезпечити наочність процесу оцінювання та сформувати вихідні результати ОС у форматі, який необхідний для гармонізації функціонування системи управління розвитком спроможностей.

На базі наведеної методики може бути створений програмний додаток для оцінювання спроможностей.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Оборонне планування. Порядок організації проведення оцінювання спроможностей Збройних Сил України в умовах правового режиму воєнного стану в Україні (за скороченою процедурою). Військовий стандарт 01.040.009. (Видання 1). ГШ ЗС України, 2021.
2. Manual for the Operation of the Joint Capabilities Integration and Development System (JCIDS Manual 31 August 2018). URL: https://www.acq.osd.mil/asda/jrac/docs/2018-JCIDS.pdf. (дата звернення 19.09.2024).
3. JCIDS Process. Joint Capabilities Integration and Development System (JCIDS) Process Overview. URL: https://acqnotes.com/acqnote/acquisitions/jcids-overview. (дата звернення 20.09.2024).
4. Report on Joint Capabilities Integration and Development System (JCIDS). URL:

https://apps.dtic.mil/sti/pdfs/AD1180239.pdf. (дата звернення 21.09.2024).
5. Загорка О., Загорка І., Фучко А. Методичний підхід до оцінювання спроможностей міжвидового угруповання військ під час планування реформування (розвитку) Збройних Сил України. ЗНП ЦВСД НУОУ. 2021. С. 6–15.
6. Семененко О. та ін. Рекомендації щодо оцінювання та прогнозування приросту рівня спроможностей Збройних Сил України з урахуванням достатності фінансування. ЗНП ЦВСД НУОУ. 2022. С. 60–67.
7. An evaluation model and tool for Defence capability options. MODSIM2021, 24th International Congress on Modelling and Simulation. Modelling and Simulation Society of Australia and New Zealand, 2021.
8. ВКП 5-00(67).01.01. Доктрина з оборонного планування у Збройних Силах України: затверджена Головнокомандувачем ЗС України, 2020.
9. Про затвердження Порядку організації та здійснення оборонного планування в Міністерстві оборони України, Збройних Силах України та інших складових сил оборони. Наказ Міністерства оборони України від 22.12.2020 №484.
10. Крикун П., Павленко В., Корендович В., Ясенко С. Оборонне планування в умовах правового режиму воєнного стану. Особливості та напрями вдосконалення. Наука і оборона, №2 (2023). С.3-7.
11. Єдиний перелік (каталог) спроможностей Міністерства оборони України, Збройних Сил України та інших складових сил оборони: затверджений Міністром оборони України, 2021.
12. Перелік типових завдань Збройних Сил України за сценаріями виникнення та розвитку ситуацій воєнного характеру: затверджений Начальником Генерального штабу – Головнокомандувачем Збройних Сил України, 2019.
13. Порядок організації в системі Міністерства оборони України внутрішнього контролю та управління ризиками: затверджено наказом МО України №145 від 02.04.2019.
14. Дерек Мау. Повний посібник із діаграм Ганта URL: https://www.microsoft.com/uk-ua/microsoft-365/business-insights-ideas/resources/gantt-chart-guide. (дата звернення 19.07.2024).

References

1. Oboronne planuvannya. Poryadok orhanizatsiyi provedennya otsinyuvannya mozhlyvostey Zbroynykh syl Ukrayiny v umovakh pravovoho rezhymu voyennoho stanu v Ukrayini (za skorochenoyu protseduroyu). Viys'kovyy standart 01.040.009. (Vy-dannya 1). HSH ZS Ukrayiny, 2021.
2. Kerivnytstvo z ekspluatatsiyi systemy intehratsiyi ta rozvytku ob"yednanykh mozhlyvostey (Kerivnytstvo JCIDS vid 31 serpnya 2018). Available from : https://www.acq.osd.mil/asda/jrac/docs/2018-JCIDS.pdf. (data zvernennya 19.09.2024).
3. JCIDS Process. Joint Capabilities Integration and Development System (JCIDS) Process Overview. Available from : https://acqnotes.com/acqnote/acquisitions/jcids-overview. (дата звернення 20.09.2024).
4. Report on Joint Capabilities Integration and Development System (JCIDS). Available from : https://apps.dtic.mil/sti/pdfs/AD1180239.pdf. (дата звернення 21.09.2024).
5. Zahorka O., Zahorka I., Fuchko A. Metodychnyy pidkhid do otsinyuvannya efektyvnosti mizhvydovoho uhrupovannya viys'k pid chas planuvannya reformuvannya (rozvytku) Zbroynykh Syl Ukrayiny. ZNP TSVSD NUOU. 2021. S. 6–15.

6. Tsemenenko O. ta in. Rekomendatsiyi shchodo otsinyuvannya ta prohnozuvannya pryrostu rivnya spryyatlyvosti Zbroynykh Ukrayiny z otsinkoyu dostupnosti finansuvannya. ZNP TSVSD NUOU. 2022. S. 60–67.
7. An evaluation model and tool for Defence capability options. MODSIM2021, 24th International Congress on Modelling and Simulation. Modelling and Simulation Society of Australia and New Zealand, 2021.
8. VKP 5-00(67).01.01. Doktryna z oboronnoho planuvannya u Zbroynykh Si-lakh Ukrayiny: zatverdzheno Holovnokomanduvachem ZS Ukrayiny, 2020.
9. Pro zatverdzhennya Poryadku orhanizatsiyi ta zdiysnennya oboronnoho planuvannya v Ministerstvakh oborony Ukrayiny, Zbroynykh sylakh Ukrayiny ta inshykh skla-dovykh syl oborony. Nakaz Ministerstva oborony Ukrayiny vid 22.12.2020 №484.
10. Krykun P., Pavlenko V., Korendovych V., Yasenko S. Oboronne planuvannya v umovakh pravovoho rezhymu voyennoho stanu. Osoblyvosti ta napryamy vdoskonalennya. Nauka i oborona, №2 (2023). S.3-7.
11. Yedynyy perelik (kataloh) spromozhnostey Ministerstva oborony Ukrayiny, Zbroynykh Syl Ukrayiny ta inshykh skladovykh syl oborony: zatverdzheno Ministrom oborony Ukrayiny, 2021.
12. Perelik typovykh zavdan' Zbroynykh Syl Ukrayiny za stsenariyamy vynyk-nennya ta rozvytku sytuatsiy viys'kovoho kharakteru: zatverdzhenyy Nachal'nykom Heneral'noho shtabu – Holovnokomanduvachem Zbroynykh Syl Ukrayiny, 2019.
13. Poryadok orhanizatsiyi v systemi Ministerstva oborony Ukrayiny vnutrishn'oho kontrolyu ta upravlinnya ryzykamy: zatverdzheno nakazom MO Ukrayiny №145 vid 02.04.2019.
14. Derek Mau. Povnyy posibnyk iz diahramy Hanta. Available from : https://www.microsoft.com/uk-ua/microsoft-365/business-insights-ideas/resources/gantt-chart-guide. (data zvernennya 19.07.2024).

Методика оцінювання загроз об’єктам критичної інфраструктури під час вогневого впливу противника

Methodology for assessing threats to critical infrastructure objects during enemy fire

Ілля Капля [A]
Corresponding author: ад’юнкт кафедри, e-mail: kaplia1607@gmail.com, ORCID: 0000-0002-1424-4175
Богдан Тертишний [A]
доктор філософії, старший викладач кафедри, e-mail: hlor2007@gmail.com, ORCID:0000-0002-9060-761X

IlliaKaplia [A]
Corresponding author: Graduate Student of the Department, e-mail: kaplia1607@gmail.com, ORCID: 0000-0002-1424-4175
Bohdan Tertyshnyy [A]
Doctor of Philosophy, Senior Lecturer of the Department, e-mail: hlor2007@gmail.com, ORCID:0000-0002-9060-761X

[A] Національний університет оборони України, м. Київ, Україна
[A]National Defense University of Ukraine, Kyiv, Ukraine

Received: October 4, 2024 | Revised: October 20, 2024 | Accepted: October 31, 2024

DOI: 10.33445/sds.2024.14.5.21

Мета роботи: мінімізація наслідків загроз об’єктам критичної інфраструктури від вогневого впливу противника.
Метод: експертних оцінок, статистичного аналізу, теорії ймовірності.
Результати дослідження: розробка методики оцінювання загроз об’єктам критичної інфраструктури під час вогневого впливу противника з урахуванням їх сумарного ефекту, яка враховує об’єднаний вплив різних загроз при їх одночасній дії.
Теоретична цінність дослідження: попередження надзвичайних ситуацій від вогневого впливу противника шляхом подальшої пріоритезації загроз та розробки заходів захисту.
Тип статті: огляд і дослідження.

Purpose: minimization of the consequences of threats to critical infrastructure objects from a concentrated enemy fire strike.
Method: expert assessments, statistical analysis, probability theory.
Findings: development of a methodology for assessing threats to critical infrastructure objects during enemy fire, taking into account their total effect, which takes into account the combined impact of various threats when they act simultaneously.
Theoretical implications: prevention of emergency situations from enemy attacks by further prioritization of threats and development of protection measures.
Papertype: review and research.

Ключові слова: критична інфраструктура, надзвичайна ситуація, оцінювання загроз, вогневий вплив, захист.

Key words: critical infrastructure, emergency, threat assessment, fire impact, protection.

Вступ

Загрози для об’єктів критичної інфраструктури в сучасному світі, стають більш складними та різноманітними. Це обумовлено як розвитком технологій, так і збільшенням кількості загроз різного характеру, які можуть створити небезпеку – від воєнних дій до терористичних актів. Внаслідок цього виникає актуальна потреба яка полягає в оцінці ризиків для об’єктів критичної інфраструктури, що в свою чергу потребують розроблення нових математичних моделей для їх оцінки. Сучасні загрози часто мають синергетичний характер, і їх одночасна дія може істотно посилити негативний вплив на об’єкти критичної інфраструктури. Тому важливо не тільки визначити ці загрози, а й розробити методи їх комплексного аналізу.

В рамках даного дослідження пропонується удосконалена методика оцінювання загроз об’єктів критичної інфраструктури, що включає використання факторів сумарного впливу. Ці фактори визначаються коефіцієнтом сумарного впливу, який дозволяє більш точно оцінити загальний ризик, враховуючи взаємодію кількох загроз об’єктам критичної інфраструктури та їх вплив одна на одну. Запропонована методика складається з кількох основних етапів, серед яких ідентифікація об’єктів критичної інфраструктури, визначення ймовірності виникнення загрози об’єктам критичної інфраструктури на основі статистичних даних, оцінка впливу загрози

об’єктам критичної інфраструктури, моделювання комбінованого впливу, а також оцінка сукупності впливу на об’єкти критичної інфраструктури.

Теоретичні основи дослідження

Огляд останніх публікацій [1–8] показує, що, на думку багатьох провідних експертів, які досліджували питання оцінки загроз та ризиків для об’єктів критичної інфраструктури (ОКІ), загальноприйнятого підходу для оцінки ризиків та загроз для цих об’єктів досі не існує. Існують тільки часткові рішення, які охоплюють окремі типи об'єктів або конкретні варіанти техногенних загроз. Реалізація таких рішень призводить до зменшення наслідків надзвичайних ситуацій на ОКІ. Однак дані методики оцінки ризиків ОКІ зосереджені на реактивних діях для ліквідації наслідків атак на ці об’єкти, а не на проактивних заходах для попередження загроз.

У сучасних умовах де ризики значно ускладнюються масованими ракетно-дроновими ударами, наявні методики оцінки загроз для ОКІ залишаються недостатньо дієвими. Ці підходи часто не враховують комплексний характер взаємодії різних загроз ОКІ і обмежуються аналізом ризиків на локальному рівні, що не забезпечує інтегрованого підходу до управління ризиками. З досвіду міжнародної практики також видно, що увага більшого зосереджується на відновленні об’єктів після нападу, а не на попередженні або мінімізації загроз на ці об’єкти.

Загалом, аналіз зазначених наукових джерел свідчить, що сучасні підходи до захисту ОКІ мають бути орієнтованими на запобігання та зниження ймовірності загроз на ці об’єкти. Це вимагатиме розробки нових стандартів у сфері управління ризиками, які б інтегрували всі види загроз на ОКІ, передбачали можливість одночасної взаємодії різних типів ризиків і забезпечили комплексний підхід до стійкості ОКІ.

Постановка проблеми

У сучасних умовах глобалізації та технологічного прогресу ОКІ піддаються численним загрозам, які залишаються дедалі складнішими та різноманітнішими. Системи енергетики, транспорту, водопостачання, а також інформаційні технології можуть знати як фізичні, так і кібернетичні атаки, які можуть мати серйозні наслідки для національної безпеки. В умовах вогневого впливу противника виникає потреба не тільки в ефективному захисті цих об’єктів, а й у комплексному аналізі ризиків для цих об’єктів, пов’язаних із їх діяльністю. Класичні підходи до оцінки ризиків для ОКІ часто не враховують складні взаємозв’язки між більшістю типів загроз які впливають на ці об’єкти. В умовах, коли загрози для ОКІ можуть діяти синергетично, просто підсумовування ймовірностей ризиків для цих об’єктів не відображає реального стану справ та важко передбачити за допомогою традиційних моделей.

Таким чином, метою цієї роботи є удосконалення методики оцінювання загроз ОКІ під час вогневого впливу противника з урахуванням сумарного впливу загроз на ці об’єкти, яка враховує сукупний вплив різних загроз, зокрема синергетичний ефект від їх одночасної дії.

Результати

Загрози для ОКІ стають дедалі складнішими та різноманітнішими, що потребує розробки нових математичних моделей для їх оцінки. Зокрема, сучасні загрози часто є сумарними – тобто їх одночасна дія може значно підсилити негативний вплив. У цій моделі запропоновано врахувати коефіцієнт сумарного впливу K_{sum}, який дозволить більш повно оцінити загальний ризик при одночасній дії кількох загроз.

Основними етапами розробки методики оцінювання загроз ОКІ під час вогневого впливу противника з урахуванням сумарного коефіцієнту загроз яка представлена на рис. 1, є:

- ідентифікація ОКІ та потенційних загроз для цих об’єктів.

- обчислення ймовірності виникнення загроз ОКІ на основі статистичних даних та експертних оцінок.
- оцінка впливу загроз ОКІ з урахуванням індивідуальних характеристик для цих об'єктів.
- моделювання комбінованого впливу загроз ОКІ з урахуванням нової компоненти – коефіцієнта сумарного впливу.
- оцінка сукупного ризику та пріоритезація загроз ОКІ для оптимізації ресурсів захисту.

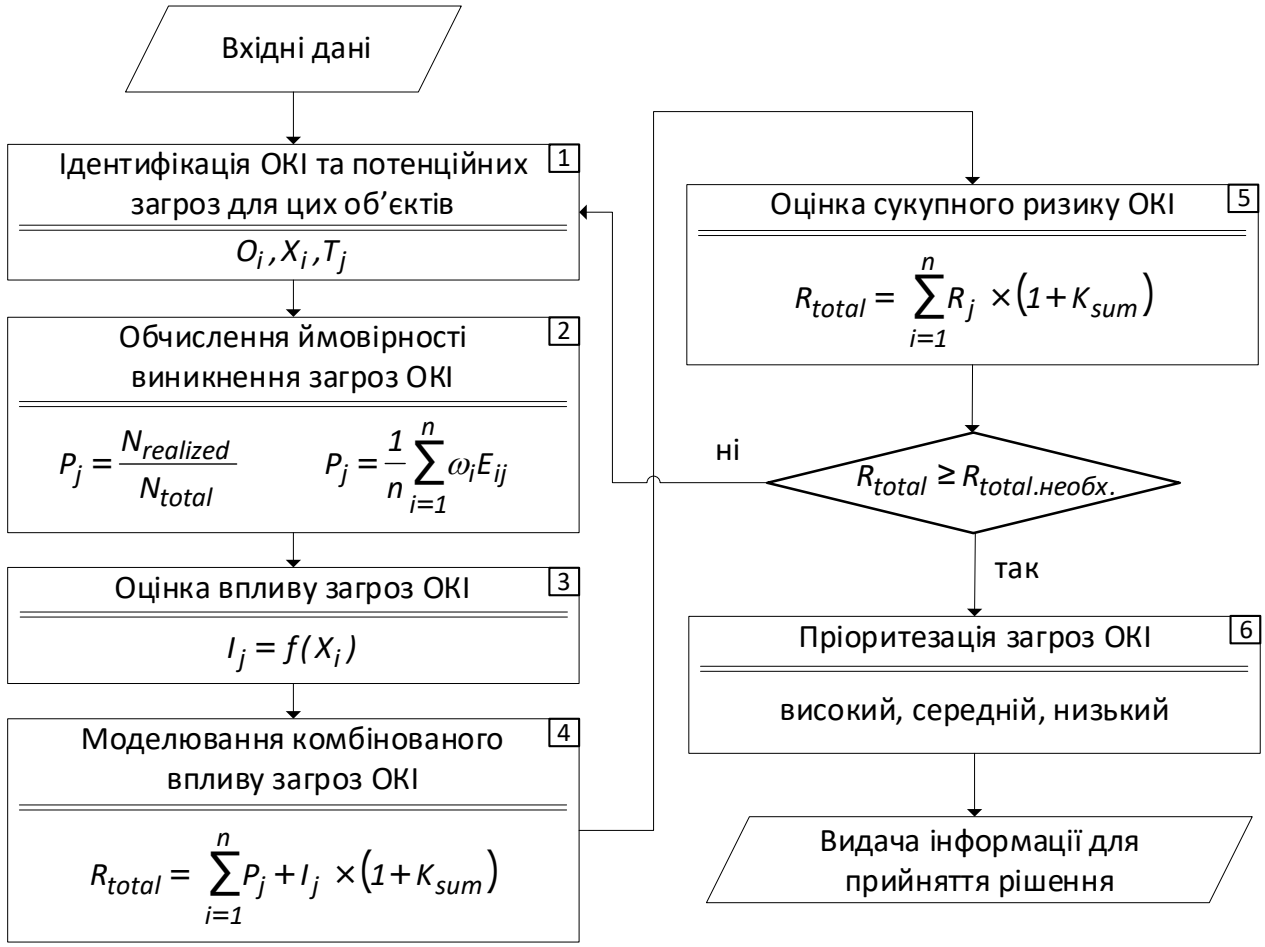


Рисунок 1– Структурно-логічна схема методики оцінювання загроз ОКІ під час вогневого впливу противника з урахуванням сумарного коефіцієнту загроз

Блок 1. Ідентифікація ОКІ та потенційних загроз для цих об'єктів.

Нехай існує множина об'єктів критичної інфраструктури O, де кожен об'єкт O_i характеризується набором параметрів X_i, що включають такі фактори, як фізична вразливість, кібернетична захищеність, критичність для національної безпеки тощо.

Загрози представляються множиною T, де кожна загроза T_j може бути фізичною, техногенною або кібернетичною. Для кожної загрози можна оцінити ймовірність виникнення P_j та її вплив на об'єкт I_j.

Блок 2. Обчислення ймовірності виникнення загроз ОКІ на основі статистичних даних та експертних оцінок.

Ймовірність виникнення кожної загрози P_j можна визначити на основі статистичних даних або експертних оцінок:

$$P_j = \frac{N_{realized}}{N_{total}}, \quad (1)$$

де, $N_{realized}$ – кількість випадків реалізації загрози за певний період,

N_{total} – загальна кількість випадків.

Якщо немає достатньо даних, використовуються експертні оцінки:

$$P_j = \frac{1}{n}\sum_{i=1}^{n}\omega_i E_{ij}, \quad (2)$$

де, E_{ij} – оцінка ймовірності загрози експертом i,

ω_i – ваговий коефіцієнт, що відображає досвід експерта.

Блок 3. Оцінка впливу загроз ОКІ з урахуванням індивідуальних характеристик для цих об’єктів.

Для кожної загрози оцінюється її можливий вплив на ОКІ I_j. Вплив може бути оцінений в економічних показниках (вартість збитків), руйнуванні інфраструктури або втратах людських життів. Вплив описується як функція від параметрів об’єкта:

$$I_j = f(X_i), \quad (3)$$

де, X_i – набір характеристик об'єкта O_i.

Блок 4. Моделювання комбінованого впливу загроз ОКІ з урахуванням нової компоненти – коефіцієнта сумарного впливу.

Загрози не завжди діють ізольовано. Часто вони взаємодіють, що може посилювати або послаблювати загальний негативний ефект. Для врахування цього синергетичного ефекту вводимо **коефіцієнт сумарного впливу** K_{syn}.

Загальний ризик для об'єкта при одночасній дії кількох загроз можна обчислити за формулою:

$$R_{total} = \sum_{i=1}^{n} P_j + I_j \times \left(1 + K_{sum}\right), \quad (4)$$

де, P_j – ймовірність виникнення загрози j,

I_j – вплив загрози j,

K_{sum} – коефіцієнт, що враховує сумарний ефект.

Приклад сумарного впливу:

Кібернетична атака на ОКІ може призвести до вимкнення систем управління, що робить його вразливішим для фізичної атаки. У такому випадку коефіцієнт K_{sum} може мати позитивне значення, скажімо K_{sum} = 0,2, що збільшує загальний ризик.

Блок 5. Оцінка сукупного ризику ОКІ.

Для кожної загрози T_j оцінюється індивідуальний ризик:

$$R_j = P_j \times I_j, \quad (5)$$

де, R_j – ризик для загрози j,

P_j – ймовірність виникнення загрози,

I_j – вплив загрози на об'єкт.

Сукупний ризик для ОКІ визначається з урахуванням всіх загроз на цей об’єкт:

$$R_{total} = \sum_{i=1}^{n} R_j \times (1 + K_{sum}), \quad (6)$$

Якщо коефіцієнт K_{sum} = 0**,** ризики загроз ОКІ не взаємодіють, і їх сумарний ефект є простим додаванням. Якщо K_{sum} > 0, загрози ОКІ підсилюють одна одну, якщо K_{sum} < 0, загрози ОКІ послаблюють одна одну.

Блок 6. Пріоритезація загроз ОКІ.

Після розрахунку сукупного ризику для кожного ОКІ можна виконати пріоритезацію загроз на цей об’єкт. Це дозволяє визначити, на які загрози ОКІ слід зосередити увагу першочергово для розробки відповідних заходів захисту.

Пріоритезація проводиться за рівнем ризику:

1. Високий ризик (потрібні негайні заходи).
2. Середній ризик (необхідні заходи протягом певного часу).
3. Низький ризик (достатньо стандартних заходів захисту).

Таким чином, запропонована в статті методика дозволяє систематично підходити до оцінки ризиків для ОКІ в умовах складних і комбінованих загроз для цих об’єктів. З урахуванням сумарного впливу вона забезпечує більш точну і гнучку оцінку, яка відображає реальні умови взаємодії різних типів загроз ОКІ. Застосування такої методики дозволяє більш ефективно розподілити ресурси, спрямовані на захист ОКІ, визначити пріоритети щодо захисних заходів та забезпечити готовність до можливих сценаріїв під час вогневого впливу противника.

Крім того, врахування коефіцієнта сумарного впливу робить можливим оцінювання ситуацій, де з’єднання загроз ОКІ створює нові, більш небезпечні умови для цих об’єктів. Це дозволяє системі захисту переходити від реактивних заходів до превентивних, забезпечуючи випереджувальне планування та підвищуючи загальний рівень надійності й стійкості ОКІ.

Висновки

У статті запропонована методика оцінювання загроз об’єктам критичної інфраструктури під час вогневого впливу противника з урахуванням сумарного коефіцієнту загроз. Дана методика дозволяє:

- оцінити загрози, які взаємодіють і мають підсилюючий або послаблюючий ефект на ОКІ;
- передбачити складні сценарії атак і більш точно планувати заходи захисту ОКІ;
- адаптувати її для різних типів ОКІ та різних типів загроз для цих об’єктів.

Описана методика може бути використана для підвищення стійкості ОКІ та ефективнішого розподілу ресурсів для їх захисту а також створить підґрунтя для вдосконалення існуючої національної системи безпеки.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Фурсенко О.М., Чумаченко С.М. та Кармазин С.В. (2015). Експертна оцінка загроз для об’єктів критичної інфраструктури газотранспортної системи України з використанням методу

аналізу ієрархій. Техногенно-екологічна безпека та цивільний захист, 9, 68-77. URL : http://tes.igns.gov.ua/wp-content/uploads/2018/02/V9.pdf [Дата перегляду 1.10.2024].
2. Мурасов Р. (2023). Методика оцінки ризиків для критичної інфраструктури в умовах бойових дій з урахуванням їх руйнівного та кумулятивного потенціалу. Соціальний розвиток і безпека, 13 (1), 152-160. https://doi.org/10.33445/sds.2023.13.1.13 [Дата звернення 1.10.2024].
3. Куртсеітов, Т., Мурасов, Р., & Мельник, Я. (2022). Обчислення надійності системи критичної інфраструктури шляхом декомпозиції її як складної системи. Social Development and Security, 12(5), 84-92. https://doi.org/10.33445/sds.2022.12.5.8 [Дата звернення 1.10.2024].
4. Мурасов Р., Нікітін А., Мещеряков І., Підгородецький М., Поплавець С. (2024). Удосконалення науково-методичного апарату для розрахунку ризиків виникнення та аналізу сценаріїв надзвичайних ситуацій на об'єктах критичної інфраструктури. Social Development and Security, 14 (1), 205-217. https://doi.org/10.33445/sds.2024.14.1.17 [Дата звернення 1.10.2024].
5. Мурасов Р., Нікітін А., Мещеряков І., Підгородецький М., Поплавець С. (2024). Методика оцінювання загроз і ризиків для об'єктів критичної інфраструктури за сценаріями розвитку надзвичайних ситуацій. Сучасні інформаційні технології у сфері безпеки та оборони, 3(48), 35-43. https://doi.org/10.33099/2311-7249/2023-48-3-35-43 [Дата звернення 1.10.2024].
6. Мурасов Р., Мещеряков І. (2023). Інформаційно-технічний спосіб попередження надзвичайних ситуацій терористичного характеру шляхом оцінки можливості поступового наростання руйнівних явищ, викликаних каскадними наслідками первинного терористичного впливу. Соціальний розвиток і безпека, 13 (5), 180-191. https://doi.org/10.33445/sds.2023.13.5.17 [Дата звернення 1.10.2024].
7. Яременко О.І., Страхніцький Я.О. (2022). Визначення та управління загрозами у структурі державної політики захисту критичної інфраструктури. Університетські наукові записки, 3 (87), 73-82. https://doi.org/10.37491/UNZ.87.6 [Дата звернення 1.10.2024].
8. Бобро Д. (2015). Визначення критеріїв оцінки та загроз критичній інфраструктурі. Стратегічні пріоритети. Серія: Економіка, 4, 83-93. URL : http://nbuv.gov.ua/UJRN/spe_2015_4_12 [Дата звернення 1.10.2024].

References

1 Fursenko O.M., Chumachenko S.M. & Karmazyn S.V. (2015). Expert assessment of threats to objects of critical infrastructure of the gas transportation system of Ukraine using the method of analysis of hierarchies. *Technogenic and ecological safety and civil protection*, 9, 68-77. Available from : http://tes.igns.gov.ua/wp-content/uploads/2018/02/V9.pdf [View date 1.10.2024].
2. Murasov, R. (2023). The method of risk assessment for critical infrastructure in the conditions of hostilities, taking into account their destructive and cumulative potential. *Social Development and Security*, 13(1), 152-160. https://doi.org/10.33445/sds.2023.13.1.13 [Accessed date 1.10.2024].
3. Kurtseitov, T., Murasov, R., & Melnyk, Y. (2022). Calculating the reliability of a critical infrastructure system by decomposing it as a complex system. *Social Development and Security*, 12(5), 84-92. https://doi.org/10.33445/sds.2022.12.5.8 [Accessed date 1.10.2024].
4. Murasov, R., Nikitin, A., Meshcheriakov, I., Pidhorodetskyi, M., & Poplavets, S. (2024). Improvement of the scientific and methodological apparatus for calculating the risks of occurrence and analyzing scenarios of emergency situations at critical infrastructure facilities.

Social Development and Security, 14(1), 205-217. https://doi.org/10.33445/sds.2024.14.1.17 [Accessed date 1.10.2024].

5. Murasov, R., Nikitin, A., Meshcheriakov, I., Pidhorodetskyi, M., & Poplavets, S. (2024).Methodology for assessing threats and risks for critical infrastructure objects under emergency development scenarios. *Modern Information Technologies in the Sphere of Security and Defence*, 3(48), 35-43. https://doi.org/10.33099/2311-7249/2023-48-3-35-43 [Accessed date 1.10.2024].
6. Murasov, R., & Meshcheriakov, I. (2023). The information and technical method of preventing emergency situations of a terrorist nature by assessing the possibility of gradual growth of destructive events caused by the cascading consequences of the primary terrorist impact. *Social Development and Security*, 13(5), 180-191. https://doi.org/10.33445/sds.2023.13.5.17 [Accessed date 1.10.2024].
7. Yaremenko O., Strahnitskyi Y. (2022). Detection and Management of Threats in the Structure of State Policy for Critical Infrastructure Protection. University Scientific Notes, 3 (87), 73-82. https://doi.org/10.37491/UNZ.87.6 [Accessed date 1.10.2024].
8. Bobro D. (2015). Determination of assessment criteria and threats to critical infrastructure. *Strategic priorities. Series: Economics*, 4, 83-93. Available from : http://nbuv.gov.ua/UJRN/spe_2015_4_12 [View date 1.10.2024].

Аналіз вразливостей великих мовних моделей

Analysis of vulnerabilities in large language models

Віктор Кольченко [A]
Corresponding author: аспірант, асистент кафедри захисту інформації, e-mail: viktor.v.kolchenko@lpnu.ua, ORCID: 0009-0002-0718-6859

Дмитро Сабодашко [A]
доктор філософії, старший викладач кафедри захисту інформації, e-mail: dmytro.v.sabodashko@lpnu.ua, ORCID: 0000-0003-1675-0976

Марія Швед [A]
к.т.н, старший викладач кафедри захисту інформації, e-mail: mariia.y.shved@lpnu.ua, ORCID: 0000-0003-0428-7777

Юрій Хома [A]
д.т.н., доцент кафедри інформаційно-вимірювальних технологій, e-mail: yurii.v.khoma@lpnu.ua, ORCID: 0000-0002-4677-5392

Назар Максимів [A]
студент кафедри захисту інформації, e-mail: nazar.maksymiv.mkbas.2023@lpnu.ua, ORCID: 0009-0009-6496-4056

Viktor Kolchenko [A]
Corresponding author: Postgraduate student, Assistant Lecturer, e-mail: viktor.v.kolchenko@lpnu.ua, ORCID: 0009-0002-0718-6859

Dmytro Sabodashko [A]
Doctor of Philosophy, Senior Lecturer of Department, e-mail: dmytro.v.sabodashko@lpnu.ua, ORCID: 0000-0003-1675-0976

Mariia Shved [A]
Candidate of Technical Sciences, Senior Lecturer of Department, e-mail: mariia.y.shved@lpnu.ua, ORCID: 0000-0003-0428-7777

Yuriy Khoma [A]
Dr of Technical Sciences, Associate Professor of Department, e-mail: yurii.v.khoma@lpnu.ua, ORCID: 0000-0002-4677-5392

Nazar Maksymiv [A]
Student of the Department of Information Security, e-mail: nazar.maksymiv.mkbas.2023@lpnu.ua, ORCID: 0009-0009-6496-4056

[A] Національний університет "Львівська політехніка", м. Львів, Україна
[A] Lviv Polytechnic National University, Lviv, Ukraine

Received: October 18, 2024 | Revised: October 28, 2024 | Accepted: October 31, 2024

DOI: 10.33445/sds.2024.14.5.22

Мета роботи: аналіз вразливостей великих мовних моделей (LLM) на основі класифікації OWASP Top 10 для застосунків LLM, проведення оцінки потенційних загроз та розробка рекомендацій щодо підвищення рівня безпеки цих моделей.

Метод: кількісні методи, зокрема використання інструменту Garak для ідентифікації та аналізу вразливостей у великих мовних моделях.

Результати дослідження: проаналізовано декілька критичних вразливостей, серед яких ін'єкції запитів, небезпечна обробка виводів, отруєння навчальних даних, розкриття конфіденційної інформації та інші. Навіть найсучасніші моделі, зокрема GPT-4, не забезпечують повної захищеності від цих загроз.

Теоретична цінність дослідження: дослідження поглиблює розуміння безпекових ризиків, пов'язаних з використанням великих мовних моделей, і пропонує нові підходи до їх аналізу. Це може стати основою для подальших теоретичних розробок у галузі кібербезпеки стосовно LLM.

Практична цінність дослідження: дослідження пропонує рекомендації для розробників, науковців і організацій, які використовують LLM. Впровадження безпечних практик розробки та постійний аудит моделей можуть суттєво підвищити захист використання LLM.

Цінність дослідження: використано інноваційний підхід для тестування безпеки LLM через імітацію різноманітних атак, зокрема ін'єкції запитів, отруєння даних, галюцинації та витоки інформації, що дозволяє виявити потенційні слабкі місця у функціонуванні моделей.

Майбутні дослідження: у подальших дослідженнях планується розширення спектра моделей і методів, що спрямовані на оптимізацію безпеки. Це сприятиме формуванню більш комплексного розуміння проблеми та вдосконаленню стратегій забезпечення безпеки.

Тип статті: Концептуальне дослідження.

Ключові слова: великі мовні моделі, LLM, OWASP, кібербезпека, вразливості.

Purpose: analyzing the vulnerabilities of large-scale language models (LSLMs) based on the OWASP Top 10 classification for LSLM applications, assessing potential threats, and developing recommendations for improving the security of these models.

Method: quantitative methods, including the use of the Garak tool to identify and analyze vulnerabilities in large language models.

Findings: Several critical vulnerabilities have been identified, including query injection, insecure output processing, training data poisoning, disclosure of confidential information, and others. Even the most advanced models, including GPT-4, do not provide full protection against these threats.

Theoretical implications: The study deepens the understanding of security risks associated with the use of large language models and suggests new approaches to their analysis. This can serve as a basis for further theoretical developments in the field of cybersecurity with respect to LLMs.

Practical implications: The study offers recommendations for developers, researchers, and organizations that use LLMs. Implementing safe development practices and continuous model auditing can significantly increase the security of LLMs.

Value: an innovative approach was used to test the security of LLMs by simulating various attacks, including query injection, data poisoning, hallucinations, and information leaks, which allows identifying potential weaknesses in the functioning of the models.

Future research: In further research, we plan to expand the range of models and methods aimed at optimizing security. This will contribute to a more comprehensive understanding of the problem and improve security strategies.

Paper type: Conceptual research.

Key words: large language models, LLM, OWASP, cybersecurity, vulnerabilities.

Вступ

У сучасному світі штучний інтелект і машинне навчання набувають все більшого значення в різних сферах, зокрема в охороні здоров'я, освіті, бізнесі та наукових дослідженнях. Однією з найважливіших технологій у цьому контексті є великі мовні моделі (LLM від англ. large language model), які є інноваційною технологією, яка забезпечує машинне розуміння та генерацію тексту на рівні, близькому до людського, з безпрецедентною масштабністю [1]. Глибокі нейронні мережі, що складаються з мільярдів параметрів, на прикладі моделі GPT-3, використовуються для виявлення складних лінгвістичних шаблонів і контекстуальних залежностей [2].

Найбільш поширенішими LLM є GPT-3.5, GPT-4, які демонструють високі показники продуктивності в задачах генерації тексту, природньо-мовної обробки та адаптивного навчання, що робить їх ефективними інструментами для різноманітних застосувань в галузях штучного інтелекту та обчислювальної лінгвістики [3]. Проте, ефективність великих мовних моделей у застосунках генеративного штучного інтелекту робить їх привабливими цілями для зловмисників, що створюють унікальні виклики у виявленні, попередженні та мінімізації вразливостей [4].

Тому дослідження вразливостей великих мовних моделей (LLM), зокрема таких, як ін'єкція запитів, небезпечна обробка виводу, отруєння навчальних даних, відмова в обслуговуванні моделі, вразливості ланцюга поставок, розкриття конфіденційної інформації, небезпечне проектування плагінів, надмірні повноваження агентів, надмірна залежність і викрадення моделі, а також шляхи їхнього вирішення, є актуальним і потребує ретельного вивчення.

Теоретичні основи дослідження

Великі мовні моделі (LLM) представляють собою клас моделей глибокого навчання, які набули значної популярності завдяки своїм видатним можливостям в обробці природної мови. Ці моделі, засновані на архітектурах нейронних мереж, використовуються для аналізу та генерації людської мови, що дозволяє досягати високого рівня точності в таких завданнях, як автоматичний переклад, генерація текстів, розпізнавання емоцій та інших аспектів аналізу текстових даних. Навчання LLM відбувається на масивних наборах даних, які включають текстові дані різного типу, що підвищує здатність моделей адаптуватися до різноманітних мовних контекстів [5].

Серед найбільш поширених та перспективних великих мовних моделей (LLM) виокремлюються GPT-3.5, GPT-4 та Mistral 7B, які підлягатимуть детальному аналізу в наступних розділах цієї статті.

GPT-3.5 є міжгенераційною моделлю, розробленою OpenAI, яка стоїть між GPT-3 та GPT-4 [6]. Ця модель є вдосконаленою версією GPT-3 з додатковими оптимізаціями, що покращують її здатність до розуміння тексту та генерації відповідей. GPT-3.5 має велику кількість гіперпараметрів, хоча їх менше, ніж у GPT-4, що дозволяє їй ефективно обробляти мовні структури та генерувати тексти, які є релевантними та зв'язними. Модель була навчена на великому обсязі даних з різних джерел, що охоплюють широкий спектр тем і стилів. В ході експериментів використовувалася остання версія GPT-3.5 Turbo, яка була опублікована в січні 2024 року.

GPT-4 є четвертим поколінням трансформерної архітектури, розробленої OpenAI [7]. Це покращена версія попередніх моделей, яка має більшу кількість параметрів, що дозволяє їй генерувати більш точні та зв'язні тексти, краще розуміти контекст та виконувати різноманітні завдання, такі як переклад, резюмування текстів та відповіді на запитання. GPT-4 була навчена

на величезному обсязі даних, що охоплюють різні галузі знань, що робить її універсальною в застосуванні.

Mistral 7B є моделлю машинного навчання з відкритим кодом, яка також була розроблена для задач обробки природної мови. На відміну від моделей GPT від OpenAI, Mistral 7B менш відома, але вона також має значний потенціал для вирішення конкретних задач у галузі NLP (Natural Language Processing) [8]. Модель поширюється під ліцензією Apache 2.0, що робить її доступною для модифікації та використання дослідниками та розробниками для реалізації власних потреб. У дослідженні використовувалася версія Mistral 7Bv-0.1, опублікована у грудні 2023 року.

Однією з основних причин проведення досліджень у цій сфері є те, що великі мовні моделі, мають величезний потенціал для розвитку багатьох галузей, але одночасно вони є складними системами, що вимагають особливого підходу до забезпечення їхньої безпеки. Наприклад, вони можуть бути використані для автоматизації бізнес-процесів, створення систем штучного інтелекту, що відповідають на запитання користувачів, надають аналітичні висновки, допомагають у медичних діагнозах або виконують переклад текстів з однієї мови на іншу. У той же час, вразливість до атак, таких як ін’єкція запитів або витік даних, може спричинити серйозні наслідки, особливо в умовах застосування цих моделей у високочутливих системах, таких як банківська справа або охорона здоров’я.

Проте, із розвитком генеративних мовних моделей зростає небезпека використання їх для дезінформаційних кампаній, маніпуляції громадською думкою або автоматизованого створення шкідливого контенту. Вразливості в таких моделях можуть бути використані для підриву довіри до інформаційних систем, що ставить під загрозу не лише конфіденційність даних, але й надійність сучасної інформаційної екосистеми.

Постановка проблеми

Основною проблемою, розглянутою в цій статті, є недостатній рівень безпеки великих мовних моделей (LLM), які широко застосовуються у різних галузях, але мають низку критичних вразливостей, що можуть бути використані зловмисниками. Такі моделі, як GPT-3.5, GPT-4 та Mistral 7B, не гарантують повного захисту, що створює ризики, пов'язані з ін’єкціями запитів, витоками конфіденційної інформації та генерацією небажаного або шкідливого контенту.

Окрім цього, деякі мовні моделі мають функції, які не завжди чітко описані в технічній документації, що може бути використано для потенційних атак. Ця проблема набуває особливої важливості в умовах зростаючого використання LLM у критично важливих системах, де будь-які вразливості можуть призвести до серйозних наслідків.

Методологія дослідження

У даному дослідженні для аналізу вразливостей великих мовних моделей було використано сканер Garak [9]. Який використовує обширний діапазон тестів та запитів до великої мовної моделі, імітуючи атаки, та використовує ряд детекторів для аналізу результатів відповіді моделі, щоб побачити, чи була модель вразлива до будь-якої з цих атак. Garak перевіряє наявність галюцинацій, витоку даних, ін’єкції запитів, поширення неправдивої інформації, генерації токсичності та багатьох інших вразливостей. Після завершення тестування моделі, garak надає звіти з результатами у форматі HTML та JSONL, які в подальшому були проаналізовано.

Класифікацію вразливосте проводили на основі проєкту OWASP Top 10 for Large Language Model Applications (Top 10 вразливостей для застосунків, побудованих на основі великих мовних моделей) [10]. Даний проєкт ідентифікує десять найкритичніших вразливостей безпеки в застосунка.

Результати

В ході дослідження було проведено аналіз вразливостей та яким чином вони можуть реалізовуватися та розроблено рекомендації по захисту від них [4].

Аналіз вразливості LLM01: Prompt Injection (Ін'єкція запитів)

Ця вразливість виникає, коли зловмисник вводить спеціально підготовлені запити (промпти) або дані, маніпулюючи LLM для отримання непередбачуваних або шкідливих результатів [11]. Це використовує можливості моделі генерувати відповіді, що призводить до порушення цілісності у відповідях моделі.

Ін'єкції запитів можуть бути двох видів:

- Пряма ін'єкція запитів: Зловмисник перезаписує або розкриває базовий системний запит. Це може дозволити нападникам експлуатувати системи на серверній частині, взаємодіючи з ненадійними функціями та сховищами даних, до яких можна отримати доступ через LLM.
- Непряма ін'єкція запитів: LLM приймає вхідні дані з зовнішніх джерел, який контролюються нападником, наприклад, з вебсайтів або файлів. Нападник може вставити ін'єкцію запиту в зовнішній вміст, захоплюючи контекст розмови. Це дозволить нападнику маніпулювати користувачем або додатковими системами, до яких може отримати доступ LLM. Крім того, для непрямих ін'єкцій запитів не обов'язково бути видимими чи читабельними для людини, досить, щоб текст оброблявся LLM.

Приклади вразливості:

- Зловмисник створює пряму ін'єкцію запиту до LLM, яка наказує йому ігнорувати системні запити застосунку та виконати запит, який повертає приватну, небезпечну або іншу небажану інформацію.
- Користувач використовує LLM для підсумовування вебсторінки, яка містить непряму ін'єкцію запиту. Це приводить до того, що застосунок отримує чутливу інформацію у користувача та здійснює витік даних через JavaScript або Markdown.

Рекомендації по захисту:

- Забезпечте контроль привілеїв доступу LLM до бекенд-систем. Надайте LLM власні API токени для розширюваної функціональності, такої як плагіни, доступ до даних і дозволи на рівні функцій. Дотримуйтесь принципу найменших привілеїв, обмежуючи LLM лише мінімально необхідним рівнем доступу для його призначених операцій.
- Додайте людину в процес для розширеної функціональності. При виконанні привілейованих операцій, таких як відправлення або видалення електронних листів, зробіть так, щоб додаток вимагав попередньої згоди користувача на таку дію. Це зменшує можливість непрямої ін'єкції запитів, які можуть призвести до несанкціонованих дій від імені користувача без його відома або згоди.
- Відокремлюйте зовнішній контент від запитів користувача. Виділяйте та позначайте, де використовується ненадійний контент, щоб обмежити його вплив на запити користувачів.
- Встановіть довірчі межі між LLM, зовнішніми джерелами та плагінами. Ставтеся до LLM як до ненадійного користувача та зберігайте остаточний контроль користувача над процесами прийняття рішень. Скомпрометована LLM може діяти як посередник (man-in-the-middle) між API вашого застосунку та користувачем, оскільки вона може

приховувати або маніпулювати інформацією перед її представленням користувачеві. Виділяйте потенційно ненадійні відповіді візуально для користувача.

- Періодично вручну проводьте моніторинг вхідних та вихідних даних LLM, щоб перевірити, чи вони відповідають очікуванням. Хоча це не є засобом пом'якшення, це може надати необхідні дані для виявлення слабкостей і їх усунення.

Аналіз вразливості LLM02: Insecure Output Handling (Небезпечна обробка виводу)

Проблема ризикованої обробки результатів стосується неадекватної перевірки, очищення та керування виводами, що створюються великими мовними моделями, перед їх передачею іншим елементам та системам. Це пов’язано з тим, що вміст, сформований за допомогою LLM, можуть регулювати зовнішні запити, що подібне до надання користувачам доступу до додаткового функціоналу. Відмінність ризикованої обробки виводів від надмірно залежності (вразливість LLM09) полягає в тому, що вона стосується результатів, генерованих LLM, перш ніж вони передаються далі, тоді як надмірна залежність зосереджується на ширших питаннях, пов’язаних із занадто великою залежністю від точності та доречності виводів LLM. Успішне використання вразливості небезпечної обробки виводу може призвести до XSS (міжсайтовий скриптинг) та CSRF (міжсайтова підробка запиту) у веб-браузерах, а також SSRF (підробка запитів на стороні сервера), підвищення привілеїв або виконання віддаленого коду на бекенд-системах [12].

Наступні умови можуть збільшити вплив цієї вразливості:

- Застосунок надає LLM привілеї, що виходять за межі того, що призначено для кінцевих користувачів, дозволяючи підвищення привілеїв або виконання віддаленого коду.
- Застосунок вразливий до атак через непряму ін’єкцію запитів, що може дозволити нападнику отримати привілейований доступ до середовища цільового користувача.
- Плагіни третіх сторін не забезпечують належної валідації вхідних даних.

Приклади вразливостей:

- Вивід LLM безпосередньо вводиться в системний командний рядок або функцію, таку як exec або eval, що призводить до виконання віддаленого коду.
- JavaScript або Markdown, згенеровані LLM, повертаються користувачеві. Потім код інтерпретується браузером, що призводить до XSS.

Рекомендації по захисту:

- Ставтеся до моделі як до будь-якого іншого користувача, застосовуючи підхід нульової довіри та застосовуйте належну валідацію вхідних даних відповідей, що надходять від моделі до функцій бекенду.
- Дотримуйтесь рекомендацій OWASP ASVS (Стандарт верифікації безпеки застосунків) [13] для забезпечення ефективної валідації та санітації вводу або інших рекомендацій з пост-процесінгу відповідей моделі [14].

Аналіз вразливості LLM03: Training Data Poisoning (Отруєння навчальних даних)

Отруєння навчальних даних відбувається, коли дані, що використовуються для тренування LLM, змінюються зі зловмисною метою, що призводить до упередженої, некоректної або шкідливої поведінки моделі [15]. Це може кардинально підірвати надійність та точність моделі, а також нанести шкоду репутації компанії.

Приклади вразливостей:

- Модель навчається використовуючи дані, джерело яких не було перевірене за походженням або змістом на будь-якому з етапів навчання, що може призвести до помилкових результатів, якщо дані є забрудненими (отруєними) або некоректними.
- Відсутність контролю доступу до інфраструктури або недостатня ізоляція може дозволити моделі отримувати небезпечні навчальні дані, що призведе до упереджених або шкідливих результатів.

Рекомендації по захисту:

- Перевіряйте ланцюг постачання даних для навчання, особливо коли вони отримані з зовнішніх джерел.
- Перевіряйте легітимність цільових джерел даних та отриманих даних під час навчання та тонкого налаштування.
- Перевіряйте ваші варіанти використання LLM та застосунок, з яким модель буде інтегровано. Створіть різні моделі за допомогою окремих навчальних даних або тонкого налаштування для різних варіантів використання, щоб отримати більш детальний і точний вихід генеративного ШІ відповідно до його визначеного варіанту використання.
- Забезпечити достатню ізоляцію за допомогою налаштувань прав доступу, щоб запобігти моделі зчитувати ненавмисні джерела даних, які можуть перешкодити результатам машинного навчання.
- Використовуйте суворий відбір або фільтри введення для певних навчальних даних або категорій джерел даних, щоб контролювати обсяг сфальсифікованих даних. Очищення даних, за допомогою таких методів, як виявлення статистичних аномалій, дозволяє виявити та видалити отруєні дані, які можуть бути використані на етапах тренування або тонкого налаштування.

Аналіз вразливості LLM04: Model Denial of Service (Відмова у обслуговуванні моделі)

Це означає атаки, спрямовані на перевантаження LLM, або шляхом перевантаження обчислювальних ресурсів інфраструктури, або шляхом спричинення поведінки моделі, що веде до її збою або значного сповільнення, тим самим перешкоджаючи її доступності та надійності.

Приклади вразливостей:

- Створення ресурсного голоду. Зловмисник надсилає запити, які призводять до збільшеного використання ресурсів через масове створення завдань для моделі.
- Зловмисник надсилає неочікувані запити, що споживають багато ресурсів, використовуючи нестандартну орфографію або послідовності.
- Зловмисник надсилає LLM потік вхідних даних, який перевищує вікно контексту, змушуючи модель споживати надмірні обчислювальні ресурси.
- Зловмисник створює вхідні дані, які запускають рекурсивне розширення контексту, змушуючи LLM повторно розширювати та обробляти вікно контексту.

Рекомендації по захисту:

- Валідація та очищення вхідних даних. Цей метод гарантує, що вхідні дані від користувачів відповідають встановленим обмеженням, а також фільтрує будь-який шкідливий вміст.
- Обмеження ресурсів, що виділяються на кожен запит або крок, сповільнюючи виконання запитів, які залучають складні елементи.

- Обмеження кількість запитів до API, які може зробити окремий користувач (авторизований, або ідентифікований за IP-адресою) за певний проміжок часу.
- Обмеження черги дій: Цей метод обмежує кількість дій, що очікують на виконання, та загальну кількість дій у системі, які реагують на відповіді LLM.
- Постійний моніторинг використання ресурсів LLM для виявлення аномальних сплесків, які можуть вказувати на атаку типу “відмова в обслуговуванні” (DoS).
- Обмеження вхідних даних: Цей метод встановлює строгі обмеження на розмір вхідних даних на основі вікна контексту LLM, запобігаючи перевантаженню та виснаженню ресурсів.
- Підвищення обізнаності серед розробників щодо потенційних DoS-вразливостей у моделях та затосунках.

Аналіз вразливості LLM05: Supply Chain Vulnerabilities (Вразливості ланцюга поставок)

В ланцюгу постачання великих мовних моделей існують вразливості, що негативно впливають на цілісність навчальних даних, моделей машинного навчання та платформ для розгортання. Такі слабкі місця можуть спричинити виникнення упередженості в результатах, порушення у сфері безпеки або навіть катастрофічні збої у системі. Раніше акцент зазвичай робився на вразливостях програмних компонентів, однак у сфері машинного навчання ця проблематика розширюється через використання попередньо тренованих моделей і навчальних даних від сторонніх постачальників, які можуть бути піддані атакам, спрямованим на їхню зміну чи “отруєння” [16].

Приклади вразливостей:

- Традиційні вразливості сторонніх програмних пакетів, бібліотек, включаючи застарілі або непідтримувані компоненти.
- Використання вразливої попередньо навченої моделі для тонкого налаштування може призвести до вразливості всієї моделі.
- Використання забруднених даних з відкритих джерел для навчання моделі може призвести до того, що модель буде генерувати шкідливий або неправдивий вихід.
- Використання застарілих або непідтримуваних моделей, які більше не оновлюються, може призвести до проблем із безпекою.
- Нечіткі умови використання та політика конфіденційності даних операторів моделі можуть призвести до того, що конфіденційні дані програми будуть використані для навчання моделі, а потім оприлюднені. Це також може стосуватися ризиків використання моделі, яка містить матеріали, захищені авторським правом.

Рекомендації по захисту:

- Ретельно перевіряйте джерела даних і постачальників, включаючи їхні умови використання та політику конфіденційності. Співпрацюйте лише з надійними постачальниками. Переконайтеся, що в них запроваджено належні та незалежно перевірені заходи безпеки, а політика оператора моделі відповідає вашій політиці захисту даних (тобто ваші дані не використовуються для навчання їхніх моделей). Також отримайте гарантії та правові заходи щодо неналежного використання захищеного авторським правом матеріалу від обслуговуючих організацій моделі.
- Ознайомтеся та застосуйте методи запобігання вразливостей, описані в розділі A06:2021 – “Вразливі та застарілі компоненти” стандарту OWASP Top 10 [13]. До цього належить сканування вразливостей, управління ними та оновлення компонентів.

Також застосовуйте ці методи контролю в середовищах розробки, які мають доступ до конфіденційних даних.

- Використовуйте цифровий підпис для моделей і коду під час роботи із зовнішніми моделями та постачальниками.
- Виявлення аномалій у даних та тестування на стійкість до спроб ввести в оману моделей можуть допомогти виявити фальшування та отруєння.
- Реалізуйте належний моніторинг для виявлення вразливостей компонентів та середовища, використання неавторизованих плагінів та застарілих компонентів, включаючи модель та її артефакти.
- Впровадьте політику патчів для усунення вразливих або застарілих компонентів. Переконайтеся, що програма використовує підтримувані версії API та базової моделі.
- Регулярно переглядайте та аудітуйте безпеку та доступ постачальників, щоб переконатися, що їхній рівень безпеки та умови використання не змінилися.

Аналіз вразливості LLM06: Sensitive Information Disclosure (Розкриття конфіденційної інформації)

Застосунки на основі LLM можуть ненавмисно розкривати конфіденційну інформацію, власні алгоритми або інші конфіденційні дані через свої відповіді. Це може призвести до несанкціонованого доступу до чутливих даних, порушення інтелектуальної власності, порушення конфіденційності та інших проблем безпеки.

Приклади вразливостей:

- Оператор непрямо вводить чутливі або конфіденційні дані в процеси навчання моделі, які потім повертаються у результатах генерації LLM.
- Неповне або неправильне фільтрування конфіденційної інформації в відповідях LLM.
- Надмірне навчання або запам’ятовування конфіденційних даних під час навчання моделі.
- Ненавмисне розкриття конфіденційної інформації через неправильне тлумачення моделлю, відсутність методів очищення даних або як результат помилки.

Рекомендації по захисту:

- Застосуйте належні методи очищення даних, щоб запобігти потраплянню конфіденційних даних до навчальних даних моделі.
- Впровадьте надійні методи перевірки та очищення вхідних даних для виявлення та фільтрації потенційно шкідливих елементів, щоб запобігти отруєнню моделі.
- Будь-яка інформація, що вважається конфіденційною в даних для тренування або тонкого налаштування, може бути потенційно розкрита користувачеві. Тому застосовуйте принцип мінімальних привілеїв і не навчайте модель на інформації, до якої має доступ користувач із найвищими привілеями, якщо вона може бути відображена користувачеві з нижчими привілеями.
- Слід обмежити доступ до зовнішніх джерел даних
- Застосуйте суворі методи контролю доступу до зовнішніх джерел даних та ретельний підхід до підтримки безпечного ланцюга поставок.

Аналіз вразливості LLM07: Insecure Plugin Design (Небезпечне проектування плагінів)

У контексті LLM, небезпечне проектування плагінів стосується інтеграції додаткових функцій або розширень, які належним чином не захищені, потенційно вносячи вразливості в безпечну базову модель.

Приклади вразливостей:

- Плагін приймає всі параметри в одному текстовому полі замість окремих параметрів вводу.
- Плагін приймає рядки конфігурації замість параметрів, які можуть перезаписати всі налаштування конфігурації.
- Плагін приймає невідформатовані SQL-запити або частини коду замість параметрів.
- Автентифікація виконується без явної авторизації для конкретного плагіна.
- Плагін розглядає весь вміст LLM як повністю створений користувачем і виконує будь-які запити без додаткової авторизації.

Рекомендації по захисту:

- Плагіни повинні, за можливості, використовувати суворий параметризований ввод та включати перевірку типу та діапазону вхідних даних. Якщо це неможливо, слід запровадити додатковий рівень, що здійснює аналіз запитів та застосовує валідацію та очищення. У випадках, коли за логікою програми необхідно приймати неформатовані дані, їх слід ретельно перевіряти, щоб гарантовано запобігти виклику потенційно шкідливих методів.
- Розробники плагінів повинні застосовувати рекомендації OWASP ASVS (Application Security Verification Standard) [13] для забезпечення належної валідації та очищення вхідних даних.
- Плагіни повинні пройти ретельне тестування та перевірку для забезпечення належної валідації.
- Плагіни повинні використовувати відповідні протоколи авторизації, такі як OAuth2, для застосування ефективного контролю доступу.
- Вимагайте ручного дозволу користувача та підтвердження будь-якої дії, виконаної чутливими плагінами.
- Оскільки плагіни зазвичай це REST API, розробники повинні застосовувати рекомендації, наведені в OWASP Top 10 API Security Risks – 2023 [17], щоб мінімізувати загальні вразливості.

Аналіз вразливості LLM08: Excessive Agency (Надмірні повноваження агенту)

В розробці програмного забезпечення “агент” зазвичай означає програму або програмний компонент, який діє автономно від імені користувача, іншої програми або системи. Агенти призначені для виконання певних завдань або прийняття рішень на основі заздалегідь визначених правил, алгоритмів або моделей машинного навчання. Вони можуть працювати незалежно або співпрацювати з іншими агентами для досягнення спільних цілей. Надмірні повноваження агенту в застосунках заснованих на LLM, є вразливістю, спричиненою надмірними дозволами, надмірною функціональністю або занадто великою автономією. Ця вразливість може призвести до широкого спектру наслідків, що впливають на конфіденційність, цілісність та доступність даних, і залежить від того, з якими системами може взаємодіяти застосунок.

Приклади вразливостей:

- Надмірна функціональність: агент має доступ до плагінів, які містять функції, що не потрібні для належної роботи системи. Наприклад, розробник повинен надати сервісу LLM можливість читати документи зі сховища, але сторонній плагін, який він обирає використовувати, також дозволяє редагувати та видаляти документи.
- Надмірні дозволи: Плагін має дозволи на інших системах, які не потрібні для належної роботи програми. Наприклад, плагін, призначений для читання даних, підключається

до сервера бази даних за допомогою облікового запису, який має не тільки дозволи SELECT, але й дозволи UPDATE, INSERT та DELETE.

- Надмірні дозволи: Плагін, призначений для виконання операцій від імені користувача, отримує доступ до нижчестоящих систем за допомогою загальної облікового запису з високими правами. Наприклад, плагін для читання сховища документів поточного користувача підключається до сховища документів за допомогою облікового запису з високими правами, який має доступ до файлів усіх користувачів.
- Надмірна автономія: Програма або плагін на основі LLM не може самостійно перевіряти та підтверджувати дії з високим впливом результату. Наприклад, плагін, який дозволяє видаляти документи користувача, виконує видалення без будь-якого підтвердження з боку користувача.

Рекомендації по захисту:

- Обмежте плагіни або інструменти, які дозволено викликати агентам, лише мінімально необхідними функціями. Наприклад, якщо система не потребує можливості отримувати вміст URL-адреси, то такий плагін не слід пропонувати агенту LLM.
- Обмежте функціонал, реалізовані в плагінах/інструментах, мінімально необхідним. Наприклад, плагіну, який отримує доступ до поштової скриньки користувача для аналізу електронних листів, може знадобитися лише можливість читати листи, тому плагін не повинен містити інших функцій, таких як видалення або надсилання повідомлень.
- За можливості слід уникати функцій з гнучкою поведінкою (наприклад, виконання команди системної оболонки, отримання URL-адреси тощо) та використовувати плагіни/інструменти з більш детальною функціональністю. Наприклад, програмі може знадобитися записати вихідні дані у файл. Якщо б це було реалізовано за допомогою плагіна для виконання функції системної оболонки, тоді сфера застосування небажаних дій була б дуже широкою (можна виконати будь-яку іншу команду оболонки). Більш безпечною альтернативою було б створити плагін для запису файлів, який міг би підтримувати лише цю конкретну функцію.
- Відстежуйте авторизацію користувача та область безпеки, щоб гарантувати, що дії, які виконуються від імені користувача, здійснюються на нижчестоящих системах у контексті цього конкретного користувача та з мінімально необхідними привілеями. Наприклад, плагін, який читає репозиторій коду користувача, має вимагати від користувача автентифікації через OAuth із мінімально необхідною областю безпеки.

Аналіз вразливості LLM09: Overreliance (Надмірна залежність)

Надмірна залежність може виникнути, коли LLM генерує помилкову інформацію і подає її як достовірну. Хоча LLM можуть створювати креативний та інформативний контент, вони також можуть генерувати контент, який є фактично неточним, недоречним або небезпечним. Це називається галюцинацією або конфабуляцією [18]. Коли люди або системи довіряють цій інформації без контролю чи підтвердження, це може призвести до витоку безпеки, дезінформації, непорозумінь, юридичних проблем та шкоди репутації.

Приклади вразливостей:

- Неточність під маскою авторитетності: LLM може надавати невірну інформацію, при цьому уявляючи її як абсолютно достовірну та правдиву. Системи, розроблені без належних перевірок та контролю якості, можуть сприймати цю інформацію як істину, що вводить користувачів в оману та потенційно призводить до шкоди.

- Небезпечні підказки: LLM може пропонувати небезпечний або помилковий код, який, якщо його інтегрувати в програмне забезпечення без належної перевірки та підтвердження, може створити вразливості в системі.

Рекомендації по захисту:

- Регулярно контролюйте та переглядайте вихідні дані LLM. Узгоджуйте і відфільтровуйте несумісний текст. Порівняння відповідей декількох моделей для одного запиту може допомогти краще оцінити якість та узгодженість вихідних даних.
- Перевіряйте вихідні дані LLM з надійними зовнішніми джерелами. Цей додатковий рівень перевірки допоможе гарантувати, що інформація, надана моделлю, є точною та достовірною.
- Підвищення якості виведення за допомогою тонкого налаштування. Загальні попередньо навчені моделі частіше генерують неточну інформацію порівняно з тонко налаштованими моделями в конкретній області. Для цього можна застосувати такі методи, як проектування запитів (prompt engineering) [19], повне налаштування моделі та підказки щодо ланцюга міркувань.
- Впровадження механізмів автоматичної перевірки для порівняння згенерованого виводу з відомими фактами або даними. Це може забезпечити додатковий рівень безпеки та зменшити ризики, пов’язані з галюцинаціями або конфабуляцією.
- Створіть API та інтерфейси користувача, які сприяють відповідальному та безпечному використанню LLM. Це може включати такі заходи, як:
    - Фільтри вмісту: Запобігання створенню або поширенню шкідливого чи образливого контенту.
    - Попередження користувачів про можливі неточності: Інформування користувачів про те, що LLM може генерувати неточну інформацію, та заохочення до критичної оцінки вихідних даних.
    - Чітке маркування контенту, створеного штучним інтелектом: Інформування користувачів про те, що певний контент був створений LLM, а не людиною.

Аналіз вразливості LLM10: Model Theft (Викрадення моделі)

Викрадення моделі включає несанкціоноване копіювання або екстракцію LLM, або їхні ваги та параметри витягуються для створення функціонального еквівалента. Така крадіжка може бути використана для конкурентної переваги, зловмисних цілей або для обходу ліцензійних обмежень, а також отримання несанкціонованого доступу до чутливої інформації, що міститься в навчальних даних [20].

Приклади вразливостей:

- Зловмисник використовує вразливість в інфраструктурі компанії, щоб отримати несанкціонований доступ до сховища LLM через помилки конфігурації мережевих або програмних налаштувань безпеки.
- Сценарій внутрішньої загрози, коли незадоволений співробітник викрадає модель або пов’язані з нею артефакти.
- Зловмисник надсилає запити до API моделі, використовуючи ретельно підготовлені вхідні дані та методи ін’єкції запитів (LLM01), щоб зібрати достатню кількість вихідних даних для створення “тіньової” моделі. Тіньова модель – це спроба відтворити оригінальну модель шляхом аналізу її вихідних даних.
- Зловмисник може обійти методи фільтрації вхідних даних LLM, щоб здійснити атаку з побічним каналом і зрештою викрасти ваги та інформацію про архітектуру моделі. Атака з побічним каналом – це техніка, яка дозволяє витягувати конфіденційну

інформацію з комп'ютерної системи, аналізуючи її неявні витоки, такі як час виконання, споживання пам'яті або інші показники.

Рекомендації по захисту:

- Впровадьте надійний контроль доступу (наприклад, RBAC та принцип мінімальних привілеїв) та потужні механізми аутентифікації, щоб обмежити несанкціонований доступ до сховищ моделей LLM та середовищ навчання.
- Обмежте доступ LLM до мережевих ресурсів, внутрішніх служб та API.
- Регулярно здійснюйте моніторинг та перевіряйте журнали доступу та дії, пов'язані зі сховищами моделей, щоб швидко виявляти та реагувати на будь-яку підозрілу або несанкціоновану поведінку.
- Автоматизуйте розгортання з керуванням робочими процесами відстеження та затвердження для посилення контролю доступу та розгортання в межах інфраструктури.
- Впровадьте засоби керування та стратегії усунення ризиків, щоб зменшити ризик використання методів ін'єкції підказок, що призводять до атак з побічним каналом.
- Застосовуйте обмеження швидкості викликів API, де це можливо, або фільтри для зменшення ризику викрадення даних із програм LLM.
- Посилення заходів фізичної безпеки.

Впровадьте фреймворк водяних знаків на етапах вбудовування та тонкого налаштування життєвого циклу LLM.

Висновки

У даній роботі було розглянуто питання вразливостей великих мовних моделей (LLM) у контексті їхнього застосування в сучасних інформаційних системах. Основна увага була зосереджена на аналізі критичних вразливостей, серед яких ін'єкція запитів, небезпечна обробка виводів, отруєння навчальних даних та розкриття конфіденційної інформації. В ході дослідження особливу увагу було приділено вивченню методів захисту, заснованих на рекомендаціях OWASP Top 10 для застосувань LLM, які є найбільш перспективними та теоретично придатними для впровадження у сучасні моделі.

Під час дослідження із застосуванням інструменту Garak було знайдено можливість ідентифікації низки базових вразливостей у великих мовних моделях, таких як GPT-3.5, GPT-4 та Mistral 7B. Основним досягненням цього дослідження стало те, що за допомогою інструменту вдалося ідентифікувати потенційні загрози, такі як ін'єкція запитів та небезпечна обробка виводів, що можуть призвести до витоку інформації або генерації небажаного контенту.

Отримані результати відкривають широкі можливості для подальшого дослідження та впровадження нових методів захисту мовних моделей. Використання методів захисту, таких як фільтрація виводів та обмеження доступу до навчальних даних, допоможе суттєво підвищити безпеку великих мовних моделей, зокрема для застосувань у галузях з високими вимогами до конфіденційності та надійності даних. Таким чином, дане дослідження показало важливість впровадження комплексних заходів для підвищення захищеності великих мовних моделей, що дозволить забезпечити їх безпечне використання в реальних умовах, мінімізуючи ризики несанкціонованого доступу та викрадення інформації.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Sreerakuvandana, S., Pappachan, P., Arya, V. (2024). Understanding large language models. In Advances in computational intelligence and robotics book series (pp. 1–24). https://doi.org/10.4018/979-8-3693-3860-5.ch001
2. Chen, Z., Xu, L., Zheng, H., Chen, L., Tolba, A. et al. (2024). Evolution and prospects of foundation models: from large language models to large multimodal models. Computers, Materials & Continua, 80(2), 1753-1808. https://doi.org/10.32604/cmc.2024.052618.
3. Brown, T. B., Mann, B., Ryder, N., Subbiah, M., Kaplan, J., Dhariwal, P., ... Amodei, D. (2020). Language Models are Few-Shot Learners. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2005.14165
4. Brown, H., Lee, K., Mireshghallah, F., Shokri, R., Tramèr, F. (2022). What Does it Mean for a Language Model to Preserve Privacy? 2022 ACM Conference on Fairness, Accountability, and Transparency. https://doi.org/10.1145/3531146.3534642
5. Gholami, N. Y. (2024b). Large Language Models (LLMs) for Cybersecurity: A Systematic review. World Journal of Advanced Engineering Technology and Sciences, 13(1), 057–069. https://doi.org/10.30574/wjaets.2024.13.1.0395
6. Ye, J., Chen, X., Xu, N., Zu, C., Shao, Z., Liu, S., …Cui, Y. (2023). A comprehensive capability analysis of GPT-3 and GPT-3.5 series models. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2303.10420
7. OpenAI. (2023). GPT-4 Technical Report. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2303.08774
8. Jiang, A. Q., Sablayrolles, A., Mensch, A., Bamford, C., Chaplot, D. S., De Las Casas, D., …Bressand, F. (2023). Mistral 7B. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2310.06825
9. Derczynski, L., Galinkin, E., Majumdar, S. (2024). Garak: A framework for large language model red teaming. [Електронний ресурс] // Garak Ai – URL : https://garak.ai
10. OWASP. (2023). OWASP top 10 for LLM applications, version 1.1.[Електронний ресурс] // OWASP – URL : https://owasp.org/www-project-top-10-for-large-language-model-applications/assets/PDF/OWASP-Top-10-for-LLMs-2023-v1_1.pdf
11. Capitella, D. (n.d.). Forging thoughts and observations in REACT-based LLM agents via prompt injection. [Електронний ресурс] // Wi Labs – URL : https://labs.withsecure.com/publications/llm-agent-prompt-injection
12. Петрів, П., Опірський, І. (2023). АНАЛІЗ ПРОБЛЕМАТИКИ ВИКОРИСТАННЯ ІСНУЮЧИХ СТАНДАРТІВ З ВЕБ-ВРАЗЛИВОСТЕЙ. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(22), 96–112. https://doi.org/10.28925/2663-4023.2023.22.96112
13. OWASP Application Security Verification Standard (ASVS) [Електронний ресурс] // OWASP. URL : https://owasp.org/www-project-application-security-verification-standard/
14. Goldstein, J. A., Sastry, G., Musser, M., DiResta, R., Gentzel, M., Sedova, K. (2023). Generative language models and automated influence operations: emerging threats and potential mitigations. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2301.04246
15. Aghakhani, H., Dai, W., Manoel, A., Fernandes, X., Kharkar, A., Kruegel, C., …Vigna, G. (2023). TrojanPuzzle: Covertly Poisoning Code-Suggestion Models. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2301.02344

16. Yao, Y., Duan, J., Xu, K., Cai, Y., Sun, Z., Zhang, Y. (2023). A survey on Large Language Model (LLM) Security and Privacy: The Good, the bad, and the ugly. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2312.02003
17. Team, O. W. A. S. P. (n.d.). OWASP Top 10 API Security Risks – 2023 - OWASP API Security Top 10. [Електронний ресурс] // OWASP URL : https://owasp.org/API-Security/editions/2023/en/0x11-t10/
18. Zhang, M., Press, O., Merrill, W., Liu, A., Smith, N. (2023). How language model hallucinations can snowball. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2305.13534
19. White, J., Fu, Q., Hays, S., Sandborn, M., Olea, C., Gilbert, …Schmidt, D. (2023). A Prompt Pattern Catalog to Enhance Prompt Engineering with ChatGPT. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2302.11382
20. Shayegani, E., Mamun, A., Fu, Y., Zaree, P., Dong, Y., Abu-Ghazaleh, N. (2023). Survey of vulnerabilities in large language models revealed by adversarial attacks. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2310.10844

References

1 Sreerakuvandana, S., Pappachan, P., Arya, V. (2024). Understanding large language models. In Advances in computational intelligence and robotics book series (pp. 1–24). https://doi.org/10.4018/979-8-3693-3860-5.ch001
2. Chen, Z., Xu, L., Zheng, H., Chen, L., Tolba, A. et al. (2024). Evolution and prospects of foundation models: from large language models to large multimodal models. Computers, Materials & Continua, 80(2), 1753-1808. https://doi.org/10.32604/cmc.2024.052618.
3. Brown, T. B., Mann, B., Ryder, N., Subbiah, M., Kaplan, J., Dhariwal, P., ... Amodei, D. (2020). Language Models are Few-Shot Learners. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2005.14165.
4. Brown, H., Lee, K., Mireshghallah, F., Shokri, R., Tramèr, F. (2022). What Does it Mean for a Language Model to Preserve Privacy? 2022 ACM Conference on Fairness, Accountability, and Transparency. https://doi.org/10.1145/3531146.3534642
5. Gholami, N. Y. (2024b). Large Language Models (LLMs) for Cybersecurity: A Systematic review. World Journal of Advanced Engineering Technology and Sciences, 13(1), 057–069. https://doi.org/10.30574/wjaets.2024.13.1.0395
6. Ye, J., Chen, X., Xu, N., Zu, C., Shao, Z., Liu, S., …Cui, Y. (2023). A comprehensive capability analysis of GPT-3 and GPT-3.5 series models. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2303.10420
7. OpenAI. (2023). GPT-4 Technical Report. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2303.08774
8. Jiang, A. Q., Sablayrolles, A., Mensch, A., Bamford, C., Chaplot, D. S., De Las Casas, D., …Bressand, F. (2023). Mistral 7B. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2310.06825
9. Derczynski, L., Galinkin, E., Majumdar, S. (2024). Garak: A framework for large language model red teaming. // Garak Ai – Available from : https://garak.ai
10. OWASP. (2023). OWASP top 10 for LLM applications, version 1.1. // OWASP Available from : https://owasp.org/www-project-top-10-for-large-language-model-applications/assets/PDF/OWASP-Top-10-for-LLMs-2023-v1_1.pdf
11. Capitella, D. (n.d.). Forging thoughts and observations in REACT-based LLM agents via prompt injection. // Wi Labs – Available from : https://labs.withsecure.com/publications/llm-agent-prompt-injection

12. Petriv, P., Opirskyi, I. (2023). Analysis of the problems of using existing web vulnerability standards. *Cybersecurity: education, science, technology*, 2(22), 96–112. https://doi.org/10.28925/2663-4023.2023.22.96112
13. OWASP Application Security Verification Standard (ASVS) [Електронний ресурс] // OWASP - Available from : https://owasp.org/www-project-application-security-verification-standard/
14. Goldstein, J. A., Sastry, G., Musser, M., DiResta, R., Gentzel, M., Sedova, K. (2023). Generative language models and automated influence operations: emerging threats and potential mitigations. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2301.04246
15. Aghakhani, H., Dai, W., Manoel, A., Fernandes, X., Kharkar, A., Kruegel, C., …Vigna, G. (2023). TrojanPuzzle: Covertly Poisoning Code-Suggestion Models. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2301.02344
16. Yao, Y., Duan, J., Xu, K., Cai, Y., Sun, Z., Zhang, Y. (2023). A survey on Large Language Model (LLM) Security and Privacy: The Good, the bad, and the ugly. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2312.02003
17. Team, O. W. A. S. P. (n.d.). OWASP Top 10 API Security Risks – 2023 - OWASP API Security Top 10. [Електронний ресурс] // OWASP – Available from : https://owasp.org/API-Security/editions/2023/en/0x11-t10/
18. Zhang, M., Press, O., Merrill, W., Liu, A., Smith, N. (2023). How language model hallucinations can snowball. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2305.13534
19. White, J., Fu, Q., Hays, S., Sandborn, M., Olea, C., Gilbert, …Schmidt, D. (2023). A Prompt Pattern Catalog to Enhance Prompt Engineering with ChatGPT. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2302.11382
20. Shayegani, E., Mamun, A., Fu, Y., Zaree, P., Dong, Y., Abu-Ghazaleh, N. (2023). Survey of vulnerabilities in large language models revealed by adversarial attacks. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2310.10844

Проблематика процесу реалізації охорони державної таємниці в Україні

Problems of the implementation process of state secret protection in Ukraine

Юрій Янчук
e-mail: yura.yanchuk1994@gmail.com, ORCID: 0009-0008-0962-4166
[A] Міністерство оборони України, м. Київ, Україна

Yurii Yanchuk
e-mail: yura.yanchuk1994@gmail.com, ORCID: 0009-0008-0962-4166
[A] Ministry of Defense of Ukraine, Kyiv, Ukraine

Received: October 4, 2024 | Revised: October 28, 2024 | Accepted: October 31, 2024

DOI: 10.33445/sds.2024.14.5.23

Мета роботи: аналіз існуючої нормативно-правової бази в Україні щодо захисту державної таємниці, виявлення проблемних аспектів і розробка рекомендацій для їх усунення
Метод: аналітичний та компаративний.
Результати дослідження: проведено аналіз нормативно-правової бази в сфері охорони державної таємниці та надано рекомендації щодо її удосконалення.
Теоретична цінність дослідження: аналіз дає змогу оцінити актуальні проблеми процесу забезпечення охорони державної таємниці.
Цінність дослідження: сучасне бачення проблематики забезпечення охорони державної таємниці на законодавчому рівні.
Майбутні дослідження: у ході подальших досліджень доцільно опрацювати алгоритми, на основі яких можливо створити підґрунтя для удосконалення нормативно-правових документів та внесення змін щодо них.
Тип статті: теоретична.

Purpose: analysis of the existing regulatory and legal framework in Ukraine regarding the protection of state secrets, identification of problematic aspects and development of recommendations for their elimination
Method: analytical and comparative.
Research results: an analysis of the regulatory framework in the field of state secret protection was carried out and recommendations for its improvement were provided.
The theoretical value of the research: the analysis makes it possible to assess the actual problems of the process of ensuring the protection of state secrets.
The value of the research: a modern vision of the issues of ensuring the protection of state secrets at the legislative level.
Future research: in the course of further research, it is expedient to develop algorithms on the basis of which it is possible to create a basis for improving regulatory and legal documents and making changes to them.
Papertype: theoretical.

Ключові слова: державна таємниця, захист інформації, інформаційна безпека, кібербезпека, національна безпека, нормативно-правове регулювання, міжнародні стандарти.

Key words: state secret, information protection, information security, cyber security, national security, regulatory and legal regulation, international standards.

Вступ

У статті проведено аналіз охорони державної таємниці як суб’єкта правого регулювання в Україні, зосереджено увагу на основних законодавчих і нормативних актах, які визначають порядок захисту та обробки інформації, що становить державну таємницю. Досліджено ключові положення Закону України “Про державну таємницю”, який регламентує правила класифікації інформації, що підлягає засекречуванню, а також визначає процедури для її захисту, розсекречення та контролю. Розглянуто кроки вітчизняного законодавства щодо забезпечення інтеграції міжнародних стандартів у національну правову систему та практичні механізми забезпечення належного режиму секретності.

Висвітлено проблеми, що виникають у процесі реалізації законодавчих норм, зокрема, пов'язані з дотриманням режиму секретності в умовах сучасних технологічних викликів. Проведено аналіз ефективності існуючих систем захисту інформації, а також ролі державних органів у забезпеченні безпеки інформації, що є важливим для забезпечення національної безпеки. Окрему увагу приділено аспектам правового контролю за дотриманням режиму секретності та можливими правопорушеннями у цій сфері.

У статті наголошується на необхідності подальшого вдосконалення національного законодавства щодо забезпечення ефективного захисту державної таємниці в умовах постійних змін у сфері інформаційних технологій і міжнародних відносин. Підкреслено

важливість системного підходу до регулювання державної таємниці, який би враховував як вимоги забезпечення національної безпеки, так і права громадян на інформацію, що є необхідним для відкритості та прозорості державного управління.

Теоретичні основи дослідження

Охорона державної таємниці є основоположним аспектом забезпечення національної безпеки будь-якої держави, і Україна не є винятком у цьому контексті. Наявність спеціально розробленої законодавчої бази є критично важливою для охорони чутливої інформації, що має стратегічне значення для держави. Законодавство України в цій сфері передбачає комплексний підхід до регулювання питань, пов’язаних із захистом державної таємниці, включаючи визначення критеріїв та процедур для засекречування та розсекречування інформації [14, с.42].

Однак, навіть з наявністю цього законодавства, система охорони державної таємниці стикається з рядом серйозних проблем. По-перше, існуючі правові механізми часто виявляються недостатньо ефективними для реагування на нові виклики, що постають перед державою у зв'язку з розвитком технологій і зростанням загроз кібербезпеці. По-друге, відзначається недостатня координація між різними державними органами, що ускладнює забезпечення комплексного підходу до охорони чутливої інформації.

Серед основних проблем можна виділити недоліки в технічному захисті інформаційних систем і недостатню увагу до фізичної охорони інформаційних носіїв. Зокрема, існує потреба в удосконаленні процедур перевірки осіб, які мають доступ до державної таємниці, а також в проведенні регулярних тренінгів та навчання персоналу, щоб запобігти порушенням і підвищити рівень обізнаності [13, с.49].

Постановка проблеми

Охорона державної таємниці є вагомим аспектом забезпечення інформаційної безпеки, як важливої складової національної безпеки, що потребує чіткого і ефективного нормативно-правового регулювання. В Україні, як і в інших країнах, існує система законодавчих актів, що визначають порядок класифікації, захисту та обробки інформації, що становить державну таємницю. Однак у зв’язку з швидким розвитком інформаційних технологій і зростанням міжнародних загроз виникає необхідність постійного вдосконалення нормативних актів для забезпечення ефективного захисту конфіденційної інформації. Порушення режиму секретності або недоліки у правовому регулюванні можуть мати серйозні наслідки для безпеки держави і її стратегічних інтересів.

На сучасному етапі виникають нові виклики, пов’язані з інтеграцією міжнародних стандартів у національне законодавство та адаптацією правових механізмів до нових технологічних умов. Це створює потребу у детальному аналізі існуючих законодавчих норм та їх практичного застосування, а також у розробці ефективних рішень для вирішення проблем, що виникають у процесі забезпечення режиму секретності. Зокрема, важливо забезпечити узгодженість між вимогами національної безпеки та правами громадян на інформацію, що є ключовим для підтримання прозорості та довіри до державного управління.

Аналіз досліджень і публікацій. Питання розглядали у своїх наукових працях такі вчені, як С. Булавіна, В. Грицієнко, Ю. Дрейс, Л. Казакова, І. Корж, О. Лемак, І. Павленко, В. Нагірний, В. Потапенко, Є. Маляревський, Д. Половинка, К. Рудницька, В. Сергійчук, А. Супруненко.

Мета статті – всебічний аналіз існуючої нормативно-правової бази в Україні щодо захисту державної таємниці, виявлення проблемних аспектів і розробка рекомендацій для їх усунення.

Методологія дослідження

Державна таємниця являє собою сукупність найважливіших для країни відомостей, які охоплюють різні аспекти її життєдіяльності, включаючи оборонні, економічні, науково-технічні, політичні, інформаційні та інші сфери. Ці відомості мають критичне значення для збереження державного суверенітету, стабільності та безпеки, і їх витік може спричинити серйозні негативні наслідки не тільки для окремих галузей, але й для всієї країни. Втрата контролю над такою інформацією може призвести до підриву національних інтересів, дестабілізації внутрішньої ситуації, створення загроз для державного управління та навіть міжнародних відносин [1, с.18].

У всіх державах світу, незалежно від їхнього політичного устрою чи економічного розвитку, існують законодавчі та організаційні механізми, спрямовані на захист державної таємниці. Вони є невід'ємною частиною системи управління державою та її суверенітету, адже забезпечують надійний захист інформації, від якої залежить стабільність і безпека національної державності. Державна таємниця є важливим інструментом захисту національних інтересів, оскільки дозволяє контролювати доступ до критично важливих даних, запобігати їхньому несанкціонованому розповсюдженню та використанню в інтересах третіх сторін [2, с.29]. Захист державної таємниці також має важливий міжнародний аспект. У сучасному глобалізованому світі, де інформаційні технології відіграють центральну роль, держави співпрацюють між собою у сфері забезпечення безпеки конфіденційних відомостей, обмінюються досвідом і технологіями захисту інформації. Це дозволяє зміцнити міжнародні відносини та забезпечити спільну безпеку, адже витік інформації в одній країні може мати вплив на глобальну безпекову ситуацію [8, с.66].

Інформація, яка вважається найбільш важливою для держави, отримує статус державної таємниці, і саме вона підлягає найсуворішому захисту. Цей особливий правовий статус надається відомостям, що мають критичне значення для безпеки, стабільності та розвитку країни. Вони стосуються таких важливих сфер, як оборона, економіка, наука і техніка, зовнішні відносини, державна безпека та охорона правопорядку. Розголошення або втрата контролю над цією інформацією може призвести до серйозних наслідків, завдати шкоди національним інтересам та підірвати безпеку держави.

Основним нормативно-правовим актом, що визначає правовий режим державної таємниці в Україні, є Закон України “Про державну таємницю” [15]. Цей Закон є фундаментальним документом, що регулює відносини, які виникають у процесі віднесення певних відомостей до категорії державної таємниці, їх засекречення, захисту та розсекречення. Закон не лише визначає, які відомості можуть бути класифіковані як державна таємниця, але й регламентує порядок поводження з ними, встановлюючи чіткі правила та процедури, що забезпечують їхню захищеність в інтересах національної безпеки України [10].

Однією з ключових функцій цього закону є визначення компетенції різних органів державної влади, органів місцевого самоврядування та їхніх посадових осіб у сфері охорони державної таємниці. Закон чітко окреслює повноваження цих органів у питаннях засекречування, зберігання, використання та передачі інформації, що має статус державної таємниці. Це включає в себе визначення відповідальності за дотримання правил секретності, а також забезпечення контролю за збереженням та обігом секретної інформації [6, с.54].

Крім того, Закон регулює питання здійснення права власності на секретну інформацію та її матеріальні носії. Власність на таку інформацію може бути державною, а також належати юридичним чи фізичним особам, однак її використання, передача або зберігання підпорядковуються відповідним правилам, встановленим законом. Це забезпечує гарантії того, що секретна інформація не потрапить до рук осіб, які не мають доступу до неї, та буде захищена від будь-яких спроб несанкціонованого використання або розголошення [15].

Згідно зі статтею 1 Закону України “Про державну таємницю”, державна таємниця, або секретна інформація, є видом таємної інформації, яка включає відомості, що стосуються таких важливих сфер, як оборона, економіка, наука і техніка, зовнішні відносини, державна безпека та охорона правопорядку. Розголошення цієї інформації може завдати суттєвої шкоди національній безпеці України, тому вона підлягає охороні з боку держави у відповідності до порядку, встановленого цим Законом [15].

Процес віднесення інформації до державної таємниці являє собою складну і відповідальну процедуру, яка передбачає ухвалення державним експертом з питань таємниць рішення про присвоєння певним категоріям або конкретним відомостям статусу державної таємниці. Це рішення базується на глибокому аналізі та обґрунтуванні можливої шкоди, яку може завдати розголошення цих відомостей національній безпеці України. Визначивши ступінь секретності інформації, експерт включає її до Зводу відомостей, що становлять державну таємницю. Цей звід є офіційним документом, що містить перелік усіх відомостей, які підлягають державному захисту, і він регулярно оновлюється та публікується разом із внесеними до нього змінами [16].

Засекречування матеріальних носіїв інформації є наступним етапом, що передбачає встановлення законодавчих обмежень на поширення та доступ до конкретних секретних відомостей. Це досягається шляхом присвоєння відповідного грифу секретності документам, виробам або іншим матеріальним носіям інформації. Гриф секретності свідчить про те, що доступ до цих матеріалів дозволено лише обмеженому колу осіб, які мають відповідний рівень допуску.

Існують чіткі межі у визначенні державної таємниці. Не може бути засекреченою інформація, що стосується надзвичайних ситуацій, які загрожують безпеці громадян, стану навколишнього середовища або соціально-економічного добробуту населення. Таке обмеження запобігає порушенню конституційних прав і свобод громадян, а також гарантує, що державна таємниця не буде використовуватись для шкоди здоров’ю та безпеці населення. Таким чином, система захисту державної таємниці повинна збалансовувати потреби національної безпеки з правами та свободами людини.

Згідно з українським законодавством, існує чітко визначений список інформації, яка не може бути класифікована як державна таємниця. Це відображено в статті 8 Закону України “Про державну таємницю”, яка надає вичерпний перелік даних, що не підлягають засекречуванню. Сюди входять:

- *екологічні та споживчі дані*: інформація про стан навколишнього середовища, якість харчових продуктів, а також предмети побутового вжитку. Це включає відомості про екологічні умови, які можуть безпосередньо впливати на здоров’я населення, а також дані про безпеку і якість товарів, які використовуються в повсякденному житті громадян;

- *надзвичайні ситуації*: відомості про аварії, катастрофи, небезпечні природні явища та інші надзвичайні події, які вже відбулися або можуть статися, якщо вони загрожують безпеці населення. Ця інформація необхідна для оперативного реагування на надзвичайні ситуації та забезпечення своєчасної допомоги постраждалим [7, с.93];

- *соціально-економічні показники*: інформація про стан здоров’я населення, рівень його життя, що охоплює аспекти, такі як харчування, одяг, житло, медичне обслуговування і соціальне забезпечення. Також сюди входять соціально-демографічні дані, інформація про правопорядок, освіту та культурний розвиток населення. Ці відомості є критично важливими для оцінки загального добробуту та якості життя громадян;

- *порушення прав і свобод*: дані про порушення прав і свобод людини, а також інформація про неправомірні дії з боку органів державної влади, місцевого самоврядування і їх посадових осіб. Ця інформація забезпечує прозорість у діяльності органів влади та є важливою для захисту прав і свобод громадян;

- *міжнародні та законодавчі обмеження*: інші види інформації, які згідно з українськими законами і міжнародними договорами, ратифікованими Верховною Радою України, не можуть бути засекречені. Це включає дані, які за чинним законодавством і міжнародними зобов'язаннями не підлягають конфіденційному режиму [4, с.43].

Інформаційні відносини постійно еволюціонують, що спричинило появу нових категорій, таких як комерційна та банківська таємниця, таємниця особистого життя, результати голосування тощо. У цьому контексті дослідники зазначають, що захист державної таємниці не є таким же ефективним, як захист комерційної або банківської інформації. Це пов'язано з тим, що наразі в законодавстві не передбачена кримінальна відповідальність за незаконне збирання чи використання інформації, яка становить державну таємницю, за відсутності явних ознак державної зради чи шпигунства.

Зазвичай держави прагнуть захистити свою державну таємницю як засіб забезпечення національної безпеки. Водночас, охорона державної таємниці має також істотний вплив на загальний рівень інформаційної безпеки, і можна стверджувати, що ця охорона є важливою функцією в порівнянні з більш сучасними аспектами інформаційної безпеки. Поняття державна таємниця та потреба її захисту, тобто безпека інформації, з'явилося разом з формуванням державності та набула особливої значимості як складова інформаційної безпеки лише у XXI столітті [11].

Однією з характерних ознак режиму державної таємниці є наявність відповідального суб'єкта її забезпечення. Це можуть бути органи державної влади, органи місцевого самоврядування, підприємства, установи або організації, які несуть відповідальність за забезпечення режиму державної таємниці та контроль за дотриманням встановлених правил. Тобто, функція охорони державної таємниці є складовою забезпечення інформаційної безпеки як важливого напряму забезпечення національної безпеки.

Основи правового регулювання в сфері охорони державної таємниці в Україні закладені у Законі України "Про інформацію", який визначає правові принципи створення, функціонування та захисту інформаційних систем. Додаткові нормативно-правові акти доповнюють це регулювання, охоплюючи питання доступу до інформації, процедури класифікації інформації як державної таємниці та відповідальність за її незаконне розголошення.

Охорона державної таємниці здійснюється різними категоріями суб'єктів. До державних органів, відповідальних за забезпечення таємності, відносяться: Президент України, Кабінет Міністрів України, інші органи виконавчої влади та органи місцевого самоврядування. Юридичні особи, зокрема підприємства, установи та організації, що мають відношення до державної таємниці, також виконують роль у цій системі [16].

Об'єктами охорони є відомості, що класифікуються як державна таємниця, незалежно від форми їх представлення. Це можуть бути документи, матеріали, вироби, речовини, носії інформації та інші ресурси, які містять конфіденційну інформацію.

Для забезпечення охорони державної таємниці використовуються різноманітні заходи. Класифікація інформації здійснюється шляхом розподілу даних за категоріями, відповідно до їх значущості для держави. Режим секретності включає комплекс обмежень та вимог, які встановлюються для захисту таємної інформації. Контроль за доступом передбачає перевірку осіб на предмет їх права доступу до державної таємниці та облік таких доступів. Захист інформації реалізується через технічні засоби, фізичну охорону приміщень і сховищ, а також захист від витоків через канали зв'язку. Просвітницька робота включає інструктажі, семінари та навчання персоналу, що стосуються охорони державної таємниці [5, с.74].

Отже, інституційний механізм забезпечення охорони державної таємниці в Україні складається з комплексної системи організаційних і правових заходів, які забезпечують належний рівень захисту конфіденційної інформації. Цей механізм включає в себе розгорнуту

законодавчу базу, що охоплює закони та інші нормативно-правові акти, які визначають правові основи для створення, функціонування та захисту інформаційних систем. Основними суб'єктами цієї системи є державні органи, юридичні особи та фізичні особи, які мають доступ до державної таємниці, а також об'єкти охорони, що представляють собою інформацію будь-якої форми, що підлягає класифікації як державна таємниця.

Окрім основного Закону "Про державну таємницю", в Україні діють й інші нормативно-правові акти, які регулюють цю сферу. Зокрема, Кримінальний кодекс України містить статті, що встановлюють кримінальну відповідальність за розголошення державної таємниці. Адміністративний кодекс України також визначає відповідальність за порушення законодавства в цій сфері. Крім того, розроблені відповідні інструкції та положення, які деталізують порядок роботи з державною таємницею в різних сферах діяльності, що дозволяє забезпечити практичне застосування правових норм у конкретних ситуаціях.

Сучасний стан правового регулювання охорони державної таємниці в Україні є результатом тривалого розвитку законодавчої та нормативно-правової бази, що забезпечує комплексний підхід до захисту конфіденційної інформації. Ця сфера права є критично важливою для національної безпеки, і тому її регулювання включає велику кількість норм і актів, що забезпечують відповідний рівень захисту інформації, яка має значення для безпеки держави [8, с.19].

Ефективність існуючих правових механізмів охорони державної таємниці є критично важливим аспектом забезпечення національної безпеки та захисту стратегічно важливої інформації. В Україні правове регулювання у цій сфері базується на комплексній системі законодавчих і нормативних актів, які встановлюють чіткі правила і процедури для охорони державної таємниці.

Головним документом, що регулює відносини у сфері охорони державної таємниці, є Закон України "Про державну таємницю". Цей закон визначає поняття державної таємниці, критерії віднесення інформації до цієї категорії, а також порядок засекречування і розсекречування. Важливим аспектом є те, що закон встановлює різні рівні секретності, що дозволяє диференціювати заходи захисту залежно від ступеня важливості інформації. Цей підхід забезпечує не тільки гнучкість у захисті критичних даних, але й гарантує адекватний баланс між необхідністю охорони інформації та правами громадян на доступ до певної інформації [15].

Оцінка ефективності існуючих правових механізмів охорони державної таємниці в Україні є ключовим етапом для забезпечення національної безпеки та стабільності держави. Основним законодавчим актом у цій сфері є Закон України "Про державну таємницю", який визначає ключові аспекти охорони інформації з високим рівнем секретності. Цей закон чітко регулює поняття державної таємниці, встановлює критерії для її класифікації, а також визначає порядок засекречування та розсекречування інформації. Ефективність цього закону значною мірою залежить від його здатності адаптуватися до змін у безпековій ситуації та забезпечувати належний захист стратегічної інформації [15].

Законодавча база доповнюється іншими нормативно-правовими актами, такими як Кримінальний кодекс та Адміністративний кодекс України, які встановлюють відповідальність за порушення режиму секретності. Кримінальний кодекс передбачає відповідні кримінальні санкції за розголошення державної таємниці, що забезпечує значний рівень запобігання правопорушенням. Адміністративний кодекс доповнює це, вводячи адміністративні штрафи та інші санкції для менш серйозних порушень. Таким чином, законодавчий контекст забезпечує багатоаспектний підхід до контролю і покарання за порушення.

Досвід країн з розвинутою системою охорони державної таємниці, таких як США, Німеччина, Китай та Великобританія, надає Україні важливі орієнтири для вдосконалення власного законодавства в цій сфері. Запровадження багаторівневої класифікації інформації, як

це практикується в зазначених країнах, дозволить Україні точніше визначати рівень секретності та відповідні заходи захисту інформації. Наприклад, система трирівневої класифікації, застосована у США та Німеччині, може бути адаптована для підвищення ефективності управління інформацією в Україні, що забезпечить кращий контроль над чутливими відомостями.

Окрім того, приклад Великобританії, де інформація класифікується на чотири рівні, і Китаю, з його спеціалізованими органами, демонструє важливість чіткої регламентації та централізованого управління державною таємницею. Імплементація таких практик в Україні дозволить створити більш надійну систему захисту інформації та забезпечити ефективне реагування на можливі загрози. Важливо також врахувати досвід країн у сфері покарань за порушення, що підвищить відповідальність за зловживання при роботі з інформацією. Загалом адаптація національного законодавства до міжнародних стандартів забезпечить Україні високий рівень захисту державної таємниці, відповідний сучасним вимогам безпеки.

Результати

Основні проблеми, що виникають у сфері охорони державної таємниці, включають застарілість існуючого законодавства. Законодавчий акт, що регулює питання державної таємниці в Україні, був прийнятий ще в 1990-х роках минулого століття. За цей час відбулося значне зміщення в суспільних, технологічних і безпекових умовах, що суттєво вплинуло на національні інтереси. Як результат, деякі положення та норми чинного закону вже не відповідають сучасним реаліям і потребам.

Усі ці фактори створюють реальні ризики для національної безпеки, знижують довіру до державних органів і ускладнюють міжнародне співробітництво. Тому для досягнення належного рівня захисту державної таємниці необхідно провести всебічне оновлення законодавства, уточнити правові норми і вдосконалити практичні механізми захисту, а також забезпечити відповідний рівень обізнаності та технічного захисту.

Забезпечення надійної охорони державної таємниці в умовах сучасних викликів, пов'язаних із розвитком цифрових технологій і глобалізацією потребує суттєвого вдосконалення нормативно-правового регулювання цієї сфери.

Для вдосконалення законодавства в області захисту державної таємниці варто врахувати декілька ключових пропозицій.

Слід оновити визначення поняття “державна таємниця” з урахуванням електронних форм, що передбачало б закріплення цього поняття в контексті цифрових даних і впровадження специфічних вимог до їх захисту. Зокрема, важливо визначити, як класифікувати та обробляти електронну інформацію, що має гриф обмеження доступу, щоб відповідати сучасним вимогам технологій.

Необхідно регулювати використання хмарних технологій, які все частіше застосовуються для зберігання та обробки інформації. Розробити та впровадити конкретні правила і норми для безпечного використання хмарних сервісів, зокрема щодо захисту даних, які мають гриф державної таємниці [12, с.58].

Критично важливим також є забезпечення належного захисту від кіберзагроз. Законодавство має включати положення про посилення захисту інформаційних систем від можливих кібератак, зокрема через впровадження сучасних криптографічних засобів і систем для виявлення та реагування на інциденти, що несуть загрози інформаційній безпеці [9, с.103]. Це дозволить зменшити ризики витоку, спотворення та знищення чутливих даних у цифровому середовищі.

З метою підвищення ефективності охорони державної таємниці в Україні необхідно зосередитися на спрощенні процедур і посиленні відповідальності за порушення. Важливо

провести зміни в нормативно-правові акти, які дозволять зменшити бюрократичні перепони та забезпечити жорсткий контроль за дотриманням законодавства.

Оптимізація процедур є ключовим напрямом для покращення регулювання охорони державної таємниці. Передусім, слід спростити процеси отримання та зняття грифу обмеження доступу до інформації. Це включає в себе скорочення бюрократичних бар'єрів і зменшення термінів розгляду заявок, що сприятиме оперативнішій обробці запитів і зменшенню затримок. Крім того, варто зосередитися на уніфікації форм документів, які використовуються для оформлення інформації, що має гриф обмеженого доступу. Розробка єдиних форм та чітких вимог до їх заповнення дозволить уникнути плутанини та підвищити прозорість процесу [7, с.126].

Вдосконалення системи охорони державної таємниці потребує підвищення рівня відповідальності за її розголошення як з кримінальної, так і з адміністративної точки зору. Це має включати посилення санкцій для фізичних осіб та введення жорсткіших покарань для юридичних осіб, що порушують законодавство. Запровадження відповідальності для юридичних осіб допоможе забезпечити більш ефективний контроль за дотриманням норм охорони державної таємниці та запобігти порушенням на рівні організацій.

Важливим елементом удосконалення системи охорони державної таємниці є міжнародне співробітництво, оскільки воно дозволяє інтегрувати національні практики в глобальні рамки забезпечення захисту інформації. І першочерговим завданням є узгодження національного законодавства з міжнародними стандартами, що потребує адаптації українських норм до вимог, встановлених міжнародними організаціями, такими як НАТО та Європейський Союз. Це забезпечить гармонізацію політики і процедур з міжнародними стандартами, що, в свою чергу, підвищить ефективність захисту державної таємниці та полегшить співпрацю з міжнародними партнерами [3, с.66].

Висновки

Охорона державної таємниці є критично важливим аспектом забезпечення інформаційної безпеки як важливої складової національної безпеки, що включає захист інформації, яка має стратегічне значення для країни. В Україні цей процес регулюється Законом «Про державну таємницю», який визначає, що саме відомості можуть бути віднесені до категорії державної таємниці, а також встановлює порядок їхнього засекречування, зберігання та розсекречення. Закон гарантує, що інформація, яка є критично важливою для оборони, економіки, науки та інших сфер, отримує найсуворіший захист.

Процес класифікації інформації як державної таємниці є складним і відповідальним, включаючи аналіз можливих наслідків її розголошення для національної безпеки. Важливим етапом є визначення ступеня секретності інформації та включення її до офіційного Зводу відомостей. Закон також передбачає чітке регулювання відповідальності органів державної влади та юридичних осіб за дотримання режиму секретності, що включає контроль за доступом і фізичний захист матеріальних носіїв інформації.

Водночас, система охорони державної таємниці повинна балансувати між забезпеченням національної безпеки та захистом прав і свобод громадян. Інформація про надзвичайні ситуації, екологічний стан, соціально-економічні показники та порушення прав людини не може бути засекречена, що гарантує відкритість і прозорість у питаннях, які впливають на безпеку та добробут населення. Сучасний стан правового регулювання в Україні є результатом тривалого процесу вдосконалення законодавства, що забезпечує ефективний захист інформаційної безпеки та державної таємниці.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Булавіна, С. Є. Правова система захисту державної таємниці за часів незалежності України. The 5th International scientific and practical conference “World science: problems, prospects and innovations” (January 27-29, 2021) Perfect Publishing, Toronto, Canada. 2021. 1300 p.
2. Грицієнко В. Тлумачення поняття державної таємниці національним законодавцем України. Editorial board 2022 p. 247 c.
3. Дрейс Юрій. Аналіз стану забезпечення охорони державної таємниці в умовах дії військового стану. Редакційна колегія 2023 p. 255c.
4. Казакова Л.О. Національна безпека держави: понятійно-категорійний аппарат. Регіональні студії. – Ужгород, Видавничий дім «Гельветика». Вип. 24. 2021. С. 128-132.
5. Корж І. Ф. Державна безпека: методологічні підходи до системи складових поняття. Правова інформатика. 2012. Вип. No 4 (36). С. 69–75
6. Лемак О. В. Українська нація і національна безпека: аспекти співвідношення. Науковий вісник УжНУ. Серія «Право». 2014. Випуск 27. Том 3. С. 40–44.
7. Особливості правового регулювання захисту державної таємниці в Україні та за її межами URL: http://pgp-journal.kiev.ua/archive/2021/1/37.pdf (дата звернення: 02.07.2024).
8. Павленко І., Нагірний В., Потапенко В., Маляревський Є. Аналіз загроз національній безпеці у сфері внутрішньої політики. https://doi.org/10.53679/NISS-analytrep.2023.06 (дата звернення: 16.07.2024).
9. Половинка Д. Понятійні проблеми інституту державної таємниці. Editorial board 2022 p. 256 c.
10. Про затвердження Зводу відомостей, що становлять державну таємницю : Наказ Служби безпеки України від 12.08.2005 р. No 440. URL: https://zakon.rada.gov.ua/laws/show/z0902-05#Text (дата звернення: 16.07.2024).
11. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII (2469-19) зі змінами і доповненнями. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 17.07.2024).
12. Рудницька К. Питання щодо допуску громадян до державної таємниці. The XI International Science Conference «Modern aspects of science and practice», November 30–December 03, 2021, Melbourne, Australia. 590 c.
12. Сергійчук В. В. Розголошення державної таємниці: кримінально-правова та кримінологічна характеристика. Diss. спец. 12.00.08, 2021 р. С. 71-74.
14. Супруненко А. М. Організація охорони державної таємниці в Україні. 2020 р. С. 67-78.
15. Про державну таємницю : Закон України від 21.01.1994 р. No 3855-XII. URL: https://zakon.rada.gov.ua/laws/show/3855-12#top (дата звернення: 20.07.2024).
16. Про Раду національної безпеки і оборони України: Указ Президента України. URL: https://zakon.rada.gov.ua/laws/show/772/96#Text (дата звернення: 20.07.2024).

References

1. Bulavina, S. E. The legal system of protection of state secrets during the independence of Ukraine. The 5th International scientific and practical conference “World science: problems,

prospects and innovations" (January 27-29, 2021) Perfect Publishing, Toronto, Canada. 2021. 1300 p.
2. Hrytsienko V. Interpretation of the concept of state secrecy by the national legislator of Ukraine. Editorial board 2022. 247 c.
3. Dreys Yuriy. Analysis of the state of state secret protection in the conditions of martial law. Editorial board 2023. 255 p.
4. Kazakova L.O. National security of the state: conceptual and categorical apparatus. Regional studios. – Uzhgorod, "Helvetika" Publishing House. Vol. 24. 2021. C. 128-132.
5. Korzh I. F. State security: methodological approaches to the system of components of the concept. Legal informatics. 2012. Issue. No 4 (36). C. 69–75
6. Lemak O. V. The Ukrainian nation and national security: aspects of the relationship. Scientific Bulletin of UzhNU. "Law" series. 2014. Issue 27. Vol. 3. C. 40–44.
7. Peculiarities of the legal regulation of the protection of state secrets in Ukraine and abroad. Available from : http://pgp-journal.kiev.ua/archive/2021/1/37.pdf (date of application: 02.07.2024).
8. Pavlenko I., Nagirnyi V., Potapenko V., Malyarevskyi E. Analysis of threats to national security in the field of domestic policy. https://doi.org/10.53679/NISS-analytrep.2023.06 (date of application: 16.07.2024).
9. Polovynka D. Conceptual problems of the institute of state secrets. Editorial board 2022 p. 256 c.
10. On the approval of the Compendium of information constituting a state secret: Order of the Security Service of Ukraine dated 12.08.2005. No 440. Available from : https://zakon.rada.gov.ua/laws/show/z0902-05#Text (date of application: 16.07.2024).
11. On national security of Ukraine: Law of Ukraine from 21.06.2018 № 2469-VIII (2469-19) with changes and additions. Available from : https://zakon.rada.gov.ua/laws/show/2469-19#Text (date of application: 17.07.2024).
12. Rudnytska K. Questions regarding the admission of citizens to state secrets. The XI International Science Conference «Modern aspects of science and practice», November 30–December 03, 2021, Melbourne, Australia. 590 c.
12. Serhiychuk V. V. Disclosure of state secrets: criminal-legal and criminological characteristics. Diss. спец. 12.00.08, 2021. P. 71-74.
14. Suprunenko A. M. Organization for the Protection of State Secrets in Ukraine. 2020. P. 67-78.
15. On state secrets: Law of Ukraine dated 21.01.1994. No 3855-XII. Available from : https://zakon.rada.gov.ua/laws/show/3855-12#top (date of application: 20.07.2024).
16. About the National Security and Defense Council of Ukraine: Decree of the President of Ukraine. Available from : https://zakon.rada.gov.ua/laws/show/772/96#Text (date of application: 20.07.2024).

Методичні підходи до визначення чисельності персоналу служби внутрішнього аудиту Міністерства оборони України в ризик-орієнтованому плануванні діяльності

Methodological approaches to determining the number of staff of the Internal Audit Service of the Ministry of Defense of Ukraine in risk-oriented planning of activities

Анатолій Лойшин [A]
Corresponding author: доктор філософії, заступник начальника інституту з навчальної роботи, e-mail: aloishyn@gmail.com, ORCID: 0000-0003-2769-9336

Олександр Титковський [B]
директор департаменту внутрішнього аудиту Міністерства оборони України, e-mail: tytkovskyi@ukr.net, ORCID: 0009-0004-0403-9962

Владислав Карелін [A]
доктор юридичних наук, доцент, професор кафедри, e-mail: vlad.karelin1989@ukr.net, ORCID: 0000-0002-6271-2447

Олександр Остапенко [C]
кандидат економічних наук, професор кафедри, e-mail: ap080011@knu.ua, ORCID: 0000-0003-3194-0372

Ірина Серебрянська [A]
доктор філологічних наук, професор, помічник начальника відділу забезпечення якості освітньої діяльності та вищої освіти, e-mail: serebryanska@ukr.net, ORCID: 0000-0002-1720-4873

Олексій Гродовський [D]
кандидат економічних наук, головний спеціаліст Департаменту внутрішнього аудиту, e-mail: grodovskiy100@ukr.net, ORCID: 0000-0002-4638-0286

Anatolii Loishyn [A]
Corresponding author: Ph.D, Deputy Chief of the Military Institute for Academic Affairs, e-mail: aloishyn@gmail.com, ORCID: 0000-0003-2769-9336

Oleksandr Tytkovskyi [B]
Director of the Internal Audit Department of the Ministry of Defense of Ukraine, e-mail: tytkovskyi@ukr.net, ORCID: 0009-0004-0403-9962

Vladyslav Karelin [A]
Doctor of Law, Associate Professor, Professor of the Department, e-mail: vlad.karelin1989@ukr.net, ORCID: 0000-0002-6271-2447

Oleksandr Ostapenko [C]
Ph.D, Professor at the Department, e-mail: ap080011@knu.ua, ORCID: 0000-0003-3194-0372

Iryna Serebryanska [A]
Doctor of Philology, Professor, Assistant Head of the Department for Quality Assurance of Educational Activities and Higher Education, e-mail: serebryanska@ukr.net, ORCID: 0000-0002-1720-4873

Oleksii Grodovskyi [D]
Ph.D, Chief Specialist of the Internal Audit Department, e-mail: grodovskiy100@ukr.net, ORCID: 0000-0002-4638-0286

[A] Військовий інститут Київського національного університету імені Тараса Шевченка, м. Київ, Україна
[B] Департамент внутрішнього аудиту Міністерство оборони України, м. Київ, Україна
[C] Київський національний економічний університет імені Вадима Гетьмана, м. Київ, Україна
[D] Державна служба зв'язку і захисту інформації України, м. Київ, Україна

[A] Military Institute of Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
[B] Internal Audit Department of the Ministry of Defense of Ukraine, Kyiv, Ukraine
[C] Kyiv National Economic University named after Vadym Hetman, Kyiv, Ukraine
[D] State Service for Special Communications and Information Protection of Ukraine, Kyiv, Ukraine

Received: October 4, 2024 | Revised: October 28, 2024 | Accepted: October 31, 2024

DOI: 10.33445/sds.2024.14.5.24

Мета роботи: розроблення та обґрунтування методичних підходів до визначення чисельності персоналу служби внутрішнього аудиту Міністерства оборони України в ризик-орієнтованому плануванні діяльності їх відповідності обсягу робіт і фінансовим ризикам, що виникають в умовах дії правового режиму воєнного стану.

Метод дослідження: методи аналізу, синтезу, дедукції та індукції, метод аналогії та порівняння.

Практична цінність дослідження: у результаті дослідження розроблено та аргументовано методичні підходи щодо визначення чисельності персоналу служби внутрішнього аудиту Міністерства оборони України в ризик-

Purpose: develop and substantiate methodological approaches to determining the number of personnel of the internal audit service of the Ministry of Defense of Ukraine in risk-oriented planning of their activities in accordance with the scope of work and financial risks arising under the legal regime of martial law.

Method: methods of analysis, synthesis, deduction and induction, analogy and comparison.

Practical implications: result of the study, methodological approaches to determining the number of staff of the internal audit service of the Ministry of Defense of Ukraine in risk-oriented planning of activities were developed and argued, and their

орієнтованому плануванні діяльності та обґрунтовано їх відповідність обсягу робіт і фінансовим ризикам, що виникають в умовах дії правового режиму воєнного стану.

Цінність дослідження: полягає в удосконаленні науково-методичних підходів до визначення чисельності персоналу служби внутрішнього аудиту Міністерства оборони України в ризик-орієнтованому плануванні діяльності.

Майбутні дослідження: реформування служби внутрішнього аудиту Міністерства оборони України, співпраця з міжнародними безпековими організаціями тощо.

Тип статті: теоретична та практична.

Ключові слова: внутрішній аудит, ризик-орієнтоване планування, чисельність персоналу.

compliance with the scope of work and financial risks arising under the legal regime of martial law was substantiated.

Value: the study is to improve scientific and methodological approaches to determining the number of staff of the internal audit service of the Ministry of Defense of Ukraine in risk-oriented planning of activities.

Future research: reforming the internal audit service of the Ministry of Defense of Ukraine, cooperation with international and security organizations, etc.

Paper type: theoretical and practical.

Key words: internal audit, risk-oriented planning, number of personnel.

Вступ

Міністерство оборони України (далі – МО України) за чисельним складом, застосуванням фінансових і матеріальних ресурсів держави та конституційними завданнями є основним державним органом, який забезпечує збройну відсіч агресору. Використання значних ресурсів держави спричиняє потребу збільшення як зовнішнього державного контролю над ними, так і внутрішнього, для забезпечення дотримання бюджетного законодавства під час здійснення всіх фінансового-господарських операцій та управлінських функцій.

Актуальні проблеми закупівлі продуктів харчування, палива, засобів індивідуального захисту та першої медичної допомоги для Збройних Сил України (далі – ЗС України) у 2019-2021 роках та після початку повномасштабного вторгнення створюють репутаційні ризики, що негативно впливають на діяльності відомств, викликаючи потребу оперативних перевірок і попередження зловживань. Зростання масштабів благодійної допомоги як у грошовому, так і в натуральному вимірі, збільшення загального обсягу виділеного фінансового ресурсу на військові частини, розмірів грошових винагород військовослужбовцям, недосконаліть процедур їх виплати та багато інших факторів зумовлюють зростання актуальність дослідження.

Відповідно до ст. 26 Бюджетного кодексу України, “контроль за дотриманням бюджетного законодавства, спрямований на забезпечення ефективного й результативного управління бюджетними коштами, здійснюється на всіх стадіях бюджетного процесу його учасниками. Він забезпечує:

1) оцінку управління бюджетними коштами (включаючи проведення державного фінансового аудиту);

2) правильність ведення бухгалтерського обліку та достовірність фінансової й бюджетної звітності;

3) досягнення економії бюджетних коштів, їх цільового використання, ефективності та результативності в діяльності розпорядників бюджетних коштів шляхом прийняття обґрунтованих управлінських рішень;

4) проведення аналізу та оцінки стану фінансової й господарської діяльності розпорядників бюджетних коштів;

5) запобігання порушенням бюджетного законодавства та забезпечення інтересів держави у процесі управління об’єктами державної власності;

6) обґрунтованість планування надходжень і витрат бюджету”[1].

Саме для підтримки керівника у процесі реалізації функцій установи та надання об'єктивних і науково-обґрунтованих рекомендацій призначена система внутрішнього аудиту в МО України, яка визначає діяльність, спрямовану на вдосконалення системи управління, внутрішнього контролю, запобігання фактам незаконного, неефективного та нерезультативного використання бюджетних коштів, виникненню помилок та будь-яких недоліків у діяльності розпорядника бюджетних коштів і підприємств, установ та організацій,

що належать до сфери його управління, та яка передбачає надання незалежних висновків і рекомендацій.

Теоретичні основи дослідження

Теоретичними основами дослідження є нормативно-правові акти, які регулюють діяльність МО України [1-14,18], інші джерела та публікації із внутрішнього аудиту в Україні.

Слід зазначити, що проблематикою впровадження зарубіжного досвіду внутрішнього аудиту займалися І. Дрозд [26], Н. Дорош [27], Н. Гура [28], О. Подолянчук [29], О. Петрик [30-31], М. Фенченко [31] та інші науковці. Хоча багато досліджень присвячено військово-політичним аспектам вступу України до НАТО, питання внутрішнього аудиту залишаються недостатньо розглянутими. Водночас внутрішній аудит має значний вплив на прозорість, ефективність та підзвітність урядових та військових структур, що є важливими критеріями для відповідності стандартам НАТО. Внутрішній аудит забезпечує систематичну оцінку та покращення процесів управління ризиками, контролю та корпоративного управління. Для країн, які прагнуть вступити до НАТО, важливо демонструвати високий рівень управлінських практик та прозорості, оскільки це підвищує довіру з боку інших країн-членів альянсу.

Окремі аспекти внутрішнього аудиту у сфері оборони представлені в наукових працях А. Лойшина та інших дослідників (М. Бариніна, В. Бегма, А. Ігнатенко, М. Лисенко, Ю. Луцик, С. Мазка, В. Мірненко, І. Ткач, К. Ульянов, О. Шпиталь, Н. Юрків) [33–35].

Постановка проблеми

Використання державних ресурсів в умовах дії правового режиму воєнного стану вимагає посиленого контролю, як зовнішнього, так і внутрішнього, для забезпечення законного, ефективного та результативного витрачання бюджетних коштів. Збільшення обсягів фінансування військових частин та складність управлінських процесів створюють потребу удосконалення інструментів внутрішнього аудиту.

Чисельність персоналу служби внутрішнього аудиту має бути уточнена з огляду на сучасні виклики. Недосконалість процедур визначення чисельності та розподілу навантаження на аудиторів обумовлює потребу в розробленні нових підходів та методик, які б враховували ризик-орієнтоване планування діяльності та забезпечували ефективне виконання завдань внутрішнього аудиту в МО України в умовах воєнного стану. При цьому аналіз останніх наукових та науково-методичних праць засвідчив фактичну відсутність у відкритому доступі таких джерел, які відповідали б предмету цього дослідження.

Методологія дослідження

Дослідження у предметній сфері проведено в такому порядку:

1) розглянуто теоретичні основи діяльності служби внутрішнього аудиту в сучасних умовах;

2) проаналізовано зміни обсягу виділеного фінансового ресурсу держави на потреби МО України та інших складових сектору безпеки і оборони України до та після повномасштабного вторгнення;

3) визначено обсяг навантаження на персонал служби внутрішнього аудиту Міністерства оборони України в забезпеченні дотримання законності використання бюджетних коштів військовими частинами;

4) сформульовано рекомендації щодо вдосконалення методики визначення чисельності персоналу служби внутрішнього аудиту МО України відповідно до сучасних умов функціонування військ.

Результати

Відповідно до постанови Кабінету Міністрів України від 28.09.2011 № 1001 “Деякі питання здійснення внутрішнього аудиту та утворення підрозділів внутрішнього аудиту” і вказівок Міністерства фінансів України від 19.12.2018 № 33020-07-2/33930 “Щодо організації та здійснення внутрішнього контролю та внутрішнього аудиту”, від 20.03.2022 № 33020-07-5/6432 “Щодо можливості здійснення внутрішнього аудиту в період дії правового режиму воєнного стану”, положення вищезазначеної постанови поширюються повною мірою й на всіх головних розпорядників коштів [15-17].

Відповідно до наказу Міністерства оборони України від 15.12.2020 № 475 “Про організацію діяльності з внутрішнього аудиту в системі Міністерства оборони України”, виконання завдань із проведення внутрішнього аудиту покладається саме на Службу внутрішнього аудиту Міністерства оборони, яка має право проводити внутрішні аудити в:

структурних підрозділах апарату МО України, апарату Головнокомандувача ЗС України, Генерального штабу ЗС України;

органах військового управління, з'єднаннях, військових частинах та військових навчальних закладах;

установах, організаціях та суб’єктах господарювання, що належать до сфери управління МО України [18].

Після повномасштабного вторгнення російської федерації роль внутрішнього аудиту в МО України значно зросла, адже збільшення фінансування військових частин та установ ЗС України, створення нових військових частин, комплектування ключових посад, відповідальних за реалізацію господарських операцій, особовим складом без відповідного досвіду та знань, збільшення надходження благодійної допомоги, використання відчуженого та вилученого майна в умовах правового режиму воєнного стану, а також інші операції спричинили зростання відповідних ризиків, які потребують уваги.

Саме в такому контексті нами проаналізовано динаміку виділення фінансового ресурсу на потреби окремих складових сектору безпеки й оборони України.

Аналіз державних видатків протягом 10-ти років до повномасштабного вторгнення показав, що на основні складові сектору безпеки й оборони України виділялося щонайменше 27 % видаткової частини бюджету України (понад 600 млрд грн), тоді як у 2012 році аналогічний показник складав 11 % [4-14].

Динаміку збільшення видатків на Міністерство оборони України та Міністерство внутрішніх справ України наведено на рис. 1.

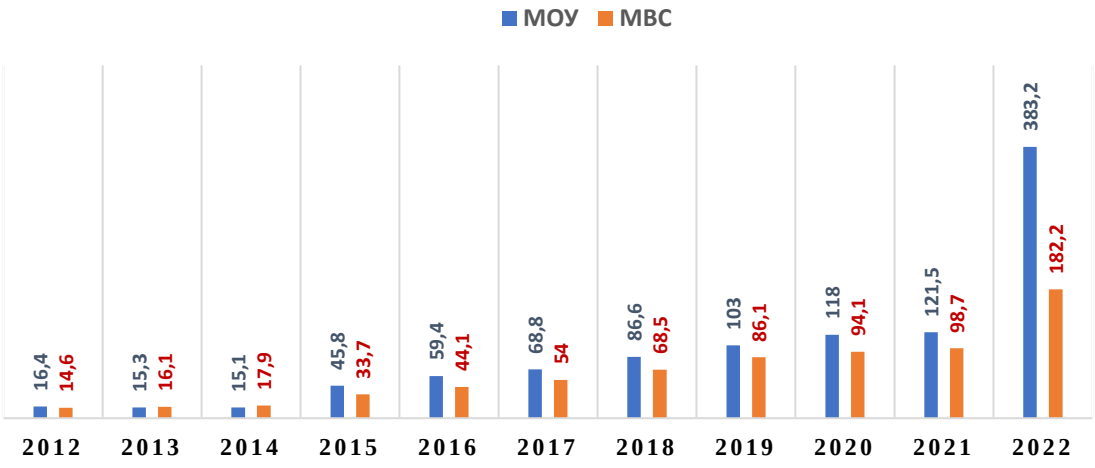


Рисунок 1. Динаміка фінансування Міністерства оборони України та Міністерства внутрішніх справ України протягом 2012 – 2022 рр.

Упродовж цього самого періоду видатки на Службу безпеки України зросли майже в 6 разів: із 3,3 млрд грн до 19 млрд грн (рис. 2).

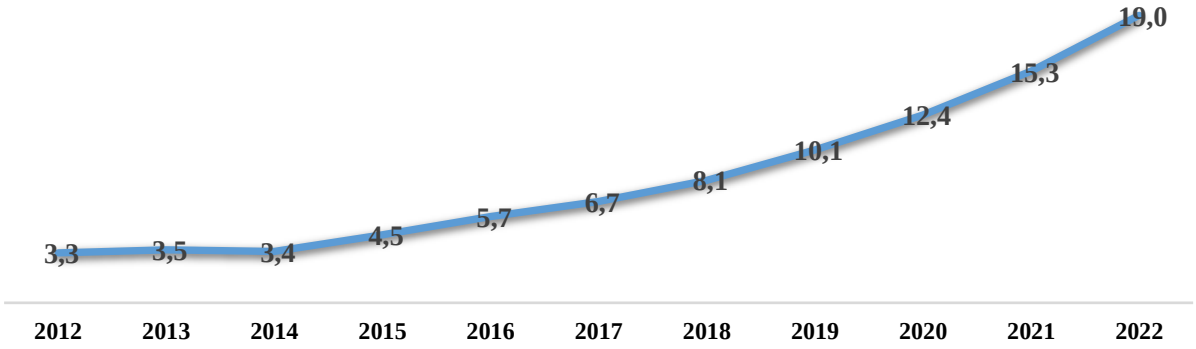


Рисунок 2. Динаміка фінансування Служби безпеки України протягом 2012–2022 рр.

Аналіз видатків на Адміністрацію державної спеціальної служби зв'язку та захисту інформації України, Управління державної охорони України, Головне управління розвідки Міністерства оборони України, Службу зовнішньої розвідки України протягом 2012–2022 рр. засвідчив збільшення показників фінансування у 13,26, 9,61, 6,43 та у 5,57 рази відповідно (рис. 3).

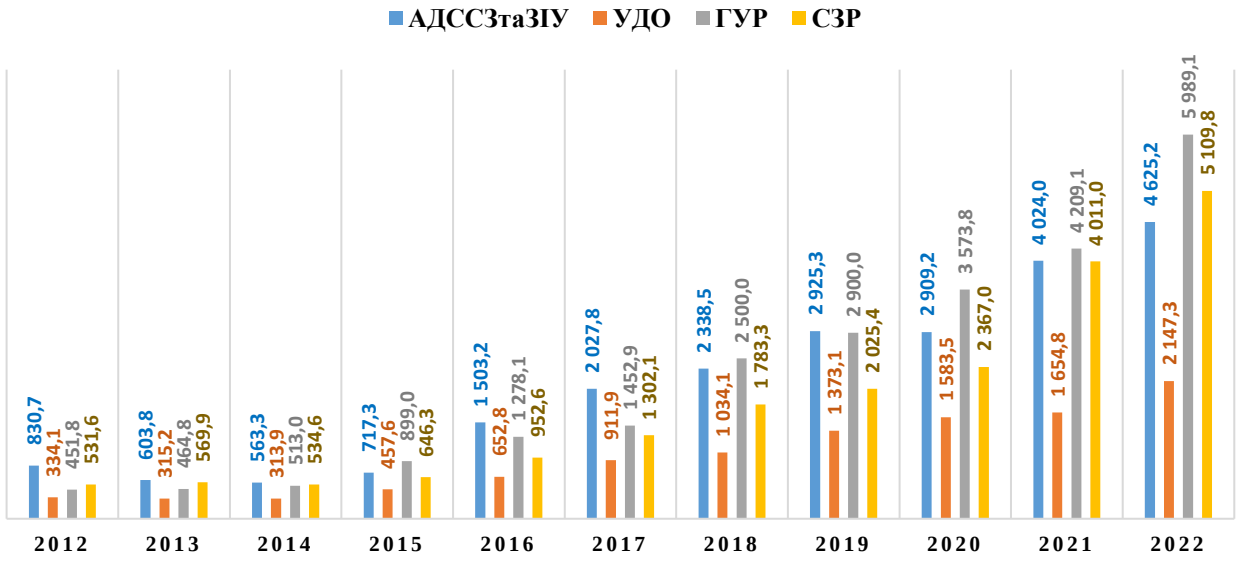


Рисунок 3. Динаміка фінансування Адміністрації державної спеціальної служби зв'язку та захисту інформації України, Управління державної охорони України, Головного управління розвідки Міністерства оборони України, Служби зовнішньої розвідки України протягом 2012–2022 рр.

Відповідно до наведених показників у законах України про державний бюджет у період 2012–2022 рр. відсоткове співвідношення виділеного фінансового ресурсу від загального обсягу видаткової частини Державного бюджету України на потреби МО України та ЗС України зросло з 3,96 % до 17,72 %, тобто в 4,5 рази. Одночасно, поряд із тенденцією до збільшення видаткової частини державного бюджету України з 413,6 млрд грн у 2012 році до 2,1 трлн грн у 2022 році, видатки МО України та ЗС України в аналогічний період зросли з 16,4 млрд грн до 383,2 млрд грн, що в 23 рази перевищує показник 2012 року.

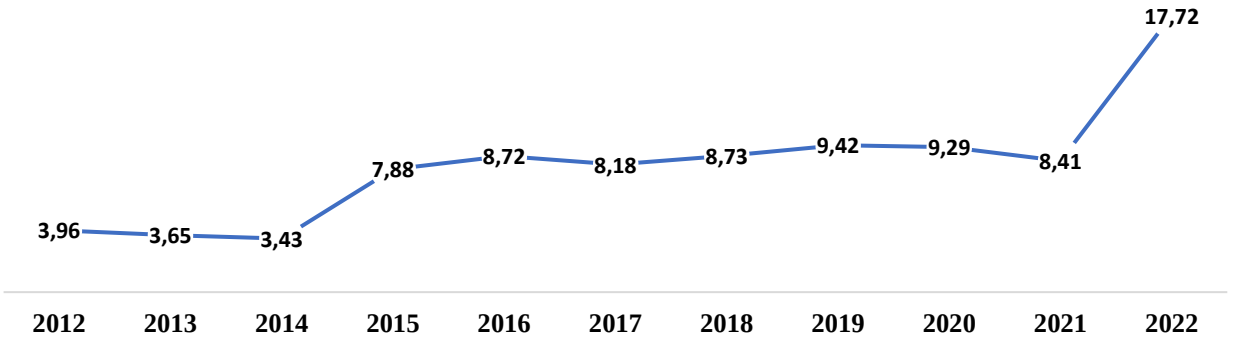


Рисунок 4. Динаміка виділення фінансового ресурсу МО України відповідно до загального обсягу видаткової частини Державного бюджету України протягом 2012–2022 рр.

Аналізуючи видатки державного бюджету України на потреби Міністерства оборони України та Державної спеціальної служби транспорту [2-4] після повномасштабного вторгнення та фактичне використання виділеного фінансового ресурсу, констатуємо збільшення фінансування як на забезпечення необхідних виплат особовому складу, так і на розвиток і закупівлю озброєння та військової техніки, експлуатаційні витрати, розвиток інфраструктури.

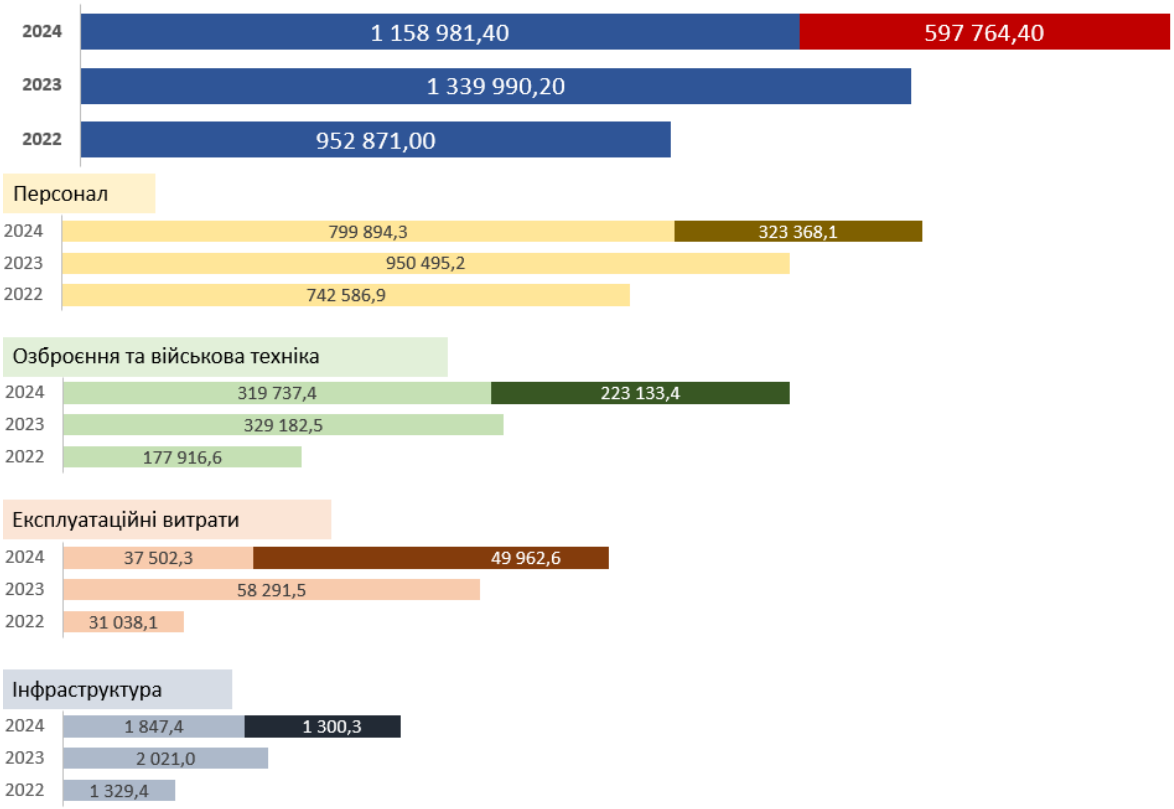


Рисунок 5. Фактичне виконання кошторису Міністерства оборони України та Державної спеціальної служби транспорту у 2022-2023 рр., з урахуванням планових показників 2024 року, млн грн.

Отже, поряд із постійним збільшенням фінансового ресурсу для забезпечення МО України загалом та ЗС України зокрема гостро зростає потреба в дотриманні ефективності управління виділеними бюджетними коштами, використанні й збереженні активів, управлінні

державним майном, правильності ведення бухгалтерського обліку та достовірності фінансової й бюджетної звітності, що, відповідно, значно збільшує роль служби внутрішнього аудиту МО України в забезпеченні цього процесу.

Виділяємо низку факторів, що безпосередньо впливають на спроможність служби внутрішнього аудиту реалізовувати покладені на неї завдання:

чисельність та стан укомплектування служби внутрішнього аудиту фахівцями за профілями виконання аудиторських завдань;

рівень інформатизації процесів та програмного забезпечення аудиторської діяльності;

недосконаліть процесу отримання інформації та обміну нею в системі органів управління (військового управління) МО України;

стан обліку озброєння та військової техніки, що використовується в районах бойових дій;

облік особового складу та прорахунки в питаннях розрахунків особового складу;

перебування підконтрольних суб'єктів або майна на непідконтрольній території та (або) суб'єкти задіяні в безпосередній відсічі нападу противника.

З усіх названих вище факторів саме чисельність та стан укомплектування служби внутрішнього аудиту в нинішніх умовах найбільше впливають на виконання поставлених завдань, оскільки за останній час вони значних змін не зазнали, а умови їх виконання докорінно змінилися.

Аналіз динаміки фактичної чисельності персоналу служби внутрішнього аудиту за 2019–2022 роки [22-25] засвідчує: незважаючи на значне збільшення виділеного фінансового ресурсу на потреби МО України та ЗС України, що передбачає кратне збільшення навантаження на одного фахівця, та фактичне зростання кількості об'єктів внутрішнього аудиту на 16 % (з 1589 до 1846), штатна чисельність персоналу служби внутрішнього аудиту залишилася майже незмінною, а фактична чисельність помітно зменшується.

Таблиця 1 – Динаміка чисельності працівників Служби внутрішнього аудиту Міністерства оборони України за 2019–2022 рр.

Чисельність персоналу	Роки			
	2019	2020	2021	2022
Штатна чисельність працівників	244	242	242	242
Фактична чисельність працівників	203	192	184	186
Працівники, безпосередньо задіяні до виконання аудиторських завдань	177	169	163	167
Кількість працівників, призначених у підрозділи служби внутрішнього аудиту	23	28	23	47
Кількість працівників, звільнених із підрозділів служби внутрішнього аудиту	23	39	31	45

Наприклад, на кінець 2022 року штатна чисельність особового складу служби внутрішнього аудиту МО України разом із підпорядкованими територіальними управліннями складала 242 посади, що були укомплектовані на 76 %. Проведені розрахунки засвідчили критичне навантаження на аудиторський склад територіальних управлінь внутрішнього аудиту, яке в окремих випадках становить 10 військових частин на одного аудитора (з урахуванням виконання аудиторських завдань аудиторськими групами проведення внутрішніх аудитів у військових частинах можливо не більше одного разу на 5-6 років, що унеможливлює якісне запобігання можливим фактам незаконного, неефективного та нерезультативного використання державних ресурсів, а також здійснення належної підтримки

та надання відповідних рекомендацій командирам – розпорядникам бюджетних коштів). Водночас, враховуючи виділений фінансовий ресурс для забезпечення потреб МО України та ЗС України, середньостатистичний обсяг фінансового ресурсу як об'єкт контролю на одного штатного фахівця служби внутрішнього аудиту за повного охоплення простору внутрішнього аудиту склав близько 5,96 млрд грн.

Слід додати, що на практиці не весь персонал підрозділів Служби внутрішнього аудиту здійснює безпосереднє виконання аудиторських завдань протягом усього робочого часу. Крім того, низку керівників меншою мірою залучають до виконання аудиторських завдань з огляду на потребу виконання адміністративних функцій.

За даними доповіді заступника Міністра оборони України, впродовж 2023 року Службою внутрішнього аудиту МО України було виконано низку завдань:

проведено 204 внутрішніх аудитів, у тому числі 59 додаткових (позапланових);

опрацьовано 218 звернень від правоохоронних та судових органів;

опрацьовано та забезпечено проведення моніторингу оцінки ризиків 567 проектів договорів на загальну суму, що перевищила 67 млрд грн.;

опрацьовано 339 проєктів наказів Міністерства оборони України, 39 проєктів постанов та розпоряджень Кабінету міністрів України та 1328 інших доручень вищого керівництва, надано понад 500 консультацій за отриманими зверненнями [20].

Крім того, у 2024 році службою внутрішнього аудиту Міністерства оборони України передбачено дослідження процесів у 128-ми установах у розрізі таких процесів:

розвиток, закупівля, модернізація та ремонт ОВТ, засобів та обладнання;

функціональне управління суб'єктами господарювання (зокрема агенції, спецекспортери, державні підприємства);

отримання, облік, зберігання та використання міжнародної технічної та гуманітарної допомоги;

здійснення оборонних закупівель;

організація обліку військовозобов'язаних;

відчуження та утилізація надлишкового військового майна;

організація обліку та списання військового майна;

відшкодування витрат на забезпечення та проведення військової підготовки громадян за програмою підготовки офіцерів запасу;

медичне забезпечення Збройних Сил України тощо.

Тож виникає гостра потреба в перегляді кількості персоналу служби внутрішнього аудиту МО України для повного та якісного забезпечення виконання покладених на неї завдань і функцій, з урахуванням обсягів навантаження та охоплення всього простору аудиту, адже наразі виконання всіх функцій та завдань забезпечується штатною чисельністю особового складу територіальних управлінь внутрішнього аудиту, встановленого до повномасштабного вторгнення російської федерації.

Відповідно до Порядку здійснення внутрішнього аудиту та утворення підрозділів внутрішнього аудиту, затвердженого Постановою Кабінету міністрів України від 28.09.2011 №1001, чисельність працівників служби внутрішнього аудиту визначається з урахуванням таких показників:

кількості та обсягу фінансування бюджетних програм, які виконуються розпорядниками бюджетних коштів відповідно до покладених на них функцій;

кількості об'єктів, щодо яких державним органом виконуються функції з управління об'єктами державної власності;

обсягу фінансових, кадрових, часових та інших ресурсів, необхідних для забезпечення охоплення об'єктів внутрішнього аудиту, визначених за результатами оцінки ризиків.

Критична потреба збільшення штатної чисельності особового складу територіальних управлінь внутрішнього аудиту після повномасштабного вторгнення російської федерації обумовлена такими факторами:

1) значне збільшення ризикових об'єктів внутрішнього аудиту, пов'язаних із використанням обмежених державних ресурсів, зокрема процесів оборонних закупівель; отримання, обліку та використання іноземної матеріальної військової (технічної) допомоги; отримання, розподіл, облік та використання гуманітарної допомоги; примусове вилучення та відчуження майна цивільних організацій; отримання, облік та використання коштів субвенцій; здійснення виплат нових видів грошового забезпечення (додаткової винагороди тощо) та одноразових виплат (одноразової грошової допомоги тощо);

2) значне збільшення кількості органів військового управління, структурних підрозділів та військових частин;

3) значне збільшення (у понад 10 разів) обсягу фінансового ресурсу МО України, який підлягає аудиторським дослідженням;

4) виконання нових для органів служби внутрішнього аудиту завдань, зокрема з проведення попереднього моніторингу проєктів низки документів, моніторингу інформаційного простору тощо;

5) залучення персоналу служби внутрішнього аудиту до складу робочих груп, проведення спільних перевірок та досліджень відповідно до окремих розпоряджень керівництва МО України;

6) наявність вимог щодо миттєвого реагування на виникнення нових ризиків практично в усіх сферах діяльності;

7) проведення позапланових аудиторських досліджень за зверненнями правоохоронних органів, зокрема в межах відкритих кримінальних проваджень.

Аналіз нормативно-правової бази діяльності підрозділів служби внутрішнього аудиту МО України, продемонстрував, що наразі немає відповідної спеціальної методики визначення кількості персоналу, а отже існує потреба в її розробленні. Це важливий чинник попередження можливих зловживань у сфері управління державними ресурсами.

Типові світові методики визначення кількості персоналу внутрішнього аудиту враховують низку ключових факторів та викликів, що впливають на сучасне бізнес-середовище:

1) методика на основі обсягу роботи (Сполучені Штати Америки, країни Європейського Союзу, Японія, Австралія, Південна Африка) – визначення кількості персоналу, виходячи з обсягу роботи, яку необхідно виконати. Обсяг роботи може бути виміряний у людино-годинах або інших одиницях. Враховується кількість об'єктів аудиту, обсяг і складність аудиторських завдань, час на проведення аудиту кожного об'єкта;

2) методика бенчмаркінгу (Велика Британія, Канада) – передбачає порівняння внутрішньої аудиторської служби з аналогічними службами в інших установах (інституціях). До розрахунку приймаються дані про кількість аудиторів у подібних установах, бюджет аудиторської служби, відношення кількості аудиторів до загальної кількості персоналу;

3) методика на основі ризиків (Сполучені Штати Америки, Австралія, Японія) – передбачає визначення кількості персоналу, виходячи з рівня наявних ризиків. Увага першочергово приділяється фінансовим, операційним, репутаційним та інші типам ризиків, які впливають на ефективність і результативність діяльності;

4) методика на основі бюджету (країни Європейського Союзу) – передбачає визначення кількості персоналу на основі доступного бюджету для служби внутрішнього аудиту. Включає визначення загального бюджету на внутрішній аудит, розрахунок витрат на одного аудитора, з'ясування максимальної кількості аудиторів, яку можна найняти в межах наявного бюджету;

5) методика на основі компетенцій (Велика Британія, Канада) – базується на аналізі необхідних компетенцій для виконання аудиторських завдань. Визначення компетенцій, необхідних для проведення аудиту та включає оцінку наявних компетенцій у поточного персоналу, визначення потреби в додаткових ресурсах або навчанні тощо [36].

Одним із ключових аспектів цих методик є використання передових аналітичних технологій для забезпечення оперативного виявлення ризиків та своєчасного оновлення аудиторських планів і обсягів. Це дозволяє аудиторським командам проводити ширший спектр діяльності з вищим ступенем точності, охоплюючи оцінку ризиків, планування аудиту та його виконання, а також забезпечувати умови для того, щоб пріоритизація аудитів та обсяг перевірок відображали високо динамічне середовище.

Важливим складником цієї системи за сучасних умов є методика ризик-орієнтованого планування діяльності внутрішнього аудиту, яка включає визначення пріоритетності об'єктів аудиту за допомогою певних факторів відбору та частоти, з якою буде досліджуватися кожний із об'єктів аудиту. За результатами оцінки ризиків у просторі аудиту визначається велика кількість об'єктів аудиту та пов'язаних із ними ризиків, для аналізу важливості яких додатково використовується набір "факторів відбору", який допомагає визначити пріоритетність (першочерговість) дослідження відповідного (найбільш доцільного) об'єкта аудиту.

В Україні використовується методика розрахунку нормативної чисельності окремих категорій працівників на основі норм праці, затверджена наказом Міністерства праці та соціальної політики України від 04.09.2000 № 222 [19], орієнтована на аналіз та оцінку обсягу робіт, що мають виконуватися, враховує специфіку діяльності установ і організацій та включає оцінку необхідної кількості годин на виконання різноманітних завдань, що дає змогу ефективно розподілити робочий час та визначити оптимальну чисельність штату з урахуванням нормативних вимог та потреб установи. Ключовим елементом цієї методики є врахування норм часу, нормативів чисельності та навантаження, часу обслуговування й норми обслуговування залежно від конкретного виду діяльності та спеціалізації працівників. Ці нормативи допомагають планувати робочий процес, оптимізувати використання ресурсів та забезпечувати високий рівень продуктивності й ефективності трудових процесів.

Важливою частиною окресленого процесу є аналіз поточного стану та потреб установи, що передбачає визначення обсягів роботи, які треба виконати, та оцінку поточної продуктивності особового складу. На основі цього аналізу можна коригувати планування штату, враховуючи майбутні зміни в обсязі й характері робіт, а також впровадження нових технологій і методів роботи та їхній вплив на норми й стандарти праці.

Для застосування цих методик у рамках МО України варто враховувати локальні особливості та специфіку управління ризиками в умовах дії правового режиму воєнного стану. Варто зазначити, що розрахунок чисельності працівників служби внутрішнього аудиту може залежати від різних факторів. Водночас є деякі загальні підходи, на які слід звернути увагу:

визначення обсягу робіт, які мають бути виконані внутрішнім аудитором, у днях, годинах або інших одиницях виміру;

визначення кількості годин, які потрібні для виконання кожного завдання внутрішнього аудиту;

розрахунок загальної кількості годин, необхідних для виконання всіх завдань внутрішнього аудиту;

розрахунок кількості повних робочих днів, які доступні для внутрішнього аудиту в період, для якого розраховується чисельність;

розрахунок середнього числа годин на день для внутрішнього аудиту;

розрахунок чисельності працівників внутрішнього аудиту шляхом поділу загальної кількості годин, необхідних для виконання всіх завдань, на кількість годин на одного працівника.

Розроблення методики визначення кількості персоналу служби внутрішнього аудиту МО України з урахуванням підходів ризик-орієнтованого планування діяльності з внутрішнього аудиту передбачає розгляд цілого комплексу факторів, які можуть вплинути на завантаженість, обсяг та складність діяльності:

фінансова важливість, тобто установи (організації) з високим рівнем ризику з меншим кошторисом будуть менш пріоритетними для внутрішнього аудиту, ніж установи та організації із середнім рівнем ризику, кошторис яких великий;

розмір і складність діяльності, яка базується на складності об'єкта аудиту, що визначається кількістю персоналу, географічним розташуванням, інтенсивністю бойових дій тощо;

загальна політика внутрішнього контролю (за наявності належної системи внутрішнього контролю в установі визначаються сфери з найбільш значними ризиками, включаючи фінансові, операційні та стратегічні ризики). У випадку слабкої системи внутрішнього контролю ймовірність шахрайства та помилок є набагато більшою;

репутаційна чутливість установи;

масштаб зміни нормативно-правових актів, кадрових змін, змін у функціях (процесах);

надійність командування;

схильність до зловживань;

питання, які цікавлять командування;

термін від попереднього аудиту;

впровадження аудиторських рекомендацій;

робоче навантаження.

Використовуючи методичні підходи визначення чисельності окремих категорій працівників на основі норм праці та орієнтуючись на фактори, які впливають на реалізацію функцій служби внутрішнього аудиту, виокремлюємо найбільш імовірний критерій для розроблення методики визначення чисельності персоналу служби внутрішнього аудиту МО України – розрахунок на основі норм навантаження, скорегований на індекс пріоритетності.

Методика розрахунку штатної чисельності працівників на основі норм навантаження в Україні передбачає визначення оптимальної кількості персоналу, необхідної для ефективного виконання певного обсягу робіт або завдань за умови нормальних умов праці. Цей процес передбачає кілька основних етапів:

1) визначення загального обсягу робіт, які необхідно виконати за певний період, зокрема шляхом аналізу даних звітності за минулі періоди, планів розвитку тощо;

2) визначення норм навантаження шляхом розроблення або використання наявних нормативів, що визначають кількість роботи, яку один працівник може виконати за одиницю часу (наприклад, годину, день, місяць);

3) розрахунок потреби в працівниках шляхом ділення загального обсягу робіт на норму навантаження на одного працівника та коригування розрахунків із врахуванням можливих відхилень (наприклад, неможливість доступу до об'єкта аудиту через бойові дії або інші обмеження, непередбачений обсяг роботи, відсутність працівників через хворобу чи відпустку, а також ефективність роботи персоналу). Це може потребувати коригування розрахункової кількості працівників у бік збільшення або зменшення.

Згідно з методикою, штатна чисельність працівників на основі норм навантаження визначається за формулою:

$$Ч_ш = (N \div Н_н) \cdot К_н \cdot Іп,$$

де N – загальна кількість виконаних робіт в одиницях вимірювання за рік;

$Нн$ – середньорічні норми навантаження в одиницях вимірювання за рік на одного виконавця;

$К_н$ – коефіцієнт можливих невиходів працівників;
$І_п$ – індекс пріоритетності.

Середня норма навантаження в одиницях вимірювання на одного виконавця розраховується за формулою:

$$Н_н = (Ф_К \div Т_{ср}),$$

де $Ф_К$ – корисний фонд робочого часу за рік, год. (у 2024 р. – 2026 год.);
$Т_{ср}$ – середні нормативні трудовитрати на виконання однієї роботи в одиницях вимірювання;

$$Т_{ср} = (Т_з \div N),$$

де $Т_з$ – загальні трудовитрати на виконання виконавцем (або виконавцями) всього обсягу встановлених робіт за рік.

Індекс пріоритетності $І_п$ визначається за допомогою набору критеріїв оцінки кожного фактора відбору, які були розглянуті вище, а також визначення частоти здійснення планових внутрішніх аудитів щодо кожного пріоритетного об'єкта аудиту. Алгоритм розрахунку цього показника передбачає кілька етапів:

1) визначення факторів відбору;

2) оцінка факторів відбору шляхом присвоєння відповідних балів від 1 до 4 де низький фактор – 1, середній фактор – 2, високий фактор – 3, дуже високий фактор – 4 [21];

3) визначення показників вагомості за окресленими факторами відбору.

Відповідно до методики ризик-орієнтованого планування діяльності з внутрішнього аудиту, розробленої Міністерством фінансів України, найбільш затребуваними факторами відбору є такі:

фінансова важливість (матеріальність) – пріоритетність об'єктів аудиту визначається рівнем використання бюджетних коштів, де об'єкти з більшими витратами мають вищу пріоритетність;

складність діяльності – об'єкти з більш складною структурою та організацією потребують більше уваги аудиту через вищий ризик невідповідного виконання;

загальна політика внутрішнього контролю – належна система внутрішнього контролю знижує ризики, тому об'єкти з ефективною системою контролю можуть мати нижчий пріоритет;

репутаційна чутливість – об'єкти, діяльність яких викликає значний інтерес суспільства та ЗМІ, мають вищу пріоритетність через ризики для репутації установи;

масштаб змін – значні зміни в об'єкті підвищують імовірність помилок, що вимагає більш ретельного аудиту;

надійність керівництва – об'єкти з менш досвідченим або часто змінюваним керівництвом мають більший ризик та потребують детальнішого аудиту;

можливість для зловживань – об'єкти з вищою ймовірністю корупційних схем вимагають більш ретельного контролю;

питання, які цікавлять керівництво – пріоритетність аудиту визначається також на основі важливості питань, які викликають занепокоєння керівництва;

час від попереднього аудиту – об'єкти, які не перевірялися протягом тривалого часу, потребують аудиту через можливе накопичення ризиків;

стан впровадження аудиторських рекомендацій – об'єкти з низьким рівнем впровадження попередніх рекомендацій мають вищу пріоритетність через підвищені ризики [21].

Враховуючи сутність зазначених показників та специфіку функціонування військових частин ЗС України як в мирний час, так і в умовах дії правового режиму воєнного стану, для визначення індексу пріоритетності в ризик-орієнтованому плануванні діяльності з внутрішнього аудиту в МО України такі фактори відбору, як загальна політика внутрішнього контролю, надійність керівництва, питання, які цікавлять керівництво, можливість для зловживань доцільно скорегувати на такі фактори, як стан внутрішнього контролю, надійність управління, стан управління ризиками, періодичність аудиту. Отже визначаючи індекс пріоритетності (*Іп)* з використанням запропонованої методики Міністерством фінансів [21], фактори відбору та відповідні показники вагомості можна представити у такому вигляді:

Таблиця 2 – Присвоєння показників вагомості факторам відбору в ризик-орієнтованому плануванні діяльності з внутрішнього аудиту (розроблено автором на основі Методичного посібника Міністерства фінансів України з ризик орієнтованого планування діяльності з внутрішнього аудиту)

Фактори відбору		Показник вагомості
A.	Фінансова важливість	Wa
B.	Складність діяльності	Wb
C.	Стан внутрішнього контролю	Wc
D.	Репутаційна чутливість	Wd
E.	Масштаб змін	We
F.	Надійність управління	Wf
G.	Схильність до зловживань	Wg
H.	Стан управління ризиками	Wh
I.	Періодичність аудиту	Wi
J.	Впровадження аудиторських рекомендацій	WJ
K.	Робоче навантаження	Wk

4) Розрахунок індексу пріоритетності:

$$\mathrm{I_п}=R_m \times \left(\frac{(A\times \mathrm{Wa})+(B\times \mathrm{Wb})+(C\times \mathrm{Wc})+(D\times \mathrm{Wd})+(E\times \mathrm{We})+(F\times \mathrm{Wf})+(G\times \mathrm{Wg})+(H\times \mathrm{Wh})+(I\times \mathrm{Wi})+(J\times \mathrm{Wj})+(K\times \mathrm{Wk})}{n}\right),$$

де *Іп* – індекс пріоритетності;
Rm – загальна оцінка ризику за ймовірністю та впливом;
A-K – бал, присвоєний за фактором відбору;
Wa-Wk – показник вагомості фактору відбору;
n – загальна кількість застосованих факторів відбору;

5) Визначення пріоритетності об'єктів аудиту за умови встановленого загального періоду внутрішнього аудиту 5 років.

Ступінь пріоритету	Частота планових внутрішніх аудитів щодо кожного пріоритетного об'єкта аудиту	Індекс пріоритетності
Дуже високий	4 рази на 5 років	≥ 100
Високий	3 рази на 5 років	61 - 99
Середній	2 рази на 5 років	41 - 60
Низький	1 рази на 5 років	≤ 40

6) Визначення частоти здійснення планових внутрішніх аудитів щодо кожного об'єкта аудиту.

Частота здійснення планових внутрішніх аудитів залежить від величини простору аудиту, результатів оцінки ризиків, кількісних та якісних спроможностей підрозділу внутрішнього аудиту (кількість аудитів, що можуть бути здійснені протягом планового періоду, фахова спеціалізація внутрішніх аудиторів, рівень навичок тощо).

За результатами розрахунків буде виявлено, що за наявними спроможностями для ефективного використання ресурсів, підрозділу внутрішнього аудиту необхідно в першу чергу концентруватися на об'єктах аудиту з "високим" та "дуже високим" ступенем пріоритету, об'єкти аудиту з "низьким" ступенем пріоритету з часом можуть викликати високі ризики, особливо коли тривалий період щодо таких об'єктів внутрішній аудит не здійснюється.

Висновки

Результати дослідження в розрізі поставлених завдань дають змогу сформулювати такі основні висновки:

1. Детальний аналіз нормативно-правових актів та основних засад функціонування служби внутрішнього аудиту МО України засвідчив, що й діяльність служби внутрішнього аудиту спрямована на вдосконалення системи управління внутрішнього контролю, запобігання незаконному та неефективному використанню бюджетних коштів військовими частинами, а також надання незалежних висновків і рекомендацій. В умовах правового режиму воєнного стану ці завдання набувають особливої важливості через зростання обсягів фінансування та збільшення ризиків.

2. Протягом останнього десятиріччя відбулися значні зміни в обсягах фінансування сектору безпеки і оборони України, зокрема Міністерства оборони України. Після початку повномасштабного вторгнення фінансування суттєво зросло: збільшено обсяг виділених державних ресурсів на потреби військових частин, виплату винагород військовослужбовцям, а також закупівлю озброєння та військової техніки. Така динаміка підкреслює потребу посиленого контролю за ефективністю та законністю використання бюджетних коштів.

3. На сьогодні чисельність персоналу Служби внутрішнього аудиту Міністерства оборони України не відповідає обсягу робіт та наявним фінансовим ризикам. Збільшення обсягів фінансування та кількості об'єктів аудиту призводить до значного навантаження на одного аудитора. Наявна чисельність персоналу є недостатньою для ефективного виконання покладених на нього завдань, що створює ризики щодо законності та ефективності використання бюджетних коштів військовими частинами.

4. Автором проаналізовано чинні методики визначення нормативної чисельності окремих категорій працівників та вперше запропоновано методику визначення чисельності персоналу служби внутрішнього аудиту МО України на основі ризик-орієнтованого підходу, яка враховує обсяги фінансування, кількість об'єктів аудиту, ризикові фактори та інші чинники, що впливають на навантаження аудиторів. Запровадження та удосконалення цієї методики дозволить забезпечити на основі науково-обґрунтованого підходу формування штату персоналу служби внутрішнього аудиту МО України, заснованого на реальних потребах, із застосуванням ризик-орієнтованого підходу до планування діяльності з внутрішнього аудиту, та значно підвищити ефективність.

5. Аналізуючи результати дослідження в розрізі поставлених завдань, слід зазначити, що його мету досягнуто. Водночас, враховуючи вимоги дії правового режиму воєнного стану в Україні та відповідні обмеження, зазначимо, що розроблена методика потребує доопрацювання та подальшого вдосконалення. Серед перспективних напрямків роботи – обговорення результатів дослідження на науково-практичних конференціях з метою

визначення актуальних питань впровадження методики та шляхів її оптимізації; доповнення факторів відбору та визначення їхньої вагомості в ризик-орієнтованому плануванні діяльності з внутрішнього аудиту; проведення емпіричних досліджень щодо впровадження розробленої методики на основі конкретних даних військ; дослідження впливу інформатизації процесів внутрішнього аудиту на його якість, ефективність та потреби в людських ресурсах для його здійснення.

Окреслені аспекти досліджень сприятимуть подальшому вдосконаленню системи внутрішнього аудиту МО України, підвищенню її ефективності та забезпеченню відповідності сучасним викликам.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Бюджетний кодекс України Закон України від 08.07.2010, № 2456-VI. URL: https://zakon.rada.gov.ua/laws/show/2456-17#Text.
2. Про Державний бюджет України на 2024 рік. Закон України від 09.11.2023, №3460-IX. URL: https://zakon.rada.gov.ua/laws/show/3460-20#Text
3. Про Державний бюджет України на 2023 рік. Закон України від 03.11.2022, №2710-IX. URL: https://zakon.rada.gov.ua/laws/show/2710-20#Text
4. Про Державний бюджет України на 2022 рік. Закон України від 02.12.2021, №1928-IX. URL: https://zakon.rada.gov.ua/laws/show/1928-20#Text
5. Про Державний бюджет України на 2021 рік. Закон України від 15.12.2020, №1082-IX. URL: https://zakon.rada.gov.ua/laws/show/1082-20#Text
6. Про Державний бюджет України на 2020 рік. Закон України від 14.11.2019, №294-IX. URL: https://zakon.rada.gov.ua/laws/show/294-20#Text
7. Про Державний бюджет України на 2019 рік. Закон України від 23.11.2018, №2629-VIII. URL: https://zakon.rada.gov.ua/laws/show/2629-19#Text
8. Про Державний бюджет України на 2018 рік. Закон України від 07.12.2017, №2246-VIII. URL: https://zakon.rada.gov.ua/laws/show/2246-19#Text
9. Про Державний бюджет України на 2017 рік. Закон України від 21.12.2016, №1801-VIII. URL: https://zakon.rada.gov.ua/laws/show/1801-19#Text
10. Про Державний бюджет України на 2016 рік. Закон України від 25.12.2015, №928-VIII. URL: https://zakon.rada.gov.ua/laws/show/928-19#Text
11. Про Державний бюджет України на 2015 рік. Закон України від 28.12.2014, №80-VIII. URL: https://zakon.rada.gov.ua/laws/show/80-19#Text
12. Про Державний бюджет України на 2014 рік. Закон України від 16.01.2014, №719-VII. URL: https://zakon.rada.gov.ua/laws/show/719-18#Text
13. Про Державний бюджет України на 2013 рік. Закон України від 06.12.2012, № 5515-VI. URL: https://zakon.rada.gov.ua/laws/show/5515-17#Text
14. Про Державний бюджет України на 2012 рік. Закон України від 22.12.2011, № 4282-VI. URL: https://zakon.rada.gov.ua/laws/show/4282-17#Text

15. Деякі питання здійснення внутрішнього аудиту та утворення підрозділів внутрішнього аудиту. Постанова Кабінету міністрів України від 28.09.2011, №1001. URL: https://zakon.rada.gov.ua/laws/show/1001-2011-%D0%BF#Text
16. Щодо організації та здійснення внутрішнього контролю та внутрішнього аудиту. Вказівка Міністерства фінансів України від 19.12.2018, №33020-07-2/33930. URL: https://1ll.ink/1eXzj
17. Щодо можливості здійснення внутрішнього аудиту в період дії правового режиму воєнного стану. Вказівка Міністерства фінансів України від 20.03.2022, № 33020-07-5/6432. URL: https://document.vobu.ua/doc/11856.
18. Про організацію діяльності з внутрішнього аудиту в системі Міністерства оборони України. Наказ міністерства оборони України від 15.12.2020, № 475. URL: https://www.mil.gov.ua/content/nakaz_moy/475_mou.PDF
19. Про Методику розрахунку нормативної чисельності окремих категорій працівників на основі норм з праці. Наказ міністерства праці та соціальної політики України від 04.09.2000, № 222. URL: https://vk24.ua/regulations_and_jurisprudence/nakazi/pro-metodiku-rozrahunku-normativnoi-ciselnosti-okremih-kategorii-pracivnikiv-na-osnovi-norm-z-praci
20. Актуалізація чисельності особового складу Служби внутрішнього аудиту Міністерства оборони України. Матеріали доповіді заступника Міністра оборони України. Київ, 2024.
21. Ризик-орієнтоване планування діяльності з внутрішнього аудиту. Методичний посібник. URL: http://surl.li/vcwtof.
22. Звіт (зведений звіт) про результати діяльності підрозділу внутрішнього аудиту Міністерства оборони України за 2022 рік. Київ, 2023.
23. Звіт (зведений звіт) про результати діяльності підрозділу внутрішнього аудиту Міністерства оборони України за 2021 рік. Київ, 2022.
24. Звіт (зведений звіт) про результати діяльності підрозділу внутрішнього аудиту Міністерства оборони України за 2020 рік. Київ, 2021.
25. Звіт (зведений звіт) про результати діяльності підрозділу внутрішнього аудиту Міністерства оборони України за 2019 рік. Київ, 2020.
26. Дрозд І.К. Контроль економічних систем. Монографія. Київ: Імекс-ЛТД, 2004. 312 с.
27. Дорош Н.І. Внутрішній контроль та аудит в управлінні ризиками на підприємстві. Вісник Львівської комерційної академії. Серія: Економічна. 2014. Вип. № 44. С. 148–152.
28. Гура Н., Склярук І. Проблеми формування собівартості та порядок її відображення в податковій звітності. Бухгалтерський облік і аудит. 2011. № 11. С. 6–13.
29. Подолянчук О.А. Інвентаризація в аудиті як прийом методу фактичного контролю. Економічні науки. Серія : Облік і фінанси. 2015. Вип. 12(1). С. 240–249.
30. Аудит в умовах сталого розвитку: колективна монографія / за загальною редакцією проф. О. А. Петрик / О. А. Петрик, Н. В. Гойло, І. І. Матієнко-Зубенко, І. О. Мариніч, Ю. Б. Слободяник ін. Київ: КНЕУ, 2021. 231с.
31. Петрик О. А., Фенченко М. Аудит у зарубіжних країнах: Навч.-метод. посібник для самост. вивч. дисц. / за заг. ред. О. А. Петрик. Київ: КНЕУ, 2002. 168 с.
32. Ульянов К., Бариніна М. Еволюція поглядів на призначення фінансово-контрольних органів Міністерства оборони України. Social development & Security. 2018. Vol. 2, No. 4. P. 59–68. URL: http://doi.org/10.5281/zenodo.1237042.
33. Лойшин А., Шпиталь О., Ткач І. Обґрунтування доцільності розробки індикаторів внутрішнього контролю в Міністерстві оборони України та Збройних Силах України. Social development & Security. 2018. Vol. 6, No. 8. P. 27–42. URL: https://paperssds.eu/index.php/JSPSDS/article/view/78/77.

34. Ignatenko, A., Lysenko, M., Loishyn, A., & Mazka, S. (2019). Аналіз процесу становлення внутрішнього аудиту в Міністерстві оборони України. *Social Development and Security*, *9*(1), 40-59. https://doi.org/10.33445/sds.2019.9.1.4
35. Луцик, Ю., Мазка, С., Бегма, В., Мірненко, В., Ульянов, К., & Юрків, Н. (2019). Підвищення ефективності державного фінансового контролю за рахунок впровадження системи ризик-орієнтованого планування. *Social Development and Security*, *9*(4), 41–60. https://doi.org/10.33445/sds.2019.9.4.3.
36. Pickett, K. H. Spencer. The Internal Auditing Handbook. 3rd ed., John Wiley & Sons, 2010. URL: https://www.perlego.com/book/1007527/the-internal-auditing-handbook.

References

1. Biudzhetnyi kodeks Ukrainy Zakon Ukrainy [Budget Code of Ukraine Law of Ukraine] vid 08.07.2010, № 2456-VI. Available from: https://zakon.rada.gov.ua/laws/show/2456-17#Text.
2. Pro Derzhavnyi biudzhet Ukrainy na 2024 rik. Zakon Ukrainy [On the State Budget of Ukraine for 2024. Law of Ukraine] vid 09.11.2023, №3460-IX. Available from: https://zakon.rada.gov.ua/laws/show/3460-20#Text.
3. Pro Derzhavnyi biudzhet Ukrainy na 2023 rik. Zakon Ukrainy [On the State Budget of Ukraine for 2023. Law of Ukraine] vid 03.11.2022, №2710-IX. Available from: https://zakon.rada.gov.ua/laws/show/2710-20#Text.
4. Pro Derzhavnyi biudzhet Ukrainy na 2022 rik. Zakon Ukrainy [On the State Budget of Ukraine for 2022. Law of Ukraine] vid 02.12.2021, №1928-IX. Available from: https://zakon.rada.gov.ua/laws/show/1928-20#Text.
5. Pro Derzhavnyi biudzhet Ukrainy na 2021 rik. Zakon Ukrainy [On the State Budget of Ukraine for 2021. Law of Ukraine] vid 15.12.2020, №1082-IX. Available from: https://zakon.rada.gov.ua/laws/show/1082-20#Text.
6. Pro Derzhavnyi biudzhet Ukrainy na 2020 rik. Zakon Ukrainy [On the State Budget of Ukraine for 2020. Law of Ukraine] vid 14.11.2019, №294-IX. Available from: https://zakon.rada.gov.ua/laws/show/294-20#Text.
7. Pro Derzhavnyi biudzhet Ukrainy na 2019 rik. Zakon Ukrainy [On the State Budget of Ukraine for 2019. Law of Ukraine] vid 23.11.2018, №2629-VIII. Available from: https://zakon.rada.gov.ua/laws/show/2629-19#Text.
8. Pro Derzhavnyi biudzhet Ukrainy na 2018 rik. Zakon Ukrainy [On the State Budget of Ukraine for 2018. Law of Ukraine] vid 07.12.2017, №2246-VIII. Available from: https://zakon.rada.gov.ua/laws/show/2246-19#Text.
9. Pro Derzhavnyi biudzhet Ukrainy na 2017 rik. Zakon Ukrainy [On the State Budget of Ukraine for 2017. Law of Ukraine] vid 21.12.2016, №1801-VIII. Available from: https://zakon.rada.gov.ua/laws/show/1801-19#Text.
10. Pro Derzhavnyi biudzhet Ukrainy na 2016 rik. Zakon Ukrainy [On the State Budget of Ukraine for 2016. Law of Ukraine] vid 25.12.2015, №928-VIII. Available from: https://zakon.rada.gov.ua/laws/show/928-19#Text.
11. Pro Derzhavnyi biudzhet Ukrainy na 2015 rik. Zakon Ukrainy [On the State Budget of Ukraine for 2015. Law of Ukraine] vid 28.12.2014, №80-VIII. Available from: https://zakon.rada.gov.ua/laws/show/80-19#Text.
12. Pro Derzhavnyi biudzhet Ukrainy na 2014 rik. Zakon Ukrainy [On the State Budget of Ukraine for 2014. Law of Ukraine] vid 16.01.2014, №719-VII. Available from: https://zakon.rada.gov.ua/laws/show/719-18#Text.

13. Pro Derzhavnyi biudzhet Ukrainy na 2013 rik. Zakon Ukrainy [On the State Budget of Ukraine for 2013. Law of Ukraine] vid 06.12.2012, № 5515-VI. Available from: https://zakon.rada.gov.ua/laws/show/5515-17#Text.
14. Pro Derzhavnyi biudzhet Ukrainy na 2012 rik. Zakon Ukrainy [On the State Budget of Ukraine for 2012. Law of Ukraine] vid 22.12.2011, № 4282-VI. Available from: https://zakon.rada.gov.ua/laws/show/4282-17#Text.
15. Deiaki pytannia zdiisnennia vnutrishnoho audytu ta utvorennia pidrozdiliv vnutrishnoho audytu. Postanova Kabinetu ministriv Ukrainy [Some Issues of Internal Audit and Establishment of Internal Audit Units. Resolution of the Cabinet of Ministers of Ukraine] vid 28.09.2011, №1001. Available from: https://zakon.rada.gov.ua/laws/show/1001-2011-%D0%BF#Text.
16. Shchodo orhanizatsii ta zdiisnennia vnutrishnoho kontroliu ta vnutrishnoho audytu. Vkazivka Ministerstva finansiv Ukrainy [On the organization and implementation of internal control and internal audit. Instruction of the Ministry of Finance of Ukraine] vid 19.12.2018, №33020-07-2/33930. Available from: https://1ll.ink/1eXzj.
17. Shchodo mozhlyvosti zdiisnennia vnutrishnoho audytu v period dii pravovoho rezhymu voiennoho stanu. Vkazivka Ministerstva finansiv Ukrainy [On the possibility of internal audit during the period of martial law. Instruction of the Ministry of Finance of Ukraine] vid 20.03.2022, № 33020-07-5/6432. Available from : https://document.vobu.ua/doc/11856.
18. Pro orhanizatsiiu diialnosti z vnutrishnoho audytu v systemi Ministerstva oborony Ukrainy. Nakaz ministerstva oborony Ukrainy [On the organization of internal audit activities in the system of the Ministry of Defense of Ukraine. Order of the Ministry of Defense of Ukraine] vid 15.12.2020, № 475. Available from: https://www.mil.gov.ua/content/nakaz_moy/475_mou.PDF.
19. Pro Metodyku rozrakhunku normatyvnoi chyselnosti okremykh katehorii pratsivnykiv na osnovi norm z pratsi. Nakaz ministerstva pratsi ta sotsialnoi polityky Ukrainy [On the Methodology for Calculating the Standard Number of Certain Categories of Employees Based on Labor Standards. Order of the Ministry of Labor and Social Policy of Ukraine] vid 04.09.2000, № 222. Available from: https://vk24.ua/regulations_and_jurisprudence/nakazi/pro-metodiku-rozrahunku-normativnoi-ciselnosti-okremih-kategorii-pracivnikiv-na-osnovi-norm-z-praci.
20. Aktualizatsiia chyselnosti osobovoho skladu Sluzhby vnutrishnoho audytu Ministerstva oborony Ukrainy. [Updating the number of personnel of the Internal Audit Service of the Ministry of Defense of Ukraine.] Materialy dopovidi zastupnyka Ministra oborony Ukrainy. Kyiv, 2024.
21. Ryzyk-oriientovane planuvannia diialnosti z vnutrishnoho audytu. [Risk-based planning of internal audit activities.] Metodychnyi posibnyk. Available from: http://surl.li/vcwtof.
22. Zvit (zvedenyi zvit) pro rezultaty diialnosti pidrozdilu vnutrishnoho audytu Ministerstva oborony Ukrainy za 2022 rik. [Report (consolidated report) on the results of the activities of the Internal Audit Unit of the Ministry of Defense of Ukraine for 2022.] Kyiv, 2023.
23. Zvit (zvedenyi zvit) pro rezultaty diialnosti pidrozdilu vnutrishnoho audytu Ministerstva oborony Ukrainy za 2021 rik. [Report (consolidated report) on the results of the activities of the Internal Audit Unit of the Ministry of Defense of Ukraine for 2021.] Kyiv, 2022.
24. Zvit (zvedenyi zvit) pro rezultaty diialnosti pidrozdilu vnutrishnoho audytu Ministerstva oborony Ukrainy za 2020 rik. [Report (consolidated report) on the results of the activities of the Internal Audit Unit of the Ministry of Defense of Ukraine for 2020.] Kyiv, 2021.
25. Zvit (zvedenyi zvit) pro rezultaty diialnosti pidrozdilu vnutrishnoho audytu Ministerstva oborony Ukrainy za 2019 rik. [Report (consolidated report) on the results of the activities of the Internal Audit Unit of the Ministry of Defense of Ukraine for 2019.] Kyiv, 2020.
26. Drozd I.K. Kontrol ekonomichnykh system. [Control of economic systems] Monohrafiia. Kyiv: Imeks-LTD, 2004. 312 s.

27. Dorosh N.I. (2014). Vnutrishnii kontrol ta audyt v upravlinni ryzykamy na pidpryiemstvi. [Internal control and audit in risk management at the enterprise.] *Visnyk Lvivskoi komertsiinoi akademii. Seriia: Ekonomichna*. 2014. Vyp. № 44. S. 148–152.
28. Hura N., Skliaruk I. Problemy formuvannia sobivartosti ta poriadok yii vidobrazhennia v podatkovii zvitnosti. [Problems of cost formation and the procedure for its reflection in tax reporting.] *Bukhhalterskyi oblik i audyt*. 2011. № 11. S. 6–13.
29. Podolianchuk O.A. Inventaryzatsiia v audyti yak pryiom metodu faktychnoho kontroliu. [Inventory in the audit as a method of actual control.] Ekonomichni nauky. Ceriia : Oblik i finansy. 2015. Vyp. 12(1). S. 240–249.
30. Audyt v umovakh staloho rozvytku: kolektyvna monohrafiia [Audit in the context of sustainable development: a collective monograph] za zahalnoiu redaktsiieiu prof. O. A. Petryk O. A. Petryk, N. V. Hoilo, I. I. Matiienko-Zubenko, I. O. Marynich, Yu. B. Slobodianyk in. Kyiv: KNEU, 2021. 231s.
31. Petryk O. A., Fenchenko M. Audyt u zarubizhnykh krainakh: Navch.-metod. posibnyk dlia samost. vyvch. dysts. [Audit in foreign countries: Study guide for self-study of disciplines]. / za zah. red. O. A. Petryk. Kyiv: KNEU, 2002. 168 s.
32. Ulianov K., Barynina M. (2018). Evoliutsiia pohliadiv na pryznachennia finansovo-kontrolnykh orhaniv Ministerstva oborony Ukrainy. [Evolution of views on the appointment of financial and control bodies of the Ministry of Defense of Ukraine.] *Social development and Security*. 2018. Vol. 2, No. 4. P. 59–68. Available from: http://doi.org/10.5281/zenodo.1237042.
33. Loishyn A., Shpytal O., Tkach I. (2018). Obgruntuvannia dotsilnosti rozrobky indykatoriv vnutrishnoho kontroliu v Ministerstvi oborony Ukrainy ta Zbroinykh Sylakh Ukrainy. [Substantiation of the expediency of developing internal control indicators in the Ministry of Defense of Ukraine and the Armed Forces of Ukraine.] *Social development and Security*. 2018. Vol. 6, No. 8. P. 27–42. Available from: https://paperssds.eu/index.php/JSPSDS/article/view/78/77.
34. Ignatenko, A., Lysenko, M., Loishyn, A., & Mazka, S. (2019). Analysis of the process of internal audit in Ministry of defense of Ukraine. *Social Development and Security*, *9*(1), 40-59. https://doi.org/10.33445/sds.2019.9.1.4
35. Lutsik, J., Mazka, S., Begma, V., Mirnenko, V., Ulianov, K., & Yurkiv, N. (2019). Improving the effectiveness of public financial control through the introduction of risk-oriented planning. *Social Development and Security*, *9*(4), 41–60. https://doi.org/10.33445/sds.2019.9.4.3
36. Pickett, K. H. Spencer. The Internal Auditing Handbook. 3rd ed., John Wiley & Sons, 2010. Available from: https://www.perlego.com/book/1007527/the-internal-auditing-handbook

Розвиток людського капіталу в умовах демографічних змін та діджиталізації економіки

Human capital development in the context of demographic changes and digitalization of the economy

Світлана Бондаренко
д. економ. н., професор, професор кафедри соціоекономіки та управління персоналом, e-mail: bondarenko.svitlana@kneu.edu.ua, ORCID: 0000-0002-1687-1172

Svitlana Bondarenko
Dr of Economics Sciences, Professor, e-mail: bondarenko.svitlana@kneu.edu.ua, ORCID: 0000-0002-1687-1172

Київський національний економічний університет імені Вадима Гетьмана, м. Київ, Україна

Kyiv National Economic University named after Vadym Hetman, Kyiv, Ukraine

Received: October 14, 2024 | Revised: October 28, 2024 | Accepted: October 31, 2024

DOI: 10.33445/sds.2024.14.5.25

Мета роботи: Теоретичне обґрунтування, розроблення методологічних положень та науково-практичних рекомендацій щодо формування системи розвитку людського капіталу в умовах демографічних змін та діджиталізації економіки.

Метод дослідження: системний підхід, економетричне моделювання, компаративний аналіз, статистичний аналіз.

Практична цінність дослідження: Розроблено методичний підхід до оцінювання впливу демографічних змін на формування людського капіталу, який враховує взаємозв'язок між віковою структурою населення та продуктивністю праці в цифровій економіці. Запропоновано механізм оптимізації інвестицій у розвиток людського капіталу та науково-практичні рекомендації щодо адаптації системи освіти до вимог цифрової економіки з урахуванням особливостей різних вікових груп населення.

Цінність дослідження: Поглиблено розуміння механізмів взаємодії між демографічними та технологічними факторами розвитку людського капіталу, розвинуто методологічний інструментарій оцінювання впливу демографічних змін, сформовано нові підходи до оптимізації розвитку людського капіталу в умовах цифрової економіки. Емпірично доведено можливість компенсації негативного впливу демографічного старіння через розвиток цифрових компетенцій.

Тип статті: Дослідницька.

Ключові слова: людський капітал, демографічні зміни, діджиталізація економіки, старіння населення, цифрові компетенції, демографічне навантаження.

Purpose: Theoretical substantiation, development of methodological principles and scientific-practical recommendations for the formation of a human capital development system under demographic changes and digitalization of the economy.

Method: a systematic approach, econometric modeling, comparative analysis, statistical analysis.

Practical value of the research: A methodological approach has been developed to assess the impact of demographic changes on human capital formation, which takes into account the relationship between population age structure and labor productivity in the digital economy. A mechanism for optimizing investments in human capital development and scientific-practical recommendations for adapting the education system to the requirements of the digital economy, considering the characteristics of different age groups, has been proposed.

Value of the research: Enhanced understanding of interaction mechanisms between demographic and technological factors of human capital development, advanced methodological tools for assessing the impact of demographic changes, and developed new approaches to optimizing human capital development in the digital economy. Empirically proven possibility of compensating for the negative impact of demographic aging through the development of digital competencies.

Type of article: research.

Key words: human capital, demographic changes, economic digitalization, population aging, digital competencies, demographic burden.

Вступ

В умовах глобальних суспільно-економічних трансформацій особливої актуальності набуває дослідження розвитку людського капіталу під впливом демографічних змін та діджиталізації економіки. Згідно з дослідженнями Lutz (2024), традиційні розуміння плавної стабілізації демографічних процесів виявляються хибними, насамперед через стрімке зниження народжуваності та прискореного старіння населення, що створює безпрецедентні виклики для системи формування людського капіталу. Емпіричні дослідження Wang et al. (2024) демонструють, що діджиталізація економіки радикально змінює вимоги до якості людського капіталу, зумовлюючи необхідність переосмислення традиційних підходів до його розвитку.

Водночас, як зазначають Sobiech Pellegrini et al. (2024), підвищення якості людського капіталу може частково компенсувати негативні наслідки демографічного старіння для економічного зростання.

Наукова проблема виникає у невідповідності наявних механізмів розвитку людського капіталу викликам, що формуються під впливом одночасної дії демографічних змін та діджиталізації економіки. За даними дослідженнями Hondroyiannis et al. (2024), демографічне старіння створює підвищений тиск на економічні системи: скорочується збільшення робочої сили при одночасному зростанні навантаження на соціально-економічні інститути. Bai et al. (2024) додатково підкреслюють, що цифрова трансформація економіки потребує принципово нових підходів до формування та розвитку людського капіталу.

Ґрунтуючись на дослідженнях Li et al. (2024) та Chishti et al. (2024), *висувається гіпотеза*, що ефективний розвиток людського капіталу в умовах демографічних змін потребує фундаментальної реконфігурації освітніх та навчальних систем відповідно до вимог цифрової економіки. При цьому результативність такої трансформації дозволяє отримати демографічні обмеження та забезпечити інклюзивність цифрового розвитку для різних вікових груп населення.

Метою дослідження є теоретичне обґрунтування, розроблення методологічних положень та науково-практичних рекомендацій щодо формування системи розвитку людського капіталу в умовах демографічних змін та діджиталізації економіки.

Для досягнення поставленої мети визначено такі завдання:

1. Розкрити теоретико-методологічні засади дослідження взаємозв'язку демографічних змін та процесів формування людського капіталу, систематизувати й узагальнити сучасні наукові підходи до оцінки впливу демографічних тенденцій на розвиток людського капіталу.

2. Обґрунтувати концептуальні положення щодо трансформації системи розвитку людського капіталу в умовах діджиталізації економіки, особливості та закономірності зміни вимог до якісних характеристик людського капіталу під впливом цифрових технологій.

Практичне значення одержаних результатів полягає в розробленні науково-методичних положень щодо розвитку людського капіталу в умовах демографічних змін та діджиталізації економіки. Запропоновано методичний підхід до оцінювання впливу демографічних змін на формування людського капіталу, який, на відміну від існуючих, враховує взаємозв'язок між віковою структурою населення та продуктивністю праці в цифровій економіці (Wang et al., 2024). Розроблено науково-практичні рекомендації щодо адаптації системи освіти до вимог цифрової економіки, які базуються на результатах дослідження Li et al. (2024) та враховують особливості різних вікових груп населення. Запропоновано механізм оптимізації інвестицій у розвиток людського капіталу, який, за результатами досліджень Sobiech Pellegrini et al. (2024), дозволяє збалансувати демографічні обмеження та потреби цифрової трансформації економіки. Теоретична значущість дослідження полягає у розвитку теорії людського капіталу в контексті сучасних демографічних викликів, поглибленні розуміння механізмів взаємодії між демографічними та технологічними факторами, а також формуванні нових підходів до оптимізації розвитку людського капіталу в умовах цифрової економіки.

Методологія дослідження

Теоретико-методологічною основою дослідження є системний підхід до аналізу взаємозв’язків між демографічними процесами, цифровою трансформацією та розвитком людського капіталу. Методологія базується на поєднанні кількісних та якісних методів дослідження, що дозволяє всебічно оцінити досліджувані процеси.

У дослідженні застосовано такі методи:

1. Системного аналізу – для визначення структурних взаємозв'язків між компонентами системи розвитку людського капіталу в умовах демографічних змін та діджиталізації. Застосування цього методу дозволило виявити ключові фактори впливу та механізми їх взаємодії.

2. Економетричного моделювання – для оцінки кількісних параметрів впливу демографічних змін та цифровізації на людський капітал. Зокрема, розроблено модель панельних даних для 36 країн ОЕСР за період 2015-2023 років, що дозволяє оцінити:

прямі ефекти демографічних та цифрових факторів;

ефекти їх взаємодії;

сукупний вплив на розвиток людського капіталу.

3. Компаративного аналізу – для порівняння тенденцій розвитку людського капіталу в різних країнах та регіонах, що дозволило виявити специфічні особливості та закономірності досліджуваних процесів.

4. Статистичного аналізу – для обробки емпіричних даних та виявлення закономірностей розвитку людського капіталу, включаючи:

аналіз динаміки ключових показників;

оцінку взаємозв’язків між змінними;

перевірку статистичної значущості результатів.

Інформаційною базою дослідження є:

демографічні показники з бази даних UN Population Division World Population Prospects 2022;

показники цифровізації з OECD Digital Economy Outlook та EU Digital Economy and Society Index;

економічні індикатори з World Bank World Development Indicators;

аналітичні звіти міжнародних організацій щодо розвитку людського капіталу.

Достовірність отриманих результатів забезпечується:

використанням надійних джерел статистичних даних;

застосуванням сучасних методів економетричного аналізу;

перевіркою результатів на статистичну значущість;

використанням робастних оцінок;

тестуванням моделей на стійкість через альтернативні специфікації.

Обмеження дослідження:

фокус на країнах ОЕСР;

відносно короткий період спостереження (2015-2023);

доступність порівнянних даних щодо цифрових навичок.

Це дозволяє забезпечити комплексний підхід до вирішення поставлених завдань та отримати надійні результати для формування практичних рекомендацій.

Літературний огляд. Людський капітал, який втілений у знаннях, навичках та здібностях людей, є одним із ключових чинників соціально-економічного розвитку. Він визначає інноваційний потенціал, продуктивність праці та конкурентоспроможність як окремих працівників, так і економіки в цілому (Arshed et al., 2024; Webb, 2024).

Методологічні аспекти дослідження розвитку людського капіталу в умовах демографічних та технологічних трансформацій представлені в роботах низки дослідників. Kozlovskyi et al. (2020) обґрунтовують доцільність використання панельного аналізу даних для оцінки впливу демографічних змін на економічні показники розвитку людського капіталу, що дозволяє враховувати як просторову, так і часову варіацію досліджуваних процесів.

Chornous & Gura (2020) розвивають методологічний інструментарій оцінювання впливу цифровізації на розвиток людського капіталу через інтеграцію систем ERP, HCM, BI та

предиктивної аналітики, що створює основу для комплексного прогнозування тенденцій розвитку людського капіталу в умовах цифрової трансформації.

Важливий внесок у розвиток методології дослідження зробили Londar et al. (2020), запропонувавши підхід до аналізу взаємозв'язку між інвестиціями в людський капітал та формуванням цифрової економіки. Kasianenko et al. (2020) розробили методологічні засади компаративного аналізу тенденцій розвитку людського капіталу в різних країнах, що дозволяє виявляти кращі практики та оцінювати ефективність різних політик.

В умовах кризових явищ особливого значення набувають методологічні підходи до аналізу трансформаційних процесів, розроблені Baranovskyi et al. (2021) та Vovk et al. (2021). Їхні дослідження демонструють важливість врахування структурних змін при оцінюванні розвитку людського капіталу.

Kuklin et al. (2021) збагатили методологічний інструментарій через включення інституційних та соціально-економічних факторів розвитку людського капіталу в контекст європейської інтеграції. Методологія Calinescu & Zelenko (2020) щодо визначення регуляторів життєздатного виробництва створює основу для прогнозування тенденцій розвитку людського капіталу в умовах міжнародного співробітництва

Дослідження виявляють низку ключових чинників, що визначають розвиток людського капіталу. Освіта, професійна підготовка та набуття затребуваних на ринку праці навичок є важливими складовими нарощування людського капіталу (Neycheva, 2024). Водночас, доступ до необхідних ресурсів, можливості для неперервного навчання та розвитку, а також соціальний капітал індивіда також мають суттєвий вплив (Mburu et al., 2024; Chisale et al., 2024; Cassetti et al., 2024). Державна політика у сферах освіти, зайнятості, соціального захисту відіграє важливу роль у створенні сприятливих умов для накопичення людського капіталу (Qing & Kumar, 2024; Neycheva, 2024).

Дослідження Sobiech Pellegrini et al. (2024) емпірично довели можливість компенсації негативного впливу старіння населення через підвищення якості людського капіталу. Демографічні зміни, зокрема старіння населення, можуть як сприяти, так і стримувати розвиток людського капіталу. З одного боку, літні працівники накопичують цінний досвід та навички, з іншого - їх продуктивність може знижуватися, а адаптація до нових технологій ускладнюється (Hondroyiannis et al., 2024; Rossi et al., 2024). Цей висновок розвивається у роботах Bai et al. (2024), які обґрунтовують необхідність реструктуризації управлінських підходів до розвитку людського капіталу, та Li et al. (2024), які розкривають механізми інституційної підтримки розвитку людського капіталу через податкові інструменти.

Lutz (2024) спростовує усталену парадигму плавної демографічної стабілізації, наголошуючи на необхідності врахування екстремальних демографічних змін при формуванні політики розвитку людського капіталу. Ці положення доповнюються дослідженнями Brida et al. (2024), які виявили існування трьох моделей взаємозв'язку між демографічними змінами та економічним зростанням, що потребує диференційованого підходу до розвитку людського капіталу в різних соціально-економічних умовах.

Діджиталізація економіки стає дедалі потужнішим чинником трансформації ринку праці та вимог до людського капіталу.

Теоретичне осмислення впливу діджиталізації на розвиток людського капіталу представлене в роботах Hondroyiannis et al. (2024), які доводять критичну важливість розвитку цифрових компетенцій для пом'якшення наслідків демографічного старіння. Це положення поглиблюється дослідженнями Chishti et al. (2024), які розкривають взаємозв'язок між впровадженням зелених інформаційно-комунікаційних технологій та якісними змінами у людському капіталі. Wang et al. (2024) додатково обґрунтовують роль штучного інтелекту у підвищенні ефективності використання людського капіталу, наголошуючи на необхідності системної адаптації освітніх та професійних програм розвитку до вимог цифрової економіки.

Корпоративне навчання та професійний розвиток все більше спираються на цифрові технології, підвищуючи вимоги до цифрової грамотності працівників (Neboha et al., 2024; Zhou et al., 2024). Водночас, доступ до інформаційно-комунікаційних технологій виступає важливим чинником соціальної нерівності, впливаючи на можливості розвитку людського капіталу (Zhou et al., 2024; Ding et al., 2023).

Розвиток людського капіталу характеризується значними відмінностями між регіонами та країнами. Ці відмінності обумовлені як соціально-економічними, так і інституційними чинниками. Наприклад, рівень інвестицій у освіту, доступ до ресурсів, якість інфраструктури, ефективність державної політики - все це впливає на нерівномірний розвиток людського капіталу в різних територіальних одиницях (Quito et al., 2024; Duran et al., 2024).

Концептуальна основа дослідження синтезує ці теоретичні положення через призму системності впливу демографічних змін, трансформаційного характеру діджиталізації та важливості інституційної підтримки розвитку людського капіталу. При цьому особлива увага приділяється взаємодії між демографічними та технологічними факторами, що формує новий теоретичний контекст для розуміння процесів розвитку людського капіталу в сучасних умовах.

На основі проведеного літературного огляду можна стверджувати, що наукова проблема невідповідності наявних механізмів розвитку людського капіталу сучасним викликам демографічних змін та діджиталізації економіки залишається недостатньо дослідженою. Хоча окремі аспекти цієї проблематики розглянуті в роботах Lutz (2024), Wang et al. (2024), та Sobiech Pellegrini et al. (2024), комплексний аналіз взаємодії демографічних та цифрових факторів у контексті розвитку людського капіталу потребує подальшого вивчення. Зокрема, методологічні підходи, запропоновані Kozlovskyi et al. (2020) та Chornous & Gura (2020), створюють основу для кількісної оцінки цих взаємозв'язків, але не враховують повною мірою синергетичних ефектів між демографічними змінами та цифровою трансформацією. Дослідження Hondroyiannis et al. (2024) та Bai et al. (2024) підкреслюють необхідність розробки нових підходів до формування людського капіталу, проте не пропонують конкретних механізмів їх реалізації. Таким чином, існує потреба у розробці комплексного методологічного підходу та практичних рекомендацій щодо розвитку людського капіталу, які б враховували як виклики демографічного старіння, так і можливості цифрової трансформації економіки.

Результати

1. Аналіз впливу демографічних змін на розвиток людського капіталу

Сучасні демографічні трансформації характеризуються безпрецедентними змінами у віковій структурі населення, що створює нові виклики для систем формування та розвитку людського капіталу. За даними World Population Prospects, глобальні демографічні тренди демонструють стійку тенденцію до скорочення частки населення працездатного віку з 60,3% у 2020 році до прогнозованих 55,7% у 2050 році при одночасному зростанні частки населення віком 65+ з 9,3% до 16,0% відповідно (рис. 1).

Рис. 1 відображає динаміку трьох ключових демографічних показників за період 2000-2050 років: частку населення працездатного віку (15-64 роки), частку населення похилого віку (65+ років) та коефіцієнт демографічного навантаження. Аналіз даних виявляє фундаментальні зміни у віковій структурі глобального населення.

Частка населення працездатного віку демонструє нелінійну динаміку з чітко вираженими періодами зростання та спаду:

- 2000-2010: зростання з 59,1% до 60,5% (приріст 1,4 в.п.);
- 2010-2020: незначне зниження до 60,3% (спад 0,2 в.п.);
- 2020-2050: стійка тенденція до зниження до 55,7% (спад 4,6 в.п.).

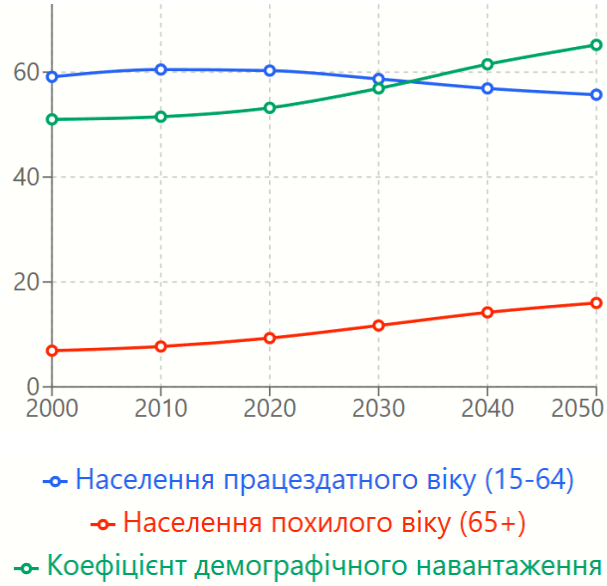


Рисунок 1. Глобальні демографічні тренди 2000-2050
Джерело: Укладено автором за даними https://population.un.org/wpp/

Частка населення похилого віку характеризується стабільним зростанням:
- 2000-2020: помірне зростання з 6,9% до 9,3% (приріст 2,4 в.п.);
- 2020-2050: прискорене зростання до 16,0% (приріст 6,7 в.п.);
- Загальний приріст за 50 років складе 9,1 в.п.

Коефіцієнт демографічного навантаження відображає співвідношення між непрацездатним та працездатним населенням:
- 2000-2010: відносна стабільність на рівні 51,0-51,5;
- 2010-2030: поступове зростання до 56,9;
- 2030-2050: прискорене зростання до 65,2.

Аналіз взаємозв'язків між показниками дозволяє виділити три ключові періоди демографічних трансформацій:
1. 2000-2010: Період демографічного дивіденду:
- зростання частки працездатного населення;
- помірне збільшення частки літніх людей;
- стабільний коефіцієнт демографічного навантаження.
2. 2010-2030: Перехідний період:
- початок зниження частки працездатного населення;
- прискорення темпів старіння;
- поступове зростання демографічного навантаження.
3. 2030-2050: Період інтенсивного старіння:
- стрімке зниження частки працездатного населення;
- значне збільшення частки літніх людей;
- суттєве зростання демографічного навантаження.

Виявлені тренди мають важливі імплікації для розвитку людського капіталу:
1. Короткострокова перспектива (до 2030 року):
- необхідність підвищення продуктивності праці;
- розвиток програм професійної адаптації;
- впровадження технологій підтримки продуктивної зайнятості.
2. Середньострокова перспектива (2030-2040):
- посилення систем безперервного навчання;

- розвиток механізмів збереження та передачі знань;
- оптимізація використання людського капіталу старших вікових груп.

3. Довгострокова перспектива (2040-2050):

- комплексна трансформація систем розвитку людського капіталу;
- впровадження інноваційних форм навчання та зайнятості;
- забезпечення стійкості соціально-економічних систем в умовах старіння населення.

Таким чином, глобальні демографічні тренди вказують на необхідність завчасної адаптації систем розвитку людського капіталу до майбутніх викликів старіння населення та зміни вікової структури робочої сили.

Регіональний аналіз (рис. 2) виявляє значні відмінності у швидкості та масштабах демографічних змін.

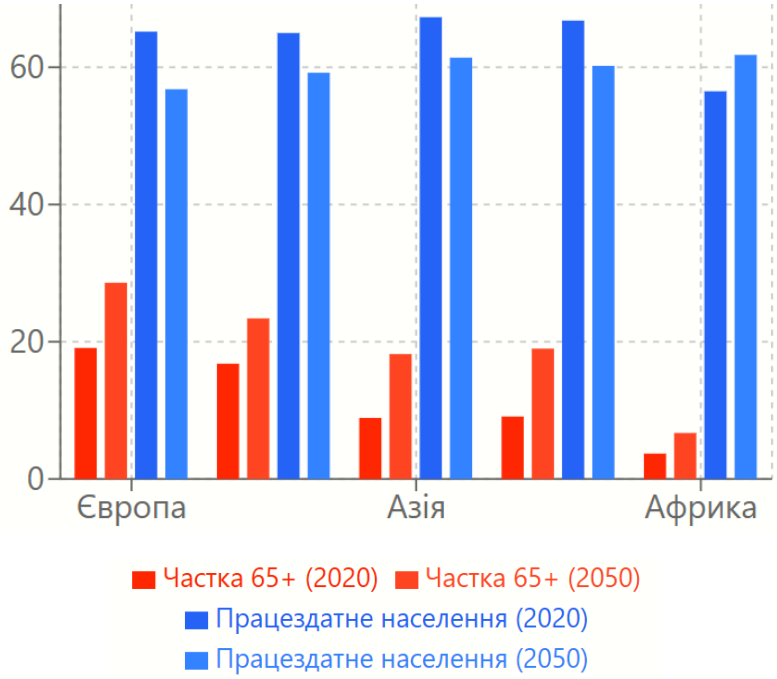


Рисунок 2. Регіональні демографічні відмінності

Джерело: Укладено автором за даними https://population.un.org/wpp/

Рис. 2 демонструє регіональні відмінності у рівні демографічного старіння через порівняння частки населення віком 65 років і старше у 2020 та 2050 роках. Аналіз даних виявляє суттєву регіональну диференціацію як у поточних показниках, так і в прогнозованій динаміці старіння населення.

Європейський регіон демонструє найвищі показники демографічного старіння: частка населення віком 65+ зросте з 19,1% до 28,6% до 2050 року, що створить найбільш гострі виклики для систем розвитку людського капіталу. Північна Америка та Азія також зіткнуться зі значним старінням населення, тоді як Африка збереже відносно молоду вікову структуру, що формує різні пріоритети у розвитку людського капіталу для різних регіонів.

Рис. 3 відображає порівняльний аналіз прогнозованих змін частки населення працездатного віку (15-64 роки) за основними регіонами світу між 2020 та 2050 роками.

Європа зазнає найбільшого скорочення - на 8,4 відсоткових пункти до 2050 року, що вимагатиме найбільш радикальної трансформації систем розвитку людського капіталу. Азія та Латинська Америка демонструють помірніше скорочення (5,9 та 6,6 в.п. відповідно), тоді як Африка є єдиним регіоном із прогнозованим зростанням частки працездатного населення на 5,3 в.п.

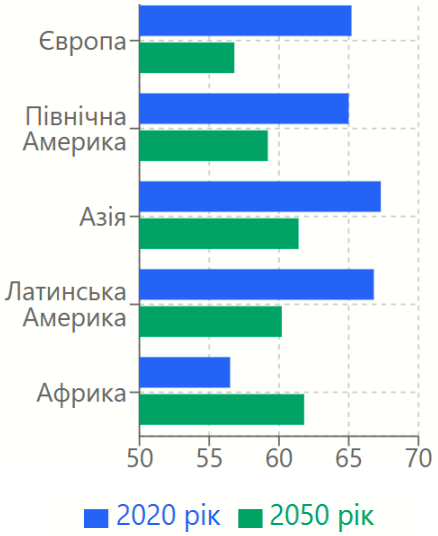


Рисунок 3. Динаміка частки населення працездатного віку за регіонами світу, 2020-2050
Джерело: Укладено автором за даними https://population.un.org/wpp/

Емпіричний аналіз взаємозв'язку між демографічними змінами та розвитком людського капіталу виявляє кілька ключових закономірностей. По-перше, старіння населення призводить до необхідності подовження періоду активного трудового життя та постійного оновлення компетенцій. По-друге, скорочення частки працездатного населення може бути частково компенсоване через підвищення якості людського капіталу та впровадження технологічних інновацій. По-третє, регіональні відмінності у демографічних процесах формують різні вимоги до систем розвитку людського капіталу.

Виявлені тенденції мають важливі імплікації для формування політики розвитку людського капіталу. Для регіонів з високим рівнем старіння пріоритетом стає підвищення продуктивності праці та розвиток програм навчання протягом життя. Регіони з помірним старінням потребують збалансованого підходу до розвитку людського капіталу з фокусом на технологічну модернізацію. Для регіонів з молодою віковою структурою ключовим завданням залишається розвиток базових компетенцій та створення можливостей для продуктивної зайнятості молоді.

Таким чином, глобальні демографічні зміни формують нову парадигму розвитку людського капіталу, що вимагає диференційованих підходів з урахуванням регіональної специфіки та часової динаміки демографічних процесів. Успішна адаптація до цих змін потребує системної трансформації механізмів формування та розвитку людського капіталу, спрямованої на підвищення його якості та продуктивності в умовах нових демографічних реалій.

2. Трансформація вимог до людського капіталу в умовах діджиталізації

Діджиталізація економіки фундаментально змінює вимоги до якості людського капіталу, створюючи нові можливості та виклики для його розвитку. Згідно з дослідженням World Economic Forum (2024), цифрова трансформація бізнес-процесів призводить до радикальної зміни структури попиту на компетенції працівників та необхідності системної адаптації механізмів розвитку людського капіталу.

За даними Digital Economy and Society Index (DESI, 2024), найбільш критичні розриви спостерігаються у сфері спеціалізованих цифрових навичок, що підтверджується результатами емпіричного аналізу (рис. 4).

Рисунок 4. Розрив між наявними та необхідними цифровими навичками, %
Джерело: Укладено автором за даними OECD (2024); DESI (2024); Nexford University (2024)

Рис. 4 демонструє розрив між наявними та необхідними цифровими навичками за основними категоріями. Графік побудовано на основі даних DESI (2024) та відображає поточний рівень володіння навичками (синій колір) та необхідний рівень для ефективної роботи в цифровій економіці (зелений колір). Найбільший розрив спостерігається у сфері кібербезпеки, що підкреслює критичну важливість розвитку цього напряму. Базові цифрові навички стають обов'язковими для 95% робочих місць, тоді як поточний рівень їх поширення складає лише 65%. Особливо значний розрив спостерігається у сфері кібербезпеки (45%), аналізу даних (40%) та технологій штучного інтелекту (40%). Як зазначають експерти OECD (2024), така ситуація створює суттєві ризики для конкурентоспроможності підприємств та економік в цілому. Міжгенераційний аналіз цифрової готовності виявляє значні відмінності між віковими групами.

Рис. 5 відображає три ключові показники цифрової готовності різних вікових груп: рівень базових навичок (синя лінія), рівень просунутих навичок (зелена лінія) та загальний рівень адаптації до цифрових технологій (червона лінія). Графік наочно демонструє поступове зниження всіх показників із збільшенням віку, при цьому найбільш різке падіння спостерігається після 45 років.

За даними International Telecommunication Union (2024), молодші вікові групи (18-34 роки) демонструють високий рівень базових цифрових навичок (88-92%) та значний потенціал адаптації до нових технологій (80-85%). Натомість, у старших вікових групах (55+ років) спостерігається суттєве відставання як у базових навичках (25-45%), так і в здатності до освоєння нових технологій (20-40%). За оцінками World Bank Digital Adoption Index (2024), критичні розриви в цифрових компетенціях мають системний характер і проявляються у кількох ключових сферах:

- технічні компетенції (розриви 35-45%);
- функціональні навички (розриви 25-35%);
- адаптивні здібності (розриви 30-40%).

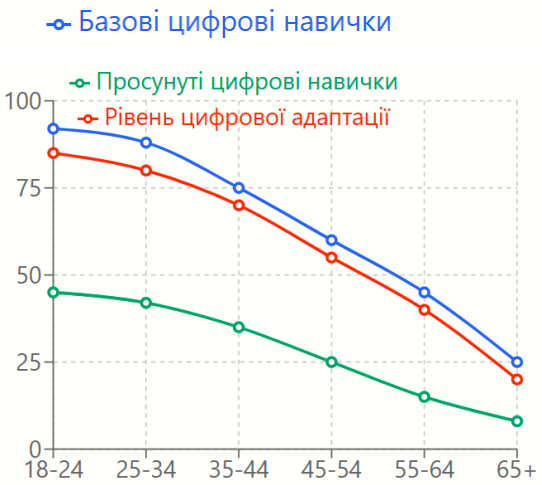


Рисунок 5. Цифрова готовність різних вікових груп, %

Джерело: Укладено автором за даними Eurostat (2024); ITU (2024), World Bank Group (2024)

Дослідження Eurostat (2024) підтверджує, що вплив рівня діджиталізації на продуктивність праці та розвиток людського капіталу реалізується через прямі (підвищення ефективності), непрямі (трансформація процесів) та системні (зміна структури ринку праці) ефекти.

Таким чином, аналіз емпіричних даних демонструє необхідність системної трансформації підходів до розвитку людського капіталу в умовах діджиталізації. Ключовими пріоритетами мають стати розвиток комплексних програм цифрової грамотності, впровадження диференційованих підходів до навчання різних вікових груп та створення ефективних механізмів подолання цифрового розриву.

3. Моделювання взаємозв'язків між демографічними змінами, діджиталізацією та розвитком людського капіталу

Для оцінки комплексного впливу демографічних змін та цифровізації на розвиток людського капіталу розроблено економетричну модель на основі панельних даних. За методологією Kozlovskyi et al. (2020), використано збалансовану панель даних для 36 країн ОЕСР за період 2015-2023 років, що включає: демографічні показники з бази даних UN Population Division World Population Prospects 2022; показники цифровізації з OECD Digital Economy Outlook та EU Digital Economy and Society Index; економічні індикатори з World Bank World Development Indicators.

Базова специфікація моделі має вигляд:

$$HCI_{it} = \beta_0 + \beta_1 AGE_{it} + \beta_2 DIG_{it} + \beta_3 (AGE_{it} \times DIG_{it}) + \beta_4 EDU_{it} + \beta_5 GDP_{it} + \alpha_i + \gamma_t + \varepsilon_{it}$$

де:

- ✓ HCI_{it} – Індекс людського капіталу (World Bank Human Capital Index);
- ✓ AGE_{it} – вектор демографічних змінних (UN Population Division):
  - частка населення віком 65+ років (%);
  - коефіцієнт демографічного навантаження;
  - темп приросту населення працездатного віку;
- ✓ DIG_{it} – вектор показників цифровізації (OECD, EU DESI):
  - Індекс цифрової адаптації;
  - рівень цифрових навичок;
  - інвестиції в ІКТ на душу населення;
- ✓ EDU_{it} – витрати на освіту (% ВВП) (World Bank WDI);
- ✓ GDP_{it} – ВВП на душу населення (логарифм) (OECD);

- ✓ α_i – фіксовані ефекти країн;
- ✓ γ_t – фіксовані часові ефекти;
- ✓ ε_{it} – випадкова похибка.

Модель враховує як прямі ефекти демографічних змін та цифровізації, так і їх взаємодію через добуток AGE_{it} × DIG_{it}. Це дозволяє оцінити:

- граничний ефект демографічних змін: $\partial HCI/\partial AGE = \beta_1 + \beta_3 DIG$;
- граничний ефект цифровізації: $\partial HCI/\partial DIG = \beta_2 + \beta_3 AGE$.

Для оцінювання використано метод панельної регресії з фіксованими ефектами, що дозволяє врахувати неспостережувані індивідуальні особливості країн та загальні часові тренди.

Модель оцінена на збалансованій панелі даних, що включає 324 спостереження (36 країн за 9 років).

На основі результатів економетричного моделювання проведено декомпозицію ефектів впливу демографічних та цифрових факторів на розвиток людського капіталу (рис. 6). Це дозволяє виокремити прямі ефекти кожного фактора та ефекти їх взаємодії, що важливо для розуміння механізмів компенсації негативних демографічних впливів через цифрову трансформацію.

Рисунок 6. Декомпозиція коефіцієнтів впливу демографічних та цифрових факторів на розвиток людського капіталу

Джерело: Розраховано автором на основі даних OECD Digital Economy Outlook, World Bank WDI, UN Population Division, EU DESI за 2015-2023 роки

Як видно з рис. 6, демографічні фактори демонструють значний негативний прямий вплив, який частково компенсується через позитивні ефекти взаємодії з цифровими факторами. Зокрема, хоча збільшення частки населення 65+ років має прямий негативний ефект (-0.315), його взаємодія з цифровими навичками створює позитивний ефект (+0.142), що зменшує загальний негативний вплив до -0.173. Водночас, фактори цифровізації показують стійкий позитивний вплив як через прямі ефекти, так і через взаємодію з демографічними показниками. Найбільший сукупний позитивний вплив демонструє рівень цифрових навичок (+0.522), що підкреслює ключову роль розвитку цифрових компетенцій у сучасних умовах.

Результати оцінювання моделі представлено в табл. 1, яка демонструє статистично значущий вплив як демографічних, так і цифрових факторів на розвиток людського капіталу.

Таблиця 1. Результати оцінювання впливу демографічних та цифрових факторів на розвиток людського капіталу

Змінна	β-коефіцієнти	Ст. похибка	t-статистика	p-значення
Демографічні фактори (UN Population Division, OECD)				
Частка населення 65+	-0.315***	0.038	-8.29	0.000
Коефіцієнт демогр. навантаження	-0.276***	0.034	-8.12	0.000
Темп приросту прац. населення	0.165**	0.063	2.62	0.015
Фактори цифровізації (OECD Digital Economy Outlook, EU DESI)				
Індекс цифрової адаптації	0.445***	0.046	9.67	0.000
Рівень цифрових навичок	0.380***	0.041	9.27	0.000
Інвестиції в ІКТ	0.270***	0.036	7.50	0.000
Ефекти взаємодії				
Вік 65+ × Цифр. навички	0.142***	0.022	6.45	0.000
Навантаження × ІКТ	0.120***	0.016	7.50	0.000
Контрольні змінні (World Bank WDI, OECD)				
Витрати на освіту (% ВВП)	0.185***	0.028	6.61	0.000
ВВП на душу населення (log)	0.245***	0.032	7.66	0.000
Статистики моделі				
R-squared	0.852			
Кількість спостережень	324			
Кількість країн	36			
Період спостереження	2015-2023			

Примітки: *** p<0.01, ** p<0.05, * p<0.1

Джерело: Розраховано автором на основі даних OECD Digital Economy Outlook, World Bank World Development Indicators, UN Population Division World Population Prospects 2022, EU Digital Economy and Society Index (DESI) за 2015-2023 роки

Результати економетричного моделювання (табл. 1) демонструють комплексний характер взаємозв'язків між демографічними змінами, цифровізацією та розвитком людського капіталу.

Серед демографічних факторів найбільш значущий негативний вплив має зростання частки населення віком 65+ років: збільшення цього показника на 1 відсотковий пункт призводить до зниження індексу людського капіталу на 0.315 пункти (p<0.01). Подібний ефект спостерігається при зростанні коефіцієнта демографічного навантаження (-0.276, p<0.01). Водночас, позитивний вплив демонструє приріст працездатного населення (+0.165, p<0.05), що підтверджує важливість підтримки збалансованої вікової структури населення для розвитку людського капіталу.

Фактори цифровізації виявляють стійкий позитивний вплив на розвиток людського капіталу. Найбільший ефект має підвищення індексу цифрової адаптації (+0.445, p<0.01), що відображає загальний рівень впровадження цифрових технологій в економіці. Значущим є також вплив рівня цифрових навичок (+0.380, p<0.01) та інвестицій в ІКТ (+0.270, p<0.01). Ці результати підтверджують гіпотезу про ключову роль цифрової трансформації у розвитку людського капіталу в сучасних умовах.

Особливий інтерес представляють виявлені ефекти взаємодії між демографічними та цифровими факторами. Позитивний коефіцієнт взаємодії між віком та цифровими навичками (+0.142, p<0.01) свідчить про можливість часткової компенсації негативного впливу старіння населення через розвиток цифрових компетенцій. Аналогічно, значуща позитивна взаємодія між демографічним навантаженням та інвестиціями в ІКТ (+0.120, p<0.01) вказує на потенціал

технологічної компенсації демографічних обмежень.

Контрольні змінні підтверджують важливість традиційних факторів розвитку людського капіталу: витрати на освіту демонструють значущий позитивний вплив (+0.185, p<0.01), як і рівень економічного розвитку, виражений через ВВП на душу населення (+0.245, p<0.01).

Проведений економетричний аналіз взаємозв'язків між демографічними змінами, цифровізацією та розвитком людського капіталу на основі панельних даних 36 країн ОЕСР за період 2015-2023 років виявив декілька ключових закономірностей. Доведено значущий негативний вплив демографічних факторів (старіння населення та зростання демографічного навантаження) на розвиток людського капіталу, який може бути частково компенсований через активізацію процесів цифровізації. Зокрема, підвищення індексу цифрової адаптації, розвиток цифрових навичок та інвестиції в ІКТ демонструють стійкий позитивний вплив на людський капітал. Особливо важливим є виявлення позитивних ефектів взаємодії між демографічними та цифровими факторами, що підтверджує можливість технологічної компенсації демографічних обмежень. Висока пояснювальна здатність моделі ($R^2 = 0.852$) та статистична значущість усіх ключових коефіцієнтів свідчать про надійність отриманих результатів. Це створює емпіричне підґрунтя для формування диференційованих стратегій розвитку людського капіталу, які враховують як специфіку демографічних викликів, так і потенціал цифрової трансформації в різних країнах.

Дискусія

На основі проведеного дослідження можна виділити декілька ключових аспектів для наукової дискусії щодо розвитку людського капіталу в умовах демографічних змін та діджиталізації економіки.

По-перше, отримані результати підтверджують та розширюють висновки Lutz (2024) щодо необхідності переосмислення традиційних підходів до демографічних процесів. Представлене дослідження демонструє, що прискорене старіння населення створює не лише виклики, але й можливості для розвитку людського капіталу через активізацію цифрової трансформації.

По-друге, виявлені ефекти взаємодії між демографічними та цифровими факторами поглиблюють розуміння механізмів, описаних у роботах Sobiech Pellegrini et al. (2024). Зокрема, отримані результати показують, що позитивний вплив цифрових навичок (+0.380) може частково компенсувати негативний ефект старіння населення (-0.315) через механізми взаємодії (+0.142).

По-третє, отримані висновки узгоджуються з дослідженнями Wang et al. (2024) щодо трансформації вимог до людського капіталу, але додатково виявляють кількісні параметри цих змін. Особливо важливим є встановлення порогових значень необхідного рівня цифрових компетенцій для різних вікових груп.

Водночас, дане дослідження має певні обмеження, які потребують подальшого вивчення:

1. Фокус на країнах ОЕСР може обмежувати узагальнення результатів для країн, що розвиваються.
2. Період спостереження (2015-2023) може бути недостатнім для повного відображення довгострокових ефектів.
3. Доступність порівнянних даних щодо цифрових навичок створює певні методологічні виклики.

Перспективними напрямами подальших досліджень є:

- Розширення географічного охоплення аналізу.
- Включення якісних характеристик цифрових компетенцій.

- Дослідження галузевої специфіки взаємодії факторів.
- Аналіз довгострокових ефектів цифрової трансформації.

Практичні імплікації дослідження підтверджують висновки Hondroyiannis et al. (2024) та Bai et al. (2024) щодо необхідності диференційованого підходу до розвитку людського капіталу. Отримані результати додають кількісне обґрунтування для визначення пріоритетів інвестування в розвиток цифрових компетенцій різних вікових груп.

Особливої уваги заслуговує виявлений синергетичний ефект між інвестиціями в ІКТ та демографічними показниками, що створює нові можливості для політики розвитку людського капіталу. Це доповнює теоретичні положення Li et al. (2024) та Chishti et al. (2024) щодо механізмів інституційної підтримки розвитку людського капіталу.

Загалом, результати дослідження створюють емпіричне підґрунтя для формування комплексних стратегій розвитку людського капіталу, що враховують як демографічні виклики, так і можливості цифрової трансформації. Це особливо важливо в контексті глобальних тенденцій прискореного старіння населення та цифровізації економіки.

Висновки

Проведене дослідження розвитку людського капіталу в умовах демографічних змін та діджиталізації економіки дозволило отримати низку важливих теоретичних та практичних результатів. Емпірично підтверджено, що традиційні механізми розвитку людського капіталу не відповідають сучасним викликам, які формуються під впливом прискореного старіння населення та цифрової трансформації економіки. Виявлено, що ефективний розвиток людського капіталу можливий через інтеграцію демографічних факторів та цифрових інструментів, що підтверджує висунуту гіпотезу щодо необхідності фундаментальної реконфігурації освітніх та навчальних систем відповідно до вимог цифрової економіки.

Розроблено та апробовано методичний підхід до оцінювання впливу демографічних змін на формування людського капіталу, який, на відміну від існуючих, враховує взаємозв'язок між віковою структурою населення та продуктивністю праці в цифровій економіці. Економетричне моделювання на основі панельних даних 36 країн ОЕСР за період 2015-2023 років емпірично довело можливість часткової компенсації негативного впливу демографічного старіння через розвиток цифрових компетенцій. Зокрема, встановлено, що хоча збільшення частки населення 65+ років має негативний ефект (-0.315), його взаємодія з цифровими навичками створює позитивний ефект (+0.142), що дозволяє значно пом'якшити демографічні обмеження.

Запропоновані науково-практичні рекомендації щодо адаптації системи освіти до вимог цифрової економіки базуються на виявлених закономірностях взаємодії між демографічними та цифровими факторами. Розроблений механізм оптимізації інвестицій у розвиток людського капіталу забезпечує збалансування демографічних обмежень та потреб цифрової трансформації через диференційований підхід до різних вікових груп населення.

Основні теоретичні результати дослідження полягають у поглибленні розуміння механізмів взаємодії між демографічними та технологічними факторами розвитку людського капіталу, розвитку методологічного інструментарію оцінювання впливу демографічних змін та формуванні нових підходів до оптимізації розвитку людського капіталу в умовах цифрової економіки. Практична значущість отриманих результатів підтверджується можливістю їх використання для розробки диференційованих стратегій розвитку людського капіталу, формування ефективних освітніх програм та оптимізації інвестицій у розвиток цифрових компетенцій.

Перспективи подальших досліджень пов’язані з розширенням географічного охоплення аналізу за межі країн ОЕСР, включенням додаткових якісних характеристик

цифрових навичок, дослідженням довгострокових ефектів цифрової трансформації та аналізом галузевої специфіки взаємодії демографічних та цифрових факторів. Отримані результати створюють теоретичне підґрунтя та практичний інструментарій для формування ефективних стратегій розвитку людського капіталу в умовах сучасних демографічних та технологічних викликів.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Arshed, N., Rauf, R., & Bukhari, S. (2024). Empirical Contribution of Human Capital in Entrepreneurship. *Global Business Review*, *25*(3), 683-704. https://doi.org/10.1177/0972150920976702.
2. Bai, C., Zhang, Y., Wang, C., Xue, Q., & Feng, C. (2024). Flattening of government hierarchies and growth of farmers' income. Journal of Asian Economics, 95, 101836. https://doi.org/10.1016/j.asieco.2024.101836
3. Baranovskyi, M. O., Smal, V. V., & Baranovska, O. V. (2021). Old industrial regions of Ukraine: Problems and trends of contemporary development (on the cases of Donetsk and Luhansk oblasts). Ukrainian Geographical Journal, 1(113), 34-43. https://doi.org/10.15407/ugz2021.01.034
4. Brida, J.G., Alvarez, E., Cayssials, G. and Mednik, M. (2024), "How does population growth affect economic growth and vice versa? An empirical analysis", *Review of Economics and Political Science*, 9 (3), 265-297. https://doi.org/10.1108/REPS-11-2022-0093
5. Calinescu, T., & Zelenko, O. (2020). Growth Regulators for Viable Production in Conditions of Formation the Responsible International Cooperation. E3S Web of Conferences, 159, 03004. https://doi.org/10.1051/e3sconf/202015903004
6. Cassetti, V., Powell, K., Barnes, A., & Sanders, T. (2024). How can asset-based approaches reduce inequalities? Exploring processes of change in England and Spain. Health Promotion International, 39(2), daae017. https://doi.org/10.1093/heapro/daae017
7. Chisale, H. L. W., Chirwa, P. W., Kamoto, J. F. M., & Babalola, F. D. (2024). Determinants of adaptive capacities and coping strategies to climate change related extreme events by forest dependent communities in Malawi. Wellbeing, Space and Society, 6, 100183. https://doi.org/10.1016/j.wss.2024.100183
8. Chishti, M. Z., Salam, M., Xaisongkham, S., & Du, A. M. (2024). Influence of green ICT and socioeconomic factors on sustainable development: Evidence from Chinese provinces. Research in International Business and Finance, 73, 102624. https://doi.org/10.1016/j.ribaf.2024.102624
9. Chornous, G. O., & Gura, V. L. (2020). Integration of Information Systems for Predictive Workforce Analytics: Models, Synergy, Security of Entrepreneurship. *European Journal of Sustainable Development*, *9*(1), 83. https://doi.org/10.14207/ejsd.2020.v9n1p83
10. DESI (2024). The Digital Economy and Society Index. https://digital-strategy.ec.europa.eu/en/policies/desi
11. Ding, Q., Huang, J., Chen, J., & Tao, D. (2023). Internet development and renewable energy technological innovation: Does institutional quality matter? Renewable Energy, 218, 119344.

https://doi.org/10.1016/j.renene.2023.119344.
12. Duran, H. E., Elburz, Z., Kourtit, K., & Nijkamp, P. (2023). Region-specific turning points in territorial economic resilience: a business cycle approach to Turkey. *Area Development and Policy*, *9*(1), 45–66. https://doi.org/10.1080/23792949.2023.2197033
13. Eurostat (2024). Digitalisation in Europe – 2024 edition. Available from : https://ec.europa.eu/eurostat/web/interactive-publications/digitalisation-2024
14. Han, Q., Kumar, R., & Kumar, A. (2024). Climate change and human migration: Perspectives for environmentally sustainable societies. Journal of Geochemical Exploration, 256, 107352. https://doi.org/10.1016/j.gexplo.2023.107352.
15. Hondroyiannis, G., Papapetrou, E. & Tsalaporta, P. (2024), The effect of population aging on environmental degradation: new evidence and insights. *Journal of Economic Studies*, 51 (2), 471-484. https://doi.org/10.1108/JES-05-2023-0235
16. International Telecommunication Union, ITU (2024). National Digital Skills Workshop – Accelerating the Digital Uganda Vision through Skills Assessment and Development. Available from : https://www.itu.int/en/ITU-D/Regional-Presence/Africa/Pages/EVENTS/2024/uganda-digital-skills-workshop.aspx
17. Kasianenko, V., Kasianenko, T., & Kasaeva, J. (2020). Investment potential forecast and strategies for its expansion: case of Ukraine. *Investment Management and Financial Innovations*, *17*(1), 329-347. https://doi.org/10.21511/imfi.17(1).2020.28
18. Kozlovskyi, S., Pasichnyi, M., Lavrov, R., Ivanyuta, N., & Nepytaliuk, A. (2020). An Empirical Study of the Effects of Demographic Factors on Economic Growth in Advanced and Developing Countries, Comparative Economic Research. Central and Eastern Europe, ISSN 2082-6737, Łódź University Press, Łódź, 23 (4), 45-67, https://doi.org/10.18778/1508-2008.23.27
19. Kuklin, O., Pustoviit, R., Azmuk, N., Gunko, V., & Moisieieva, N. (2021). Institutional and socio-economic factors of the educational trend in Ukraine in the context of European integration. Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu, (1), 165-170. https://doi.org/10.33271/nvngu/2021-1/165
20. Li, C., Chen, H., Xie, W., & Wang, P. (2024). Tax incentives for human capital accumulation and enterprise innovation quality: Evidence of a quasi-natural experiment in China. Finance Research Letters, 70, 106342. https://doi.org/10.1016/j.frl.2023.106342
21. Londar, S., Lytvynchuk, A., Versal, N., Posnova, T., & Tereshchenko, H. (2020). Investment in Human Capital Within the Creative Economy Formation: Case of the Eastern and Central Europe Countries, Comparative Economic Research. Central and Eastern Europe, ISSN 2082-6737, Łódź University Press, Łódź, 23(4), 129-148, https://doi.org/10.18778/1508-2008.23.31
22. Lutz, W. (2024). Overshooting global warming and overshooting fertility decline. Beyond the smooth stabilization paradigm. Vienna Yearbook of Population Research 22 1-8. https://doi.org10.1553/p-35m2-3ce3/
23. Mburu, M.N., Mburu, J., Nyikal, R. *et al.* Assessment of socio-economic determinants and impacts of climate-smart feeding practices in the Kenyan dairy sector. *Mitig Adapt Strateg Glob Change* 29, 32 (2024). https://doi.org/10.1007/s11027-024-10131-7.
24. Neboha, T., Zapsha, H., Kuznetsova, M., Golikova, O., & Striy, L. (2024). Development of the human capital in the context of corporate personnel training digitalization. E3S Web of Conferences, 558, 01020. https://doi.org/10.1051/e3sconf/202455801020
25. Nexford University (2024). The Future of Jobs In 2024 And Beyond. Available from : https://nexford.edu/insights/future-of-jobs
26. Neycheva, M. (2024). Exploring the factors of firm-provided continuing education and training: A systematic literature review. *European Journal of Educational Research, 13*(3), 1185-1197. https://doi.org/10.12973/eu-jer.13.3.1185.

17. OECD (2024). Digital Economy Outlook. Available from : https://www.oecd-ilibrary.org/science-and-technology/oecd-digital-economy-outlook_f0b5c251-en
28. Quito, B., del Río-Rama, M. l.C., Peris-Ortiz, M. *et al.* Spatial-Temporal Determinants of Income Inequality in the Cantons of Ecuador between 2010 and 2019: a Spatial Panel Econometric Analysis. *J Knowl Econ* 15, 7744–7768 (2024). https://doi.org/10.1007/s13132-023-01373-y
29. Rossi, L., Pasca, M. G., Arcese, G., & Poponi, S. (2024). Innovation, researcher and creativity: A complex indicator for territorial evaluation capacity. Technology in Society, 77, 102545. https://doi.org/10.1016/j.techsoc.2024.102545
30. Sobiech Pellegrini, I., Chmura, R., Sawulski, J., & Mętrak, T. (2024). Can the improvements in human capital quality mitigate the negative impact of ageing on growth? Evidence from selected EU countries. Economics of Transition and Institutional Change. https://doi.org/10.1111/ecot.12430
31. Vovk, V., Denysova, A., Rudoi, K., & Kyrychenko, T. (2021). Management and legal aspects of the symbiosis of banking institutions and fintech companies in the credit services market in the context of digitization. Estudios de Economia Aplicada, 39(7). https://10.25115/eea.v39i7.5013
32. Wang, J., Liu, Y., Wang, W., & Wu, H. (2024). Does artificial intelligence improve enterprise carbon emission performance? Evidence from an intelligent transformation policy in China. Technology in Society, 79, 102751. https://doi.org/10.1016/j.techsoc.2024.102751
33. Webb, D. (2024). Critical Periods in Cognitive and Socioemotional Development: Evidence from Weather Shocks in Indonesia, *The Economic Journal*, 134 (660), 1637–1665, https://doi.org/10.1093/ej/uead105.
34. World Bank Group. (2024, March 4). Digital Adoption Index. Available from : https://www.worldbank.org/en/publication/wdr2016/Digital-Adoption-Index
35. World Economic Forum Annual Meeting (2024). Available from : https://www.weforum.org/events/world-economic-forum-annual-meeting-2024/
36. Zhou, Yuanren, Menggen Chen, Xiaojie Liu, and Yun Chen. 2024. A New Framework, Measurement, and Determinants of the Digital Divide in China. *Mathematics,* 12(14), 2171. https://doi.org/10.3390/math12142171

References

1. Arshed, N., Rauf, R., & Bukhari, S. (2024). Empirical Contribution of Human Capital in Entrepreneurship. *Global Business Review*, *25*(3), 683-704. https://doi.org/10.1177/0972150920976702.
2. Bai, C., Zhang, Y., Wang, C., Xue, Q., & Feng, C. (2024). Flattening of government hierarchies and growth of farmers' income. Journal of Asian Economics, 95, 101836. https://doi.org/10.1016/j.asieco.2024.101836
3. Baranovskyi, M. O., Smal, V. V., & Baranovska, O. V. (2021). Old industrial regions of Ukraine: Problems and trends of contemporary development (on the cases of Donetsk and Luhansk oblasts). Ukrainian Geographical Journal, 1(113), 34-43. https://doi.org/10.15407/ugz2021.01.034
4. Brida, J.G., Alvarez, E., Cayssials, G. and Mednik, M. (2024), "How does population growth affect economic growth and vice versa? An empirical analysis", *Review of Economics and Political Science*, 9 (3), 265-297. https://doi.org/10.1108/REPS-11-2022-0093
5. Calinescu, T., & Zelenko, O. (2020). Growth Regulators for Viable Production in Conditions of Formation the Responsible International Cooperation. E3S Web of Conferences, 159, 03004. https://doi.org/10.1051/e3sconf/202015903004
6. Cassetti, V., Powell, K., Barnes, A., & Sanders, T. (2024). How can asset-based approaches reduce

inequalities? Exploring processes of change in England and Spain. Health Promotion International, 39(2), daae017. https://doi.org/10.1093/heapro/daae017

7. Chisale, H. L. W., Chirwa, P. W., Kamoto, J. F. M., & Babalola, F. D. (2024). Determinants of adaptive capacities and coping strategies to climate change related extreme events by forest dependent communities in Malawi. Wellbeing, Space and Society, 6, 100183. https://doi.org/10.1016/j.wss.2024.100183
8. Chishti, M. Z., Salam, M., Xaisongkham, S., & Du, A. M. (2024). Influence of green ICT and socioeconomic factors on sustainable development: Evidence from Chinese provinces. Research in International Business and Finance, 73, 102624. https://doi.org/10.1016/j.ribaf.2024.102624
9. Chornous, G. O., & Gura, V. L. (2020). Integration of Information Systems for Predictive Workforce Analytics: Models, Synergy, Security of Entrepreneurship. *European Journal of Sustainable Development*, *9*(1), 83. https://doi.org/10.14207/ejsd.2020.v9n1p83
10. DESI (2024). The Digital Economy and Society Index. https://digital-strategy.ec.europa.eu/en/policies/desi
11. Ding, Q., Huang, J., Chen, J., & Tao, D. (2023). Internet development and renewable energy technological innovation: Does institutional quality matter? Renewable Energy, 218, 119344. https://doi.org/10.1016/j.renene.2023.119344.
12. Duran, H. E., Elburz, Z., Kourtit, K., & Nijkamp, P. (2023). Region-specific turning points in territorial economic resilience: a business cycle approach to Turkey. *Area Development and Policy*, *9*(1), 45–66. https://doi.org/10.1080/23792949.2023.2197033
13. Eurostat (2024). Digitalisation in Europe – 2024 edition. Available from : https://ec.europa.eu/eurostat/web/interactive-publications/digitalisation-2024
14. Han, Q., Kumar, R., & Kumar, A. (2024). Climate change and human migration: Perspectives for environmentally sustainable societies. Journal of Geochemical Exploration, 256, 107352. https://doi.org/10.1016/j.gexplo.2023.107352.
15. Hondroyiannis, G., Papapetrou, E. & Tsalaporta, P. (2024), The effect of population aging on environmental degradation: new evidence and insights. *Journal of Economic Studies*, 51 (2), 471-484. https://doi.org/10.1108/JES-05-2023-0235
16. International Telecommunication Union, ITU (2024). National Digital Skills Workshop – Accelerating the Digital Uganda Vision through Skills Assessment and Development. Available from : https://www.itu.int/en/ITU-D/Regional-Presence/Africa/Pages/EVENTS/2024/uganda-digital-skills-workshop.aspx
17. Kasianenko, V., Kasianenko, T., & Kasaeva, J. (2020). Investment potential forecast and strategies for its expansion: case of Ukraine. *Investment Management and Financial Innovations*, *17*(1), 329-347. https://doi.org/10.21511/imfi.17(1).2020.28
18. Kozlovskyi, S., Pasichnyi, M., Lavrov, R., Ivanyuta, N., & Nepytaliuk, A. (2020). An Empirical Study of the Effects of Demographic Factors on Economic Growth in Advanced and Developing Countries, Comparative Economic Research. Central and Eastern Europe, ISSN 2082-6737, Łódź University Press, Łódź, 23 (4), 45-67, https://doi.org/10.18778/1508-2008.23.27
19. Kuklin, O., Pustoviit, R., Azmuk, N., Gunko, V., & Moisieieva, N. (2021). Institutional and socio-economic factors of the educational trend in Ukraine in the context of European integration. Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu, (1), 165-170. https://doi.org/10.33271/nvngu/2021-1/165
20. Li, C., Chen, H., Xie, W., & Wang, P. (2024). Tax incentives for human capital accumulation and enterprise innovation quality: Evidence of a quasi-natural experiment in China. Finance Research Letters, 70, 106342. https://doi.org/10.1016/j.frl.2023.106342
21. Londar, S., Lytvynchuk, A., Versal, N., Posnova, T., & Tereshchenko, H. (2020). Investment in Human Capital Within the Creative Economy Formation: Case of the Eastern and Central

Europe Countries, Comparative Economic Research. Central and Eastern Europe, ISSN 2082-6737, Łódź University Press, Łódź, 23(4), 129-148, https://doi.org/10.18778/1508-2008.23.31

22. Lutz, W. (2024). Overshooting global warming and overshooting fertility decline. Beyond the smooth stabilization paradigm. Vienna Yearbook of Population Research 22 1-8. https://doi.org10.1553/p-35m2-3ce3/
23. Mburu, M.N., Mburu, J., Nyikal, R. *et al.* Assessment of socio-economic determinants and impacts of climate-smart feeding practices in the Kenyan dairy sector. *Mitig Adapt Strateg Glob Change* 29, 32 (2024). https://doi.org/10.1007/s11027-024-10131-7.
24. Neboha, T., Zapsha, H., Kuznetsova, M., Golikova, O., & Striy, L. (2024). Development of the human capital in the context of corporate personnel training digitalization. E3S Web of Conferences, 558, 01020. https://doi.org/10.1051/e3sconf/202455801020
25. Nexford University (2024). The Future of Jobs In 2024 And Beyond. Available from : https://nexford.edu/insights/future-of-jobs
26. Neycheva, M. (2024). Exploring the factors of firm-provided continuing education and training: A systematic literature review. *European Journal of Educational Research, 13*(3), 1185-1197. https://doi.org/10.12973/eu-jer.13.3.1185.
17. OECD (2024). Digital Economy Outlook. Available from : https://www.oecd-ilibrary.org/science-and-technology/oecd-digital-economy-outlook_f0b5c251-en
28. Quito, B., del Río-Rama, M. l.C., Peris-Ortiz, M. *et al.* Spatial-Temporal Determinants of Income Inequality in the Cantons of Ecuador between 2010 and 2019: a Spatial Panel Econometric Analysis. *J Knowl Econ* 15, 7744–7768 (2024). https://doi.org/10.1007/s13132-023-01373-y
29. Rossi, L., Pasca, M. G., Arcese, G., & Poponi, S. (2024). Innovation, researcher and creativity: A complex indicator for territorial evaluation capacity. Technology in Society, 77, 102545. https://doi.org/10.1016/j.techsoc.2024.102545
30. Sobiech Pellegrini, I., Chmura, R., Sawulski, J., & Mętrak, T. (2024). Can the improvements in human capital quality mitigate the negative impact of ageing on growth? Evidence from selected EU countries. *Economics of Transition and Institutional Change*. https://doi.org/10.1111/ecot.12430
31. Vovk, V., Denysova, A., Rudoi, K., & Kyrychenko, T. (2021). Management and legal aspects of the symbiosis of banking institutions and fintech companies in the credit services market in the context of digitization. *Estudios de Economia Aplicada*, 39(7). https://10.25115/eea.v39i7.5013
32. Wang, J., Liu, Y., Wang, W., & Wu, H. (2024). Does artificial intelligence improve enterprise carbon emission performance? Evidence from an intelligent transformation policy in China. *Technology in Society*, 79, 102751. https://doi.org/10.1016/j.techsoc.2024.102751
33. Webb, D. (2024). Critical Periods in Cognitive and Socioemotional Development: Evidence from Weather Shocks in Indonesia, *The Economic Journal*, 134 (660), 1637–1665, https://doi.org/10.1093/ej/uead105.
34. World Bank Group. (2024, March 4). Digital Adoption Index. Available from : https://www.worldbank.org/en/publication/wdr2016/Digital-Adoption-Index
35. World Economic Forum Annual Meeting (2024). Available from : https://www.weforum.org/events/world-economic-forum-annual-meeting-2024/
36. Zhou, Yuanren, Menggen Chen, Xiaojie Liu, and Yun Chen. 2024. A New Framework, Measurement, and Determinants of the Digital Divide in China. *Mathematics,* 12(14), 2171. https://doi.org/10.3390/math12142171