The Central Research Institute
of the Armed Forces of Ukraine

# Military Science

# JOURNAL

Vol. 3 No. 2

ISSN (print): 2786-9318
ISSN (online): 2786-9326

themilitaryscience.com

The Central Research Institute
of the Armed Forces of Ukraine

# Military Science
# JOURNAL

**Vol. 3 No. 2**

ISSN (print): 2786-9318
ISSN (online): 2786-9326

themilitaryscience.com

УДК 355/359:623.09/98 (08)
DOI: 10.62524/msj.2025.3.2
ISSN (print): 2786-9318
ISSN (online): 2786-9326

**Засновник:** Центральний науково-дослідний інститут Збройних Сил України

Журнал засновано науковою радою Центрального науково-дослідного інституту Збройних Сил України, протокол № 12 від 13.12.2023 року. Внесено до Реєстру суб’єктів у сфері друкованих медіа за ідентифікатором медіа – R30-02019 (рішення Національної ради України з питань телебачення та радіомовлення від 09.11.2023 року № 1327). Внесено до Реєстру суб’єктів у сфері онлайн-медіа за ідентифікатором медіа – R40-02538 (рішення Національної ради України з питань телебачення та радіомовлення від 11.01.2024 року № 62). Включено до Переліку наукових фахових видань України (категорія “Б”) в галузях “Технічні науки”, “Військові науки”, “Економічні науки” та “Освітні науки” (накази МОН України від 26.06.2024 № 920, від 10.12.2024 № 1721 та від 24.02.2025 № 349) за спеціальностями – A1, C1, D3, F3, F5, K3, K5, K6, K7.
Видається з грудня 2023 року чотири рази на рік.

**Метою журналу** є висвітлення результатів наукових пошуків дослідників з актуальних військово-теоретичних, військово-спеціальних, воєнно-економічних питань, а також питань забезпечення національної безпеки держави.

**Науковий профіль видання:**
A1 – Освітні науки;
C1 – Економіка;
D3 – Менеджмент;
F3 – Комп’ютерні науки;
F5 – Кібербезпека та захист інформації;
K3 – Національна безпека (за окремими сферами забезпечення і видами діяльності);
K5 – Військове управління (за видами збройних сил);
K6 – Забезпечення військ (сил);
K7 – Озброєння та військова техніка.

Рекомендовано до друку науковою радою ЦНДІ ЗС України
(протокол № 6 від 25.06.2025 року)

**Адреса редакції:**
проспект Повітряних Сил, 28Б
03049, Київ, Україна

**Телефон:**
+38 (044) 520-19-44

**E-mail:**
ms. journal@post.mil.gov.ua

**Інформаційний сайт:**
themilitaryscience.com

**Журнал індексується агентствами:** Crossref, Google Scholar, OUCI, Scilit, OCLC, Національна бібліотека України імені В. І. Вернадського.

Редакція може не поділяти точку зору авторів.
Відповідальність за зміст поданих матеріалів несуть автори.

© ЦНДІ ЗС України, 2025

**РЕДАКЦІЙНА КОЛЕГІЯ**

**Голова редколегії:** Семененко О. заслужений діяч науки і техніки України; д-р військ. наук, проф.

**Заступник голови редколегії:** Дейнега О. д-р військ. наук, проф.

**Члени редколегії:**

| | |
|---|---|
| Абрамова М. | канд. екон. наук, ст. наук. співроб. |
| Антипенко Н. | д-р екон. наук, проф. |
| Бєлкова Т. | канд. пед. наук |
| Білейшіс М. | PhD, Prof. Dr. (Литовська Республіка) |
| Біляковська О. | д-р пед. наук, проф. |
| Богданович В. | заслужений діяч науки і техніки України, д-р техн. наук, проф. |
| Божидай І. | канд. екон. наук, доц. |
| Волобуєв А. | д-р техн. наук, ст. наук. співроб. |
| Волошин О. | канд. пед. наук, доц. |
| Годзь С. | д-р військ. наук, ст. дослід. |
| Гончарук В. | канд. пед. наук, доц. |
| Грищук Р. | заслужений діяч науки і техніки України, д-р техн. наук, проф. |
| Гусак Ю. | д-р військ. наук, проф. |
| Дєнєжкін М. | д-р військ. наук, проф. |
| Дибкова Л. | д-р пед. наук, проф. |
| Дудзевічюте Г. | PhD, Assoc. Prof. Dr. (Литовська Республіка) |
| Закусило П. | д-р військ. наук, проф. |
| Залужний В. | доктор філософії |
| Залуцька Х. | д-р екон. наук, проф. |
| Зелінська Г. | д-р екон. наук, проф. |
| Канцір І. | канд. екон. наук, доц. |
| Квасній Л. | канд. екон. наук, доц. |
| Керіган-Киру Д. | BA, PhD (Республіка Ірландія) |
| Кірсанов С. | д-р техн. наук, ст. наук. співроб. |
| Клят Ю. | канд. техн. наук, доц. |
| Коваль В. | канд. військ. наук, ст. наук. співроб. |
| Лисенко О. | заслужений діяч науки і техніки України, д-р техн. наук, проф. |
| Македон В. | д-р екон. наук, проф. |
| Марко І. | заслужений економіст України, д-р екон. наук, проф. |
| Машкін О. | д-р техн. наук, ст. наук. співроб. |
| Мірненко В. | заслужений працівник освіти України, д-р техн. наук, проф. |
| Павловський О. | д-р військ. наук, проф. |
| Потетюєва М. | д-р екон. наук, доц. |
| Потьомкін М. | д-р техн. наук, проф. |
| Соломицький О. | д-р військ. наук, ст. наук. співроб. |
| Телелим В. | заслужений діяч науки і техніки України, д-р військ. наук, проф. |
| Ткач І. | заслужений економіст України, д-р екон. наук, проф. |
| Ткач М. | д-р екон. наук, проф. |
| Ходаківський В. | канд. екон. наук, доц. |
| Хомчак Р. | д-р військ. наук, ст. дослід. |
| Чепурна М. | канд. пед. наук, доц. |
| Шевчук Л. | д-р пед. наук, проф. |
| Шулигіна Р. | канд. пед. наук, доц. |

**Відповідальний редактор:** Васянович М., канд. військ. наук, ст. дослід.

**Технічний редактор:** Возняк І., канд. пед. наук, доц.

# Contents

Syrskyi O., Lebedenko A., Semenenko O.
**Ukraine in a "War of Attrition": The Warfare Paradigm Shift** ..... 6

Гнатов А., Шевченко О., Семененко О., Соломицький О., Бусель В.
**Рекомендації щодо порядку укладання перемир'я (мирної угоди) під час збройного конфлікту: український досвід** ..... 20

Клят Ю., Нечаєв О., Клименко В.
**Сутність та переваги децентралізованого управління в об'єднаних операціях НАТО** ..... 32

Козачук В., Мовчан О., Гром В., Водчиць О., Тарасов О.
**Сучасні будівельні матеріали для термінового відновлення твердих аеродромних покриттів** ..... 46

Гризо А., Костиря О., Трофимов І.
**російсько-українська війна як каталізатор змін у європейській системі ППО-ПРО: від американської підтримки до стратегічної автономії** ..... 56

Barhylevych A.
**Developing Recommendations for Improving the Efficiency of Personnel Manning in the Armed Forces of Ukraine** ..... 78

Шевченко О., Семененко О., Закусило П., Харченко В., Мусієнко В., Мельничук О.
**Щодо оптимізації управління озброєнням у військах (силах)** ..... 87

Павлюк О., Дідіченко В., Череп В., Возняк С., Ремез А.
**Аналіз ризиків під час обґрунтування вимог до спроможностей складу військ (сил)** ..... 99

Didichenko V., Cherep V., Tolok P., Horhulenko V., Yarmolchyk M.
**Defence Management Issues in Ukraine: The Economic Aspect** ..... 123

Horbatiuk V., Horhulenko V., Horhulenko V., Dobrovolskyi Y., Samsonenko M.
**Recommendations on the Implementation of Defence Planning Measures for Acquiring and Developing Capabilities by the Prospective Cyber Forces of the Armed Forces of Ukraine Based on the DOTMLPFI** ..... 137

Kushnir O., Semenenko L.
**Situational conditions at the state border as a factor influencing the staffing of border guard units' headquarters with managerial personnel** ..... 151

Соломатін Д., Седляр А., Пасічник В., Луцевят О., Слюсаренко М., Ільницький С.
**Високоточне авіаційне озброєння класу "повітря – поверхня" провідних країн: стан і тенденції розвитку** ..... 162

Komarov V., Baranov S., Grazion D.
**The Post- War Development Strategy of Ukraine: Assessment of the Global Security Environment** ..... 174

Гаврилюк І.
**Аналіз наявних підходів до оцінювання та прогнозування рівня воєнно-економічної безпеки держави: закордонний та вітчизняний досвід** ..... 186

Зварич С., Хомчак Р., Зварич А., Коркіна Н.
**Кібертехнології та математичне моделювання для пришвидшення петлі Джона Бойда в асиметричній війні** ..... 201

Мельниченко А.
**Аналіз та оцінка факторів, які впливають на ефективність застосування беспілотних систем в операціях (бойових діях)** ..... 210

Семененко О., Гурковський В., Романенко Є., Вербовенко О., Митченко С.
**Обороноздатність держави: організаційно-правові аспекти підготовки громадян до національного спротиву** ..... 226

Кінь О.
**Аналіз теорії і практики розвитку когнітивних загроз у сфері воєнної безпеки: шляхи подолання** ..... 240

Леоненко О., Ремез В., Гетьман А., Мельничук Ю., Смілянський О., Пятова Ю.
**Обґрунтування змісту етапів і заходів та розроблення пропозицій щодо раціонального вибору системи захисту інформації під час створення інформаційно-комунікаційних систем** ..... 261

Войцеховський Р.
**Аналіз та оцінювання впливу факторів на вимоги до системи управління оперативного угруповання військ в операціях (бойових діях): досвід російсько-української війни** ..... 271

The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 3 No. 2 (2025)

DOI: 10.62524/msj.2025.3.2.1

# Ukraine in a "War of Attrition": The Warfare Paradigm Shift

**Oleksandr Syrskyi**
Candidate of Military Sciences
Commander-in-Chief of the Armed Forces of Ukraine
03168, Povitrianykh Syl Avenue, 6, Kyiv, Ukraine
e-mail: sirsk_os@ukr.net
ORCID: 0000-0001-6396-7559

**Andrii Lebedenko**
Deputy Commander-in-Chief of the Armed Forces of Ukraine
Office of the Commander-in-Chief of the Armed Forces of Ukraine
03168, Povitrianykh Syl avenue, 6, Kyiv, Ukraine
e-mail: a.lebedenko@mil.ua
ORCID: 0009-0002-3332-1591

**Oleh Semenenko**
Honoured Science and Technology Figure of Ukraine
Doctor of Military Sciences, Professor
Honored Worker of Science and Technology of Ukraine
Deputy Chief of the Central Research Institute of the Armed Forces of Ukraine
for Scientific Work
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl Avenue, 28 B, Kyiv, Ukraine
e-mail: aosemenenko@ukr.net
ORCID: 0000-0001-6477-3414

"*The experience shows that it is not victories that teach a nation, but rather defeats that most often become sources of reflection capable of leading a leader and people onto a new victorious path…*"
*Oleh Semenenko*

*The "war of attrition" – is a catastrophe for both sides. Firstly – it means constant losses of personnel and civilian population; secondly – it results in the destruction of infrastructure and irreversible consequences for the economy and the environment; thirdly – it is a deadlock that bleeds both countries involved in the conflict and becomes the first step towards their decline for many years. Yet if a peace agreement is impossible, then for the country losing territory – such a path is better than capitulation…*

**Abstract.** The contemporary war launched by the russian federation against Ukraine demonstrates a fundamental change in the nature of armed confrontation. This conflict is gradually moving beyond classical conceptions of war as a set of active combat actions, frontline clashes, and rapid operations. Instead, Ukraine has encountered a phenomenon that exhibits all the features of a so-called "war of attrition" – a protracted, gradual, fragmented yet systemic confrontation that causes destructive impact not only on the frontline but also in the rear, in the information space, economy,

energy sector, international diplomacy, and in the public consciousness. Therefore, the main aim of the article is to explore “war of attrition” as a phenomenon and to introduce this concept into scientific, strategic, and public discourse, as it reflects the new realities of Ukraine’s military experience that no longer fit within traditional frameworks. The main results of the article are as follows: an analysis of the military confrontation in the context of the russian-Ukrainian war is conducted in order to examine the phenomenon of a slow, incremental advance that lacks a clearly defined frontline breakthrough but is instead characterised by months-long pressure and attrition of the enemy; a conceptual and terminological justification and a definition of the philosophical concept of “war of attrition” are provided; the main principles of conducting a “war of attrition” are defined; the main characteristics of “war of attrition” are outlined; the periods of transformation of the russian-Ukrainian war into a “war of attrition” are established; possible projected consequences of “war of attrition” for russia and Ukraine are identified; the system of external and internal factors that may push russia to shift from “war of attrition” to active operations is revealed; numerical indicators of “war of attrition” based on the russian-Ukrainian experience are defined; and the foundations of the Concept of “war of attrition” are elaborated using the russian-Ukrainian conflict as an example. The materials of the article may be useful to military theorists and practitioners involved in developing strategies for contemporary warfare; security and defence analysts studying the transformation of armed conflicts; researchers in the field of the philosophy of war, military history, and international relations; as well as policymakers and military leaders who shape defence policy and military doctrines.

**Keywords:** hybrid war, military operations, military security, armed struggle, philosophy of war, military strategy, politico-military logic, strategic thinking, military leadership, technologies of war, tactics and strategy of military operations, cyber weapons, “war of attrition”, national security, global stability, methods of warfare, transformation of the armed conflicts, set of indicators (characteristics) of the “war of attrition”, forms of the armed conflict, forms of the military operations.

## Introduction

The contemporary war unleashed by the russian federation against Ukraine demonstrates a fundamental change in the nature of armed confrontation [1–5]. This conflict is gradually going beyond the classical understanding of war as a set of active combat operations, front-line clashes, and swift campaigns. Instead, Ukraine is facing a phenomenon that bears all the hallmarks of the so-called “war of attrition” – a protracted, gradual, fragmented, yet systemic confrontation that exerts a destructive impact not only on the front lines but also in the rear, in the information domain, the economy, energy sector, international diplomacy, and within the consciousness of society [1–12].

The term “war of attrition” is necessary for an adequate description of this phenomenon, as it more accurately than classical categories captures its main features: the uneven pace of combat operations, situational intensification in specific directions, informational and psychological pressure, energy and logistical blackmail, and a prolonged, exhausting campaign aimed at gradually undermining the national resilience of the adversary. The nominal “stability” of the front conceals a constant and intense struggle unfolding across multiple domains, and changes in the front line are no longer the sole measure of success or defeat.

The introduction of this term is not only conceptually justified but also philosophically grounded, as it enables a rethinking of war as a prolonged process with altered logic of time, space, and action. “War of attrition” is not merely a method, but a state. It blurs the line between peace and war, dissolves the front into the depths of the rear, stretches the notion of the beginning and end of conflict. Such a war demands not so much heroic breakthroughs, but intellectual, moral, technological, and mental resilience. It is a new paradigm in which victory lies not only in seizing positions, but in preserving will, integrity, and the capacity to adapt and evolve.

Thus, the necessity to study "war of attrition" as a phenomenon and to introduce this concept into academic, strategic, and public discourse is driven by the new realities of Ukraine's wartime experience, which do not fit within traditional frameworks. This opens up prospects for rethinking military strategy, updating defence doctrine, adapting social psychology, and shaping a new culture of resilience in response to the challenges of the 21st century.

**Materials and Methods**

In contemporary analysis of military confrontation, particularly in the context of the russo-Ukrainian war, increasing attention is being paid to the phenomenon of a slow, gradual advance that lacks a clearly defined front-line breakthrough but is instead characterised by months-long pressure and attrition of the adversary [1–21].

American military analyst Austin Bay, in his columns, refers to this phenomenon as a "creeping war of aggression" or a "creeping offensive", using these terms to describe the annexation of Crimea in 2014 and the subsequent escalation of the conflict in Donbas. The Institute for the Study of War (ISW) also consistently records "creeping offensive" or "creeping advances" as a characteristic strategy of russian forces – namely, slow, "millimetre-by-millimetre" advances aimed at tactical pressure and demoralisation.

At the same time, this term has not yet been established in Ukrainian academic discourse. None of the authoritative scholarly sources provides a definition of "war of attrition", which gives reason to consider the term "war of attrition" as authorial. Its meaning is not only purely military but also deeply philosophical and requires corresponding reflection. In particular, the following conceptual definitions are possible:

"slow erosion of the adversary" – a war waged through the gradual exhaustion of the adversary's will, resources, and mental resilience without large-scale assaults, relying on multidimensional strategies of ideological, economic, and hybrid pressure;

"temporally-processual conflict" – a form of warfare that exists as a protracted socio-political process in time, where the clear boundary between war and peace, front and rear, the beginning and end of combat operations disappears;

"hybrid-philosophical experience" – a metaphysical condition of society in a state of prolonged uncertainty, where war becomes a constant backdrop to existence, in which the civilian and the military coexist in a "bizarre entanglement".

The phenomenon of "war of attrition" as a contemporary form of armed conflict—manifested in a prolonged, gradual, and multidimensional offensive without an official declaration of war or full-scale offensive operations—still lacks a recognised scientific definition and thorough theoretical reflection in both Ukrainian and international discourse. The formulation of such concepts as "slow erosion of the adversary," "temporally procedural conflict," and "hybrid-philosophical experience" allows for a perception of war not merely as a set of combat actions, but as a condition of societal existence, a tool of systemic exhaustion of the adversary, and a long-term process of blurring the boundaries between war and peace.

Under the conditions of the russian-Ukrainian war, this form of confrontation has become a reality that requires a new theoretical toolkit for analysis, forecasting, and the development of an adequate national resistance strategy. Therefore, the theoretical study of "war of attrition" is relevant not only for military science, but also for philosophy, political science, and security studies.

**Results**

"War of attrition" is a strategy of prolonged, gradual offensive that combines local combat operations, information and psychological pressure, economic exhaustion, and hybrid aggression with the aim of undermining Ukraine's resilience as a state without declaring a general assault or launching total mobilisation.

This phenomenon integrates the concept of a "creeping offensive," as documented by analysts from the Institute for the Study of War (ISW), who describe it as a systematic, "millimetre-by-millimetre" advance of russian forces — "creeping advances." At the same time, it encompasses key elements of hybrid warfare according to the "Gerasimov doctrine," primarily the influence on public consciousness, the use of non-military means of warfare, information terror, and the erosion of the moral resilience of the civilian population.

In this context, "war of attrition" captures a new paradigm of contemporary conflict, within which russia abandons the strategy of a blitzkrieg in favour of a prolonged, multi-vector and multi-layered attack—a state of chronic hybrid aggression in which the line between war and peace, front and rear, civilian and military is blurred.

The advantages of using the term "war of attrition" are evident:

- the term clearly conveys the nature of the current confrontation — multi-level, fragmented, without a classical front or large-scale invasion;
- its conceptual strength lies in highlighting the philosophical essence of the conflict — war as a protracted, chronic condition, where "peace" is merely the illusion of a pause;
- the analytical value of the term is that it enables a systematic description of the kremlin's strategy, which is based not on rapid breakthroughs, but on the slow attrition of the adversary — militarily, mentally, economically, and socially.

That is, the term "war of attrition" is new, but timely and necessary for the contemporary military-political and academic discourse.

The philosophical concept of this term shows that "war of attrition" is perceived as a state, a process, a metaphysical presence in daily life, but the core understanding of the term is determined by the Ukrainian context—specifically, it describes russia's new strategy against Ukraine, which is based on technologies of slow displacement, attrition, and hybrid aggression that combines classical and non-classical methods of warfare.

The main principles of conducting a "war of attrition" are:

- gradual advancement without a frontal breakthrough – territorial gains or pressure are applied step by step, without a large-scale offensive, through constant probing for weak spots;
- maintaining ambiguity and controlling intensity – the intensity of hostilities fluctuates in waves, making it impossible to clearly predict phases of escalation or "ceasefire";
- multi-dimensional impact (war on all fronts) – warfare is conducted not only physically, but also across the following domains: the information domain (disinformation, psychological operations), the energy domain (attacks on infrastructure), cyberspace, and the diplomatic arena (toxic international pressure);
- attrition rather than destruction – the objective is not the rapid elimination of the enemy, but the gradual weakening of their defence capability, economy, morale, and societal resilience;
- blurring the line between peace and war – there is no clearly defined frontline; the "war" appears to be ongoing, yet it is not officially declared, nor is it universally recognised as such (a hybrid and legitimised war);
- adaptability of tactics and scenarios – that is, the constant alteration of methods of action, forms of influence, and the manoeuvring of resources and tempo.

Table 1 describes the characteristics of a "war of attrition", that is, it defines the features that distinguish it from other types of war and from war in general. In particular, these include: the gradual, protracted, and barely perceptible nature of changes along the frontline; the absence of large-scale offensive operations; the dominance of attrition tactics; the extensive use of asymmetric actions; as well as its psychological impact on both society and the military, which leads to fatigue, a decline in mobilisation enthusiasm, and an adaptation to a protracted conflict as a "new normal" in the conduct of hostilities.

**Table 1.** Characteristics of a "war of attrition" (key distinctions)

| Characteristic | "War of attrition" | Traditional war |
|---|---|---|
| Pace | Uneven, wave-like, protracted | High-intensity, staged |
| The front and rear boundary | Blurred, conditional | Clearly defined |
| Attack form | Partial offensives, psychological operations, drone attacks, terrorist acts, shelling | Large-scale combat clashes, artillery shelling, manoeuvre battles |
| Objective | Exhaustion, undermining resilience, psychological effect | Destruction or capitulation of the enemy |
| Tools | UAVs, cruise missiles, cyber weapons, psychological operations | Tanks, artillery, aviation, ground forces |
| Operation area | Entire territory of the state, rear, information domain | Primarily the combat zone |
| Legal status | May remain undeclared (hybrid) | Officially recognised war |

The main types of weapons that contributed to the formation of a "war of attrition" within the russian-Ukrainian war include:

1. UAVs (unmanned aerial vehicles), which make it possible to conduct targeted, periodic strikes deep into the territory of the country without declaring an offensive.

2. Medium-range precision missiles, which make it possible to carry out pinpoint strikes on infrastructure from deep within the territory.

3. Cyberweapons and information technologies, namely: DDoS attacks, cyber espionage, phishing, blocking critical infrastructure facilities, operations based on open-source intelligence (OSINT).

4. EW systems and anti-drone technologies, which suppress control or conduct electronic warfare on the frontline and in the rear.

5. Mine warfare and remote mining, namely remote mining systems that make advancement impossible by creating "traps" without direct contact.

"War of attrition" is not merely a military strategy, but a new type of protracted conflict, in which the primary objective is to exhaust, demoralise, and internally weaken the adversary through a multi-layered assault — on the frontline, in the rear, within public consciousness, and in the global perception. Its emergence became possible due to the technological evolution of warfare (UAVs, EW, precision weapons), while its development was enabled by the blurring of the traditional logic of "war–peace".

Let us outline the main periods of transformation of the russian-Ukrainian war into a "war of attrition", clearly identifying the stages of the transition from a traditional to a protracted, multi-layered conflict of a new type.

Main periods of the transformation of the russian-Ukrainian war into a "war of attrition".

1. February strike and blitz containment (February – April 2022). The character of the war during this period: high-intensity, manoeuvre, classical war, that is, a war of full-scale invasion. The aim of the russian federation during this period was a blitzkrieg, a change of the political regime in Ukraine. During this period, the front was advancing rapidly, the attacks had a large-scale character, that is, the war did not yet have signs of being "creeping".

2. Stabilisation of the front and transition to positional warfare (May – October 2022). The character of the war during this period: the beginning of the transition to a "creeping" form, that is, the front stabilises in key directions (Donbas, South). The war enters a phase of attritional artillery fighting with constant counter-battery combat, and unmanned systems are actively developing. The main signs of "creeping" include: local offensives with small forces; assault actions; parallel use of unmanned systems, mortars, artillery; changing pace of hostilities and the beginning of the first phase

of protraction. During this period, the first features of a "war of attrition" are formed, namely: fragmentation, attrition, attacks on the rear and so on.

3. Mass attacks on the energy sector and critical infrastructure (October 2022 – March 2023). The character of the war during this period: the war moves beyond the line of contact (the front); russia launches systematic missile strikes on energy facilities; for the first time, Shahed-type UAVs are used and so on. The main signs of "creeping" during this period include: the beginning of energy blackmail; strikes deep inside Ukraine (Kyiv, Lviv, Vinnytsia); an attempt to create psychological fatigue in the population. The war becomes multi-dimensional, that is, this is the key moment of transition into a "war of attrition".

4. Operational stagnation and wave-like attacks (April – December 2023). The character of the war during this period: positional stagnation on the front; reduction of large-scale manoeuvres; instead, growth of local battles (Avdiivka, Bakhmut); russia changes its tactics to "creeping offensives" – 100–200 metres per week. The main signs of "creeping" during this period include: mass use of FPV drones, constant attacks on logistics, railways, ports, hydroelectric power stations, grain elevators. "War of attrition" becomes the dominant form of combat operations.

5. Systemic asymmetric phase of war (2024–2025 and ongoing). The character of the war: attritional phase, with a multi-layered strategy by russia, namely: pressure on the front; strikes on the rear; information campaigns. Ukraine switches to a regime of resource economy, asymmetry, innovation. The main signs of "creeping" during this period include: mass use of UAVs and FPVs as the main strike asset, no linear offensive, only so-called "nibbling" of positions, intensification of the elements of "war for the mind" (attacks on civilians, elections, black PR). "war of attrition" has become russia's strategy to exhaust Ukraine's statehood as a system.

The russian-Ukrainian war gradually transitioned into a "creeping" phase, with its culmination in 2022–2023 and the final consolidation of this type of conflict in 2024. This is not merely an adaptation to losses, but a deliberate strategy by the russian federation aimed at protracted pressure without major breakthroughs, yet with the accumulation of destructive effect.

We shall conduct a comparative analysis of the independent, potentially foreseeable consequences of the "war of attrition" for russia and Ukraine, focusing on political, military, social, and civilisational outcomes. This takes into account that a "war of attrition" is not a blitz-type conflict but a prolonged confrontation with multiple levels — from drones and deep strikes to impacts on the economy and identity.

Possible foreseeable consequences of the "war of attrition" for russia:

- military attrition under the illusion of progress, as the constant "gnawing" at new positions creates an impression of advancement but yields no strategic breakthrough. The military burden continues to grow, with increasing losses in personnel and equipment, alongside the gradual degradation of mobilisation resources;
- systemic internal exhaustion, marked by budget depletion due to prolonged war financing, escalating issues in healthcare, education, and regional governance, and the formation of a "war-dependent" economy functioning solely to sustain the conflict (military socialism);
- isolation and loss of international influence, as even without a formal defeat, russia is degrading as a major geopolitical actor — losing its grip over the post-Soviet space, while NATO, Turkey, and China strengthen their positions relative to the russian federation;
- moral and civilisational degradation, driven by a total immersion in the cult of war as a norm, and by the historical branding of russia as an aggressor.

A "war of attrition" will not lead to victory, but it may leave the russian federation as an isolationist, authoritarian state locked in a state of chronic "military stability".

Possible foreseeable consequences of the "war of attrition" for Ukraine:

- a rethinking of the nature of statehood, as under conditions of prolonged exhaustion, the very idea of the state transforms — from a "consumer state" to a "warrior state," where security, technology, self-organisation, and horizontal structures form the core;
- strengthening of asymmetric advantages: if Ukraine does not win a "grand battle," it may prevail in "a thousand small ones" through technologies (UAVs, AI, EW), digital defence, resilient democracy, and an ability to adapt faster than the russian federation;
- endurance as a new strength, since under "war of attrition" conditions, Ukraine builds national endurance — cultural, psychological, institutional. This makes a russian victory fundamentally impossible, as russia will not be able to break Ukrainian identity — even occupation would not guarantee control;
- a shift in global role, as the world gradually recognises that Ukraine is not only a victim of aggression but also a laboratory of new warfare, a model for Europe's future security. The experience of "war of attrition" shapes Ukraine as a post-heroic nation, where victory means to survive, to hold the line, to fight innovatively, and not to vanish.

If we consider the philosophical dilemma — who will prevail in a "creeping" war? — it may be said that russia seeks ultimate control, while Ukraine fights for endless resistance. Victory will not go to the one who occupies more ground, but to the one who can endure perpetual tension and remain true to themselves. A potential victory in a "creeping" war for russia is tactical advancement and holding parts of territory, while its potential "defeat" is a strategic loss of the future, isolation, and degradation.

For Ukraine, victory means survival, preservation of the nation, adaptation, and recognition by the world, while defeat would mean exhaustion, demographic losses, a resource crisis, and territorial loss — with the worst-case scenario being the loss of statehood. Despite the actual implementation of the "war of attrition" strategy, russia continuously nurtures hopes of returning to an active, large-scale offensive phase.

The main drivers behind the russian federation's desire to return to an active phase of the war are:

*1. The military-political logic of the regime.* The political regime in russia operates under the logic of "victory or death." A "war of attrition" does not generate a victorious narrative for the domestic audience. Without a "great victory," the Kremlin cannot legitimise the sacrifices, repressions, and militarisation of life.

*2. Psychological incompatibility with positional warfare.* russian strategic culture is based on dominance and offensive action, not on defence and patience. Strategically, russia is not prepared to exist in a "no man's war." putin's leadership believes that war must end with the "signing of a capitulation," not with a stabilised frontline.

*3. A tool for pressuring the West.* Active operations offer a new opportunity for ultimatum-based blackmail of the West through the threat of escalation. A return to full-scale war allows russia to dictate political terms, undermine Western unity, and fuel "Ukraine fatigue."

*4. Fear of strategic exhaustion.* A "war of attrition" is a war of endurance, which russia may ultimately lose due to technological degradation, reduction in the quality of personnel, and increasing economic, political, and other forms of isolation.

That is, an active operation is perceived as an attempt to break the current situation while the russian federation still has resources and while there remains a certain instability in the course of support for Ukraine in its struggle for freedom.

Let us outline the system of external and internal factors that may prompt russia to shift from a "creeping" war to active operations.

The main internal factors (within the russian federation) include:

- the political need for victory, as in the face of new domestic challenges (elections, social tensions), the Kremlin may use a large-scale offensive to mobilise the population and generate a sense

of “national uplift” in order to reduce war fatigue and define a horizon for its end, thus easing the restrictions that the war currently imposes on russian society;

- military lobbying, that is, the military leadership may push for an “offensive scenario” as a means of rehabilitating itself after the defeats of 2022–2024;
- growing chaos within the army, as under conditions of positional attrition, military ferment may arise both at the tactical and strategic levels, with generals seeking initiative through active operations.

The main external factors include:

- weakening of Western support for Ukraine, meaning that delays in aid or political shifts in the United States or the EU (e.g. Trump, right-wing parties) could offer russia a window of opportunity for a breakthrough;
- global crises, as if international attention is diverted (e.g. Taiwan, the Middle East, internal EU crises), russia may seize the moment to launch a large-scale offensive;
- successes of local offensives, as a tactical breakthrough on a specific section of the front (for example, in Kharkiv region or Donbas) could trigger the escalation of full-scale hostilities.

The conducted analysis demonstrates that russia does not perceive the “war of attrition” as a desirable state of the present, as it is forced to conduct it due to its inability to achieve a full-scale victory. Its strategic goal is to break out of the deadlock and resume assault—through the frontline, diplomacy, or information escalation—but it requires political, military, and economic support, which it is currently actively seeking by various means.

The West and Ukraine must clearly understand today that the “war of attrition” is only one phase of a protracted war, the end of which is not yet in sight, because russia never abandons the idea of a “great revanche” or a “Pyrrhic victory,” at least for its own population, in order to justify the consequences of the war both domestically and internationally.

Let us attempt to quantitatively characterise the phenomenon of the “war of attrition” using the example of the russian-Ukrainian conflict (Table 2) by identifying key numerical indicators that reflect the “creeping” nature of the war.

We shall outline the core meaning of the indicators that reflect the nature of the “war of attrition”.

The core essence of the indicators of the “war of attrition” – characteristics of protractedness, slowness, and attrition through repetitive actions rather than through strategic breakthroughs.

The presented set of indicators illustrates that military effect is measured not by cities, but by positions, trenches, forest strips, and metres. This is a war of resource survival, endurance, and adaptation rather than of rapid victories.

Let us outline the foundations of the “war of attrition” Concept based on the example of the russian-Ukrainian conflict, formulated as an analytical and philosophical generalisation of a new type of conflict under the conditions of the 21st century:

The “war of attrition” concept: the Ukrainian dimension.

*A “war of attrition”* – is a new form of armed confrontation characterised by a multi-level, prolonged, and gradual nature of hostilities and by its impact on the opposing state through a set of hybrid means: military, informational, economic, political, and psychological. It has no clearly defined beginning or predictable end, and its main goal is the exhaustion of resources, the will to resist, and the destruction of the internal cohesion of the target state.

*The concept involves revealing the main distinctive features of a “war of attrition”,* namely:

- the blurring of boundaries between war and peace (no formal declaration of war, periodic statements about negotiations or “freezing” the conflict);
- a shift in the frontline paradigm, meaning that the war is conducted both along the line of contact and in the rear – in the form of terror, drone attacks, explosions, and sabotage;

- attrition rather than seizure, that is, the aim is not territorial control but the demoralisation of the enemy;
- steady, slow aggression without a clear peak or turning point;
- a dominance of technology and manipulation over the mass use of force.

**Table 2.** Numerical characteristics (indicators) of the "war of attrition" based on the russian-Ukrainian experience

| Indicator | Typical Value / Range | Explanation |
|---|---|---|
| 1. Tempo of frontline advancement | 50–300 metres per week (in active sectors) | Indicates an extremely slow pace of combat operations, without decisive breakthroughs. For example: russian advancement near Avdiivka in 2023–2024. |
| 2. Number of artillery/mortar strikes per km²/day | 200–1,000+ rounds per day on specific sections of the front | Typical of positional pressure without a shift to manoeuvre warfare. |
| 3. Share of unmanned strikes in total fire damage | 40–70% (as of 2024–2025) | The shift to remote strikes is the foundation of the "war of attrition". |
| 4. Average casualty rate of both sides (per day) | 600–1,000 personnel per day in total (killed / wounded on both sides) | Large-scale losses without decisive changes on the combat map. This is typical of exhausting "creeping" phases of war. |
| 5. Percentage of days with active combat operations during the year | 85–95% | Constant combat activity without a defined "offensive" or "ceasefire" phase. |
| 6. Number of attacks by unmanned systems on rear infrastructure (per month) | 100–300+ attacks | Part of an asymmetric war of attrition that has become the norm. |
| 7. Distance the frontline shifts in 6 months | 1–5 km of total advance along specific directions | Compared to classical offensives – this is a war "for tree lines", not for strategic centres. |
| 8. Percentage of mobilised personnel within the forces (compared to regular troops) | 50–70% in russian armed Forces, 40–60% in Ukrainian Armed Forces | "War of attrition" requires constant replenishment of manpower, which is a sign of a protracted conflict. |
| 9. Dynamics of combat losses per 1 km of frontline (annual indicator) | 2,000–5,000 personnel/km/year (in the hottest sectors) | One of the highest loss rates in wars since World War II – without strategic outcome. |
| 10. Share of battles for small settlements (up to 5,000 residents) | 80–90% of all offensive actions | "War of attrition" is focused on local battles rather than assaults on cities or regions. |

*The main weapons of a "war of attrition"* (as seen in the russian-Ukrainian war example) are:

- FPV drones, UAVs, and kamikaze drones (used daily on a massive scale in tactical mode), as well as long-range unmanned strike systems (for strategic attacks);
- "minimal advancement" artillery, meaning the destruction of fortifications followed by the occupation of positions within a few hundred metres;
- EW systems, cyberattacks, and operations in the electromagnetic spectrum;
- mass fake narratives and disinformation campaigns (including through media and social networks);
- gas and energy weapons (especially in 2022).

The stages of the formation of "war of attrition" in the russian-Ukrainian conflict within the framework of the Concept are outlined in Table 3.

*The goals of the "war of attrition" of the russian federation against Ukraine are:* to exhaust material and human resources; to demoralise the civilian population (through drone terror and shelling); to weaken European and American support for Ukraine; to destabilise political stability; to delay time until a more favourable international situation.

**Table 3.** Stages in the formation of the "war of attrition" in the russian-Ukrainian conflict within the framework of the Concept

| Period | Stage | Characteristic |
|---|---|---|
| 2014–2015 | Hybrid infiltration | Annexation of Crimea, appearance of "little green men", war in Donbas |
| 2016–2021 | Latent continuation of the war | Creation of pseudo-states, periodic shelling, diplomatic pressure |
| 2022 (February – June) | Open phase, blitzkrieg | Mass invasion by the russian federation, attempt at rapid seizure of Kyiv |
| from summer 2022 – to present | Transition to the "war of attrition" | War of attrition, positional fighting, drone warfare, gradual advances, destruction of critical infrastructure |

*Forecast of the "war of attrition" consequences.*

For Ukraine: if the resilience of the state is maintained – it is a chance for stabilisation and accumulation of advantage; if fatigue from the war occurs – it is a risk of gradual loss of control over the situation.

For the russian federation: if the tempo of the war is maintained – there is a possibility of sustaining pressure; if the war is excessively prolonged – it is a threat of internal explosion due to exhaustion.

*The role of the "war of attrition" Concept for analysis and strategy.* Understanding the "war of attrition" makes it possible to:

- adapt military strategy to the mode of "war of attrition";
- strengthen the internal resilience of the state;
- develop flexible, asymmetric responses;
- shift the narrative from "offensive-betrayal" to "management of prolonged struggle".

**Recommendations**

Understanding the essence of the "war of attrition", its goals, indicators, and consequences makes it possible to preliminarily formulate a number of recommendations for Ukraine regarding actions under the conditions of the ongoing "war of attrition", which may help to achieve a positive outcome in the long term, namely:

1. To create the conditions for constant strengthening of defensive resilience and the application of a strategy of positional flexibility. To develop deep multi-layered defence with maximum use of natural and artificial fortifications. To create opportunities for rapid deployment of mobile reserves in order to enable local counteroffensives and rapid regrouping in case of changes in the situation. It is necessary to constantly update the tactics of positional warfare through the use of contemporary innovative technologies (UAVs, EW, ESM, etc.).

2. To increase the intensity of the use of unmanned systems and long-range strike technologies against the enemy. To continue the development and implementation of UAVs for reconnaissance, fire correction, and precision strikes. It is necessary to focus on low-cost, high-precision enemy destruction systems that reduce risks for personnel, as well as on the development of networked fire control systems with rapid data exchange.

3. To pay attention to the support and development of human potential. To constantly adapt the system of mobilisation, training, and rotation of personnel in order to avoid burnout and preserve the functionality of human capital. To actively develop systems of psychological support, rehabilitation, and training of military specialists, as well as to implement measures for involving the public and volunteer movements in meeting the needs of the military (the needs of the front).

4. Strengthen intelligence and counterintelligence by employing both technical and human resources to timely detect threats and enemy manoeuvres. Work actively in the field of cybersecurity and the protection of the information space. Apply "hybrid" intelligence methods, including human assets, cyber intelligence, and open-source intelligence.

5. Create conditions for the economic and infrastructural resilience of the state by protecting critical infrastructure from strikes (energy, transport, communications), developing alternative supply routes and ensuring rapid restoration of damaged facilities, as well as supporting the wartime economy, including through the attraction of international assistance.

6. Continuously conduct active information and psychological warfare by fostering national unity, raising morale, countering enemy disinformation and propaganda, and maintaining international solidarity through effective informational influence.

7. Constantly seek and exploit opportunities for local counteroffensives by enabling conditions for surprise strikes and the de-occupation of territories at favourable moments, maintaining initiative where possible in order to force the enemy to expend resources, and ensuring flexible logistics and support for such operations.

8. Given the current situation and actions of russia, Ukraine must prepare for a protracted war by developing a strategic plan for the next 3–5 years, taking into account resource-related, social and technological challenges; continuing to develop its defence-industrial complex and scientific research to maintain technological superiority over the adversary; and establishing a system of continuous modernisation of armaments and combat tactics.

The Ukrainian experience shows that a "war of attrition" is a marathon, not a sprint. Ukraine must adopt a comprehensive approach that combines defensive endurance, technological innovation, human capital, and informational resilience. Only systemic and consistent efforts in all these areas will make it possible not only to withstand the "creeping" pressure but also to achieve strategic advantage in the long term.

**Conclusion**

The analysis of the concept of "war of attrition" in the context of the ongoing russian-Ukrainian conflict reveals significant shifts in the paradigm of warfare, reflecting the transformation of traditional military approaches towards a prolonged, gradual, and covert confrontation. The introduction of this term enables a deeper understanding of the nature of the current confrontation, which combines elements of hybrid warfare, informational pressure, economic constraints, and continuous local military actions.

The philosophical aspect of "war of attrition" presents it as a form of struggle that does not aim for a swift resolution but focuses on the gradual attrition of the enemy while simultaneously maintaining or expanding control over territories.

For Ukraine, understanding and adapting to the challenges of "war of attrition" is essential for ensuring long-term national security, upholding sovereignty, and preserving territorial integrity. A comprehensive strategy that integrates technological innovation, enhanced defence, information operations, and socio-psychological resilience can provide a pathway to a positive outcome in this prolonged confrontation.

Key prospects for further research within the scope of the article include:

- in-depth exploration of tactical and strategic models of "war of attrition" using examples from both contemporary and historical conflicts;
- development of a methodology for quantitative assessment of the effectiveness of countermeasures against "creeping war," taking into account technological, informational, and social factors;
- analysis of the role of unmanned systems, cyber operations, and information warfare as integral "war of attrition" components in the context of future military conflicts;

- examination of the impact of "war of attrition" on the civilian population, economy, and the psychological state of society, along with the development of recommendations to minimise negative consequences;
- integration of philosophical concepts and military theory to form new doctrines and strategies in response to the transformation of warfare under the conditions of "creeping" conflicts.

Overall, the topic of "war of attrition" remains highly relevant and promising for interdisciplinary research, which can contribute to a deeper understanding of contemporary challenges and to the development of effective tools for addressing them.

**Acknowledgments**

The authors declare that they have no competing interests related to the subject of the article.

**References**

1. Lytvyn, V. M. (2020). *War and peace in the context of new security challenges: The Ukrainian dimension. Strategic Priorities, 1* (54), 5–13.
2. Hoffman, F. G. (2007). *Conflict in the 21st century: The rise of hybrid wars*. Potomac Institute for Policy Studies.
3. Freedman, L. (2017). *The future of war: A history*. PublicAffairs.
4. Kaldor, M. (2012). *New and old wars: Organized violence in a global era*. (3rd ed.). Polity Press.
5. *russia's military campaign assessments, 2022–2024*. Institute for the Study of War. https://www.understandingwar.org.
6. Kulinich, O. V. (2023). *Creeping war as a new paradigm of modern military conflicts. Bulletin of Military Science of Ukraine, 12*, 45–59.
7. Tarasenko, M. V. (2022). *The transformation of war in the 21st century: New challenges and features. Military Journal, 7*, 22–35.
8. Petrov, I. I. (2024). *The russian-Ukrainian war: Stages, characteristics, and prospects*. Alterpress.
9. Smith, J. (2023). *The evolution of hybrid warfare: From conventional battles to creeping conflict*. *Journal of Strategic Studies, 46* (3), 301–325.
10. Boiko, A. S. (2024). *Unmanned systems as a tool of conducting a creeping war*. *Defense Technologies, 9* (1), 12–28.
11. Honcharenko, V. I. (2023). *Low-intensity war: Conceptual approaches and practice*. *Military Thought, 4*, 88–101.
12. Cohen, E., & Gagnon, J. (2024). *russia's incremental war in Ukraine: Implications for global security*. *Security Review Quarterly, 11* (2), 58–74.
13. Ivanov, D. (2022). *Creeping war and hybrid threats: Challenges for modern defense. International Defense Studies, 15* (4), 145–162.
14. Ivanenko, S. V. (2023). *Information war in the conditions of a creeping conflict*. *Journal of Information Security, 15*, 44–59.
15. Kozak, P. M. (2022). *Psychological aspects of conducting prolonged military conflicts*. *Military Psychology, 3*, 15–27.
16. Vlasenko, T. O. (2024). *Modernization of Ukraine's defense strategy in response to a creeping war*. *Strategic Studies, 10* (1), 5–20.
17. Kofman, M., & Bugos, S. (2023). *Lessons from russia's war in Ukraine: The nature of contemporary conflict*. *War on the Rocks.* https://warontherocks.com/2023/04/lessons-from-russias-war-in-ukraine/
18. Hoffman, F. G. (2021). *Hybrid warfare and challenges. Joint Force Quarterly, 100*, 34–40.

19. Johnson, R. (2022). *Creeping conflict: Understanding the gradual escalation in modern wars. Strategic Review, 14* (2), 89–107.
20. Gorka, S. (2018). *Understanding russia's new generation warfare. Small Wars Journal*. https://smallwarsjournal.com/jrnl/art/understanding-russias-new-generation-warfare
21. Hoffman, F. (2023). *The contemporary strategic environment and the rise of the creeping war. Parameters, 53* (1), 5–21.

## Україна в умовах "повзучої війни": зміна парадигми ведення воєнних дій

**Олександр Сирський**
кандидат військових наук
Головнокомандувач Збройних Сил України
03168, проспект Повітряних Сил, 6, Київ, Україна
e-mail: sirsk_os@ukr.net
ORCID: 0000-0001-6396-7559

**Андрій Лебеденко**
заступник Головнокомандувача Збройних Сил України
Апарат Головнокомандувача Збройних Сил України
03168, проспект Повітряних Сил, 6, Київ, Україна
e-mail: a.lebedenko@mil.ua
ORCID: 0009-0002-3332-1591

**Олег Семененко**
заслужений діяч науки і техніки України
доктор військових наук, професор
заступник начальника Центрального науково-дослідного інституту
Збройних Сил України з наукової роботи
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: aosemenenko@ukr.net
ORCID: 0000-0001-6477-3414

"*Досвід показує, що націю навчають не перемоги, а найчастіше програші стають джерелами думок, які спроможні вивести лідера та народ на новий переможний шлях…*"
*Олег Семененко*

*"Повзуча війна" – є катастрофою для обох сторін. По-перше – це постійні втрати особового складу та цивільного населення; по-друге – це знищення інфраструктури та безповоротні наслідки для економіки й екології; по-третє – це патова ситуація, яка знекровлює обидві країни учасників конфлікту та є першим кроком до їхнього занепаду на довгі роки. Але якщо мирна угода неможлива, тоді для країни, яка втрачає території, – такий шлях краще, ніж капітуляція…*

**Анотація.** Сучасна війна, розв'язана російською федерацією проти України, демонструє докорінну зміну характеру збройного протистояння. Цей конфлікт поступово виходить за межі

класичних уявлень про війну як про сукупність активних бойових дій, фронтових зіткнень і швидких операцій. Натомість Україна стикнулася з явищем, що має всі ознаки так званої “повзучої війни” – затяжного, поступового, фрагментарного, але системного протистояння, яке несе руйнівний вплив як на фронті, так і в тилу, в інформаційному просторі, економіці, енергетиці, міжнародній дипломатії та в свідомості суспільства. Отже, головною метою статті є дослідження “повзучої війни” як феномену та впровадження цього поняття в науковий, стратегічний і суспільний дискурс, що зумовлено новими реаліями українського воєнного досвіду, який не вкладається в традиційні рамки. Основними результатами статті є те, що в ній: проведено аналіз воєнного протистояння в контексті російсько-української війни для дослідження феномену повільного, поступового наступу, що не має чітко окресленого фронтового прориву, але натомість характеризується багатомісячним тиском і виснаженням супротивника; здійснено понятійно-термінологічне обґрунтування та визначення філософського концепту “повзуча війна”; визначено основні принципи ведення “повзучої війни”; визначено основні **х**арактеристики “повзучої війни”; сформовано періоди трансформації російсько-української війни у “повзучу війну”; визначено можливі прогнозовані наслідки “повзучої війн” для росії та України; розкрито систему зовнішніх та внутрішніх факторів, які можуть спонукати росію до переходу від “повзучої” війни до активних дій; визначено числові характеристики (показники) “повзучої війни” на основі російсько-українського досвіду; розкрито основи Концепції “повзучої війни” на прикладі російсько-українського конфлікту. Матеріали статті можуть бути корисними військовим теоретикам та практикам, які займаються розробленням стратегій сучасного ведення війни; аналітикам у сфері безпеки та оборони, які досліджують трансформацію збройних конфліктів; дослідникам у галузі формування філософії війни, військової історії та міжнародних відносин; політикам і військовим керівникам, які формують оборонну політику та військові доктрини.

**Ключові слова:** гібридна війна, воєнні дії, воєнна безпека, збройна боротьба, філософія війни, військова стратегія, воєнно-політична логіка, стратегічне мислення, воєнне лідерство, технології війни, тактика та стратегія воєнних дій, кіберзброя, “повзуча війна”, національна безпека, глобальна стабільність, методи ведення війни, трансформація збройних конфліктів, сукупність показників (характеристик) “повзучої війни”, форми збройного конфлікту, форми воєнних дій.

The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 3 No. 2 (2025)

DOI: 10.62524/msj.2025.3.2.2

# Рекомендації щодо порядку укладання перемир'я (мирної угоди) під час збройного конфлікту: український досвід

**Андрій Гнатов**
начальник Генерального штабу Збройних Сил України
Генеральний штаб Збройних Сил України
03186, проспект Повітряних Сил, 6, Київ, Україна
e-mail: gnatovav@ukr.net
ORCID: 0009-0000-9557-942x

**Олексій Шевченко**
кандидат історичних наук
заступник начальника Генерального штабу Збройних Сил України
Генеральний штаб Збройних Сил України
03168, проспект Повітряних Сил, 6, Київ, Україна
e-mail: shevchenko_om@asv.gov.ua
ORCID: 0000-0003-0734-6533

**Олег Семененко**
заслужений діяч науки і техніки України
доктор військових наук, професор
заступник начальника Центрального науково-дослідного інституту
Збройних Сил України з наукової роботи
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: aosemenenko@ukr.net
ORCID: 0000-0001-6477-3414

**Олексій Соломицький**
доктор військових наук, старший науковий співробітник
начальник відділу – заступник начальника управління
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: solosa1@gmail.com
ORCID:0000-0001-8061-8895

**Віталій Бусель**
начальник Центрального управління оборонних ресурсів
Генеральний штаб Збройних Сил України
03049, проспект Повітряних Сил України, 6, Київ, Україна
e-mail: Busel77vitalii@gmail.com
ORCID: 0009-0004-3043-9695

**Анотація.** Тривала збройна агресія російської федерації проти України поставила перед Україною виклики, які виходять за межі суто військового протистояння. Виснаження ресурсів, гуманітарні кризи, міжнародний тиск та очікування суспільства формують об'єктивну потребу

в обґрунтуванні та структуруванні підходів до укладання перемир'я або мирної угоди. У цьому контексті постає необхідність створення чітких, науково обґрунтованих рекомендацій щодо поетапного процесу переходу від активної фази бойових дій до стійкого миру. Стаття має особливу актуальність, оскільки інтегрує національний досвід, міжнародне гуманітарне право та практики мирного врегулювання інших збройних конфліктів, формуючи практичну "дорожню карту" дій для українських суб'єктів безпекової політики.

Метою публікації є розроблення рекомендацій щодо порядку укладання перемир'я (мирної угоди) під час збройного конфлікту, враховуючи світовий та український досвід.

Під час підготовки статті застосовано комплексний методологічний підхід. Використано методи системного аналізу, порівняльно-правового аналізу, історичного узагальнення та індуктивної логіки. Значну роль відіграли аналіз міжнародних нормативно-правових документів, практичних прикладів мирних угод, а також оцінка сучасної воєнно-політичної ситуації в Україні.

У статті визначено та розмежовано поняття "перемир'я" та "мирна угода" у контексті міжнародного права. Розкрито їхню правову природу, механізми укладення, ключові параметри, а також проаналізовано можливі ризики та переваги кожного з інструментів у сучасних умовах. Автори запропонували структурований 12-етапний алгоритм укладання перемир'я або мирної угоди. Особлива увага приділяється ролі міжнародних посередників, безпекових гарантій, а також механізмів моніторингу виконання угоди. Представлено інституціональні, військові та політичні рішення, які можуть бути адаптовані залежно від розвитку ситуації.

Результати дослідження можуть бути корисними для військових, урядовців, дипломатів, аналітиків, дослідників у сфері міжнародного права, а також для міжнародних організацій, які залучені до процесу врегулювання збройних конфліктів. Стаття має практичне значення для розроблення офіційних позицій України у мирних перемовинах, створення нормативно-правової бази для імплементації домовленостей, забезпечення безпеки на деокупованих територіях та інтеграції України до міжнародних безпекових структур.

Ухвалення такої поетапної стратегії дозволить Україні уникнути імпровізацій у критичний момент ухвалення рішень і гарантувати як власну безпеку, так і стійкий постконфліктний розвиток.

**Ключові слова:** перемир'я, мирна угода, міжнародне гуманітарне право, збройний конфлікт, безпекові гарантії, алгоритм укладання миру

**Вступ (Introduction)**

Збройна агресія російської федерації (рф) проти України, що триває з 2014 року та перейшла у фазу широкомасштабної війни 24 лютого 2022 року, кардинально змінила не лише безпекову ситуацію в регіоні, а й глобальні підходи до врегулювання збройних конфліктів у XXI столітті. Війна завдала Україні глибоких гуманітарних, соціальних, економічних і політичних втрат. Сотні тисяч загиблих і поранених, мільйони внутрішньо переміщених осіб, зруйнована інфраструктура, мінлива підтримка міжнародної спільноти, а також виснаження ресурсного потенціалу – все це створює передумови для переосмислення засобів та механізмів досягнення стійкого миру.

Ситуація на фронті характеризується стабільно високою напруженістю з обмеженими успіхами наступальних операцій, що, у поєднанні зі стратегічним вичерпанням, спонукає обидві сторони та міжнародних посередників до розгляду можливості застосування політико-дипломатичних інструментів. У такому контексті важливого значення набуває розроблення національної стратегії укладання перемир'я або мирної угоди, яка б поєднувала воєнно-стратегічну доцільність, міжнародно-правову легітимність та гуманітарну необхідність.

У світовій практиці укладення перемир'я та мирних угод є інструментами завершення або заморожування конфліктів різної інтенсивності. Однак кожен випадок має унікальний контекст, що визначає зміст і структуру домовленостей. З огляду на особливості російсько-української війни, ключовим викликом для української держави є створення власного алгоритму мирного врегулювання, який не тільки не суперечитиме національним інтересам, а й забезпечуватиме збереження суверенітету, територіальної цілісності та довгострокової безпеки.

У зв'язку із цим актуальним є створення комплексних рекомендацій, що враховують міжнародні правові норми, історичний та сучасний досвід укладання перемир'їв, а також українські реалії та перспективи післявоєнного відновлення. Особлива увага у статті приділена чіткій поетапній логіці укладання перемир'я або мирної угоди, із зазначенням відповідних органів, механізмів реалізації, ролі Збройних Сил України (ЗС України), а також міжнародних партнерів.

Мета цієї статті – представити узагальнену, практично орієнтовану модель укладання мирних домовленостей, яка може бути використана Україною у разі створення відповідного політичного і воєнного контексту для переходу до миру. Запропонований алгоритм має стати основою для стратегічного планування дій в умовах гібридної війни, де дипломатичні, воєнні та правові інструменти мають працювати синхронно, забезпечуючи досягнення стійкого миру та зміцнення національної безпеки.

**Огляд літератури (Literature review)**

Проблематика укладання перемир'їв та мирних угод в умовах збройного конфлікту висвітлюється в численних міжнародних, правових, політичних та військово-аналітичних джерелах. У контексті російсько-української війни ця тематика набуває особливої актуальності, оскільки поєднує завдання правового врегулювання, військової безпеки та постконфліктної трансформації держави.

Ключову роль у формуванні нормативно-правового підґрунтя для врегулювання збройних конфліктів відіграють документи міжнародного гуманітарного права, насамперед Женевські конвенції та Додаткові протоколи до них [1], які визначають базові правові рамки для захисту цивільного населення та ведення бойових дій. Вони є основою при визначенні правових меж для укладання перемир'їв, гуманітарних пауз і припинення вогню. Гаазька конвенція [2] також розглядається як нормативна база, що визначає механізми укладання тимчасових угод між сторонами конфлікту.

З погляду практичного досвіду, важливими орієнтирами для аналізу є перемир'я в Корейській війні [3], яке зберігає чинність і досі, незважаючи на юридично не завершений стан війни, та Дейтонська мирна угода [4], яка продемонструвала ефективність складного багатостороннього переговорного процесу під егідою міжнародних посередників. Обидва приклади ілюструють різні моделі припинення конфліктів: тимчасову зупинку бойових дій без політичного врегулювання та повне міжнародно-правове завершення війни відповідно.

Особливе значення для України мають Мінський протокол [5] та Комплекс заходів з його реалізації [6], що стали основою спроб деескалації на Донбасі. Проте їхня часткова реалізація та відсутність чітких гарантій безпеки вказують на слабкість політико-воєнних компромісів без ефективного контролю та взаємної відповідальності сторін.

Окремо слід виділити "Guidance for Effective Mediation" [7], який систематизує принципи ефективного посередництва у конфліктах, включаючи прозорість, інклюзивність, узгодженість цілей та забезпечення легітимності домовленостей. Цей документ має високу практичну цінність для формування переговорної позиції України та архітектури майбутнього мирного процесу.

Практична значущість проблеми також розкривається в публікаціях НАТО та ОБСЄ

щодо гібридних загроз, стратегічних комунікацій та миротворчих процесів – зокрема, “Hybrid Threats: A Strategic Communications Perspective” [8] та “Handbook on OSCE Peace Processes” [9], які містять практичні інструменти для проєктування структур перемовин і постконфліктної стабілізації.

Окремі аспекти укладання перемир’я / мирних угод розглядаються у [11–21].

Таким чином, аналіз літератури засвідчує, що міжнародний і національний досвід мирного врегулювання конфліктів формує багатокомпонентну методологічну та правову базу для розроблення української моделі укладання перемир’я чи мирної угоди. Проте вказані джерела потребують адаптації до сучасної геополітичної ситуації та особливостей російсько-української війни, що й обґрунтовує необхідність подальших міждисциплінарних досліджень.

**Методологічна основа (Methodological Framework)**

Дослідження проблематики укладання перемир’я або мирної угоди під час збройного конфлікту вимагає міждисциплінарного підходу, що поєднує військову науку, міжнародне право, політологію, історію та стратегічні комунікації. У цьому контексті було застосовано комплекс методів, які дозволили здійснити системний аналіз теоретичних засад, практичних прикладів і нормативно-правового регулювання процесу мирного врегулювання в умовах збройного протистояння.

По-перше, системний аналіз дозволив структурувати різні рівні процесу укладання перемир’я або мирної угоди – від політичного рішення до військової імплементації та безпекової стабілізації. Цей підхід дав змогу побудувати логічно послідовну модель дій, що охоплює як стратегічні, так і тактичні компоненти.

По-друге, застосовувався порівняльно-правовий аналіз, який передбачав вивчення юридичних аспектів перемир’їв і мирних угод у міжнародній практиці (на прикладі Корейського перемир’я, Дейтонської мирної угоди, Мінських домовленостей тощо) з метою виявлення релевантних елементів, які можуть бути адаптовані до українського контексту. Аналіз також охоплював відповідність пропонованих механізмів нормам міжнародного гуманітарного права та Віденської конвенції про право міжнародних договорів.

По-третє, було використано історико-ретроспективний метод, який дав змогу простежити еволюцію підходів до мирного врегулювання в Україні та інших країнах, що пережили збройні конфлікти, – зокрема, у Південному Судані, Боснії і Герцеговині, Іраку, Афганістані. Історичний досвід допоміг окреслити критичні помилки та фактори успіху під час укладання угод.

Крім того, важливу роль відіграв контент-аналіз нормативно-правових актів, стратегічних документів ЗС України, міжнародних угод, а також публікацій науковців і експертів у сфері безпеки та оборони. Це дало можливість верифікувати висновки дослідження на основі реальних даних та оцінок, а також забезпечити актуальність напрацьованих рекомендацій.

Окремо застосовувався метод експертного оцінювання, у тому числі через залучення авторського досвіду у військовому управлінні та стратегічному плануванні. Це дозволило не лише теоретично обґрунтувати алгоритм укладання перемир’я / мирної угоди, а й запропонувати практичні моделі для органів влади, ЗС України та міжнародних партнерів.

Отже, методологічна основа статті забезпечила міждисциплінарний, об’єктивний та практично орієнтований підхід до розроблення рекомендацій щодо мирного врегулювання збройного конфлікту на основі українського досвіду та міжнародних практик.

**Результати (Results)**

Визначимо сутність та відмінності понять “перемир’я” і “мирна угода” у системі міжнародного гуманітарного права.

*Перемир'я (armistice)* – офіційна домовленість між сторонами збройного конфлікту про тимчасове припинення бойових дій. Воно не означає завершення війни як такої, але створює передумови для деескалації, гуманітарної паузи, ведення переговорів або укладення подальшої мирної угоди [2].

До основних ключових ознак перемир'я належать:

тимчасовий або безстроковий характер;

найчастіше укладається військовими або політичними представниками сторін;

може бути досягнуте за посередництва третьої сторони або міжнародної організації;

визначає лінії розмежування, механізми контролю за дотриманням режиму тиші тощо.

Юридичний статус полягає в тому, що перемир'я:

не припиняє стан війни;

може бути порушене будь-якою стороною, якщо не має міжнародних гарантій. Приклади: перемир'я в Корейській війні (1953) досі чинне, але війна офіційно не завершена [3]; Мінські домовленості (2014–2015) – типове політико-військове перемир'я з елементами мирної угоди, яке не виконано [5–6].

*Мирна угода (peace agreement)* – офіційний міжнародно-правовий документ, який формально припиняє стан війни та врегульовує політичні, безпекові, територіальні та правові наслідки збройного конфлікту [2].

До основних ключових ознак мирної угоди належать:

має комплексний характер і включає безпекові, гуманітарні, політичні та інституційні положення;

зазвичай підписується на вищому державному рівні;

найчастіше укладається за посередництва міжнародних партнерів чи організацій (ООН, ЄС, США тощо);

передбачає створення механізмів реалізації угоди та міжнародного нагляду.

Юридичний статус полягає в тому, що мирна угода припиняє стан війни, має зобов'язуючий характер, часто реєструється в ООН.

Приклади: Дейтонська мирна угода (1995), яка припинила війну в Боснії і Герцеговині [4]; комплексна мирна угода в Південному Судані (2005), яка заклала основу нової державності [10].

Таким чином, головними відмінностями між перемир'ям та мирною угодою є те, що:

*Перемир'я* – це тактична або оперативна пауза, не завершує війну юридично.

*Мирна угода* – це стратегічне врегулювання, що формально і юридично припиняє війну.

Основні практичні особливості укладення перемир'я або мирної угоди під час збройного конфлікту між протиборчими сторонами наведено у табл. 1.

У сучасних умовах затяжної російсько-української війни питання щодо досягнення перемир'я або укладення мирної угоди набуває особливої актуальності як з гуманітарного, так і з безпекового погляду. Поступове виснаження ресурсів, загроза дестабілізації внутрішньополітичної ситуації, ризики ескалації на інших напрямках, а також очікування з боку міжнародних партнерів створюють передумови для розгляду сценарію тимчасового або постійного припинення бойових дій. Разом із тим, сам процес укладення перемир'я або мирної угоди має бути чітко структурованим, з урахуванням українських національних інтересів, принципів міжнародного гуманітарного права, а також досвіду інших країн, що проходили подібні етапи постконфліктного переходу.

На основі аналізу нормативних документів та світового досвіду автори пропонують поетапну логіку дій України, що охоплює підготовку до перемовин, підписання угод, імплементацію положень домовленостей, стабілізацію ситуації на звільнених або спірних територіях та адаптацію функціонування Збройних Сил України до нової реальності.

**Таблиця 1.** Практичні особливості укладення перемир'я або мирної угоди під час збройного конфлікту

| Параметр | Перемир'я | Мирна угода |
|---|---|---|
| Сутність | Тимчасове припинення бойових дій | Комплексне політичне врегулювання конфлікту |
| Характер | Воєнно-технічний, тактичний | Геополітичний, юридично-міжнародний |
| Мета | Зниження інтенсивності бойових дій | Завершення конфлікту, відновлення миру |
| Правовий статус | Тимчасова домовленість, часто без міжнародних гарантій | Міжнародно-правовий документ, може реєструватися в ООН |
| Зміст | Припинення вогню, лінії розмежування, зони контролю | Визначення територій, безпекових гарантій, відшкодування, умов миру |
| Термін дії | Тимчасовий (від днів до років) | Безстроковий (або до перегляду умов сторонами) |

Основні етапи алгоритму укладення (підписання) перемир'я / мирної угоди Україною (рис. 1):

*1. Визначення політико-воєнної доцільності перемир'я:*

аналіз воєнно-політичної ситуації (військові спроможності сторін, дипломатична ситуація, ризики / переваги);

визначення мети перемир'я: тимчасове припинення вогню / підготовка до тривалого миру;

формування позиції України щодо ключових принципів: суверенітет, територіальна цілісність, міжнародні гарантії.

*2. Формування переговорної стратегії:*

створення урядової переговорної групи з представників ОПУ, МЗС, Міноборони, РНБО, Верховної Ради, ЗС України;

визначення меж допустимих поступок та "червоних ліній";

ініціація консультацій з міжнародними партнерами (США, ЄС, Велика Британія, НАТО, ООН).

*3. Початок попередніх контактів і підготовчих переговорів:*

встановлення комунікаційного каналу з рф через посередників або міжнародні платформи (наприклад, ООН, Туреччина, Швейцарія);

визначення формату перемир'я (двостороннє, багатостороннє, за посередництва);

початок технічних консультацій щодо основних параметрів режиму припинення вогню.

*4. Укладення рамкових домовленостей:*

підписання попереднього політичного документа: про припинення бойових дій; відведення військ; обмін полоненими; допуск гуманітарних місій;

узгодження ролі міжнародних спостерігачів (миротворці, місії ОБСЄ, ООН, інші);

*5. Підписання перемир'я / мирної угоди – проведення офіційного підписання договору за участю гарантів, до якого необхідне включення таких пунктів:*

терміни та механізми контролю виконання;

відповідальність за порушення;

міжнародні гарантії безпеки України;

майбутня доля окупованих територій (вибори, реінтеграція, адміністрація);

статус військових формувань рф на тимчасово окупованій території (ТОТ);

формат післявоєнного співіснування.

фіксація демаркаційної лінії, потенційних демілітаризованих зон.

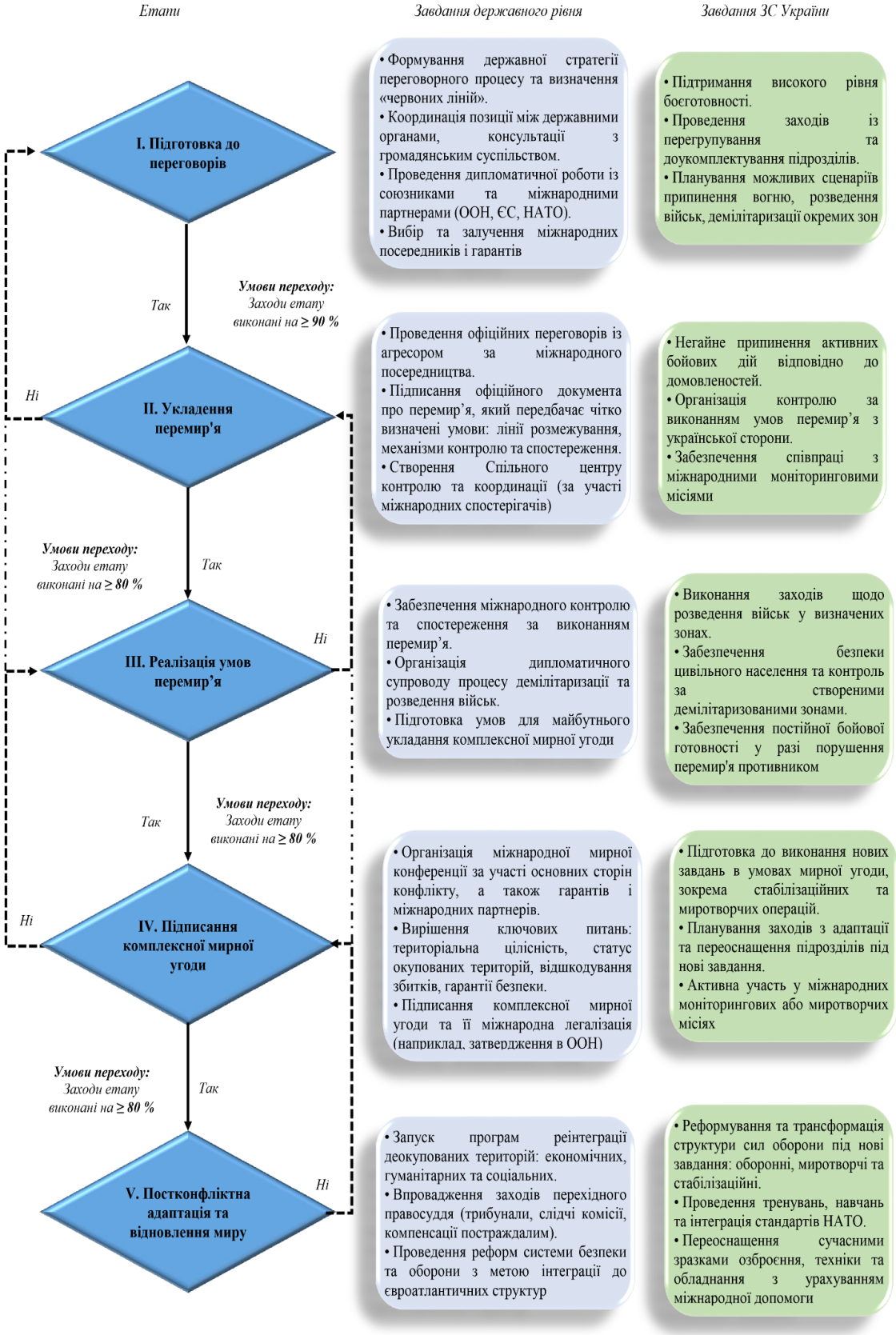



**Рисунок 1.** Загальний алгоритм укладання перемир'я / мирних угод

*6. Формування механізмів реалізації угоди:*
створення координаційного центру або Спільної контрольної місії;
розгортання миротворчих або моніторингових місій;
інституційний супровід (внутрішнє законодавство, бюджет, безпекові структури).
*7. Забезпечення безпеки під час переходу до миру:*
утримання оборонної готовності ЗС України;
оперативне реагування на можливі порушення угоди;
забезпечення режиму контролю над демілітаризованими / перехідними зонами.
*8. Адаптація завдань Збройних Сил України:*
**стратегічний рівень:**
перехід від моделі активної оборони до моделі стримування;
розвиток компонентів інформаційної, кібер- та повітряної безпеки;
участь у контролі реалізації умов перемир'я;
**оперативний рівень:**
переформатування частин, які були на передовій, у сили оперативного резерву;
підготовка до операцій стабілізації та безпеки в перехідних регіонах;
участь у розмінуванні, охороні інфраструктури, контролі кордонів;
**тактичний рівень:**
розгортання підрозділів у ключових пунктах безпеки;
підтримка правопорядку у звільнених або демілітаризованих зонах;
співпраця з цивільними адміністраціями та міжнародними місіями.
*9. Постконфліктна стабілізація та підтримка миру:*
**політичні та правові заходи:**
ухвалення національного акту або пакета законів про порядок реалізації умов перемир'я / мирної угоди;
визначення механізмів перехідного правосуддя (уникнення амністій для воєнних злочинців, одночасно – гуманітарний підхід до залучених цивільних);
розгортання місій внутрішнього нагляду за дотриманням прав людини, поверненням власності, доступом до соцпослуг;
**безпекова стабілізація:**
підготовка системи ЗС України до асиметричних загроз, гібридних атак, саботажу, внутрішньої дестабілізації;
забезпечення фізичної безпеки цивільного населення у демілітаризованих зонах;
координація з Нацполіцією, ДСНС, СБ України, Держприкордонслужбою для забезпечення інтегрованого підходу до стабілізації.
*10. Трансформація сектора безпеки та оборони:*
**інституційні реформи:**
переоцінка потреб та завдань Збройних Сил України у мирний період;
створення нових сил і командувань, здатних діяти в умовах перемир'я (наприклад, Командування стабілізаційних операцій);
розбудова Національної системи стратегічної стійкості – інтеграція воєнних, кібернетичних, інформаційних елементів захисту держави;
**військова освіта та підготовка:**
перенавчання особового складу для завдань: участі у стабілізаційних операціях; цивільно-військового співробітництва; розмінування та екологічної безпеки; миротворчих та спостережних місій.
*11. Контроль та ревізія виконання домовленостей:*
створення національного механізму моніторингу виконання угоди: участь ЗС України, СБУ, МЗС, парламентський нагляд;

щорічна ревізія безпекового середовища та перегляд формату розгортання ЗС України відповідно до нових викликів;

готовність до відновлення широкомасштабної оборони у разі порушення умов рф або відсутності гарантій.

*12. Інтеграція до системи колективної безпеки:*

активне просування інституціоналізованих гарантій безпеки – НАТО+, міжнародні гарантії (Будапешт 2.0), угоди із союзниками;

участь у спільних оборонних структурах, навчаннях, миротворчих ініціативах;

розбудова оборонного потенціалу не для війни, а для стримування агресора та гарантування миру.

**Висновок (Conclusion)**

Алгоритм укладення та реалізації перемир'я або мирної угоди з росією для України має включати поетапну, багаторівневу систему заходів, де кожен наступний крок логічно випливає з попереднього. Найбільшим викликом залишається поєднання дипломатичної гнучкості та воєнної готовності. Завершальний етап – це трансформація ЗС України: від армії, що веде виснажливу війну, до сили, яка:

гарантує мир;

утримує стримуючий потенціал;

підтримує стабільність у межах України та разом із партнерами – на міжнародному рівні.

Цей алгоритм може слугувати дорожньою картою для ухвалення рішень у найчутливіший момент сучасної української історії.

Алгоритм укладення перемир'я або мирної угоди з рф має базуватись на чіткій послідовності дій, де безпека, міжнародні гарантії та гнучкість у переговорах мають ключове значення. ЗС України залишаються центральним гарантом стабільності, навіть у постконфліктний період – через гнучку адаптацію до нових завдань у перехідній безпековій ситуації.

**Рекомендації (Recommendations)**

Стаття буде корисною для військових, урядовців, дипломатів, аналітиків, дослідників у сфері міжнародного права, а також для міжнародних організацій, які залучені до процесу врегулювання збройних конфліктів. Вона має практичне значення для розроблення офіційних позицій України у мирних перемовинах, створення нормативно-правової бази для імплементації домовленостей, забезпечення безпеки на деокупованих територіях та інтеграції України до міжнародних безпекових структур.

**Використані джерела**

1. *Женевські конвенції про захист жертв війни (1949) та Додаткові протоколи (1977).* https://zakon.rada.gov.ua/laws/show/995_199.
2. *Гаазька конвенція (IV) про закони і звичаї війни на суходолі від 18 жовтня 1907 року.* https://zakon.rada.gov.ua/laws/show/995_222.
3. *Угода про перемир'я в Кореї від 27 липня 1953 року*. https://www.usfk.mil/Portals/105/Documents/SOFA/G_Armistice_Agreement.pdf.
4. *Дейтонська мирна угода (Генеральна рамкова угода про мир у Боснії і Герцеговині) від 14 грудня 1995 року.* https://www.osce.org/bih/126173.
5. *Мінський протокол від 5 вересня 2014 року.* https://www.osce.org/uk/home/123258.
6. *Комплекс заходів щодо виконання Мінських домовленостей від 12 лютого 2015 року*. https://www.osce.org/uk/cio/140156.
7. *Guidance for Effective Mediation.* (2012). United Nations. https://peacemaker.un.org /sites/peacemaker.un.org/files/GuidanceEffectiveMediation_UNDPA2012.pdf.

8. *Hybrid Threats: A Strategic Communications Perspective*. (2019). NATO Strategic Communications Centre of Excellence. https://stratcomcoe.org/publications/hybrid-threats-a-strategic-communications-perspective/20.
9. *Handbook on OSCE Peace Processes.* OSCE. https://www.osce.org/secretariat/121741.
10. *Comprehensive Peace Agreement* (2005). https://peaceaccords.nd.edu/accord/comprehensive-peace-agreement.
11. *Будапештський меморандум про гарантії безпеки Україні від 5 грудня 1994 року.* https://zakon.rada.gov.ua/laws/show/998_158.
12. *Віденська конвенція про право міжнародних договорів* (1969). https://zakon.rada.gov.ua/laws/show/995_118.
13. *Joint Concept for Integrated Campaigning* (2018). https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concept_integrated_campaign.pdf.
14. *Revitalized Agreement on the Resolution of the Conflict in South Sudan* (2018). https://peaceaccords.nd.edu/accord/revitalized-agreement-resolution-conflict-south-sudan.
15. *Memorandum on the Creation of De-escalation Zones in Syria* (2017). https://peacemaker.un.org/node/3215.
16. *Угода про принципи мирного врегулювання конфлікту в Придністров'ї* (1992). https://www.osce.org/files/f/documents/9/9/42309.pdf.
17. *Тристороння заява про припинення вогню в Нагірному Карабаху* (2020). https://www.mid.ru/en/foreign_policy/news/1632211/.
18. *Peace Treaty between Egypt and Israel* (1979). https://peacemaker.un.org/egyptisrael-peacetreaty79.
19. *Agreement on Disengagement between Israel and Syria* (1974). https://peacemaker.un.org/israelsyria-disengagement74.
20. *Agreement for a Complete and Permanent Ceasefire in Libya* (2020). https://unsmil.unmissions.org/sites/default/files/ceasefire_agreement_between_libyan_parties_english.pdf.

**References**

1. *Geneva Conventions for the Protection of War Victims (1949) and Additional Protocols (1977).* https://zakon.rada.gov.ua/laws/show/995_199.
2. *Hague Convention (IV) on the Laws and Customs of War on Land of October 18, 1907*. https://zakon.rada.gov.ua/laws/show/995_222.
3. *Armistice Agreement in Korea of July 27, 1953.* https://www.usfk.mil/Portals/105/Documents/SOFA/G_Armistice_Agreement.pdf.
4. *Dayton Peace Agreement (General Framework Agreement for Peace in Bosnia and Herzegovina) of December 14, 1995*. https://www.osce.org/bih/126173.
5. *Minsk Protocol of September 5, 2014.* https://www.osce.org/uk/home/123258.
6. *Package of measures for the implementation of the Minsk agreements of February 12, 2015*. https://www.osce.org/uk/cio/140156.
7. *Guidance for Effective Mediation* (2012). United Nations. https://peacemaker.un.org/sites/peacemaker.un.org/files/GuidanceEffectiveMediation_UNDPA2012.pdf.
8. *Hybrid Threats: A Strategic Communications Perspective* (2019). NATO Strategic Communications Centre of Excellence. https://stratcomcoe.org/publications/hybrid-threats-a-strategic-communications-perspective/20.
9. *Handbook on OSCE Peace Processes*. OSCE. https://www.osce.org/secretariat/121741.
10. *Comprehensive Peace Agreement* (2005). https://peaceaccords.nd.edu/accord/comprehensive-peace-agreement.
11. *Budapest Memorandum on Security Assurances to Ukraine of December 5, 1994.* https://zakon.rada.gov.ua/laws/show/998_158.

12. *Vienna Convention on the Law of Treaties* (1969). https://zakon.rada.gov.ua/laws/show/995_118.
13. *Joint Concept for Integrated Campaigning* (2018). https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concept_integrated_campaign.pdf.
14. *Revitalized Agreement on the Resolution of the Conflict in South Sudan* (2018). https://peaceaccords.nd.edu/accord/revitalized-agreement-resolution-conflict-south-sudan.
15. *Memorandum on the Creation of De-escalation Zones in Syria* (2017). https://peacemaker.un.org/node/3215.
16. *Agreement on the Principles of a Peaceful Settlement of the Conflict in Transnistria* (1992). https://www.osce.org/files/f/documents/9/9/42309.pdf.
17. *Trilateral Statement on the Ceasefire in Nagorno-Karabakh* (2020). https://www.mid.ru/en/foreign_policy/news/1632211/.
18. *Peace Treaty between Egypt and Israel* (1979). https://peacemaker.un.org/egyptisrael-peacetreaty79.
19. *Agreement on Disengagement between Israel and Syria* (1974). https://peacemaker.un.org/israelsyria-disengagement74.
20. *Agreement for a Complete and Permanent Ceasefire in Libya* (2020). https://unsmil.unmissions.org/sites/default/files/ceasefire_agreement_between_libyan_parties_english.pdf.

## Recommendations on the procedure for declaring a truce (peace agreement) during an armed conflict: Ukrainian experience

**Andrii Hnatov**
Chief of the General Staff of the Armed Forces of Ukraine
General Staff of the Armed Forces of Ukraine
03186, Povitrianykh Syl, 6, Kyiv, Ukraine
e-mail: gnatovav@ukr.net
ORCID: 0009-0000-9557-942x

**Oleksii Shevchenko**
Candidate of Historical Sciences
Deputy Chief of the General Staff of the Armed Forces of Ukraine
General Staff of the Armed Forces of Ukraine
03168, Povitrianykh Syl avenue, 6, Kyiv, Ukraine
e-mail: shevchenko_om@asv.gov.ua
ORCID: 0000-0003-0734-6533

**Oleh Semenenko**
Honoured Science and Technology Figure of Ukraine
Doctor of Military Sciences, Professor
Deputy Commandant of the Central Research Institute of the
of the Armed Forces of Ukraine for scientific work
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl avenue, 28 B, Kyiv, Ukraine
e-mail: aosemenenko@ukr.net
ORCID: 0000-0001-6477-3414

**Olexii Solomitskyi**
doctor of military sciences, senior researcher
head of research department
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl avenue, 28 B, Kyiv, Ukraine
e-mail: solosa1@gmail.com
ORCID:0000-0001-8061-8895

**Vitalii Busel**
Head of the Central Defence Resources Department
General Staff of the Armed Forces of Ukraine
03168, Povitrianykh syl avenue, 6, Kyiv, Ukraine
e-mail: Busel77vitalii@gmail.com
ORCID: 0009-0004-3043-9695

**Abstract.** The Russian Federation's prolonged armed aggression against Ukraine has presented Ukraine with challenges that go beyond purely military confrontation. Resource depletion, humanitarian crises, international pressure, and public expectations create an objective need to justify and structure approaches to concluding a ceasefire or peace agreement. In this context, there is a need to develop clear, scientifically sound recommendations for a phased transition from active combat to lasting peace. The article is particularly relevant because it integrates national experience, international humanitarian law, and practices of peaceful settlement of other armed conflicts, forming a practical "road map" of actions for Ukrainian security policy actors.

The purpose of the article is to develop recommendations on the procedure for concluding a truce (peace agreement) during an armed conflict, taking into account global and Ukrainian experience.

A comprehensive methodological approach was used in the preparation of the article. Methods of systematic analysis, comparative legal analysis, historical generalization, and inductive logic were used. The analysis of international regulatory and legal documents, practical examples of peace agreements, and an assessment of the current military-political situation in Ukraine played a significant role.

The article defines and distinguishes between the concepts of "ceasefire" and "peace agreement" in the context of international law. It describes their legal nature, mechanisms of conclusion, key parameters, and analyzes the possible risks and advantages of each of these instruments in the current conditions. The authors propose a structured 12-step algorithm for concluding a ceasefire or peace agreement. Particular attention is paid to the role of international mediators, security guarantees, and mechanisms for monitoring the implementation of the agreement. The article proposes institutional, military, and political solutions that can be adapted depending on how the situation develops.

The results of the study may be useful for the military, government officials, diplomats, analysts, researchers in the field of international law, as well as for international organizations involved in the process of resolving armed conflicts. The article has practical significance for the development of Ukraine's official positions in peace negotiations, the creation of a regulatory framework for the implementation of agreements, ensuring security in de-occupied territories, and Ukraine's integration into international security structures.

The adoption of such a phased strategy will allow Ukraine to avoid improvisation at critical moments of decision-making and guarantee both its own security and sustainable post-conflict development.

**Keywords:** truce, peace agreement, international humanitarian law, armed conflict, security guarantees, peace-making algorithm

The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 3 No. 2 (2025)

DOI: 10.62524/msj.2025.3.2.3

# Сутність та переваги децентралізованого управління в об'єднаних операціях НАТО

**Юрій Клят**
кандидат технічних наук, доцент
начальник Центрального науково-дослідного інституту Збройних Сил України
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: klyatt@ukr.net,
ORCID:0000-0002-8267-3748

**Олег Нечаєв**
Організація ССО
e-mail: olegnechayev7@gmail.com
ORCID: 0009-0003-5586-2820

**Вадим Клименко**
кандидат військових наук, доцент
начальник науково-дослідного відділу наукового центру
Військова академія, м. Одеса
65009, вул. Фонтанська дорога, 10, Одеса, Одеська область, Україна
e-mail: kvn_od@ukr.net
ORCID: 0000-0001-9144-2362

**Анотація.** Актуальність досліджуваної проблеми обґрунтовується досвідом російсько-української війни, який свідчить про необхідність пошуку шляхів удосконалення системи управління з метою об'єднання зусиль сил і засобів, які приймають участь в операції угруповання військ (сил). Приклад харківської контрнаступальної операції 2022 року показав обмеженість комунікаційних можливостей внаслідок швидкоплинності бойових дій, що призводило до випадків недостатньої координації між різними підрозділами, інколи до перебоїв зі зв'язком. Велика кількість даних від різних джерел ускладнювала їх оперативний аналіз та ухвалення рішень у реальному часі, швидкість операції і глибина просування військ створювали нові виклики, пов'язані із необхідністю миттєвої реакції на зміни обстановки. Таким чином, операція продемонструвала високий рівень професіоналізму Збройних Сил України, але також виявила певні обмеження функціонування системи управління в об'єднаних операціях.

Метою статті є пошук та обґрунтування комплексу алгоритмів функціонування системи управління угруповання військ (сил), які забезпечують високий рівень синергії її компонентів, раціональний вибір сил і засобів впливу на противника, своєчасну реакцію з метою дій на випередження, багаторівневий захист, ефективний розподіл зусиль у часі та просторі, належний рівень її функціональної стійкості в умовах безперервності функціонування.

Направленість статті полягає у виявленні допоміжних інструментів, які сприяють підвищенню ефективності функціонування системи управління військ шляхом формування умов для кращого розуміння процесів, їх пояснення та обґрунтованого вибору раціонального способу дій в умовах конкретної оперативної обстановки.

У статті застосовано наукові підходи, які дозволяють здійснити критичний аналіз характеристик існуючої системи управління угруповання військ (сил), провести їх зіставлення з вимогами, що сформувалися за результатами російсько-української війни, а також сформулювати пропозиції щодо подальшого розвитку цієї системи в контексті забезпечення сумісності з практикою об'єднаних операцій сил НАТО.

Основними результатами статті є застосування системного підходу до визначення напрямів підвищення функціональної стійкості системи управління угруповання військ (сил), що сприяє суттєвому зростанню загальної ефективності її функціонування, а також обґрунтування умов для успішної децентралізації управління, яка створює передумови для прийняття більш гнучких та обґрунтованих рішень.

Практична значущість отриманих результатів полягає у визначенні ключових чинників, що сприяють досягненню успіху системи управління угруповання військ (сил) в умовах об'єднаних операцій. Зокрема:

досягнення синергії за рахунок інтеграції зусиль різнорідних компонентів військ (сил), що беруть участь в операції;

збалансування етапів операції і максимізація ефекту на основі взаємної підтримки між учасниками, що дозволяє реалізувати сильні сторони оперативного плану та забезпечити взаємодоповнення сил і засобів;

застосування комплексного підходу до планування і ведення операцій, який ґрунтується на спільному розумінні оперативної ситуації та децентралізованому прийнятті рішень;

підвищення адаптивності системи управління, що дозволяє ефективно реагувати на зміни оперативної обстановки в умовах багатокомпонентної взаємодії.

**Ключові слова:** об'єднані операції, система управління, спільні функції діяльності, децентралізація, інформаційне забезпечення, організація роботи штабу.

**Вступ (Introduction)**

Успішне застосування військ (сил) в об'єднаній операції залежить від збалансованого обрання цілей, широких підходів у виборі засобів і способів для їх досягнення. План операції описує спосіб спільного використання сил і засобів для виконання спільних функцій діяльності, при цьому визначена кількість сил і засобів можуть функціонувати одночасно під час виконання декількох завдань або послідовно під час виконання одного завдання.

Отже, під час планування операції, командири та штаби розподіляють наявні ресурси, у загальних рисах визначають де і як вони залучаються до виконання завдань, інтегрують можливості для виконання спільних дій, створення ефектів і досягнення цілей. Спільні дії є спрямованим впливом на противника шляхом застосування спільних функцій: удару, вогню, маневру, інформаційного впливу тощо. Вони підтримуються функціями розвідки, а свобода у виконанні спільних дій забезпечується спільними функціями з підтримки та захисту сил [5].

Під час виконання операції командир прагне домогтися оперативності, результативності та синергії компонентів сил, які ведуть тактичні дії для досягнення задуманого ефекту згідно плану операції. Результатом управління є ефект синергії різних функцій, завдяки чому спільні дії різнорідних сил і засобів набувають спроможностей:

використовувати призначені можливості для виконання завдань згідно плану операції;

оцінювати ефект від кожної дії з точки зору прогресу у досягненні мети, включаючи будь-які ризики і необхідні для цього успіху ресурси;

використовувати сприятливу ситуацію або пом'якшувати несприятливу, коригуючи або розробляючи нові плани;

переглядати оцінку оперативної ситуації через регулярні проміжки часу, вносити зміни якщо це продиктовано суттєвими обставинами або оцінка операції вимагає її зміну в цілому.

Синхронізація та координація зусиль наявного складу військ (сил) завжди цікавила дослідників, що намагались підкорити дії численної кількості різнорідних сил і засобів єдиному замислу і плану, створити умови їх функціонування такими, що адаптивно реагують на зміни процесу управління у такий спосіб, що допомагає їм заволодіти ініціативою та вижити у складних обставинах загальновійськового бою.

Пошуки ефективності управління військами приводили дослідників до вивчення різних методів, які застосовувались воєначальниками для досягнення мети операції (бою). Їх загальний обрис зводиться до двох протилежностей. Один з таких методів полягає у централізованому управлінні, притаманному авторитарній системі соціального устрою, заснованому на авторитеті та досвіді старшого начальника. Протилежністю йому виступає метод децентралізованого управління, який є ключовим в операціях НАТО. Сутність децентралізованого управління полягає у передачі повноважень від вищих ланок управління нижчим. Перше, про що замислюється старший командир під час формулювання свого наміру – як він буде використовувати спроможності управління молодших командирів, яку ініціативу від них очікувати, і яким чином сприяти її прояву.

Поки на тактичному рівні командири підрозділів мають достатньо сил і засобів для ведення бою (дій), володіють ініціативою, їх можливості є найбільш ефективними, якщо вони інтегровані та синхронізовані з іншими об’єднаними силами. За необхідності, командир здійснює переорієнтацію зусиль для досягнення синергії між ними. Його управління спрямоване на забезпечення життєвої стійкості, витривалості, реалізації функціональних властивостей наявних сил і засобів.

Аналізуючи систему управління за досвідом російсько-української війни слід зазначити, що органи управління працюють в умовах, які характеризуються суттєвим збільшенням кількості потоків інформації про обстановку. Одночасно підвищились вимоги до її достовірності і якості, як результат – до вибору посадовою особою ключових факторів, які впливають на прийняття рішення та швидкість процесу в цілому. Таким чином, найважливішою вимогою до управління була і залишається висока оперативність у роботі всіх органів управління, а основними критеріями їх оцінки є час, що витрачається на здійснення заходів управління, та їх якість.

До засобів управління пред’являються підвищені вимоги щодо забезпечення великих обсягів інформації з дотриманням високого рівня захисту та прихованості. Пред’являються вимоги не демаскувати свої наміри, створювати умови для введення противника в оману, тим самим, не допускати вжиття ним контрзаходів. Набагато більшими ніж раніше, є вимоги до пунктів управління тактичної ланки щодо захищеності, вони повинні мати всі необхідні інструменти та бути забезпеченими для їх сталого функціонування.

Недостатній рівень синергії компонентів сил свідчить про недосконалість існуючої системи управління, внаслідок чого відбувається нераціональний вибір сил і засобів впливу на противника, несвоєчасність реакції з метою дій на випередження, відсутність багаторівневого комплексного захисту, нерозуміння поточної обстановки, як наслідок, не ефективний розподіл зусиль у часі та просторі. Крім того, безперервність функціонування системи управління вимагає забезпечення належного рівня її функціональної стійкості. Пошук шляхів вирішення проблеми приводить до допоміжних інструментів, які краще створюють уявлення процесу, пояснюють його і сприяють до вибору раціонального способу дій.

У статті пропонується методом аналізу характеристик існуючої системи управління та співставлення їх з вимогами, які пред’являються за результатами російсько-української війни, визначити пропозиції щодо її подальшого розвитку і удосконалення в контексті сумісності застосування в об’єднаних операціях за прикладом об’єднаних операцій сил НАТО. Актуалізація уваги на зворотному зв’язку, в якому завжди були зацікавлені органи управління, який був і залишається одним із ключових факторів успішної децентралізації управління,

надають нові можливості у прийнятті обґрунтованих рішень. В умовах сучасних та майбутніх загроз застосування методу підвищення функціональної стійкості системи управління оперативно-тактичного угруповання дозволить суттєво підвищити загальну ефективність її функціонування.

**Матеріали та методи (Materials and Methods)**

Система управління, є складною сукупністю взаємопов'язаних елементів, спрямованих на досягнення цілей угруповання військ (сил), що полягають у виконанні оперативних завдань і досягаються шляхом планування, координації та контролю. Основними характеристиками такої системи є: мета, структура, функції, властивості і взаємодія із зовнішнім середовищем.

Командири приймають рішення на основі свого розуміння середовища операції. Візуалізація інформаційного процесу забезпечує командира і штаб своєчасною та актуальною інформацією для комплексного підходу у плануванні, прийнятті рішень та виконанні; включаючи всі дії, пов’язані з ідентифікацією, збором, фільтрацією, обробкою, фокусуванням, поширенням та використанням інформації.

Всі етапи об’єднаної операції повинні бути узгоджені між виконавцями і виконуються у взаємозв'язку для досягнення поставленої мети. Це досягається через координацію між підрозділами, спільне використання інформації, засобів зв’язку та озброєння. Штаб працює над синхронізацією роботи різних елементів оперативної побудови військ (сил) для досягнення загального результату. Таким чином, робота штабу оперативного угруповання спрямована на максимізацію ефективності використання сил і засобів для досягнення спільної мети, при мінімізації ризиків, дублювання зусиль і витрати ресурсів.

Робота штабу угруповання військ (сил) під час планування і ведення об'єднаної операції є ключовим елементом управління військами, спрямованим на досягнення визначених цілей. Штаб забезпечує організацію, координацію та контроль виконання завдань, використовуючи принципи оперативного мистецтва, військового управління та сучасних технологій.

Критично важливим етапом підготовки об’єднаної операції є аналіз обстановки. Від правильності оцінки вихідних даних залежить успішність подальшого планування та реалізації бойових завдань. Під час аналізу уточнюють мету операції, визначають ключові пріоритети та послідовність дій, виявляють можливі проблеми та ризики під час виконання завдання. Поглиблений аналіз ситуації охоплює оцінку противника, власних сил, місцевості, розробку сценаріїв розвитку дій: найбільш ймовірного, найгіршого, найсприятливішого. Результати отримання завдання та аналізу обстановки оформлюються у вигляді доповіді командиру висновків та рекомендацій, попереднього плану операції, узагальнених даних для підготовки бойового наказу.

Процес визначення замислу операції охоплює прогнозування можливих сценаріїв і формулювання основної ідеї застосування військ (сил). Для кожного можливого замислу штаб оцінює: чи дозволяє замисел досягти мети за мінімальних втрат, які слабкі місця замислу можуть бути використані противником, чи вистачає сил і засобів для його реалізації та наскільки він реалістичний у поточних умовах. Оцінюючи ризики штаб передбачає імовірність проведення контратак противника, застосування резервів, засобів радіоелектронної боротьби (РЕБ), високоточної зброї, можливі пастки, засідки або відволікаючі маневри противника, вплив місцевості і погодних умов, морально-психологічний стан особового складу, часові обмеження, рівень взаємодії між підрозділами. Після аналізу ризиків штаб визначає заходи для їхнього усунення або мінімізації.

Сучасні вимоги до організації роботи штабів часто вказують на недоліки, які суттєво впливають на ефективність планування, серед них надмірна бюрократизація процесів прийняття рішень, невчасна реакція на зміну обстановки, неповний або неточний аналіз обстановки, що призводить до неврахування всіх можливих сценаріїв розвитку подій,

планування без врахування альтернативних варіантів, проблеми з обміном інформацією між органами управління тощо.

Вирішальне значення для процесу прийняття рішень має використання інформації. Комунікаційні та інформаційні системи забезпечують передачу і спільне використання ситуаційної обізнаності, а ефективне управління зображеннями необхідне для підтримки обізнаності високого рівня. Гнучкість і проактивні дії в інформаційному середовищі мають ключове значення для оперативного успіху. Інформаційна функція допомагає командирам і штабам застосовувати інформацію, під час інтеграції з іншими функціями впливати на сприйняття відповідальних виконавців та прийняття рішення [6].

Інформація підлягає збору, обробці, зберіганню, й обов'язково цільовому доведенню до зацікавлених осіб, тоді вона буде мати цінність для тих, хто приймає рішення. Цей процес потрібен для створення організаційної культури, що заохочує і винагороджує обмін знаннями та інформацією для досягнення спільного розуміння. Наприклад, вільний обмін думками між командиром і штабом має вказувати на те, що ранній дизайн операцій є діяльністю, яка розділяє індивідуальність, знання багатьох функціональних експертів, і сприяє спільному розумінню. Подібним чином відбувається набуття досвіду під час операції та після її завершення в ході аналізу проведених дій, який ініціює командир або начальник штабу. Хоча цінність особистого спілкування безперечна, разом з тим колективному розумінню процесу сприяють можливості, які покращують асинхронну співпрацю на великій відстані серед розосереджених сил, що може покращити як планування, так і виконання спільних операцій.

Основною **метою** функціонування системи управління угруповання військ (сил) є забезпечення ефективної координації зусиль військових формувань різних видів та родів військ для вирішення оперативних і тактичних завдань, створення умов, у яких командування може своєчасно й ефективно управляти військами, досягати переваги над противником, яка реалізується шляхом знищення або нейтралізації противника з мінімальними втратами.

Ключовими аспектами досягнення мети є забезпечення єдності управління шляхом формування єдиної стратегії для всіх компонентів угруповання, узгодження дій між видами (родами) військ (сил). Одним з надзвичайно проблематичних питань, яке за всіх часів прагнули вирішити і на що спрямовані дослідження зараз – це організація тісної взаємодії між підрозділами для досягнення єдиного розуміння оперативного замислу, забезпечення синхронності та узгодженості дій у часі та просторі, раціональний розподіл завдань і ресурсів між учасниками операції, їх своєчасна доставка запасів та поповнення.

Управління, яке прагне заволодіти ініціативою в умовах змінного середовища, має бути проактивним і гнучким. Гнучкість забезпечується прогнозуванням потенційних викликів, ступенем їхнього впливу на обстановку, пошуком можливостей для вирішення завдань, делегуванням повноважень для оперативного прийняття рішень. Це дозволяє адаптуватися до викликів навіть у найскладніших умовах. Заволодіння ініціативою у складних і динамічних умовах зміни оперативної обстановки залежить від здатності ефективно синхронізувати дії сил і засобів [7].

Синхронізовані дії в рамках загальної конструкції операції є стандартною практикою децентралізованого управління на оперативному рівні. Вона потрібна для того, щоб змусити елементи домовитися і взяти на себе зобов'язання, заздалегідь узгодити курс дій для досягнення очікуваного ефекту. Синхронні дії можуть складатися з елементів, що працюють незалежно, але знають один одного, або тісно співпрацюють разом. Такий підхід дозволяє здійснити зусилля інших дискретних силових елементів зосереджено, у час і в місці, які, будуть вирішальними. Динамічна координація та синхронізація дій забезпечують більшу взаємодію між силовими елементами та потенціал для досягнення кращої взаємної підтримки та узгодженості елементів оперативної побудови.

Переваги такого підходу очевидні: поширити зону командування та контролю над операцією; підвищити оперативний темп; збільшити ефективність проведення операції і можливості щодо введення противника в оману.

Синхронізація дій вимагає тривалого планування та репетицій, але має користь від зменшення ризиків. Динамічна синхронізація, можливо, пропонує більші винагороди, але значною мірою покладається на здатність підрозділів сил та командування всіх рівнів ефективно реагувати на зміни оперативної обстановки. На всіх рівнях динамічної координації і синхронізації дій потрібні ефективні комунікаційні та інформаційні системи, щоб увімкнути обидва усвідомлення ситуації та ефективне командування та контроль. Таким чином, управління полегшується завдяки поєднанню управління бойовим простором і спільному усвідомленню ситуації на всіх рівнях командування: стратегічному, оперативному, тактичному [8].

**Структура системи управління** оперативно-тактичним угрупованням створюється з метою забезпечення ефективного планування, координації та контролю дій сил і засобів угруповання у зоні відповідальності в різних умовах бойової обстановки. Ключовими елементами системи управління, як відомо, є органи, пункти та засоби управління [9].

Органи управління забезпечують керівництво і координацію дій усіх складових міжвидового угруповання. До них належать: основний командний пункт (ОКП) угруповання – основний орган управління, який відповідає за координацію дій усіх видів (родів) військ, штаб угруповання – структурний підрозділ, що забезпечує планування операцій, аналіз бойової обстановки та координацію дій між видами (родами) військ, оперативні групи – підрозділи, які взаємодіють із штабами підпорядкованих частин та підрозділів. Для забезпечення гнучкості управління розгортаються резервні командні пункти (ЗКП), пересувні пункти управління (ТакКП).

Пункти управління – підготовлені місця, на яких розгорнуті та працюють органи управління.

Засоби управління – засоби, що забезпечують стійкий та безперервний зв’язок між органами управління та силами і засобами. Це перш за все система зв’язку, яка забезпечує безперервну, стійку і захищену передачу інформації між органами управління, штабами, бойовими підрозділами. Засоби радіо- та супутникового зв'язку, засоби передачі даних (захищені мережі, автоматизовані системи управління, польові мережі). Резервні системи зв’язку для забезпечення безперервності управління. Автоматизовані системи управління (АСУ), які використовуються для обробки даних, планування операцій та координації дій, наприклад, DELTA, GIS Arta, ВІРАЖ-планшет. Інтегровані інформаційно-комунікаційні системи для всіх рівнів управління.

До структури системи управління окремо слід віднести систему розвідки, яка забезпечує отримання інформації про противника, обстановку та прогнозування розвитку подій. Вона включає розвідувальні підрозділи всіх видів (родів) військ. БпЛА (безпілотні літальні апарати) та супутникові системи спостереження, засоби радіоелектронної розвідки тощо.

Також, як окремий, але тісно взаємопов'язаний компонент, який підтримує основну діяльність військ, присутня система забезпечення – це підсистема, яка підтримує боєздатність угруповання, забезпечення матеріальними ресурсами, боєприпасами, пальним тощо, медичне забезпечення (евакуація поранених), технічне обслуговування і ремонт техніки.

**Функції системи управління** угруповання військ (сил) забезпечують ефективне планування, координацію, контроль та підтримку бойових і допоміжних дій. Разом з тим, внаслідок високої складності умов сучасної об’єднаної операції виникають серйозні виклики до системи управління оперативно-тактичним угрупованням, які потребують перегляду її основних функцій в контексті приведення реакції органів управління у відповідність до оперативної обстановки. Ключовим показником ефективності системи виступає час, який

витрачається на цикл управління, але висока динамічність дій, наприклад у контрнаступальній операції, призводила до того, що функції ставали обтяжливими і не відповідали вимогам своєчасності та обстановці.

Втрата часу під час оперативного аналізу обстановки вплинула на ефективність функції планування в частині корекції планів у зв'язку зі змінами обстановки. Обмеженість у можливостях опрацьовувати в реальному часі дані з великої кількості джерел призводила до несвоєчасного доведення завдань до підлеглих, орієнтування про небезпеку, надання вогневої підтримки, швидке реагування на дії противника тощо.

Узгодження одночасних дій між бригадами та батальйонами, що діяли на окремих напрямах, вимагало між ними високого рівня синхронізації. Через швидкість розвитку подій координація між штабами, командирами та підрозділами була ускладненою. Місцями спостерігався розрив між планами і реальними діями, що призводило до необхідності прийняття рішень “на місці” без повного розуміння загальної ситуації. Успіх операції базувався на раптовості для противника, що вимагало суворого збереження секретності та обмеження кількості осіб, які володіли повним планом операції. Це ускладнювало координацію, оскільки частина виконавців отримувала завдання вже в процесі бойових дій. Крім того, операція потребувала координації не лише між Збройними Силами України, а й з іншими військовими формуваннями та правоохоронними органами, внаслідок чого виникали проблеми з обміном розвідувальними даними або узгодженням спільних дій.

Перебої зі зв’язком вплинули на ефективність функції контролю, а також функції захисту стійкості та безпеки системи управління. В умовах швидкого просування військ виникали проблеми зі зв’язком, зокрема через заглушення сигналів противником та географічні особливості місцевості, внаслідок чого в деяких випадках підрозділи діяли на основі попередніх вказівок, без оперативного оновлення інформації, що могло створювати ризики неузгоджених дій.

Швидкий темп іноді перевищував можливості штабів підтримувати логістичну підтримку на всіх рівнях, це приводило до труднощів із забезпеченням підрозділів паливом та боєприпасами. Це негативно впливало на концентрацію зусиль у потрібних точках у потрібний момент, та показало недостатню ефективність функції забезпечення, що спрямована на підтримку боєздатності військ.

Внаслідок перевантаження роботи засобів управління мету функції інформаційного забезпечення, яка пов'язана зі збором, обробкою, аналізом і передачею інформації, було реалізовано не у повній мірі, оскільки деякі підрозділи могли стикатися із несподіваними силами противника без попередньої координації з іншими частинами угруповання.

Таким чином, аналіз результатів функціонування системи управління потребує пошуку шляхів її удосконалення, зміни умов функціонування штабу, як основного структурного підрозділу управління [10].

Підвищення швидкості можливе за рахунок поєднання окремих функцій, а надійність можливо досягнути завдяки підвищенню функціональної стійкості. Разом з тим, поєднання функцій з метою прискорення процесу управління можливе виключно за умов забезпечення якості прийнятого рішення або процесу його реалізації.

Практика показує, що тривалість процесу планування значно зростає, а якість зменшується, якщо оперативний відділ (відділення) недостатньо укомплектовані фахівцями, яких завжди не вистачає. Кваліфіковані відповіді на переважну більшість питань оперативної або тактичної обстановки може бути надана обмеженим колом фахівців, якими є, перш за все, офіцери-оператори. Обтяжливість викликана також недостатнім рівнем цифровізації процесу.

Надмірна централізація розподілу ресурсів знижує можливості щодо своєчасного використання їх на місцях. Тобто у підрозділів недостатньо можливостей по використанню

запасів, і є очевидним, що з метою прискорення даного процесу, їх потрібно збільшувати цільовим призначенням.

Заходи, що спрямовані на зменшення негативних наслідків пов’язаних із вогневим впливом противника, можливі за рахунок дій на випередження. Одним із способів підвищення швидкості реакції підрозділів є покращення ситуаційної обізнаності командирів тактичної ланки.

Досвід НАТО свідчить, що децентралізоване управління має суттєві переваги над системою управління противника за умов одноманітного розуміння обстановки вищою і нижчою ланками управління, заволодінням ініціативи в результаті переходу до дій на випередження, збереження якості процесу управління, що демонструється скоординованим на високому рівні виконанням вогню і маневру, рівнем підготовленості командирів і штабів, тобто “кращі командири – кращі бригади”, підвищенням контролю над оперативною обстановкою за рахунок досягнення багаторівневого стійкого зворотного зв’язку з підрозділами.

Складність системи децентралізованого управління у забезпеченні координації між підрозділами компенсується вищою швидкістю реакції завдяки делегуванню повноважень органам управління тактичного рівня, що є безперечною перевагою у динамічному безкомпромісному середовищі загальновійськового бою. Штаб, як координаційний орган розробляє план, в якому виконавці отримують автономію для реалізації своїх завдань у межах єдиної концепції. Операція вимагає гармонійного поєднання ефективного оперативного планування та тактичної ініціативності. Однак, якщо оперативне рішення недостатньо креативне, але супроводжується низкою корисних тактичних рішень, це може забезпечити кращий результат, ніж навіть блискуче оперативне рішення без тактичного втілення. В основі концепції децентралізованого управління має бути гнучкий алгоритм, який забезпечує ефективність її функціонування: комунікація систем зв’язку та обміну інформацією мають бути швидкими та надійними, контроль та зворотний зв'язок відповідати самим високим вимогам, щодо захищеності та стійкості.

**Властивості системи управління** угруповання військ (сил) визначають її здатність ефективно функціонувати в умовах складної та динамічної бойової обстановки і включають: цілеспрямованість, централізованість і децентралізацію, гнучкість, оперативність, стійкість, інтегрованість, масштабованість, інформаційну забезпеченість, захищеність, модульність, надійність, простоту, прогнозованість, економічність, взаємодію, синергетичність, стандартизованість. Ці властивості забезпечують ефективність функціонування системи управління угруповання військ в умовах сучасного високотехнологічного бойового середовища.

Доцільно акцентувати увагу на властивостях, спрямованих на виконання спільних функцій системи управління, які виступають підґрунтям для розвитку ефективності її функціонування і забезпечують міжфункціональні об’єднання для сумісних дій.

Інтегрованість, як узгоджена взаємодія між силами і засобами будується на використанні спільних платформ управління, стандартизованих процедур та автоматизованих систем. Її актуальність обґрунтовується досягненням синергетичного ефекту, коли сумарна бойова ефективність угруповання перевищує ефективність окремих його компонентів, але досвід російсько-української війни свідчить про низку інформаційних та технологічних проблем, пов’язаних із відсутністю уніфікованої платформи обміну даними внаслідок того, що різні системи, такі як західне обладнання й радянські зразки, часто несумісні між собою, має місце низька швидкість передачі даних між видами військ через відсутність єдиної системи управління та обміну інформацією. Вирішення цих проблем полягає у розробці та впровадженні інтегрованої системи управління військами, яка об’єднує розвідку, управління, зв’язок, координацію та бойові дії.

Масштабованість характеризується здатністю системи адаптуватися до будь-якого рівня бойових дій – від тактичного до стратегічного. Ефективне управління як малими підрозділами, так і великими угрупованнями призводить до своєчасного реагування та оптимального використання ресурсів у різних умовах і масштабах.

Інформаційна забезпеченість пов'язує мережею каналів органи управління системи, завдяки чому відбувається постійний збір, аналіз та розповсюдження інформації про бойову обстановку. Вона є основою для ефективного прийняття рішень та реалізації завдань в умовах бойових дій і реалізується завдяки використанню сучасних засобів автоматизації для обробки даних і підтримки прийняття рішень.

Одним із способів забезпечення функціональній стійкості системи управління виступає модульність – побудова її з окремих модулів, що можуть бути швидко змінені, замінені чи інтегровані без порушення загальної структури. Тобто це важлива властивість системи, яка дозволяє змінювати структуру залежно від масштабу операцій й підключати нові функціональні елементи без порушення її загальної функціональності.

Використання єдиних стандартів і протоколів для спрощення взаємодії між різними компонентами забезпечує підтримку сумісності з як з внутрішніми, та і з зовнішніми елементами оперативної побудови військ (сил) [11].

До властивостей децентралізованого управління слід віднести також високий рівень корисних тактичних рішень, які створюють фундамент для успішного виконання навіть посереднього оперативного плану, забезпечують адаптивність, масштабованість і стабільність. Аналіз результатів таких рішень є критично важливим етапом оцінки ефективності підготовки та проведення операції, важливим інструментом для покращення взаємодії в середині системи управління у майбутніх операціях. Рівень організації взаємодії системи управління значно сприяє її функціональної стійкості, яка дозволяє зберігати контроль за обстановкою навіть у складних та непередбачуваних ситуаціях.

**Взаємодія системи управління** угруповання військ (сил) із зовнішнім середовищем є важливим елементом, який забезпечує ефективне виконання бойових завдань та адаптацію до динамічних змін обстановки.

Зовнішнє середовище включає як військові, так і цивільні структури, природні та техногенні фактори. Основні аспекти такої взаємодії полягають в узгодженні рішень з державними органами та цивільними структурами, використанні державних ресурсів для підтримки угруповання, у співпраці для забезпечення гуманітарної допомоги та евакуації населення, залученні місцевих ресурсів для виконання завдань, забезпечення безпеки критичної інфраструктури.

Взаємодія з силами і засобами інших військових формувань та правоохоронних органів держави передбачає обмін інформацією, передачу розвідувальних даних, узгодження дій через спільні командні пункти, організацію спільних бойових завдань, підтримку та забезпечення, спільне використання матеріальних ресурсів, проведення навчань для підвищення взаємодії [12].

Інформаційна взаємодія – це протидія інформаційним атакам і дезінформації, проведення інформаційних операцій для підтримки морального стану військ і населення, узгодження інформації, що надається військовими, з медіа та іншими організаціями, використання мас-медіа для досягнення стратегічних цілей.

Взаємодія з цивільним населенням проявляється у забезпеченні гуманітарної допомоги, організації евакуації цивільного населення із зони бойових дій, розподілі продовольства, медикаментів та інших необхідних ресурсів, забезпечення населення достовірною інформацією про стан безпеки, попередження про можливі небезпеки (артобстріли, мінування тощо).

Взаємодія з природним середовищем передбачає оцінку природних умов, аналіз погодних, кліматичних і географічних особливостей регіону, мінімізацію впливу бойових дій на екосистеми, захист критичної інфраструктури, охорону енергетичних, транспортних і комунікаційних об'єктів, попередження та мінімізація техногенних ризиків.

**Висновок (Conclusion)**

Сучасні об'єднані операції військ (сил) – це комплекс заходів, який передбачає спільне та скоординоване застосування різних видів збройних сил і родів військ для досягнення спільної мети в умовах бойового середовища. Планування, координація та виконання об’єднаних операцій відбувається в умовах, які постійно змінюються, вимагають високого рівня адаптивності, координації та мислення оперативного рівня. Ефективне управління в такому середовищі можливе за умови інтеграції технологій, точного аналізу та швидкої реакції на зміни. Успіх залежить від злагодженого функціонування різних систем зброї, здатності адаптуватися до нових викликів і максимального використання можливостей, наданих технологіями та людським фактором.

Структура системи управління являє собою ієрархію підсистем, зв’язаних мережею вертикальних та горизонтальних зав’язків, її функціонування потребує адекватно-гнучкого алгоритму який розкриває методологію оптимально-раціонального втручання вищої ланки управління в ситуацію не руйнуючі принцип децентралізації, для того, щоб не забирати ініціативу нижчої ланки, а навпаки створювати умови для прогресивного розвитку подій знизу-вверх, залишаючи за собою функцію контролю.

Оцінка ефективності системи управління вимагає статистичних даних результатів прямого та опосередкованого впливу на загрозу, що по суті є результатом прийнятих рішень. Для самого органу управління статистика проявляється через контроль і зворотній зв'язок. На заключному етапі циклу управління командир спостерігає за результатами прийнятого рішення, проте внаслідок недосконалості функціонування системи, а саме недостатньої пропускної спроможності, командир і штаб можуть бути обмежені в інформації, яка містить повне уявлення про причинно-наслідкові зв'язки подій.

Прагнення діяти на випередження вимагає від органу управління прогнозування, що на даний час є суб’єктивним і обмежується знаннями, навичками і досвідом командира. Тому проблема полягає у технологічному розширенні можливостей командира і штабу.

Одним з основних показників ефективності роботи системи управління залишається швидкість реагування на зміни обстановки, тому досягнення значення швидкості реакції, яка переважає над противником – це ключова мета командира і штабу угруповання військ (сил), яка забезпечує гнучкість та адаптацію системи управління до динамічних змін у бойовій обстановці, можливості щодо швидкого прийняття рішень та їх доведення до виконавців, здатність циклу управління до своєчасної переорієнтації сил і засобів залежно від умов обстановки.

Об’єднані операції є важливим елементом сучасного військового мистецтва, оскільки дозволяють ефективно використовувати переваги кожного з компонентів у комплексному середовищі бойових дій. Особливої уваги заслуговують функції системи управління в об’єднаній операції, як характеристика, що є ґрунтовною в її описанні. До них відносяться: планування операції, організація підготовчих заходів, координація зусиль між військами (силами), мотивація учасників до виконання завдань, контроль і коригування дій у разі відхилень від запланованих, які проявляються у прийнятті нових або уточнені попередніх рішень. Таким чином, об’єднання функцій органів управління – перехід до об’єднаних функцій в управлінні.

**Рекомендації (Recommendations)**

Подальше удосконалення системи управління в інтересах досягнення результатів об’єднаної операції полягає у підвищенні її функціональної стійкості, яка забезпечує гарантований багаторівневий захист її функціонування і проявляється у готовності до роботи в умовах невизначеностей, що мають місце під час планування операції та ході її проведення. Завдання полягає у пошуку та описанні слабких місць у зв’язках між складовими процесу, підтвердження практичних наслідків втрати результативності, як висновок, пошук способів вирішення проблеми, створення запобіжників, недопущення таких ситуацій, пошук альтернативних шляхів, створення мереж з більшою пропускною інформаційною спроможністю, які більше відповідають вимогам сьогодення.

Система повинна бути готовою адаптуватись до постійно змінного середовища, в результаті чого вона набуває перевагу та заволодіває ініціативою. Результатом такої переваги є позитивний вплив суб’єктів на об’єкти управління, підготовка їх до хаосу, тертя і невизначеності, формування готовності до прояву ініціативу, що є перевагою децентралізованого управління.

Застосування додаткового інструментарію системи управління повинно стати запобіжником при помилковому уявленні того, що нижча ланка зрозуміла завдання і спроможна управляти на заданому рівні, але на практиці в силу багатьох причин це може бути не так, що змушує вищі органи управління шукати способи у наданні допомоги та створенні додаткових умов для виконання завдання.

Виходячи з недоліків, досвіду та актуальності об’єднаних операцій виникає потреба в об’єднаних функціях органів управління різнорідних сил і засобів оперативно-тактичного угруповання. Інтеграція різних компонентів вимагає висококваліфікованих фахівців, технічна складова системи управління потребує використання сучасних систем комунікації для підтримки постійного зв’язку, забезпечення доступу до максимально вичерпної інформації у всіх ланках в режимі реального часу в межах компетенції органу управління.

Ефективність децентралізованого управління забезпечується свободою командирів і штабів тактичної ланки управління у реалізації визначених їм завдань в межах планів вищого командування, розмежуванням повноважень між ланками управління, забезпеченням підтримки зверху, вчасним наданням ресурсів та допомоги з боку старшого командування, регулярним аналізом результатів діяльності для коригування роботи командирів на місцях. Децентралізоване управління дозволяє досягти високої гнучкості, прискорення процесу прийняття рішень та ефективного використання ініціативи. Однак для його успіху потрібна належна підготовка, довіра, чітка структура управління та сучасні засоби комунікації. Це особливо важливо для сучасних об'єднаних операцій у складних і динамічних умовах.

Для ефективної організації роботи штабу критично важливо, щоб інформаційне забезпечення працювало в тісній взаємодії з управлінськими процесами. Всі дані повинні бути оброблені, надані своєчасно, чітко і в доступному форматі для командирів на всіх рівнях. Ефективна взаємодія дозволяє системі залишатися стабільною, адаптивною та результативною навіть у складних умовах.

В об’єднаній операції командир може вибирати з широкого спектру наявних сил і засобів ті їх можливості, що на його думку дадуть максимальний ефект у конкретному випадку, а також поєднувати їх різними способами для виконання спільних функцій. Спільні функції пов’язаних між собою можливостей забезпечують надійну структуру згуртованих разом видів тактичних дій. Це дозволяє командирам інтегрувати, синхронізувати та управляти різними можливостями і діями в об’єднаних операціях. Використовуючи спільні функції, командири можуть визначити нові вимоги до застосування сил і засобів.

**Використані джерела**

1. Кучеренко, Ю., Носик, А., Ткачов, А., & Шубін, С. (2019). Визначення ефективності функціонування системи управління військового призначення з врахуванням вагомості, своєчасності та якості виконання завдань у підсистемах. *Збірник наукових праць Харківського національного університету Повітряних Сил*, *4*(62), 53–60. https://doi.org/10.30748/zhups.2019.62.07.
2. NATO. (2019). *Allied joint doctrine for the conduct of operations (AJP-3)* (Ed. C, Ver. 1). https://www.nato.int/cps/en/natolive/official_texts.htm.
3. Генеральний штаб Збройних Сил України. (2020, 30 липня). *Доктрина «Об'єднані операції»* (Наказ № 101). РВВ ЦЗСД МО та ГІП ЗС України.
4. Корендович, В., & Чіркалов, О. (2020). Проблема децентралізації управління військами (силами) в гібридній війні. *Наука і оборона, 3*, 32–40.
5. Головнокомандувач Збройних Сил України. (2020, 22 грудня). *Доктрина «Об'єднане планування»* (Наказ № 225).
6. Гавриленко, А. (2024). Ефективність функціонування системи підтримки прийняття рішень органів військового управління на основі сучасних інформаційно-аналітичних технологій. *Науково-технічний журнал Державного науково-дослідного інституту випробувань і сертифікації озброєння та військової техніки*, *2*(4), 40–44.
7. Гриб, Д., Демідов, Б., Борисенко, М., & Кузнєцова, М. (2019). Інформатизація управління структурною динамікою складних багато структурних систем військового призначення при динамічній зміні обстановки в районі ведення бойових дій. *Збірник наукових праць Харківського національного університету Повітряних Сил*, *60*, https://doi.org/10.30748/zhups.2019.60.01.
8. Кучеренко, Ю., Носик, А., Камак, Д., & Возний, О. (2024). Мережецентрична система управління і її вплив на бойові можливості міжвидового угруповання. *Науково-технічний журнал Державного науково-дослідного інституту випробувань і сертифікації озброєння та військової техніки*, *1*(3), 52–58.
9. Загорка, О., Поліщук, С., & Загорка, І. (2019). Оцінювання оперативно-тактичної важливості пунктів управління угруповання військ. *Наука і оборона*, *3*, 45–50.
10. Гриб, Д., Демідов, Б., Хмелевський, С., & Матющенко, О. (2019). Інтелектуальні технології у задачах управління структурною динамікою складних багато структурних систем військового призначення. *Системи обробки інформації*, *3*(158), 15–26. https://doi.org/10.30748/soi.2019.158.02.
11. Музиченко, Д., Філюнкін, Є., Швалючинський, В., та ін. (2018). *Процедури процесу прийняття військового рішення (за стандартами НАТО): навч. посібн.* НУОУ.
12. Залож, В., & Сімчук, П. (2023). Аналіз проблемних питань, що знижують ефективність взаємодії підрозділів державної прикордонної служби з військовими формуваннями та правоохоронними органами сил оборони під час виконання завдань з оборони держави, та можливі шляхи їх вирішення. *Збірник наукових праць Національної академії Державної прикордонної служби України*, *1*(90), 43–52. https://doi.org/10.32453/3.v90i1.1335.

**References**

1. Kucherenko, Y., Nosyk, A., Tkachev, A., & Shubin, S. (2019). Determining the efficiency of functioning of military control systems taking into account the importance, timeliness, and quality of task execution in subsystems. *Collection of Scientific Papers of the Kharkiv National Air Force University*, *4*(62), 53–60. https://doi.org/10.30748/zhups.2019.62.07.
2. NATO Standardization Office. (2019). *AJP-3 Allied Joint Doctrine for the Conduct of Operations* (Edition C, Version 1, February). NATO.

3. General Staff of the Armed Forces of Ukraine. (2020, July 30). *Doctrine "Joint Operations"* (Order No. 101). Publishing and Printing Center of the Central Command and Control System and Information Support of the Armed Forces of Ukraine.
4. Korendovych, V., & Chirkalov, O. (2020). The problem of decentralization of troop (force) command in hybrid warfare. *Science and Defense, (3)*, 32–40.
5. Armed Forces of Ukraine. (2020, December 22). *Doctrine "Joint Planning"* (Order of the Commander-in-Chief of the Armed Forces of Ukraine No. 225).
6. Havrylenko, A. (2024). Efficiency of functioning of decision support systems in military command bodies based on modern information and analytical technologies. *Scientific and Technical Journal of the State Research Institute for Testing and Certification of Weapons and Military Equipment, 2*(4), 40–44.
7. Hryb, D., Demidov, B., Borysenko, M., & Kuznetsova, M. (2019). Informatization of management of structural dynamics of complex multi-structural military systems under dynamic changes in the combat zone. *Collection of Scientific Papers of the Kharkiv National Air Force University, 2*(60), 7–15. https://doi.org/10.30748/zhups.2019.60.01
8. Kucherenko, Y., Nosyk, A., Kamak, D., & Voznyi, O. (2024). Network-centric command system and its impact on the combat capabilities of a joint inter-service group. *Scientific and Technical Journal of the State Research Institute for Testing and Certification of Weapons and Military Equipment, 1*(3), 52–58.
9. Zahorka, O., Polishchuk, S., & Zahorka, I. (2019). Assessment of the operational and tactical significance of command points of a troop grouping. *Science and Defense, (3)*, 45–50.
10. Hryb, D., Demidov, B., Khmelevskyi, S., & Matiushchenko, O. (2019). Intelligent technologies in the tasks of managing the structural dynamics of complex multi-structural military systems. *Information Processing Systems, 3*(158), 15–26. https://doi.org/10.30748/soi.2019.158.02
11. Muzychenko, D., Filyunkin, Ye., & Shvaluchynskyi, V. (2018). *Procedures of the military decision-making process (according to NATO standards): Textbook*. National University of Defense of Ukraine.
12. Zalozh, V., & Simchuk, P. (2023). Analysis of problematic issues reducing the effectiveness of cooperation between State Border Guard Service units and military formations and law enforcement agencies of the Defense Forces during state defense tasks, and possible ways to solve them. *Collection of Scientific Papers of the National Academy of the State Border Guard Service of Ukraine, 1*(90), 43–52. https://doi.org/10.32453/3.v90i1.1335.

## The essence and advantages of decentralized control in NATO joint operations

**Yurii Kliat**
Candidate of technical sciences, Associate professor,
Head of the Central Research Institute of the Armed Forces of Ukraine
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl avenue, 28 B, Kyiv, Ukraine
e-mail: klyatt@ukr.net
ORCID: 0000-0002-8267-3748

**Oleh Nechayev**
Organization of the Special Operations Forces
e-mail: olegnechayev7@gmail.com
ORCID: 0009-0003-5586-2820

**Vadym Klymenko**
Candidate of Military Sciences, Associate Professor
Head of the Research Department of the Scientific Center
Military Academy, Odessa
65009, Fontanska Road, 10, Odesa, Ukraine
e-mail: kvn_od@ukr.net
ORCID: 0000-0001-9144-2362

**Abstract.** The relevance of the studied problem is substantiated by the experience of the Russian-Ukrainian war, which underscores the need to improve command and control systems in order to integrate the efforts of forces and assets involved in joint force operations. The 2022 Kharkiv counteroffensive serves as an illustrative example, highlighting the limitations of communication capabilities due to the rapid dynamics of combat, which led to instances of inadequate coordination between various units and occasional disruptions in communication. The large volume of data from multiple sources complicated real-time analysis and decision-making, while the speed and depth of the advance presented new challenges requiring immediate responses to changing operational conditions. Thus, while the operation demonstrated the high level of professionalism of the Armed Forces of Ukraine, it also revealed certain limitations in the functioning of the command and control system during joint operations.

The purpose of this article is to identify and substantiate a set of algorithms for the functioning of the joint force command system that ensure a high level of synergy among its components, the rational selection of forces and means for influencing the adversary, timely preemptive actions, multi-layered defense, effective allocation of efforts across time and space, and a sufficient level of functional resilience under continuous operation.

The article is aimed at identifying supporting instruments that enhance the effectiveness of command system operations by fostering improved understanding of operational processes, providing clear explanations, and enabling rational decision-making under specific operational conditions.

The study applies scientific approaches that facilitate a critical analysis of the current characteristics of the joint force command system, a comparison with emerging requirements derived from the Russian-Ukrainian war, and the formulation of proposals for further development of the system in the context of ensuring interoperability with NATO joint operations practices.

The main outcomes of the article include the application of a systems approach to identify ways to enhance the functional resilience of the joint command system, thereby significantly improving its overall effectiveness. The article also substantiates the conditions necessary for successful decentralization of command, which enables more flexible and well-grounded decision-making.

The practical significance of the findings lies in identifying key factors contributing to the success of the joint command system in the context of combined operations. These include:

achieving synergy through the integration of diverse force components involved in operations;

balancing operational phases and maximizing effect based on mutual support among participants, which allows for leveraging the strengths of the operational plan and ensuring complementarity of forces and assets;

implementing a comprehensive approach to operational planning and execution grounded in a shared understanding of the operational environment and decentralized decision-making;

enhancing the adaptability of the command system to effectively respond to changes in operational conditions within a multi-component interaction framework.

**Keywords**: joint operations, command and control system, joint operational functions, decentralization, information support, command post organization.

The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 3 No. 2 (2025)

DOI: 10.62524/msj.2025.3.2.4

# Сучасні будівельні матеріали для термінового відновлення твердих аеродромних покриттів

**В'ячеслав Козачук**
кандидат технічних наук, старший науковий співробітник
провідний науковий співробітник
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
k71419@ukr.net
ORCID: 0000-0002-0207-7461

**Олег Мовчан**
кандидат технічних наук, старший науковий співробітник
начальник науково-дослідного центру
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: alex-717@ukr.net
ORCID: 0000-0001-5245-7051

**Вадим Гром**
кандидат військових наук
провідний науковий співробітник
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: Hrom_v@ukr.net
ORCID: 0009-0009-5415-9758

**Олександр Водчиць**
кандидат технічних наук, доцент
начальник кафедри військової підготовки
Національний авіаційний університет
03058, проспект Любомира Гузара, 1, Київ, Україна
e-mail: agv64agv@gmail.com
ORCID: 0000-0002-3294-7632

**Олег Тарасов**
кандидат військових наук, доцент
доцент кафедри військової підготовки
Національний авіаційний університет
03058, проспект Любомира Гузара, 1, Київ, Україна
e-mail: tarasovo@ukr.net
ORCID: 0000-0002-6763-8653

**Анотація.** Актуальність дослідження визначається тим, що під час ведення бойових дій (особливо високої інтенсивності) Збройні Сили України неминуче зазнають певних втрат аеродромів. Унаслідок вогневого впливу ракетно-бомбових ударів тверді аеродромні покриття

злітно-посадкової смуги зазнають суттєвих пошкоджень, які заважають надійній експлуатації повітряних суден.

Актуальність статті обумовлена тим, що існує необхідність швидкого відновлення твердих аеродромних покриттів, при цьому має бути використано матеріали, до яких висуваються досить жорсткі вимоги. В останні роки в Україні почали пропонувати до застосування сучасні модифіковані будівельні матеріали, які дозволяють значно скоротити час відновлення: за умови правильної організації робіт час може становити не більше 7–10 діб, при цьому необхідні значення характеристик міцності під час стискання та розтягання досягаються повністю. Наслідком застосування таких матеріалів є забезпечення незначної перерви функціонування аеродрому (штатного використання злітно-посадкової смуги ~~ЗПС~~), що в умовах ведення бойових дій є актуальним питанням для Повітряних Сил Збройних Сил України.

Мета статті полягає в необхідності пошуку нових підходів до ремонту злітно-посадкової смуги, яка зазнає механічного пошкодження внаслідок завданих ракетно-бомбових ударів, в обмежені терміни з використанням сучасних будівельних матеріалів.

В основу дослідження покладено аналіз даних щодо сучасних будівельних матеріалів, які можуть бути використані для ремонту злітно-посадкової смуги, їхніх фізико-технічних характеристик, часових показників, необхідних для забезпечення максимального значення міцності використаних матеріалів.

Авторами визначено основні фактори, які впливають на деструкційні процеси твердих аеродромних покриттів у мирний час, – це природний вплив, а також навантаження під час здійснення зльотів і посадок повітряних суден. Слід виділити серед експлуатаційних факторів механічні впливи, а також силові й температурні впливи газового струменя реактивних двигунів літаків. У разі виявлення будь-яких пошкоджень покриття злітно-посадкової смуги потрібно вжити заходів щодо їх негайного усунення, оскільки в іншому випадку є ризик появи аварійного пошкодження й закриття смуги на тривалий ремонт. Але у разі виявлення дефектів, що загрожують безпеці польотів, їх усувають негайно до їх початку. Це дуже важливе питання щодо експлуатації твердих аеродромних покриттів: воно обумовлює необхідність застосування таких матеріалів для відновлення злітно-посадкової смуги, які мають найкоротші терміни набуття необхідних значень експлуатаційних характеристик твердих бетонних покриттів.

Основним результатом статті є те, що для виконання ремонтних робіт може бути використано різноманітні матеріали, але якщо діють два обмеження – термін до початку експлуатації та тривалість виконання робіт, то найбільш доцільним є використання сучасних матеріалів. Такі ремонтні матеріали мають відповідати вимозі: матеріали за міцністю мають забезпечувати носійну здатність не менше, ніж наявні аеродромні покриття, і відповідати встановленим вимогам до них.

Практична значущість результатів дослідження полягає у визначенні матеріалів для термінового ремонту злітно-посадкової смуги.

**Ключові слова:** ракетно-бомбові удари, тверді аеродромні покриття, злітно-посадкова смуга, навантаження, пошкодження, ремонт, ремонтні матеріали, носійна здатність, мінеральне в’яжуче, полімерне в’яжуче.

## Вступ (Introduction)

Цього року противник регулярно, майже кожні три-чотири доби завдає ракетно-бомбових ударів по аеродромній інфраструктурі Збройних Сил України (ЗС України), намагаючись, по-перше, знищити літальні апарати Повітряних Сил ЗС України; по-друге, вивести з ладу аеродромну інфраструктуру, заздалегідь перешкоджаючи розміщенню на ній літаків типу Dassault Mirage 2000 і F-16.

Унаслідок бомбардування тверді аеродромні покриття зазнають пошкоджень, які заважають надійній експлуатації повітряних суден. У результаті цього тверді аеродромні покриття потребують відновлення, при цьому має бути використано матеріали, до яких висуваються досить жорсткі вимоги. До недавнього часу для відновлення твердих аеродромних покриттів використовували виключно цементобетонні матеріали, які мали майже такі самі характеристики, що й аеродромні покриття. Такі матеріали мають доволі широкий діапазон фізико-технічних характеристик, передусім такі, як міцність, простота у використанні, а також те, що вони не потребують високої кваліфікації виконавців робіт. Але час відновлення злітно-посадкової смуги (ЗПС) під час застосування таких матеріалів із традиційними характеристиками обумовлений насамперед часом гідратації цементного каменю – 28 діб до максимального набору міцності. Крім того, практика експлуатації аеродромних покриттів свідчить про те, що ресурс ділянок, які було відремонтовано з використанням поширених матеріалів, як правило, в умовах мирного часу не перевищує 2–3 років [1]. Однією із причин зниження довговічності відновлених ділянок є невідповідність значень характеристик застосованих ремонтних сумішей навантаженням, які виникають у процесі експлуатації.

Варто зазначити, що впродовж останніх років в Україні почали пропонувати сучасні модифіковані будівельні матеріали, які дозволяють значно скоротити час відновлення: за умови правильної організації робіт час може становити не більше 7–10 діб, при цьому необхідні значення характеристик міцності під час стискання та розтягання досягаються повністю. Наслідком застосування таких матеріалів є забезпечення незначної перерви функціонування аеродрому (штатного використання ЗПС), що в умовах ведення бойових дій є актуальним питанням для Повітряних Сил ЗС України.

## Методологічна основа (Methodological Framework)

Дослідження останніх років, які було проведено до лютого 2022 року, було присвячено ремонту пошкоджень бетонних аеродромних покриттів, отриманих у мирний час, тобто тоді, коли деструктивними факторами є погодно-кліматичні умови та експлуатаційні чинники [2–4]. Але відкритих публікацій щодо технологічних рішень та сучасних матеріалів, які дають можливість швидко відновити бетонні аеродромні покриття, усунути наслідки завданих ракетно-бомбових та артилерійських ударів з таким результатом, що вважається прийнятним, наразі не знайдено. Одна з найгостріших проблем полягає у тому, що пошкодження воєнного часу більш сильні, часу для їх усунення значно менше, тому більшість матеріалів, які пропонуються в дослідженнях [5–8], не можуть бути використані в умовах відсічі збройній агресії, яка триває.

## Результати і обговорення (Results and Discussions)

На аеродромах військової авіації в Україні застосовують тверді аеродромні покриття, які мають або монолітну, або збірну конструкцію з попередньо напружених залізобетонних плит. Їхні пошкодження можна умовно поділити на пошкодження мирного часу та пошкодження воєнного часу.

Основні фактори, які впливають на деструкцію твердих аеродромних покриттів у мирний час, – це природний вплив, а також навантаження під час здійснення зльотів і посадок повітряних суден. Слід виділити серед експлуатаційних факторів механічні впливи, а також силові й температурні впливи газового струменя реактивних двигунів літаків.

Природні фактори, які впливають на покриття ЗПС:

– перепади температур протягом доби і сезону, кількість циклів “заморожування – розморожування”;

– вологість повітря;

– опади (їхня частота, кількість і розподіл за сезонами);

– глибина промерзання ґрунту;
– вітри, їхня сила, напрямок і тривалість;
– зледеніння покриття: шар льоду на поверхні ЗПС.

Унаслідок впливу деструктивних факторів виникають такі дефекти:
– усадочні та наскрізні тріщини;
– лущення верхнього шару бетону;
– руйнування верхнього шару покриття на глибину більше 10 мм;
– раковини та вибої;
– відколи країв і кутів плит;
– просідання та пролами карти покриття;
– руйнування заповнювача швів;
– оголення арматури.

Найпоширеніші пошкодження монолітного цементобетонного покриття у мирний час, які виникають внаслідок дії атмосферних та експлуатаційних факторів, – лущення верхньої поверхні бетону, вибої, раковини. Кількість плит із такими пошкодженнями становить приблизно 60% від загального числа дефектних плит [1]. Пошкодження воєнного часу, через які аеродромні покриття виходять з ладу, – це вибої, вирви, що утворюються внаслідок ракетних, бомбових, артилерійських ударів.

У разі виявлення будь-яких пошкоджень покриття ЗПС має бути вжито заходів щодо їх негайного усунення, оскільки в іншому випадку є ризик появи аварійного пошкодження й закриття смуги на тривалий ремонт. Але у разі виявлення дефектів, що загрожують безпеці польотів, їх усувають негайно до їх початку. Це дуже важливе питання щодо експлуатації твердих аеродромних покриттів: воно обумовлює необхідність застосування таких матеріалів для відновлення ЗПС, які мають найкоротші терміни набуття необхідних значень експлуатаційних характеристик твердих бетонних покриттів.

Умовно ремонт твердих бетонних покриттів розділяють на поточний і капітальний.

***Поточний ремонт*** проводиться без припинення експлуатації ЗПС. Цей вид ремонту передбачає роботи з постійного запобігання передчасному зношуванню аеродромного покриття шляхом усунення невеликих ушкоджень. Обсяг робіт під час поточного ремонту не перевищує 1% від усієї площі аеродромного покриття. Роботи передбачають:
– заміну ушкоджених ділянок покриття (плит);
– закладення усадкових і наскрізних тріщин, раковин, вибоїв, відколів, лущення верхньої поверхні бетону;
– заповнення мастикою деформаційних швів;
– ремонт дефектних стиків і арматур, що оголилася, у збірних плитах;
– усунення уступів, тріщин, колій, осідань і проламів (в асфальтобетонних покриттях).

Під час ***капітального ремонту*** усуваються значні руйнування та деформації твердих бетонних покриттів аеродромів. Найчастіше під час його проведення експлуатація ЗПС тимчасово зупиняється. Під час виконання капітального ремонту твердих покриттів виконуються такі роботи:
– заміна окремих деформованих плит або їхніх частин (ділянок) покриттів обсягом до 10% від загальної площі аеродромних покриттів;
– вирівнювання покриття, яке просіло, у разі якщо його обсяг становить до 10% від загальної площі. Виконується методом укладання нового шару покриття з бетону, що виготовлений зі спеціальних розчинів – як правило, зі швидкотвердних;
– усунення поверхневих дефектів покриття: сколів кутів і кромок плит, лущення верхньої поверхні бетону покриття, раковин, вибоїв плит на ділянках площею до 30% від загальної площі аеродромних покриттів;
– вирівнювання й посилення наявних покриттів за допомогою укладання нового шару

бетону на окремих частинах покриття (обсяг виконуваних робіт – від 30% до 100% від загальної площі покриття аеродрому).

Для виконання ремонтних робіт може бути використано різноманітні матеріали, насамперед традиційні цементно-бетоні немодифіковані ремонтні матеріали для відновлення аеродромних поверхонь. Такі матеріали мають одну суттєву перевагу – простий склад, завдяки чому їхня вартість порівняно невисока.

Недоліки використання традиційних ремонтних матеріалів в умовах воєнного часу досить суттєві. По-перше, час визрівання традиційного бетону – два тижні для набору 70% відсотків міцності щодо стискання, та 4 тижні для набору 100% міцності. Крім того, традиційні ремонтні суміші для відновлення бетону мають менші значення характеристик міцності щодо стискання, розтягування та скручування порівняно з модифікованими ремонтними матеріалами.

Отже, якщо є чинними два обмеження – а саме вони наразі є чинними – термін до початку експлуатації та тривалість виконання робіт, то найбільш доцільним є використання сучасних модифікованих ремонтних матеріалів. Такі ремонтні матеріали мають відповідати вимозі: матеріали за міцністю мають забезпечувати носійну здатність не менше, ніж наявні аеродромні покриття, і відповідати встановленим вимогам, які наведено в табл. 1.

***Відновлення покриттів, якщо дефекти мають глибину до 10 мм***. У цьому випадку передусім виконують фрезерування та шліфування пошкодженої поверхні. Потім оброблену поверхню очищують від пилу та маленьких шматочків бетону і здійснюють її насичення шляхом нанесення на поверхню рідкого складу, що ущільнює бетон, – так званого пенетруючого матеріалу.

**Таблиця 1.** Фізико-механічні показники бетонів для відновлення цементобетонних покриттів [9]

| Показник | Значення |
|---|---|
| Міцність під час стискання через 1 добу, МПа | 20–40 |
| Морозостійкість, цикли | 150–200 |
| Усадка, мм/м | 0,9–1 |
| Міцність зчеплення зі “старим” бетоном (адгезія), МПа | 1,5–2,0 |

Найбільш високий результат досягається під час використання рідких літій-іонових складів, наприклад, Sikafloor CureHard LI, з витратами 100–150 мл на квадратний метр за умови нанесення в один шар. Але для отримання належного результату слід наносити не менше двох шарів. Додатковий ефект використання таких пенетруючих матеріалів – збільшення морозостійкості обробленого шару бетону [10].

Також ефективним вважається використання рідких пенетруючих матеріалів на основі силікатів, наприклад, Prosfas. Цей матеріал має високу проникну здатність. Після оброблення верхній шар бетону, насичений цим складом, становить до декількох сантиметрів, а морозостійкість після оброблення збільшується вдвічі [11].

Для ремонту вирв глибиною від 10 мм до 50 мм може бути застосовано матеріал Mapegrout SV-R Fiber. Цей матеріал є безусадковим, швидко твердішає, містить полімерну фібру. Міцність під час стискання через 28 діб досягає значення більше 65 МПа, міцність на розтягування через 28 діб становить 14 МПа. Марка морозостійкості – F300 (300 циклів “замерзання – розмерзання”), що є запорукою високої довговічності. Адгезія до сталі та бетону – 2 МПа.

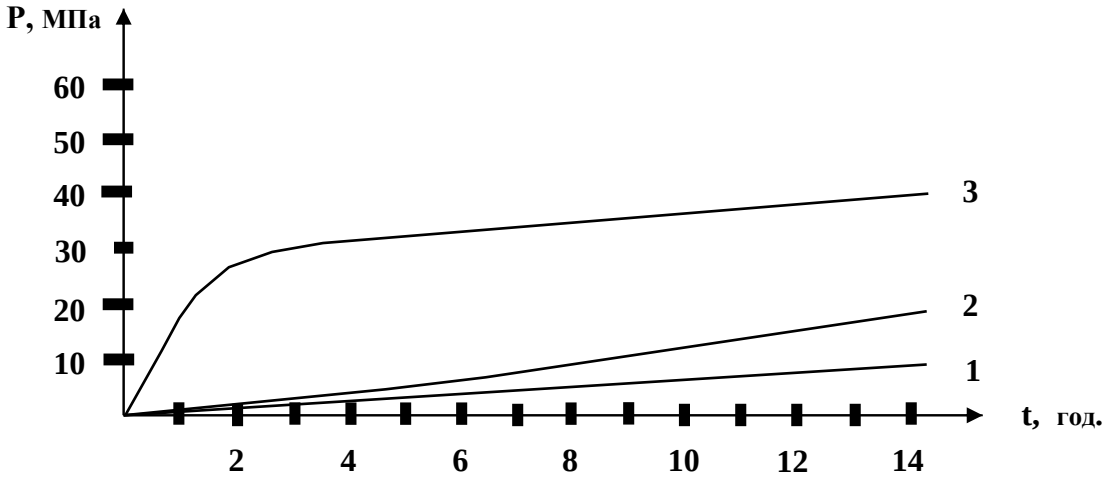
Під час ремонту дефектів глибиною до 70–100 мм використовувати ремонтні системи на цементній основі недоцільно, найбільш дієвий результат досягається, якщо застосовувати матеріали на цементно-епоксидній основі, наприклад, Sikagard-720 EpoCem, який наносять

шарами товщиною до 5 мм. Sikagard-720 Epocem – трикомпонентна цементна суміш, яка модифікована водною емульсією епоксидної смоли з підвищеною хімічною стійкістю.

Інший приклад – ремонт дефектів (передусім вирв) глибиною більше 100 мм. У цьому випадку доцільно використовувати, наприклад, матеріали ARB-10F або ARB-10. Ці матеріали дозволяють ліквідовувати вирви глибиною від 50 мм до 300 мм. Матеріали ARB-10F або ARB-10 – це суміші на основі цементу, вони є безусадковими, швидко твердішають, містять фібру: ARB-10 – полімерну, ARB-10F – полімерну та стальну. Міцність під час стискання через 28 діб досягає значення більше 75 МПа, міцність під час розтягування через 28 діб становить 8 МПа (ARB-10) та 15 МПа (ARB-10F). Марка морозостійкості – F300. ARB-10F та ARB-10 мають високу адгезію до сталі та бетону – більше ніж 2 МПа.

Усунути дефекти глибиною від 100 мм до 600 мм можна за технологією Rapid set. Це суміш на основі цементу, яка характеризується досить малими значеннями усадки, швидким твердінням, стійкістю до впливу агресивних хімічних сполук, у тому числі й штучного походження. Примітною особливістю цього матеріалу є швидкий набір міцності під час стискання (рис. 1). Максимального значення міцності під час стискання розчин досягає через 28 діб – приблизно 50 МПа [12].

Необхідно зазначити, що в останній час для відновлення працездатності твердих аеродромних покриттів широко пропонують ремонтні матеріали не лише на основі в'яжучого мінерального, а й на основі різноманітних полімерних в'яжучих матеріалів – поліуретанових, епоксидних, силоксанових тощо. Але в більшості випадків так звані полімерні ремонтні суміші мають нижчі значення найбільш важливих параметрів. Для порівняння в табл. 2 наведено деякі параметри ремонтних матеріалів на основі в'яжучого мінерального та в'яжучого полімерного.




1 – розчин із портландцементу ПЦ-500, не модифікований;
2 – розчин із портландцементу ПЦ-500, модифікований;
3 – розчин із Rapid Set.

**Рисунок 1.** Залежність набору міцності будівельних розчинів від часу [12]

**Таблиця 2.** Основні характеристики ремонтних матеріалів

| Показник | Значення показника | |
|---|---|---|
| | **на основі в'яжучого мінерального** | **на основі в'яжучого полімерного** |
| Міцність під час стискання, МПа | 40–90 | до 37 |
| Міцність під час розтягування, МПа | 8–16 | 26 |
| Модуль пружності $E$, $1\times10^3$ МПА | 18–25 | 20–27 |
| Міцність зчеплення зі "старим" бетоном (адгезія), МПа | 2–3 | 1,5–4 |
| Товщина шару ремонтного матеріалу, мм | 30–100 | 5–40 |

## Висновок (Conclusion)

Порівнявши значення, автори дійшли висновку про те, що вибір ремонтного матеріалу обумовлюється насамперед метою виконання ремонтних робіт. Ділянки, де, наприклад, мають бути високі значення міцності під час стискання, слід виконувати лише з матеріалів на основі в'яжучого мінерального. Ділянки, для яких цей параметр не є найкритичнішим, може бути відремонтовано з матеріалів на основі в'яжучого полімерного, що особливо важливо в умовах обмеженого часу.

Варто наголосити, що технології використання сучасних ремонтних матеріалів для відновлення твердих аеродромних покриттів не відрізняються підвищеною складністю. Як правило, виробник ремонтної суміші надає такі рекомендації з усунення ушкоджень, які містять загальні вимоги до виконання робіт поточного ремонту, технологію виконання робіт ямковим ремонтом і для усунення відколу плити залежно від геометричних параметрів дефектної ділянки, конструктивних особливостей закладення дефектної ділянки.

## Рекомендації (Recommendations)

У статті надано рекомендації щодо вибору сучасних будівельних матеріалів для використання під час відновлення твердих аеродромних покриттів в умовах збройної агресії. Рекомендації розроблено з урахуванням наявності необхідних будівельних матеріалів в Україні. Для прикладів наведено значення найбільш важливих параметрів продуктів таких продуцентів, як Sika, Mapei, Rapid. Визначено, що описані у статті ремонтні матеріали для відновлення твердих аеродромних покриттів цілком відповідають вимогам державних стандартів та державних будівельних норм України.

Перспективою подальших досліджень є визначення можливого вигляду, структури та складу системи відновлення твердих аеродромних покриттів для максимально результативного ремонту під час відсічі збройній агресії.

## Використані джерела

1. Попов, А. Н. (2022). Аэродромное покрытие — путь к безопасному полету. Научное обоснование требований к материалам для оперативного ремонта аэродромных покрытий. *Материально-техническое обеспечение, 10*, 27–34.
2. Красиникова, Н. М., Морозов, И. М., Хохряков, О. В., & Хозин, В. Г. (2014). Оптимизация состава цементного бетона для аэродромных покрытий. *Известия казанского государственного архитектурно-строительного университета, 2*, 166–172.
3. Ziari, H. A., Hayati, P. A., & Sobhani, J. B. (2017). Air-Entrained Air Field Self-Consolidating Concrete Pavements: Strength and Durability. *International Journal of Civil Engineering, 15* (1), 21–33.

4. Woodman, G. R., & Robinson, N. D. (2013). Concrete block surfacing for airfield pavements. *Proceedings of the Institution of Civil Engineers: Transport, 117* (3), 168–176.
5. Каримова, А. А., & Парамонова, М. И. (2019). Разрушения и ремонт искусственных покрытий взлетно-посадочных полос. *Alfabuild, 2* (9), 17–28.
6. Кульчицкий, В. А., Макагонов, В. А., Васильев, Н. Б., Чеков, А. Н., & Романков, Н. И. (2002). *Аэродромные покрытия. Современный взгляд.* Физико-математическая литература.
7. Леденев, А. А., Перова, Н. С., Внуков, А. Н., Козодаев, С. П., Баранов, Е. В., & Перцев, В. Т. (2021). Оперативный ремонт и восстановление аэродромного покрытия и объектов аэродромной инфраструктуры. *Вестник инженерной школы ДВФУ, 3* (48), 115–123.
8. Лещицкая, Т. П., & Попов, В. А. (1999). *Современные методы ремонта аэродромных покрытий.* МАДИ-ТУ.
9. *ДБН В.2.2-ХХ:2022 Будівлі та споруди. Аеродроми. Ч. І: Проєктування. Ч. ІІ: Будівництво.*
10. Ремонті матеріали Сіка https://gcc.sika.com/en/construction/refurbishment/concrete-repair/sikagard-720-epocem.html.
11. Матеріали Мапей https://www.mapei.com/ua/uk/materialy-i-tekhnichni-rishennia.
12. Продукти Мапей https://www.mapei.com/ru/ru/produkty/spisok-produktov/opisanie-produkta/arb-10f.
13. Технологія Rapid set https://www.ctscement.com/datasheet/CEMENT_ALL_Datasheet_DS_024_EN?c=&t=Professionals.

**References**

1. Popov, A. N. (2022). Airfield Pavement — The Way to Safe Flight. Scientific Justification of Requirements for Materials for Operational Repair of Airfield Pavements. *Material and Technical Support, 10*, 27–34.
2. Krasinikova, N. M., Morozov, I. M., Khokhryakov, O. V., & Khozin, V. G. (2014), Optimization of Cement Concrete Composition for Airfield Pavements. *Proceedings of the Kazan State University of Architecture and Engineering, 2*, 166–172.
3. Ziari, H. A., Hayati, P. A., & Sobhani, J. B. (2017). Air-Entrained Air Field Self-Consolidating Concrete Pavements: Strength and Durability. *International Journal of Civil Engineering, 15* (1), 21–33.
4. Woodman, G. R., & Robinson, N. D. (2013). Concrete Block Surfacing for Airfield Pavements. *Proceedings of the Institution of Civil Engineers: Transport, 117* (3), 168–176.
5. Karimova, A. A., & Paramonova, M. I. (2019). Damage and Repair of Artificial Runway Surfaces. *Alfabuild, 2* (9), 17–28.
6. Kulchitsky, V. A., Makagonov, V. A., Vasiliev, N. B., Chekov, A. N., & Romankov, N. I. (2002). *Airfield Pavements: A Modern View.* Physico-Mathematical Literature Publishing.
7. Ledenev, A. A., Perova, N. S., Vnukov, A. N., Kozodayev, S. P., Baranov, E. V., & Pertsev, V. T. (2021). Rapid Repair and Restoration of Airfield Pavement and Airfield Infrastructure Facilities. *Bulletin of the School of Engineering of FEFU, 3* (48), 115–123.
8. Leshitskaya, T. P., & Popov, V. A. (1999). *Modern Methods for Repairing Airfield Pavements.* MADI-TU.
9. *DBN V.2.2-XX:2022 Buildings and Structures. Aerodromes. Part I: Design. Part II: Construction.*
10. Material SIKA https://gcc.sika.com/en/construction/refurbishment/concrete-repair/sikagard-720-epocem.html.
11. Material MAPEI https://www.mapei.com/ua/uk/materialy-i-tekhnichni-rishennia

12. Material MAPEI https://www.mapei.com/ru/ru/produkty/spisok-produktov/opisanie-produkta/arb-10f.
13. Technologies Rapid set https://www.ctscement.com/datasheet/CEMENT_ALL_Datasheet_DS_024 _EN?c=&t=Professionals.

# Forecast of the development of the economy of Ukraine for the long term

**Viacheslav Kozachuk**
Candidate of Technical Science, Senior Research
Leading Researcher
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl avenue, 28 B, Kyiv, Ukraine
e-mail: k71419@ukr.net
ORCID: 0000-0002-0207-7461

**Oleh Movchan**
Candidate of Technical Science, Senior Research
Head of the center
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl avenue, 28 B, Kyiv, Ukraine
e-mail: alex-717@ukr.net
ORCID: 0000-0001-5245-7051

**Vadim Hrom**
Candidate of Military Science, Leading Researcher
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl avenue, 28 B, Kyiv, Ukraine
e-mail: Hrom_v@ukr.net
ORCID: 0009-0009-5415-9758

**Oleksandr Vodchyts**
Candidate of Technical Sciences, Associate Professor
Head of the Military Training Department
National Aviation University
03058, Lubomyr Huzar Avenue, 1, Kyiv, Ukraine
e-mail: agv64agv@gmail.com
ORCID: 0000-0002-3294-7632

**Oleh Tarasov**
Candidate of Military Sciences, Associate Professor
Associate Professor of the Military Training Department
National Aviation University
03058, Lubomyr Huzar Avenue, 1, Kyiv, Ukraine
e-mail: tarasovo@ukr.net
ORCID: 0000-0002-6763-8653

**Abstract.** The relevance of the study is determined by the fact that during combat operations (especially high-intensity ones), the Armed Forces of Ukraine inevitably suffer certain losses of airfields. As a result of the fire effect of rocket and bomb strikes, hard airfield runway surfaces suffer significant damage, which interferes with the reliable operation of aircraft. As a result, hard airfield surfaces require rapid restoration, and materials with fairly stringent requirements must be used. In recent years, modern modified building materials have begun to be offered for use in Ukraine, which allow significantly reducing the restoration time: provided that the work is properly organized, the time can be no more than 7–10 days, while the required values of the strength characteristics for compression and tension are fully achieved. The result of using such materials is to ensure a minor interruption in the functioning of the airfield (regular use of the runway), which in conditions of combat operations is a pressing issue for the Air Force of the Armed Forces of Ukraine.

The purpose of the article is the need to find new approaches to the repair of runways that are mechanically damaged during missile and bomb strikes, in a limited time using modern building materials.

Methodological approaches. The study is based on the analysis of existing data on modern building materials that can be used to repair runways, their physical and technical characteristics, and time indicators necessary to ensure the maximum strength of the materials used.

The authors have identified the main factors that affect the destructive processes of hard airfield surfaces in peacetime, which are natural influences, as well as loads during takeoffs and landings of aircraft. Among the operational factors, mechanical influences, as well as force and temperature influences of the gas jet of aircraft jet engines, should be highlighted. In case of detection of any damage to the runway surface, measures must be taken to eliminate them immediately, since otherwise there is a risk of accidental damage and closure of the strip for long-term repairs. But in case of detection of defects that threaten flight safety, they are eliminated immediately before their start. This is a very important issue regarding the operation of hard airfield surfaces: it determines the need to use such materials for the restoration of runways that have the shortest terms of acquiring the necessary values of operational characteristics of hard concrete surfaces.

Various materials can be used to perform repair work, but if there are two restrictions - the period before the start of operation and the duration of the work, then the most appropriate is the use of modern materials. Such repair materials must meet the requirement: materials in terms of strength must provide a bearing capacity not less than the existing airfield surfaces, and meet the established requirements for them.

The practical significance of the research results lies in determining materials for urgent runway repairs.

**Keywords:** rocket and bomb strikes, hard airfield surfaces, runway, loading, damage, repair, repair materials, bearing capacity, mineral binder, polymer binder.

The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 3 No. 2 (2025)

DOI: 10.62524/msj.2025.3.2.5

# російсько-українська війна як каталізатор змін у європейській системі ППО-ПРО: від американської підтримки до стратегічної автономії

**Андрій Гризо**
кандидат технічних наук, доцент
начальник науково-дослідної лабораторії
Харківський національний університет Повітряних Сил імені Івана Кожедуба
61023, вул. Сумська, 77/79, Харків, Україна
e-mail: a.hryzo@hups.mil.gov.ua
ORCID: 0000-0003-2483-5953

**Олександр Костиря**
доктор технічних наук, старший науковий співробітник
провідний науковий співробітник науково-дослідної лабораторії
Харківський національний університет Повітряних Сил імені Івана Кожедуба
61023, вул. Сумська, 77/79, Харків, Україна
e-mail: kostyria1958@gmail.com
ORCID: 0000-0003-3363-2015

**Іван Трофимов**
кандидат технічних наук, старший дослідник
професор кафедри
Харківський національний університет Повітряних Сил імені Івана Кожедуба
61023, вул. Сумська, 77/79, Харків, Україна
e-mail: tininterpritor@ukr.net,
ORCID: 0000-0001-7080-909X

**Анотація.** Актуальність дослідження обумовлена необхідністю трансформацій наявних систем протиповітряної та протиракетної оборони через їхню невідповідність новим типам загроз, які з'явилися під час широкомасштабної збройної агресії росії проти України. Масоване застосування крилатих і балістичних ракет, безпілотних систем та інших засобів ураження висвітлило дефіцит спроможностей системи протиповітряної оборони європейського континенту та обумовило потребу в її інтеграції і модернізації для забезпечення ефективного захисту об'єктів критичної інфраструктури й території країн Європи.

Метою роботи є визначення перспектив розвитку європейської системи протиповітряної та протиракетної оборони у контексті прагнення до стратегічної автономії і шляхів подолання викликів, які виникли під час російсько-української війни. У зв'язку із цим статтю спрямовано на визначення основних напрямів трансформації розвитку європейської системи протиповітряної та протиракетної оборони, аналіз впливу відповідних військово-політичних та економічних рішень на її розвиток. Особливу увагу приділено використаним формам та способам урахування українського досвіду інтенсивних бойових дій.

Провідним методом дослідження є системний аналіз, що дозволяє комплексно розглянути проблеми функціонування наявної європейської системи протиповітряної та протиракетної оборони. Для вивчення інформаційних матеріалів застосовано контент-аналіз. Для обґрунтування припущень та висновків – метод прогнозування та кількісний аналіз

статистичних даних.

У статті розкрито зміст основних заходів, спрямованих на підвищення можливостей європейської системи протиповітряної та протиракетної оборони у контексті врахування досвіду, набутого Повітряними Силами Збройних Сил України під час російсько-української війни. Розглянуто основні протиріччя та виклики, які при цьому виникають.

Матеріали статті становлять практичну цінність для військових експертів, аналітиків та осіб, відповідальних за ухвалення рішень у сфері оборони, їх може бути використано у плануванні закупівель систем оборонного призначення та розробленні концепцій їх застосування.

**Ключові слова:** протиповітряна оборона, протиракетна оборона, російсько-українська війна, європейська безпека, стратегічна автономія.

**Вступ (Introduction)**

Широкомасштабне вторгнення росії в Україну суттєво змінило безпекове середовище в Європі та виявило недосконаліть наявної європейської системи протиповітряної та протиракетної оборони (ППО-ПРО). Висока інтенсивність бойових дій на лінії розмежування військ і постійні обстріли важливих державних та військових об’єктів на всю глибину території України продемонстрували здатність агресора швидко адаптуватися, розробляти нові зразки озброєння, запозичувати вдалі технічні рішення та швидко масштабувати їх виробництво [1–3]. З метою досягнення військово-політичних цілей противник постійно випробовує нові тактичні прийоми застосування засобів повітряного нападу (ЗПН), зокрема масоване та комбіноване використання безпілотних літальних апаратів (БпЛА), крилатих ракет, інших високоточних засобів ураження, засобів радіоелектронної боротьби (РЕБ) повітряного та наземного базування, що змушує переглянути наявні підходи до побудови системи ППО-ПРО [2, 4].

Актуальність дослідження зумовлена необхідністю вивчення досвіду адаптації європейських систем ППО-ПРО до нових викликів та загроз, які обумовлені наслідками російсько-української війни. Досвід бойових дій показав, що системи ППО-ПРО європейських країн не відповідають сучасним вимогам та потребують суттєвого оновлення. Особливо гостро постало питання щодо захисту важливих державних та військових об’єктів від малорозмірних БпЛА, які здатні долати традиційні системи виявлення та ураження і “просочуватися” крізь систему ППО-ПРО через їх масове використання та мале значення ефективної поверхні розсіювання (ЕПР) [2, 3].

Крім того, суттєве занепокоєння в політичних колах європейських країн викликає можлива зміна безпекової ролі США у Європі. російсько-українська війна загострила дискусію щодо залежності європейської безпеки від американських гарантій та необхідності розвитку власних оборонних можливостей. Останні заяви та дії керівництва США підтверджують цю тенденцію.

Слід зазначити, що тенденція до зменшення військової підтримки європейських країн з боку США відзначалася політичними експертами багатьох країн Європи та світу ще до президентства Д. Трампа. Після його інавгурації почалися відкриті розмови щодо різних сценаріїв зменшення ролі США аж до виходу з блоку НАТО [5], зокрема тривають інтенсивні дискусії навколо ймовірної стратегії “сплячого” НАТО [6]. Планується, що за такого підходу США відмовилися б від фінансування Альянсу, активізація сил відбувалась би лише під час кризи. Ця модель передбачає зменшення кількості американських сил у Європі та трансформацію НАТО таким чином, щоб європейські країни мали переважну більшість звичайних сил, необхідних для стримування росії, покладаючись на США лише у питанні ядерного стримування.

Безперечно, що шляхом до посилення обороноздатності європейських країн є значне збільшення фінансових витрат на оборону. Європейська громадськість також відчуває цю загрозу: під час опитування Європейської ради з міжнародних відносин (ECFR), проведеного влітку 2024 року [7] в Україні та 14 інших європейських країнах, значна кількість респондентів оцінили можливий напад росії на іншу європейську країну протягом наступних двох років як “швидше ймовірний” або “дуже ймовірний”.

У дослідженнях [8, 9] зазначається, що однією з основних проблем європейської системи оборони є недостатня кількість засобів перехоплення, що особливо відчутно у випадку масованих атак з боку противника. Більшість систем розміщено навколо стратегічних об’єктів, тобто захист менш важливих регіонів залишається слабким, інтеграція різних національних систем ППО в єдину архітектуру стикається з низкою проблем та вимагає значних ресурсів і часу.

Європейські зусилля щодо інвестування в оборону різко прискорилися з початком російського вторгнення. Згідно з оцінками НАТО на 2024 рік країни – члени ЄС зараз витрачають на оборону на 150 мільярдів євро на рік більше, ніж у 2014 році. З огляду на високу вартість набуття оборонних спроможностей, доцільним є об’єднання зусиль задля прискорення спільного придбання або розроблення деяких відсутніх ключових стратегічних систем. Таким чином, збільшення витрат на власну військову промисловість та зменшення військової залежності від США є основною стратегією країн Європи [10].

Аналіз ставлення європейських експертів та політиків до зміни безпекової ролі США у Європі свідчить про зростаюче усвідомлення необхідності кооперації та розвитку власних оборонних можливостей, зокрема у сфері ППО-ПРО, за збереження трансатлантичної співпраці. Цей вектор безпосередньо впливає на формування європейської системи ППО-ПРО та визначає контекст її подальшого розвитку.

Метою дослідження є визначення перспектив розвитку європейської системи ППО-ПРО в контексті прагнення до стратегічної автономії та шляхів подолання викликів, які виникли під час російсько-української війни.

Наукова новизна роботи полягає в комплексному аналізі впливу російсько-української війни на трансформацію європейської системи ППО-ПРО. У дослідженні розширено теоретичні уявлення про взаємозв’язок між досвідом бойових дій в Україні та зміною підходів до формування багаторівневої системи ППО-ПРО в Європі, а також проаналізовано протиріччя між прагненням до стратегічної автономії та необхідністю інтеграції з системами блоку НАТО.

Теоретичне значення дослідження полягає у розширенні наукових уявлень про сучасні тенденції розвитку систем ППО-ПРО в умовах зміни характеру збройної боротьби. Результати роботи можуть стати підґрунтям для подальших досліджень у сфері військової безпеки та оборонного планування.

Практичне значення отриманих результатів визначається можливістю їх використання у плануванні закупівель систем ППО-ПРО та розробленні концепцій їх застосування. Висновки та рекомендації дослідження можуть бути корисними для військових експертів, аналітиків та осіб, відповідальних за ухвалення рішень у сфері оборони.

**Методологічна основа (Methodological Framework)**

Вирішення завдань дослідження вимагає комплексного підходу до аналізу військових, технологічних та політичних аспектів.

Методологічну основу дослідження становлять загальнонаукові методи, зокрема системний та порівняльний аналіз, прогнозування. Інформаційною базою дослідження слугували офіційні документи НАТО та ЄС, аналітичні матеріали провідних дослідницьких

центрів, публікації у фахових виданнях, а також відкриті джерела інформації про перебіг російсько-української війни.

Метод системного аналізу було використано від час розгляду європейської ППО-ПРО як цілісної системи зі взаємозв'язаними компонентами. Для зіставлення стану європейської системи ППО-ПРО до та після 2022 року застосовувався порівняльно-історичний підхід, що дозволило простежити еволюцію концепції оборони європейського континенту та політико-економічних підходів до її втілення. Проаналізовано взаємодію підсистем європейської системи ППО-ПРО у контексті сучасних загроз, оцінено вплив зовнішніх політичних та промислово-технологічних факторів на розвиток системи. Вивчення інформаційних матеріалів здійснювалося із застосуванням контент-аналізу. Для обґрунтування припущень та висновків використовувались метод прогнозування та кількісний аналіз статистичних даних.

До обмеження методології слід віднести:

- недоступність конфіденційних даних НАТО щодо результатів навчань, поточного стану та напрямів розвитку системи ППО-ПРО Європи;
- зміст уроків російсько-української війни визначався на підставі тільки інформації, яка є у відкритому доступі;
- можлива суб'єктивність висновків аналітичних публікацій та матеріалів дослідницьких центрів через лобіювання певних політичних позицій окремими дослідниками або організаціями;
- вплив динаміки війни в Україні та розвитку політичної ситуації у світі на актуальність висновків (наприклад, зміна політичних пріоритетів декількох розвинених країн світу).

**Результати (Results)**

Військові аналітики європейських країн, враховуючи досвід війни між росією та Україною, агресивних дій хуситів у Червоному морі та конфлікту між Ізраїлем і ХАМАС, відзначають суттєве вдосконалення тактики використання та технічних характеристик ракетного озброєння, БпЛА, гіперзвукових ракет і засобів РЕБ [9, 11]. Унаслідок цього вимоги до європейської системи ППО-ПРО значно зросли, тоді як її поточний стан не відповідає сучасним викликам.

Значна частина дослідників вважають, що використання БпЛА на полі бою та за його межами докорінно змінюють методи ведення бойових дій завдяки їхнім невеликим розмірам, низькій собівартості, здатності здійснювати політ на малій висоті та значному руйнівному потенціалу [12, 13]. У партнерів та країн – членів НАТО зростає занепокоєння через можливість прориву або знищення ключових елементів систем ППО-ПРО США та Європи за допомогою комбінованих атак.

Ключову загрозу становить здатність БпЛА долати систему ППО-ПРО супротивника шляхом ураження її елементів або шляхом прихованого "просочування", уникаючи виявлення засобами розвідки. Вважається, що поєднання можливостей БпЛА та РЕБ змінює співвідношення сил та засобів на користь наступальних дій, роблячи протиповітряну оборону структурно вразливою.

Перші аналітичні оцінки дій Повітряних Сил (ПС) Збройних Сил (ЗС) України з боку іноземних експертів почали з'являтися майже одразу після початку війни. На підставі цих досліджень було зроблено висновки щодо ефективності та можливостей національних систем ППО-ПРО в умовах сучасного бойового середовища, визначено доцільність подальшого впровадження наявних концепцій та необхідності розроблення нових.

На підставі вивчення офіційних документів НАТО та ЄС, публікацій провідних дослідницьких центрів та фахових видань, а також відкритих джерел інформації про перебіг російсько-української війни наведено висновки щодо перебігу російсько-українського конфлікту, шляхи та приклади їх урахування при подальшому розвитку європейської системи

ППО-ПРО. Інформацію згруповано за дев'ятьма основним напрямами.

*1. Концепція гнучкого бойового застосування.*

Одним із головних уроків російсько-української війни є успішний досвід адаптації дій частин та підрозділів ПС ЗС України з метою зменшення ефективності ударів ЗПН та підвищення захищеності елементів військової та критичної інфраструктури. Така стратегія ґрунтується на:

- мобільності елементів системи ППО, що ускладнює прогнозування їхніх дій противником;
- розосередженні, що, особливо на початку війни, дозволило уникнути ударів ЗПН та значно скоротило втрати серед техніки та персоналу;
- адаптивності до змін тактики дій противника та появи нових ЗПН, що передбачає пошук і швидке впровадження у практику військ вдалих рішень, апробованих у бойових умовах.

Цей урок знайшов відображення у розвитку концепції "Гнучкого бойового застосування" (Agile Combat Employment, ACE), ухваленої ВПС США 23.08.2022 року, яка також застосовується у НАТО та передбачає використання багатьох географічно розосереджених баз (включаючи цивільні аеродроми та автотраси) для забезпечення гнучкості й стійкості управління і збереження бойового потенціалу. Зазначається, що такий підхід особливо актуальний за наявності у противника можливостей з масованого застосування високоточної зброї (ВТЗ). Зміст основних заходів концепції залежно від стану напруженості наведено у табл. 1.

**Таблиця 1.** Зміст основних заходів у рамках концепції ACE

| Стан політичного середовища | Зміст основних заходів |
|---|---|
| **Співпраця** | - створення постійних і додаткових угод із країнами-партнерами, які дозволяють: проліт територією, безпосередню координацію із силами оборони країни перебування, розміщення витратних матеріалів, обладнання тощо;<br>- організація, навчання та оснащення сил та засобів для реалізації концепції ACE;<br>- набуття взаємосумісності із союзниками та партнерами. |
| **Протистояння** | - проведення операцій ACE та демонстрація спроможностей спільно із союзниками та країнами-партнерами, як активний засіб стримування конфлікту;<br>- збереження свободи доступу та маневру. |
| **Конфлікт** | - забезпечення неперервного бойового застосування та логістики за умов вогневого впливу противника;<br>- ускладнення противнику циклу спостереження – аналіз – рішення – дії;<br>- збереження бойового потенціалу;<br>- нарощування бойової потужності. |

Використання концепції ACE під час проведення операцій дає змогу спиратися не на централізовану інфраструктуру, а на функціональні кластери менших розмірів, які розосереджені по різних локаціях. Такий підхід може ускладнити противнику планування, підвищити стійкість до вогневого впливу і надати більше можливостей із застосування своїх підрозділів.

Концепція насамперед застосовується в авіації, але її принципи є корисними в інших галузях військової справи. Фактично йдеться про ефективне використання наявних ресурсів та сил шляхом розосередження і підвищення мобільності, що дозволяє швидко адаптуватися до змінних умов та підвищувати ефективність операцій. Загальну структуру та рівні інтеграції ACE наведено на рис. 1.

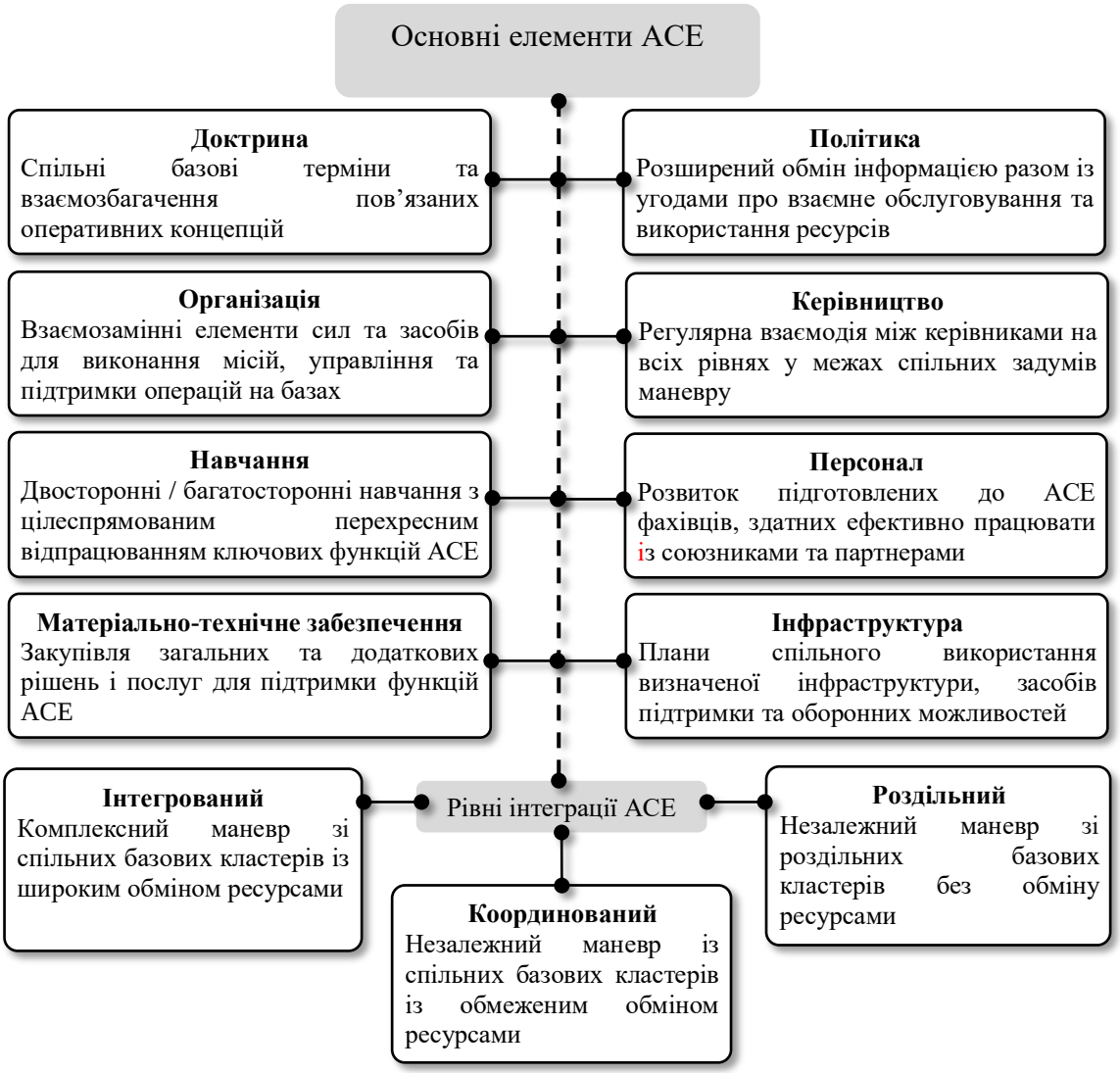



**Рисунок 1.** Елементи ACE та рівні інтеграції

Відзначається, що хоча підготовка до дій у рамках ACE зазвичай спрямована насамперед на розвиток технічних та функціональних навичок, важливим напрямом є розвиток мовних, культурних та інших навичок, які можуть забезпечити ефективну інтеграцію сил. Як приклад, ВПС США пропонують програму для льотчиків, щоб покращити знання мови, регіональних традицій та культури ключових партнерів. [14].

Протягом 2023–2024 років було проведено низку практичних заходів щодо набуття спроможностей, необхідних для втілення цієї концепції, зокрема, у 2023 році Командування повітряних сил НАТО провело свій другий симпозіум щодо моделі ACE НАТО, об'єднавши міжнародні зацікавлені сторони для обговорення отриманих уроків, еволюції та шляхів розвитку концепції. Штаб ВПС США 27–28.02.2024 року провів конференцію Agile Combat Employment Interoperability and Integration за участю семи союзників і партнерів. Практичне відпрацювання дій з метою апробації та навчання відбувалось під час інтенсивних навчань, основні з них:

- спільні навчання ВПС Чехії та Франції 25–29.11.2024 року з практичного відпрацювання дій у розосереджених операціях;

- у листопаді 2024 року ВПС Франції провели навчання за концепцією ACE, розгорнувши винищувачі Rafale на базах у Німеччині та Хорватії [15]. Ця операція дозволила відпрацювати питання щодо розгортання, підготовки, обслуговування та бойового застосування літаків з віддалених місць під керівництвом НАТО;

- 30 січня 2024 року естонські та голландські військові провели навчання за концепцією ACE на авіабазі Амарі в Естонії. Ця операція включала участь винищувачів F-35 та була спрямована на розвиток компетенцій у сфері обслуговування сучасних літаків.

*2. Інтеграція систем ППО.*

Другим важливим уроком, як відзначають військові експерти, є необхідність інтеграції різних систем ППО-ПРО для створення єдиного розвідувально-інформаційного простору та єдиної зони вогневого впливу (Kill zone). Йдеться про досвід, набутий ПС ЗС України з інтеграції різних систем озброєння, зокрема радянського виробництва розробки 80-х років минулого століття, сучасних вітчизняних та іноземних зразків, які тільки починають вироблятися серійно. Корисним досвідом є адаптація ЗРК та літаків радянського виробництва до використання сучасних керованих ракет. Прикладом є так званий проєкт FrankenSAM, який передбачає використання західних ракет, таких як AIM-9M Sidewinder та RIM-7 Sea Sparrow ЗРК радянського виробництва, зокрема “Бук-М1” [16].

Керівництву ПС ЗС України вдалося створити територіально розподілену, багатошарову систему виявлення ЗПН, яка дозволяє поєднувати інформацію різних джерел – від спостерігачів до сучасних багатофункціональних РЛС. Системи РЕБ та вогневого впливу побудовані за схожими принципами та забезпечують радіоелектронний і вогневий вплив протягом усього маршруту польоту ЗПН у всьому діапазоні висот. Зокрема, для ураження ЗПН застосовуються як засоби дальньої дії, наприклад, ЗРК Patriot, так і надмалої дальності, наприклад, ЗРК Hawk та мобільні вогневі групи, озброєні великокаліберними кулеметами.

У відповідь на ці виклики НАТО вже розробляє програму сучасної, оперативно-сумісної, здатної до різноманітних дій та надійної системи на 2035 рік і на подальші роки. Зразком такої системи є інтегрована система ППО-ПРО НАТО (Integrated Air Defence System, IAMD), положення про яку НАТО вперше оприлюднило 13.02.2025 року. Взаємодія різних її компонентів забезпечує ефективний захист від сучасних повітряних загроз. Прийнята архітектура поєднує національні елементи та технології НАТО, що вимагає високої інтеграції, адаптивності та надійності.

Європейські військові експерти, взявши до уваги аналіз можливостей росії, досвід російсько-української війни, географію та стратегічну глибину Європи, виділяють два важливих фактори [8, 9, 17].

По-перше, визначається, що не може бути всеосяжного захисту від російських високоточних ударів. На думку експертів, стратегічне значення ППО-ПРО в мирний час або в загрозливий період полягає в посиленні стримування. Це пояснюється тим, що такі системи створюють для агресора невпевненість щодо результату атаки. Вони також збільшують кількість засобів озброєння, необхідних для атаки, більш масштабна атака означає більший ризик ескалації, що може бути стримуючим фактором для агресора. У разі військового конфлікту система ППО-ПРО створює надійний захист важливих державних та військових об’єктів від ударів з повітря, що забезпечує підтримку спроможностей військ.

По-друге, немає універсального рішення проти можливостей різноманітних російських засобів дальньої дії. Потрібна архітектура ППО-ПРО з високим рівнем інтеграції її елементів, яка об’єднує різні взаємосумісні системи виявлення, центри управління, системи передачі даних та системи озброєння у всіх вимірах і, в ідеалі, узгоджує їх таким чином, щоб створювати рівні та домени, що взаємно перекриваються.

Складовими елементами IAMD є різні національні системи ППО-ПРО. Теоретично це досягається не лише за рахунок сумісності самих систем, а й за допомогою оперативно-

сумісних та ефективних структур управління боєм, зв'язку та C2 (Command and Control), таких як система повітряного командування та управління НАТО (ACCS, Air Command and Control System). Відомості щодо вогневих засобів системи ППО-ПРО, які були придбані країнами Європи, наведено у табл. 2.

**Таблиця 2.** Ключові засоби ураження системи ППО-ПРО, які були придбані країнами Європи у період з 2018 року по 2023 рік

| Країна | Засіб ураження | Категорія | Стан | Рік |
|---|---|---|---|---|
| Швеція | Patriot PAC-2, 3 | ЗРК великої дальності | Поставлено | 2018 рік |
| Польща | Patriot PAC-3 | ЗРК великої дальності | Поставлено | 2018 рік |
| Норвегія | IRIS-T | Самохідний ЗРК малої дальності | Поставлено | 2019 рік |
| Угорщина | NASAMS III | ЗРК малої дальності | Поставлено | 2020 рік |
| Франція, Італія | SAMP/T NG | Самохідний ЗРК великої дальності | Поставлено | 2021 рік |
| Чехія | Spyder-MR | Самохідний ЗРК середньої дальності | Поставлено | 2021 рік |
| Польща | CAMM (Narew) | ЗРК малої дальності | Поставлено | 2022 рік |
| Німеччина | IRIS-T SLM | Самохідний ЗРК середньої дальності | Поставлено | 2023 рік |
| Німеччина | Arrow-3 | Пускова наземна установка ракет ПРО | Очікується поставка у IV кварталі 2025 року | 2023 рік |
| Фінляндія | "David's Sling" ("Праща Давида") | ЗРК середньої дальності | Підписано угоду між Фінляндією та Ізраїлем. Терміни поставки та розгортання не розголошуються | 2023 рік |
| Естонія, Латвія | IRIS-T SLM | ЗРК середньої дальності | Розпочато виробництво компонентів. Перші системи IRIS-T SLM мають надійти до Латвії та Естонії у 2026 році | 2023 рік |
| Польща | Patriot PAC-3 | ЗРК великої дальності | Поставлено 2 батареї ЗРК Patriot із 8 замовлених. Локалізація виробництва | 2023 рік |

Оборонні установи НАТО також досягли різноманітних домовленостей про співпрацю для покращення можливостей IAMD, але їхня імплементація потребує вирішення проблем взаємодії, інтеграції та політичного узгодження.

*3. Розроблення власних систем ППО.*

З початком війни ПС ЗС України відчули гостру нестачу сучасних систем ППО, виробничих потужностей для відновлювального ремонту та обслуговування як систем іноземного виробництва, так і вітчизняного [9, 10, 18]. Украй недостатньо було зенітних керованих ракет. Наприклад, наявні ЗРК С-300 та Бук-М1 не могли протидіяти застосуванню балістичних ракет. ЗРК Patriot здатний знищувати балістичні ракети завдяки ракетам PAC-3 та MSE, але кількість таких ЗРК обмежена, крім того, є залежність від поставок ракет.

Зважаючи на цей урок, президент Єврокомісії Урсула фон дер Ляєн у 2024 році оголосила про плани збільшення виробництва озброєнь у Європі, що може позитивно вплинути на розвиток власних систем ППО країн – членів ЄС. У 2025 році Європейська комісія виділила понад 1 мільярд євро для підтримки розвитку критичних оборонних технологій та можливостей у рамках програми європейського оборонного фонду (European Defence Fund, EDF). Ці інвестиції спрямовані на посилення обороноздатності Європи та підтримку інновацій у сфері оборони.

Яскравим прикладом розроблення власних систем ППО є:

- SAMP/T: французько-італійський комплекс, який може знищувати балістичні ракети

завдяки ракетам Aster-30, є аналогом системи Patriot і використовується для захисту об'єктів від різних повітряних загроз, включаючи балістичні ракети;

- IRIS-T SLM: німецький зенітно-ракетний комплекс середньої дальності, розроблений компанією Diehl Defence. Компанія планує збільшити виробництво комплексів IRIS-T до 10 батарей на рік, що свідчить про зростання потенціалу виробництва цієї системи.

Аналіз нещодавнього придбання країнами НАТО систем ППО-ПРО (табл. 2) висвітлює дві серйозні проблеми – час і вартість. Термінові потреби для забезпечення спроможностей IAMD були визначені ще у 2022 році, а поставки замовлених зразків озброєння кінцевим користувачам відбудуться через кілька років. Зокрема, батареї Patriot, замовлені Польщею в 2018 році, почали надходити в країну лише наприкінці 2022 року. Із замовлених у 2023 році 8 батарей поставлено лише 2, інші 6 планується поставити протягом 2025 року.

Водночас вартість сучасних систем ППО-ПРО достатньо висока. Системи малої та середньої дальності, такі як IRIS-T і NASAMS, коштують сотні мільйонів доларів США. Захист від балістичних ракет великої дальності коштує мільярди доларів США.

Окрім вартості самої системи слід враховувати вартість ракет, які є витратним ресурсом, що потребує своєчасного поповнення із запасів, які треба створювати заздалегідь. Орієнтовну вартість ракет до систем ППО-ПРО наведено у табл. 3. Вартість розраховано за даними у відкритих джерелах або за інформацією про обсяг та вартість контракту. Умови та послуги, що входять до контракту, зазвичай не розголошуються, тому реальна вартість може відрізнятися від вказаних значень.

З огляду на те, що лише чотири з 29 європейських країн – членів НАТО наразі витрачають на оборону понад 30 мільярдів доларів США, це великі витрати, які можуть дозволити собі небагато держав.

*4. Співпраця між європейськими країнами*

Успішна співпраця України з країнами-партнерами щодо постачання озброєння та інформації, логістичної підтримки, ремонту й навчання персоналу є важливим уроком російсько-української війни.

Сусідні держави, у томі числі й європейські, як правило, вразливі до одних і тих самих ракетних загроз. Історично такі міркування спонукали до оборонної співпраці між державами і це обґрунтування також мотивувало до співпраці у рамках IAMD НАТО. Мабуть, найамбітнішим проєктом IAMD зі співпраці є Європейська ініціатива European Sky Shield Initiative (ESSI), що була запропонована Німеччиною в серпні 2022 року [19, 20], ESSI має на меті розбудову європейської системи ППО-ПРО шляхом спільного придбання систем з акцентом на готових можливостях, їхній сумісності та інтеграції.

На сьогодні до ініціативи приєдналася 21 країна (43% від кількості країн Європи), як основна перевага розглядається можливість економії під час проведення закупівлі великого обсягу. Передбачається, що у подальшому співпраця поширюється на логістику, технічне обслуговування та навчання. Мета ініціативи – скорочення витрат і швидке набуття можливостей шляхом якнайшвидшої закупівлі великої кількості систем ППО-ПРО та включення їх до IAMD НАТО.

Як критична потреба відзначається захист ближньої та дуже близької зони. Задля усунення цих загроз розроблено концепцію перспективної німецької системи військової ППО LVS NNbS (Luftverteidigung durch das Luftverteidigungssystem Nah- und Nächstbereichsschutz, "Протиповітряна оборона малої дальності та ближньої дії"). Практичну реалізацію концепції доручено консорціуму з трьох компаній Rheinmetall, Hensoldt і Diehl [8, 9, 20].

European Sky Shield Initiative (рис. 2) дотримується багаторівневого підходу, зосереджуючись насамперед на наземній системі ППО-ПРО.

**Таблиця 3.** Орієнтовна вартість ракет до систем ППО-ПРО

| Назва | Вартість, дол. |
|---|---|
| Next Generation Interceptor (NGI) | 111 000 000 |
| Ground Based Interceptor (GBI) | 70 000 000 |
| Standard Missile 3 (SM-3) Block IIA | 27 915 600 |
| Standard Missile 3 (SM-3) Block IB | 9 698 600 |
| Standard Missile 6 (SM-6) | 3 901 880 |
| Patriot PAC-3 | 3 729 700 |
| Arrow 3 | 62 000 000 |
| Standard Missile 2 (SM-2) Block IV | 2 100 000 |
| Aster 30 (SAMP-T) | 2 000 000 |
| Meteor BVRAAM | 2 398 000 |
| Evolved Sea Sparrow Missile (ESSM) | 2 031 800 |
| NASAM AMRAAM 120 | 1 200 000 |
| Rolling Airframe Missile (RAM) | 921 300 |
| 48N6 (S-300) | 1 000 000 |
| BARAK-8 | 553 400 |
| IRIS-T | 450 000 |
| NASAM AIM-9X | 400 000–500 000 |
| Mistral M3 | 545 600 |
| Aspide Mk1/Mk2 | 100 000 |
| Stinger Missile/ ПЗРК | 480 000 |
| APKWS Missile/ ПЗРК VAMPIRE | 30 000–50 000 |
| Tamir (Iron Dome) | 20 000–100 000 |
| C-RAM (вартість одного залпу 70–100 снарядів) | 8 100 |
| Directed Energy (Iron Beam) (вартість електроенергії на один постріл) | 3.50 |

Виділяють чотири рівні перехоплення із запланованими до складу такими системами:

1. Малий радіус дії: Skyranger 30.
2. Середній радіус дії: переважно IRIS-T SLM.
3. Великий радіус дії: MIM-104 “Патріот”.
4. Дуже великий радіус дії (екзоатмосферний шар): Arrow-3.

Ініціативи типу ESSI хоча й мають певні проблеми з підтримкою, однак можуть стати кроком до спільної закупівлі та розвитку систем ППО-ПРО країн Європи. Такі спільні проєкти можуть підвищити ефективність використання ресурсів та створити єдину європейську систему ППО-ПРО.

Розглянута ініціатива ще є на початковому етапі й країни-учасниці ще мають чітко визначити її цілі, масштаби та механізми. Наприклад, не зрозуміло, чи буде ESSI сприяти спільному розвитку нових можливостей і придбанню наявних систем, і якщо так, то як вона збалансує ці два підходи. Інше відкрите питання полягає у тому, як будуть узгоджуватися та координуватися між усіма державами-учасницями конкретні вимоги до можливостей системи.

Заявлена мета керівництва Німеччини полягає у тому, щоб якнайшвидше поставити на озброєння більше систем ППО-ПРО, інтегрувати їх до IAMD НАТО та спонукати інші країни-учасниці зробити те саме під егідою ESSI. Німеччина пропонує IRIS-T SLM і Patriot як “офіційні” системи ESSI та які будуть придбані в рамках ESSI. Крім того, Німеччина купує систему ПРО Arrow 3 в ізраїльської компанії IAI, яку було розроблено спільно з США.

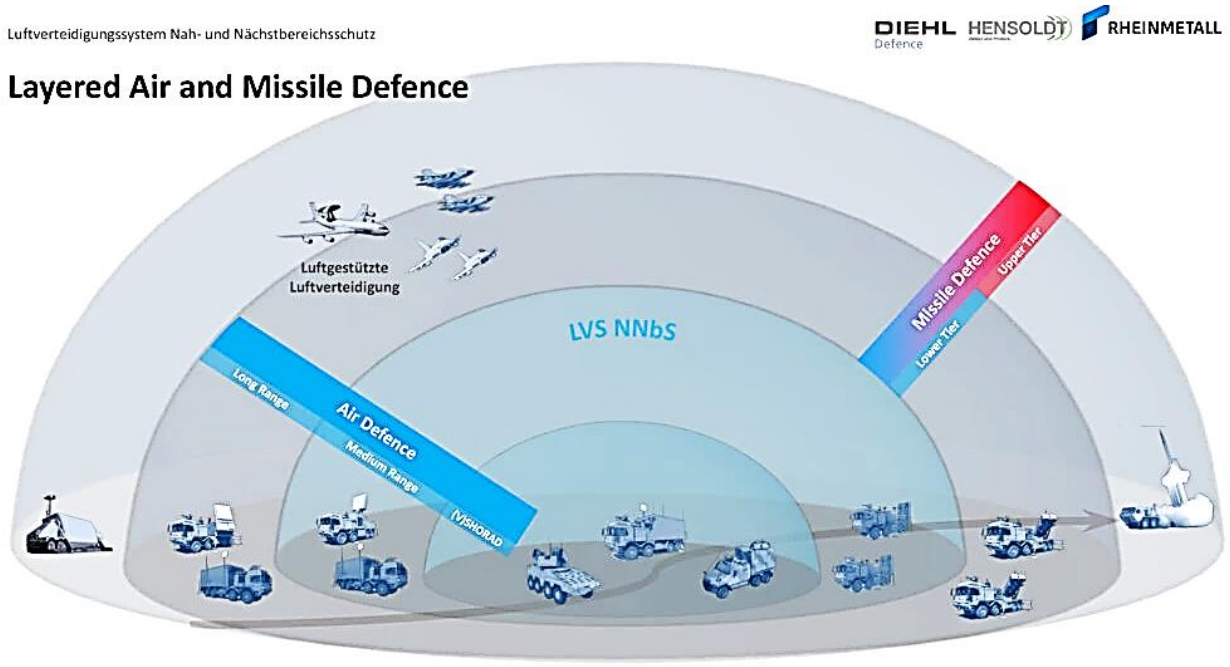



**Рисунок 2.** Ілюстративна модель ESSI

Такий підхід не підходить тим країнам, які вже використовують інші системи в цих категоріях або вже ухвалили рішення про їх закупівлю. Це Франція та Італія з їхніми системами SAMP/T, а також Польща, яка нещодавно закупила у Великої Британії систему ближнього радіуса дії Sky Sabre, як альтернативу IRIS-T. Однак більш вагомими є політичні фактори, Франція вже давно виступає за європейську "стратегічну автономію", яка передбачає надання переваг та підтримку європейської оборонної промисловості. Очевидно, що французька концепція пріоритетності європейської промисловості утворює протиріччя з цілями ESSI, які засновані на "прагматичних рішеннях" і "швидкому прогресі", та надає перевагу системам, які виробляються серійно і готові до розгортання, а не витратам ресурсів і часу на довгострокові та дорогі програми розроблення.

Країни Європи докладають значних зусиль з метою поглиблення співпраці. Зокрема,19.11.2024 року на рівні міністрів оборони вперше підписано листи про співпрацю держав – членів ЄС у чотирьох сферах: інтегрована ППО-ПРО – 18 країн; радіоелектронна боротьба – 17 країн; баражуючі боєприпаси – 14 країн; бойове надводне судно – 7 країн.

*5. Протидія сучасним загрозам*

Мабуть, найбільш важливим уроком російсько-української війни є масоване та комбіноване використання росією крилатих, балістичних та гіперзвукових ракет, а також ударних БпЛА, що вимагає нових підходів до організації захисту.

Відповіддю на ці виклики є майбутня інтеграція до системи ППО-ПРО європейського континенту високоточних систем ПРО дальньої дії, таких як Arrow 3, та розвиток існуючого у рамках Європейського поетапного адаптивного підходу (European Phased Adaptive Approach, EPAA) щодо розгортання системи ПРО в Європі для захисту від балістичних ракет середньої та малої дальності.

Основні характеристики EPAA:

- головна мета – захист країн НАТО від загрози застосування противником ВТЗ;
- гнучкість та поетапне розгортання: система з відкритою архітектурою, модернізація проводиться у кілька етапів;
- інтеграція з НАТО: система будується як частина системи протиракетної оборони НАТО (Ballistic Missile Defence, BMD).

Основні компоненти ЕРАА:

- РЛС AN/TPY-2 – розгорнута в Туреччині для раннього виявлення ракет;
- ракети-перехоплювачі SM-3 – базуються на кораблях Aegis BMD у Середземному морі та наземних комплексах Aegis Ashore (в Румунії та Польщі);
- система управління та контролю C2BMC – інтегрує ЕРАА з системами ПРО США та НАТО.

Етапи розвитку ЕРАА:

- Фаза 1 (2011): РЛС у Туреччині та кораблі Aegis у Середземному морі;
- Фаза 2 (2016): База Aegis Ashore у Румунії (SM-3 Block IB);
- Фаза 3 (2023–2025): База Aegis Ashore у Польщі (SM-3 Block IIA);
- Фаза 4 (скасовано): передбачала модернізацію для перехоплення МБР.

Основні елементи ПРО НАТО європейського континенту наведено у табл. 4.

**Таблиця 4.** Протиракетна оборона НАТО – основні елементи та національні внески після російського вторгнення в Україну

| Система | Підтримка проєкту | Оператор/ розміщення | Опис |
|---|---|---|---|
| Бойові кораблі із системою Aegis | США | Іспанія/ Рота | З 2014 року на військово-морській базі в Роті розміщено чотири американські есмінці класу Arleigh Burke з Aegis BMD для забезпечення ПРО Європи в рамках (ЕРАА). У 2022 році США оголосили про збільшення контингенту до шести кораблів. |
| Наземна версія ПРО Aegis Ashore | США | Румунія/ Девеселу | Діє з 2016 року, будівництво в рамках ЕРАА. Використовує ракети SM-3 Block IB для перехоплення ворожих ракет. Є ключовим елементом ЕРАА Phase 2. |
| Наземна версія ПРО Aegis Ashore | США | Польща/ Редзіково | Діє з 2023 року, будівництво в рамках ЕРАА. Оснащена найновішими ракетами SM-3 Block IIA, що мають збільшену дальність і точність. Частина ЕРАА Phase 3, забезпечує додатковий захист Європи. |
| Радар AN/TPY-2 | США | Туреччина/ Куречік | Розгорнута в Туреччині з 2011 року як частина ЕРАА, дозволяє відстежувати балістичні ракети та попереджати про них. |
| Командування та контроль, управління боєм і зв'язок (C2BMC) | США | Німеччина/ Рамштайн | У рамках ЕРАА програмне забезпечення C2BMC System інтегрує засоби ПРО США Aegis у Європі з радаром AN/TPY-2 у Туреччині. |
| Командний центр ПРО НАТО | НАТО | Німеччина/ Рамштайн | Штаб повітряного командування об'єднаних збройних сил НАТО розташований на базі ВПС США Рамштайн і включає Оперативний центр повітряного контролю та ПРО. |
| *Розгортання військ Альянсу після широкомасштабного вторгнення росії в Україну у 2022 році* | | | |
| Система ППО-ПРО Patriot *(2022–2023)* | Німеччина | Польща | У січні 2023 року Німеччина почала розміщення трьох батарей Patriot на польсько-українському кордоні для захисту польської території та посилення східного флангу НАТО. Рішення про розміщення батарей Patriot було ухвалено у зв'язку з підвищеною напруженістю в регіоні через війну в Україні та для зміцнення оборонних можливостей Польщі, а також для посилення колективної безпеки НАТО, зокрема на східному фланзі Альянсу. |
| Система ППО-ПРО Patriot *(2022–2023)* | Німеччина | Словаччина | У рамках двонаціональної німецько-голландської групи ППО-ПРО (BAMDTF) навесні 2022 року для захисту території Словаччини та посилення східного флангу НАТО Німеччина та Нідерланди розгорнули три батареї Patriot. Розгортання BAMDTF відбувалось під німецьким керівництвом та координацією, хоча в групі також беруть участь Нідерланди |
| Система ППО-ПРО Patriot *(2022–2023)* | Нідерланди | Словаччина | |
| Система ППО-ПРО SAMP/T (МАМБА) | Франція | Румунія | Розгорнута навесні 2022 року система призначена для захисту французьких та інших сил НАТО, розгорнутих у Румунії у складі бойових груп посиленої передової присутності НАТО. |

На додаток до можливостей, орієнтованих на стратегію США щодо розгортання системи ПРО в Європі EPAA, кілька членів Альянсу використовують системи ППО-ПРО меншої дальності (ЗРК Patriot), здатні нейтралізувати тактичні балістичні ракети. Хоча теоретично вони були доступні НАТО завдяки тому, що члени Альянсу мали їх на своєму озброєнні, невідомо, чи були вони повністю інтегровані у структуру ПРО НАТО.

Щодо боротьби з БпЛА різних класів прикладом розвитку є перспективна німецька система військової ППО LVS NNbS, яка є частиною ESSI (рис. 2). Передбачається, що система LVS NNbS зможе забезпечити об'єктову та зональну систему ППО. При цьому застосування нових мобільних елементів системи може надати відомі переваги експлуатаційного та оперативного характеру. Працюючи у складі єдиної системи ППО, нові елементи системи повинні будуть виявляти та знищувати широкий спектр ЗПН на відстанях до 40 км та висотах до 20 км.

"Дальнім ешелоном перехоплення" в такій системі будуть комплекси IRIS-T SLM, які будуть оснащені відповідними РЛС та зенітними керованими ракетами (ЗКР). Наступний рубіж оборони будуватиметься на основі самохідного комплексу FlaRakPz із дальністю ураження до 15 км, а захист ближньої зони буде забезпечуватися зенітною самохідною установкою (ЗСУ) Skyranger 30 із 30-мм гарматою (рис. 3).

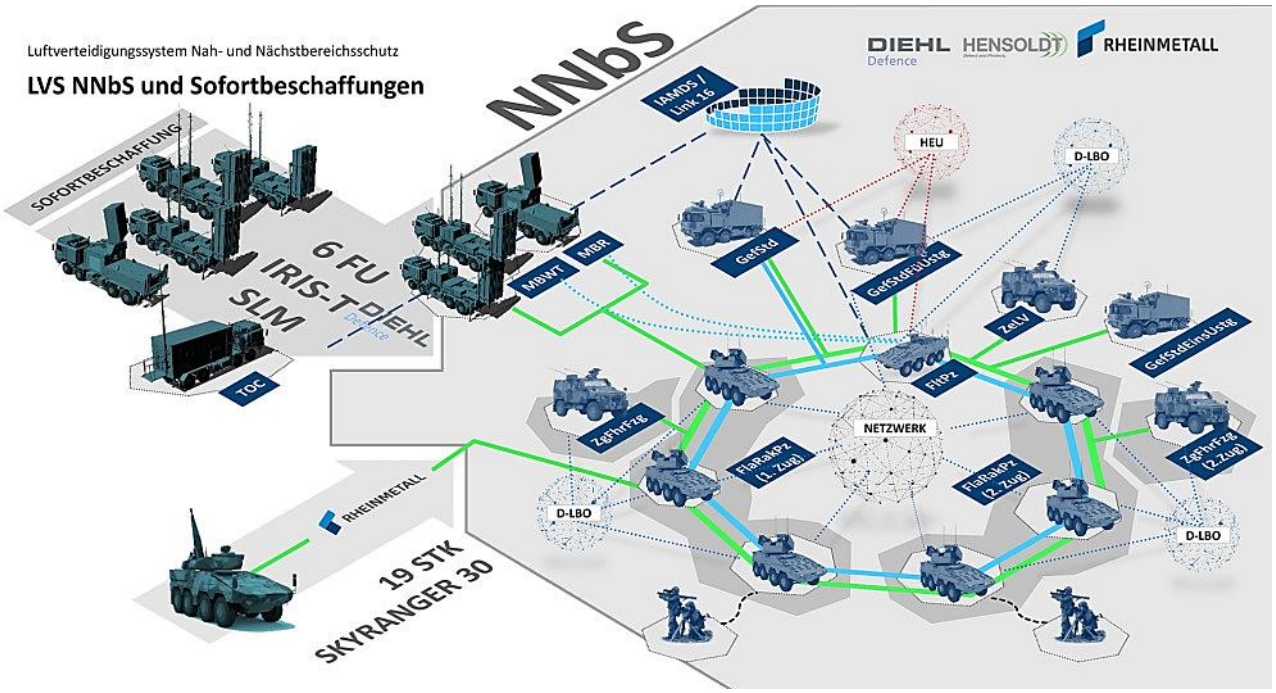



**Рисунок 3.** Схема перспективної німецької системи військової ППО LVS NNbS

Така система ППО зможе боротися з усіма сучасними та перспективними ЗПН. Літаки, крилаті ракети тощо пропонується вражати ЗКР, а для боротьби з ударними (розвідувальними) БпЛА та іншими подібними об'єктами в систему включено гарматну ЗСУ. При цьому система LVS NNbS зможе здійснювати взаємодію з іншими засобами ППО.

Передбачається, що окремі компоненти систем озброєння з'єднуються між собою за допомогою радіо- або оптоволоконних кабелів і обмінюються даними про повітряну обстановку. Управління, як правило, здійснюється зі стаціонарного командного пункту (GefStd) або з бронемашини управління вогнем (FltPz) з тими самими функціями у складі мобільного угруповання військ. Зв'язок із зовнішніми мережами встановлюється через

командний пункт підтримки управління (GefStsFüUstg), це може бути використано, наприклад, для зв'язку з національними системами ППО країни базування або з вищими командними пунктами.

*6. Диверсифікація постачальників та інвестиції у власну промисловість.*

Україна значною мірою залежить від військової допомоги США та інших західних країн. Перебіг війни показав, що західні партнери часом вагаються щодо надання певних видів зброї, що може бути критично важливим у військових операціях. Натомість росія налагодила постачання зброї від таких країн, як Іран та Північна Корея, що забезпечило їй стабільний потік озброєння. Війна підкреслила ризики залежності від імпорту критичних матеріалів і технологій, критичну важливість посилення власної промислової бази через модернізацію оборонної промисловості, підвищення готовності до тривалих конфліктів та розвиток новітніх технологій подвійного призначення. Українська програма BRAVE1 стала прикладом того, як уряд може сприяти розвитку стартапів і швидкому впровадженню нових рішень [21].

США відіграють ключову роль у забезпеченні оборони європейського регіону, водночас останнім часом низка європейських політиків висловлювали занепокоєння щодо дій США, які можуть вплинути на їхню роль як надійного партнера з оборони. На тлі останніх новин європейські військові експерти відзначають, що роль США, як лідера у набутті Європою спроможностей з ПРО, створює вразливість, якщо пріоритети США щодо європейської безпеки зміняться.

Агресія росії в Україні підкреслила важливість швидкого та стабільного постачання ракет-перехоплювачів у воєнний час, коли противник має великі запаси крилатих і балістичних ракет. Хоча ПС ЗС України успішно протистояли низці російських загроз, у тому числі аеробалістичним ракетам Х-47М2 АРК "Кинджал", це сталося ціною скорочення запасів як західних, так і радянських ракет-перехоплювачів. Країни – партнери України вживають заходів для запобігання цьому, зокрема, окрім надання додаткових пускових установок і ракет, ЄС інвестує в розвиток української оборонної промисловості, наприклад, норвезька компанія Kongsberg Defense & Aerospace планує розгорнути виробництво ракети NASAMS в Україні.

Дуже важливим є приклад Франції, яка послідовно демонструє незалежність у сфері технологій, постачаючи власні ракети та супутниковий зв'язок для України; створила та виробляє винищувач п'ятого покоління Rafale, власні системи ППО-ПРО, такі як SAMP/T. Франція володіє незалежними силами ядерного стримування та розвиненою атомною енергетикою, незалежними військовими засобами зв'язку та супутниками розвідки.

Великим потенціалом володіє Німеччина: компанія Rheinmetall є одним з найбільших виробників військової техніки в Німеччині та Європі. Вона виробляє танки Leopard, бойові машини Marder, Boxer, Fuchs та інші військові системи. Німецька оборонна компанія Rheinmetall у травні 2024 року офіційно "зайшла" в оборонно-промисловий комплекс України, створивши з акціонерним товариством "Укроборонпром" спільне підприємство у бронетанковій сфері. Загалом Rheinmetall планує побудувати в Україні чотири заводи – один вже працює, ще три на різних стадіях реалізації.

Важливим є досвід Польщі, яка активно працює над розширенням своїх можливостей з ППО через співпрацю зі США та іншими країнами НАТО. У майбутньому очікується подальше посилення військової інфраструктури країни завдяки внутрішньому виробництву складових частин систем захисту повітряного простору. Зокрема, у червні 2024 року польський оборонний підрядник Wojskowe Zaklady Lotnicze № 1 (WZL-1), який належить до державної групи PGZ, розпочав виробництво транспортно-пускових контейнерів для ракет PAC-3 MSE системи Patriot. Компанія відзначає високий попит на ці контейнери і розглядає можливість збільшення виробництва. Поточна потужність дозволяє виготовляти близько 150 контейнерів на рік.

У серпні 2024 року Польща підписала угоду з американською компанією Raytheon про виробництво 48 пускових установок M903 для систем ППО-ПРО Patriot. Ці установки будуть виготовлені компанією Huta Stalowa Wola як частина другої фази програми “Вісла”. Виготовленні установки дадуть можливість створити щонайменше шість батарей Patriot і будуть готові до використання з 2027 року.

Однак нарощування виробничих ліній відбувається повільно. Це свідчить про необхідність утворення та підтримки певних обсягів боєздатних ЗРК та ракет країнами – членами НАТО для забезпечення можливостей IAMD.

Країни Європи намагаються зменшити критичну залежність від американського озброєння. Очікується, що придбання Німеччиною ізраїльської системи ПРО Arrow-3, здатної перехоплювати балістичні ракети верхнього рівня, значно підсилить IAMD. Крім того, Латвія та Естонія спільно вирішили закупити систему ППО середньої дальності IRIS-T. Контракт коштує близько 600 мільйонів євро, систему буде доставлено до Латвії у 2026 році. Іспанія також розгорнула наземну систему ППО NASAMS у Латвії в березні 2023 року, потім перемістивши її до Литви та розгорнувши другу в Естонії. Крім того, у березні 2022 року Велика Британія оголосила про розгортання наземної системи ППО малої та середньої дальності Sky Sabre (Land Ceptor) у Польщі для забезпечення ешелонованої протиповітряної оборони.

З 2023 року спільна політика безпеки та оборони Європейського Союзу (CSDP) зазнала кількох важливих змін у відповідь на російсько-українську війну та загальні зміни у сфері безпеки Європи. Задля вирішення можливої проблеми залежності від постачальників ЄС у березні 2022 року ухвалив “Стратегічний компас”, у якому викладено спільне стратегічне бачення політики безпеки та оборони на 10 років. Документ підкреслює необхідність зменшення залежності від зовнішніх постачальників.

Як інструмент для фінансування спільних оборонних досліджень та розробок створено Європейський оборонний фонд (European Defence Fund, EDF). Фонд підтримує проєкти в таких сферах, як наземні бойові дії, космос, повітряні та морські бойові дії, а також забезпечення стійкості енергетичної системи.

У березні 2024 року Комісія ЄС запропонувала Європейську оборонно-промислову стратегію (EDIS) [22], яка прагне усунути недоліки в обороннній готовності ЄС, ці недоліки стали очевидними через війну в Україні. Європейська комісія у 2025 році через EDF виділила понад 1 мільярд євро на дослідження і розроблення новітніх оборонних технологій. Основні напрями досліджень: технології для наземного, повітряного та космічного бою; кібербезпека і штучний інтелект для захисту критичної інфраструктури; стимулювання інновацій. Стратегія передбачає перехід від короткострокових надзвичайних заходів, ухвалених у 2023 році та які завершуються у 2025 році, до більш структурованого і довгострокового підходу до досягнення оборонної промислової готовності.

Голова Єврокомісії Урсула фон дер Ляєн у березні 2025 року виступила з планом переозброєння Європи “ReArm Europe” та наголосила, що Європа мусить взяти на себе більше відповідальності за власну безпеку та “переозброїтися”. Планується створити новий інструмент позик державам-членам для інвестицій в оборону на 150 мільярдів євро. План передбачає мобілізацію до 800 мільярдів євро на оборонні потреби протягом наступних чотирьох років. Основні напрями: інвестиції у системи ППО-ПРО, артилерійські системи, БпЛА та технології протидії, розширення виробництва боєприпасів і військової техніки в межах ЄС для зменшення залежності від імпорту. Такий підхід дозволяє уникнути залежності від одного постачальника, забезпечити диверсифікацію джерел постачання та розвиток внутрішніх виробничих потужностей.

*7. Використання новітніх технологій.*

Важливим уроком російсько-української війни є підвищення ролі БпЛА і штучного інтелекту в сучасній війні.

Зараз практично всі країни світу здійснюють інвестування у розвиток БпЛА та автоматизованих систем управління, зокрема EDF виділив 8 мільярдів євро на розробклення та дослідницькі проєкти у цій сфері з 2021-го по 2027 рік.

Розробляється відповідна нормативно-правова база, 01.08.2024 було ухвалено Європейський закон про штучний інтелект (Artificial Intelligence Act), перший у світі комплексний нормативний акт щодо штучного інтелекту.

Польща активно веде пошук способів використання штучного інтелекту для аналізу даних і прогнозування атак, ухвалено Стратегію військового штучного інтелекту (2024-2039), основними напрямами якої є розвиток автономних систем, розвідка та аналіз даних, кібербезпека, співпраця з НАТО та США у цих сферах.

У Франції 23.02.2023 року було оголошено про співпрацю Thales і LuxCarta у сфері використання штучного інтелекту для розвідки та військової картографії.

Німецька Helsing і французька Mistral AI 10.02.2025 року оголосили про угоду про спільне розроблення систем штучного інтелекту для оборони. Компанія OpenAI у грудні 2024 року оголосила про партнерство з військовою технологічною компанією Anduril у сфері розроблення рішень для захисту об'єктів від ударів БпЛА.

Верховний головнокомандувач НАТО з питань трансформації адмірал П'єр Вандьє на конференції, присвяченій військовому штучному інтелекту, заявив, що члени Альянсу тепер використовують штучний інтелект у циклі спостереження – аналіз – рішення – дії. Аналіз, на який раніше потрібно було витратити години або дні, зокрема оброблення великої кількості даних, тепер можна виконати за лічені секунди.

**Обговорення (Discussions)**

У дослідженні представлено аналіз впливу російсько-української війни на трансформацію європейської системи ППО-ПРО. Зокрема, показано, що:

- війна в Україні продемонструвала невідповідність наявних систем ППО європейських країн сучасним вимогам, особливо в контексті захисту від малорозмірних, маловисотних БпЛА та балістичних ракет;
- переважна більшість країн Європи усвідомлює необхідність співпраці та розвитку власних оборонних можливостей, за збереження трансатлантичної співпраці;
- досвід, набутий ПС ЗС України з успішної адаптації дій для зменшення ефективності ударів ЗПН і підвищення захищеності підрозділів та інфраструктури, знайшов відображення у низці нормативних документів НАТО та ЄС;
- важливим уроком є необхідність інтеграції різних систем ППО для створення єдиного розвідувально-інформаційного простору та єдиної зони вогневого впливу, як це було реалізовано в Україні;
- залежність від імпорту озброєння робить країну вразливою до перебоїв у постачанні та впливу зовнішньої політики.

Сучасні збройні конфлікти демонструють здатність агресора змінюватися, розробляти нові зразки озброєння, запозичувати вдалі технічні рішення та швидко масштабувати їх виробництво. Результати дослідження підтверджують нагальну потребу в модернізації та адаптації європейської системи ППО-ПРО до сучасних викликів. російсько-українська війна стала каталізатором цих змін, виявивши вразливості та недоліки наявних систем.

Останні заяви та дії керівництва США свідчать про можливу зміну безпекової ролі США у Європі. Це загострює дискусію щодо залежності європейської безпеки від американських гарантій та необхідності розвитку власних оборонних можливостей. Інструментом посилення обороноздатності європейських країн є значне збільшення фінансових витрат на оборону. Для

ефективного використання цих коштів планується інтеграція зусиль та надання переваги розвитку власної оборонної промисловості, що зменшить критичні недоліки оборонного потенціалу та залежність від можливостей США.

Аналіз останніх політичних кроків та ухвалених рішень у військово-промисловій та економічній сферах ЄС свідчить про усвідомлення необхідності їх швидкого розроблення та втілення. Заходи мають комплексний характер, передбачають високий рівень інтеграції та консолідації й розраховані на синергетичний ефект змін у всіх сферах економіки.

Однак у цьому процесі є певні протиріччя. З одного боку, є прагнення до стратегічної автономії та зменшення залежності від США, з іншого – необхідність інтеграції з системами НАТО. Це потребує збалансованого підходу до розвитку власних оборонних можливостей, які б могли ефективно взаємодіяти з союзниками.

**Висновок (Conclusion)**

Дослідження дозволяє зробити наступні висновки:

російсько-українська війна суттєво вплинула на трансформацію європейської системи ППО-ПРО, виявивши необхідність її модернізації та адаптації до сучасних викликів;

досвід застосування частин та підрозділів сил оборони України з адаптації та гнучкого застосування систем ППО є цінним для європейських країн, активно узагальнюється та вивчається;

європейська система ППО-ПРО розвивається у напрямі стратегічної автономії, інтеграції та створення багатошарової системи ППО-ПРО;

зміни задля розвитку системи ППО-ПРО стосуються широкого кола питань, частина яких лежить в економічній та політичній сферах та передбачає непопулярні, але необхідні рішення, насамперед збільшення витрат на оборону. Слід зазначити, що інвестиції у національні військово-промислові комплекси у стратегічній перспективі призведуть до розвитку промисловості, у тому числі малих та середніх підприємств, які є “двигуном” інноваційної діяльності та регіональної економіки.

**Рекомендації (Recommendations)**

Досвід адаптації Європейської системи ППО-ПРО до сучасних викликів, який включає стратегії розосередження сил, інтеграції різнорідних систем, посилення міжнародної координації, впровадження новітніх технологій та розвиток національного військово-промислового комплексу, доцільно врахувати під час розбудови української системи ППО-ПРО та співпраці з країнами-партнерами.

На підставі результатів дослідження можна запропонувати такі рекомендації:

задля підтримки та набуття необхідних спроможностей потрібно збільшити інвестиції у модернізацію та розвиток власних систем ППО-ПРО, приділяючи особливу увагу захисту від малорозмірних, маловисотних БпЛА;

доцільно розвивати співпрацю з країнами-партнерами, насамперед із сусідніми країнами, у напрямі забезпечення інтеграції розвідувально-інформаційних систем, військово-промислового виробництва, створення спільних запасів військового призначення;

варто активно впроваджувати концепцію гнучкого бойового застосування (ACE) для підвищення стійкості та мобільності національних систем ППО-ПРО та брати участь у міжнародній співпраці з країнами-партнерами у цій сфері;

критично важливим є забезпечення можливості інтеграції різних систем ППО-ПРО в єдину відкриту архітектуру, що дозволить створити єдиний розвідувально-інформаційний простір та єдину зону вогневого впливу;

необхідно збалансувати прагнення до національної автономії з необхідністю інтеграції з системами НАТО або країн-сусідів, розвиваючи власні оборонні можливості, які б могли ефективно взаємодіяти з союзниками;

слід враховувати напрям розвитку європейської системи ППО-ПРО під час планування закупівель систем ППО-ПРО та розроблення концепцій їх застосування;

підготовка персоналу є визначальним фактором у реалізації спільних дій та опануванні (або наданні) допомоги від країн-партнерів;

потрібно забезпечувати постійний обмін досвідом, координацію зусиль та співпрацю з партнерами у сфері ППО-ПРО, враховуючи український досвід ведення бойових дій в умовах сучасної війни та можливості країн-партнерів з постачання систем озброєння.

**Подяки (Acknowledgments)**

Автори заявляють, що у них немає конкуруючих інтересів за тематикою статті.

**Використані джерела**

1. Henriksen, D., & Bronk, J. (Eds.). (2024). *The Air War in Ukraine: The First Year of Conflict (1st ed.)*. Routledge. https://doi.org/10.4324/9781003454120.
2. Трофимов, І. М., Худов, Г. В., Білецький, С. С., Гризо, А. А., & Гладіщук, О. В. (2024). Особливості бойового застосування радіотехнічних військ Повітряних Сил Збройних Сил України в ході російсько-української війни. *Наука і техніка Повітряних Сил Збройних Сил України, 2* (55), 76–85. https://doi.org/10.30748/nitps.2024.55.08.
3. Гризо, А. А., Костиря, О. О., Лісогорський, Б. А., & Ткаченко, В. І. (2023). Аналіз характеристик та оцінка ефективності застосування потенційних засобів вогневого ураження елементів системи протиповітряної оборони у російсько-українській війні. *Наука і техніка Повітряних Сил Збройних Сил України, 1* (50), 70–81. https://doi.org/10.30748/nitps.2023.50.08.
4. Watling, J., & Reynolds, N. (2023). *Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine*. Royal United Services Institute for Defence and Security Studies. https://static.rusi.org/403-SR-Russian-Tactics-web-final.pdf.
5. Bergmann, M. *How european transatlanticists might approach an isolationist U.S. administration*. Center for Strategic & International Studies. https://www.csis.org/analysis/how-european-transatlanticists-might-approach-isolationist-us-administration
6. Maitra, S. *Policy brief: pivoting the US away from europe to a dormant NATO | the center for renewing america*. The Center for Renewing America. https://americarenewing.com/policy-brief-pivoting-the-us-away-from-europe-to-a-dormant-nato/
7. Grand, C. *Defending Europe with less America.* European Council on Foreign Relations (ECFR). https://ecfr.eu/publication/defending-europe-with-less-america/
8. Muravska, J. *European Integrated Air and Missile Defence in NATO: Progress and Persistent Challenges.* King's College London. https://www.kcl.ac.uk/warstudies/assets/paper-16-julia-muravska-european-integrated-air-and-missile-defence.pdf.
9. Barrie, D. *Europe's air of dependence.* International Institute for Strategic Studies (IISS). https://www.iiss.org/online-analysis/military-balance/2025/03/europes-air-of-dependence/
10. Popescu, N. *The four pillars of European defence*. European Council on Foreign Relations (ECFR). https://ecfr.eu/article/the-four-pillars-of-european-defence/
11. Wachs, L. (2023). *Russian Missiles and the European Sky Shield Initiative*. SWP Comment, Stiftung Wissenschaft und Politik. https://www.swp-berlin.org/publikation/russian-missiles-and-the-european-sky-shield-initiative.

12. Philip Wane, Michael J. Boyle. (2022). The Drone Age: How Drone Technology Will Change War and Peace. *Prometheus*, *38* (3), 365–370. https://doi.org/10.13169/prometheus.38.3.0365.
13. Jojart, K. (2024). The war against Ukraine through the prism of Russian military thought. *Journal of Strategic Studies*, *47* (6–7), 801–831. https://doi.org/10.1080/01402390.2024.2414079.
14. McCurry, M. LEAP: *The solution to language, culture barriers in large-scale military exercises*. Air Force. https://www.af.mil/News/Article-Display/Article/3566792/leap-the-solution-to-language-culture-barriers-in-large-scale-military-exercises/
15. *France demonstrates operational resilience during Agile Combat Employment.* NATO. https://ac.nato.int/archive/2024/france-demonstrates-operational-resilience-during-agile-combat-employment-?utm_source=chatgpt.com
16. FrankenSAM для України від США: перші гібридні ЗРК вже у ЗСУ – на що вони здатні? *Defense Express.* https://defence-ua.com/weapon_and_tech/frankensam_dlja_ukrajini_vid_ssha_zrk_vzhe_protestovani_ta_do_kintsja_oseni_budut_u_zsu_na_scho_voni_zdatni-13313.html
17. Di Mizio, G., Gjerstad, M. *Ukraine's ground-based air defence: evolution, resilience and pressure.* International Institute for Strategic Studies. https://www.iiss.org/online-analysis/military-balance/2025/02/ukraines-ground-based-air-defence-evolution-resilience-and-pressure/
18. Sollfrank, A., & Boeke, S. (2024). Enablement and Logistics as Critical Success Factors for Military Operations: Comparing Russian and NATO Approaches. *The RUSI Journal, 169* (7), 10–22. https://doi.org/10.1080/03071847.2024.2434137.
19. Desmarais, A. (2024). How Sky Shield, Europe's proposed Iron Dome, would work and why it's becoming controversial. *Euronews.* https://www.euronews.com/next/2024/07/28/how-skyshield-europes-proposed-iron-dome-would-work-and-why-its-becoming-controversial.
20. Monaghan, S. (2023). *European Sky Shield: Opportunities and challenges. Center for* Strategic and International Studies. https://csis-website-prod.s3.amazonaws.com/s3fspublic/2023-05/230519_Monaghan_European _SkyShield.pdf.
21. Сабадишина, Ю. Десятки компаній працюють над розробкою українських ракет. Керівниця Brave1 про гранти для розробників і плани на цей рік. *DOU.ua.* https://dou.ua/lenta/news/brave1-in-2025/
22. *European defence industrial strategy.* Epthinktank. https://epthinktank.eu/2024/09/19/european-defence-industrial-strategy/

**References**

1. Henriksen, D., & Bronk, J. (Eds.). (2024). *The Air War in Ukraine: The First Year of Conflict (1st ed.)*. Routledge. https://doi.org/10.4324/9781003454120.
2. Trofimov, I. M., Khudov, G. V., Biletskyi, S. S., Hryzo, A. A., & Hladishuk, O. V. (2024). Features of Combat Use of the Radio Engineering Troops of the Air Force of the Armed Forces of Ukraine During the Russo-Ukrainian War. *Science and Technology of the Air Force of the Armed Forces of Ukraine*, *2* (55), 76–85. https://doi.org/10.30748/nitps.2024.55.08.
3. Hryzo, A. A., Kostyria, O. O., Lisohorskyi, B. A., & Tkachenko, V. I. (2023). Analysis of Characteristics and Evaluation of the Effectiveness of Potential Firepower Means Against Air Defense System Elements in the Russo-Ukrainian War. *Science and Technology of the Air Force of the Armed Forces of Ukraine, 1* (50), 70–81. https://doi.org/10.30748/nitps.2023.50.08.
4. Watling, J., & Reynolds, N. (2023). *Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine*. Royal United Services Institute for Defence and Security Studies. https://static.rusi.org/403-SR-Russian-Tactics-web-final.pdf.

5. Bergmann, M. *How european transatlanticists might approach an isolationist U.S. administration*. Center for Strategic & International Studies. https://www.csis.org/analysis/how-european-transatlanticists-might-approach-isolationist-us-administration
6. Maitra, S. *Policy brief: pivoting the US away from europe to a dormant NATO | the center for renewing america*. The Center for Renewing America. https://americarenewing.com/policy-brief-pivoting-the-us-away-from-europe-to-a-dormant-nato/
7. Grand, C. *Defending Europe with less America*. European Council on Foreign Relations (ECFR). https://ecfr.eu/publication/defending-europe-with-less-america/
8. Muravska, J. *European Integrated Air and Missile Defence in NATO: Progress and Persistent Challenges.* King's College London. https://www.kcl.ac.uk/warstudies/assets/paper-16-julia-muravska-european-integrated-air-and-missile-defence.pdf.
9. Barrie, D. *Europe's air of dependence.* International Institute for Strategic Studies (IISS). https://www.iiss.org/online-analysis/military-balance/2025/03/europes-air-of-dependence/
10. Popescu, N. *The four pillars of European defence*. European Council on Foreign Relations (ECFR). https://ecfr.eu/article/the-four-pillars-of-european-defence/
11. Wachs, L. (2023). *Russian Missiles and the European Sky Shield Initiative*. SWP Comment, Stiftung Wissenschaft und Politik. https://www.swp-berlin.org/publikation/russian-missiles-and-the-european-sky-shield-initiative.
12. Philip Wane, Michael J. Boyle, (2022). The Drone Age: How Drone Technology Will Change War and Peace. *Prometheus*, *38* (3), 365–370. https://doi.org/10.13169/prometheus.38.3.0365.
13. Jojart, K. (2024). The war against Ukraine through the prism of Russian military thought. *Journal of Strategic Studies, 47(6–7),* 801–831. https://doi.org/10.1080/01402390.2024.2414079.
14. McCurry, M. LEAP: *The solution to language, culture barriers in large-scale military exercises*. Air Force. https://www.af.mil/News/Article-Display/Article/3566792/leap-the-solution-to-language-culture-barriers-in-large-scale-military-exercises/
15. *France demonstrates operational resilience during Agile Combat Employment*. NATO. https://ac.nato.int/archive/2024/france-demonstrates-operational-resilience-during-agile-combat-employment-?utm_source=chatgpt.com
16. FrankenSAM for Ukraine from the U.S.: The First Hybrid SAM Systems Already in the Armed Forces of Ukraine – What Are They Capable Of? *Defense Express.* https://defence-ua.com/weapon_and_tech/frankensam_dlja_ukrajini_vid_ssha_zrk_vzhe_protestovani_ta_do_kintsja_oseni_budut_u_zsu_na_scho_voni_zdatni-13313.html
17. Di Mizio, G., & Gjerstad, M. *Ukraine's ground-based air defence: evolution, resilience and pressure. International Institute for Strategic Studies*. https://www.iiss.org/online-analysis/military-balance/2025/02/ukraines-ground-based-air-defence-evolution-resilience-and-pressure/
18. Sollfrank, A., & Boeke, S. (2024). Enablement and Logistics as Critical Success Factors for Military Operations: Comparing Russian and NATO Approaches. *The RUSI Journal, 169* (7), 10–22. https://doi.org/10.1080/03071847.2024.2434137.
19. Desmarais, A. (2024). How Sky Shield, Europe's proposed Iron Dome, would work and why it's becoming controversial. *Euronews.* https://www.euronews.com/next/2024/07/28/how-skyshield-europes-proposed-iron-dome-would-work-and-why-its-becoming-controversial.
20. Monaghan, S. (2023). *European Sky Shield: Opportunities and challenges*. Center for Strategic and International Studies. https://csis-website-prod.s3.amazonaws.com/s3fspublic/2023-05/230519_Monaghan_European _SkyShield.pdf.

21. Dozens of Companies Are Working on the Development of Ukrainian Missiles: The Head of Brave1 on Grants for Developers and Plans for This Year. *DOU.ua.* https://dou.ua/lenta/news/brave1-in-2025/
22. *European defence industrial strategy*. Epthinktank. https://epthinktank.eu/2024/09/19/european-defence-industrial-strategy/

## russo-ukrainian war as a catalyst for changes in the european air and missile defense system: from american support to strategic autonomy

**Andrii Hryzo**
Candidate of Technical Sciences, Associate Professor
Head of the Research Laboratory
Ivan Kozhedub Kharkiv National Air Force University
61023, Sumska St., 77/79, Kharkiv, Ukraine
e-mail: a.hryzo@hups.mil.gov.ua
ORCID: 0000-0003-2483-5953

**Oleksandr Kostyria**
Doctor of Technical Sciences, Senior Researcher
Leading Researcher at the Research Laboratory
Ivan Kozhedub Kharkiv National Air Force University
61023, Sumska St., 77/79, Kharkiv, Ukraine
e-mail: kostyria1958@gmail.com
ORCID: 0000-0003-3363-2015

**Ivan Trofymov**
PhD in Technical Sciences, Senior Researcher
Professor of the Department
Ivan Kozhedub Kharkiv National Air Force University
61023, Sumska St., 77/79, Kharkiv, Ukraine
e-mail: tininterpritor@ukr.net
ORCID: 0000-0001-7080-909X

**Abstract.** The relevance of this study is driven by the necessity to transform existing air and missile defense systems due to their inadequacy in countering new types of threats that have emerged during russia's full-scale armed aggression against Ukraine. The extensive use of cruise and ballistic missiles, unmanned systems, and other strike capabilities has exposed the deficiencies of Europe's air defense system and highlighted the need for its integration and modernization to ensure the effective protection of critical infrastructure and European territories.

The objective of this paper is to identify the prospects for the development of the European air and missile defense system in the context of the pursuit of strategic autonomy and ways to overcome the challenges posed by the russo-ukrainian war. Accordingly, this article focuses on defining the key directions of transformation for the European air and missile defense system and analyzing the impact of relevant military-political and economic decisions on its development. Special attention is given to the methods and approaches used to integrate Ukraine's combat experience into these efforts.

The leading research method is system analysis, which enables a comprehensive examination of the challenges associated with the current European air and missile defense system. Additionally,

content analysis has been applied to study relevant information materials. Forecasting methods and quantitative analysis of statistical data were employed to justify assumptions and conclusions.

This article explores key measures aimed at enhancing the capabilities of the European air and missile defense system, particularly in light of lessons learned by the Air Force of the Armed Forces of Ukraine during the russo-ukrainian war. It also examines the primary contradictions and challenges associated with this transformation.

The article's materials are of practical value for military experts, analysts and decision-makers in the defence sector, and can be used in planning the procurement of defence systems and developing concepts for their use.

**Keywords:** air defence, missile defence, russian-ukrainian war, european security, strategic autonomy.

The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 3 No. 2 (2025)

DOI: 10.62524/msj.2025.3.2.6

# Developing Recommendations for Improving the Efficiency of Personnel Manning in the Armed Forces of Ukraine

**Anatolii Barhylevych**
Candidate of Military Sciences
General Inspector at the Ministry of Defence of Ukraine
The Staff of the Ministry of Defence of Ukraine
03168, Povitrianykh Syl Avenue, 6, Kyiv, Ukraine
e-mail: A.barhilevych@mil.ua
ORCID: 0000-0002-4799-0908

**Abstract.** Manning the Armed Forces of Ukraine is one of the key aspects of the state's defence capability, particularly under the conditions of a protracted armed conflict. A reduction in mobilisation resources, socio-economic challenges, and a low level of trust in military structures complicate the process of attracting personnel. This article provides an analysis of the existing issues and possible solutions and aims to develop recommendations that may contribute to more effective manning of the Armed Forces of Ukraine in line with current challenges and NATO standards.

The research employs methods of systems analysis, structural-functional approach, and comparative analysis. It uses statistical data on personnel numbers, sociological surveys, and analytical reviews of international army manning practices. SWOT analysis methods were also applied to assess the strengths and weaknesses of the current manning system.

The aim of the research is to identify systemic problems in the manning of the Armed Forces of Ukraine and to develop effective ways to improve mobilisation and contractual mechanisms. For this purpose, structural, statistical, and comparative analyses were applied, with a focus on the experience of partner countries.

The article analyses two main categories of sources for manning the Armed Forces of Ukraine: the mobilisation resource and contractual service. It outlines the key issues negatively affecting the manning process, including insufficient motivation, management problems, socio-economic factors, information challenges, and the low level of new recruits' training. A set of measures is proposed to improve manning efficiency, in particular: improving recruitment, digitalising military record-keeping processes, strengthening social protection for service members, and enhancing personnel training mechanisms.

The future research should focus on developing mechanisms for adapting the manning system to new security challenges, particularly under hybrid warfare conditions. An important aspect is the analysis of international experience with the aim of implementing best practices into the Ukrainian manning model. The impact of social factors on shaping a positive image of military service also requires dedicated attention.

The results of the research may be useful for military analysts, representatives of the Ministry of Defence of Ukraine, experts in military administration, as well as scholars working in the field of national security and military reform. The article may also be of interest to policymakers involved in shaping defence sector development strategies.

**Keywords:** Armed Forces of Ukraine, manning, ratio, recruiting, mobilisation resource, manning level.

**Introduction**

Manning the Armed Forces of Ukraine (AF of Ukraine) with military personnel is a key factor in ensuring national security and the state's defence capability, particularly under the conditions of armed conflict. The effectiveness of the mobilisation system, the level of citizens' motivation for military service, and the organisation of recruiting processes determine the combat effectiveness of military formations and their ability to accomplish operational tasks.

Following the launch of the full-scale aggression by the russian federation in 2022, Ukraine faced unprecedented challenges in the domain of force generation. High personnel losses, significant migration of the working-age population, socio-economic difficulties, and psychological factors have critically impacted the country's mobilisation potential. At the same time, the need is growing for highly skilled personnel capable of adapting to modern warfare conditions, including the use of advanced technologies, robotic systems, and cyber operations.

Despite the adoption of a number of reforms in the field of military service, including the introduction of new manning standards, many systemic problems remain. The lack of sufficient trust in Territorial Recruitment and Social Support Centres (TRC and SSC), inadequate civil-military cooperation, and limited social support for service personnel are factors that hinder the recruitment of new personnel.

The relevance of the research lies in the need to develop effective mechanisms for manning the Armed Forces of Ukraine (AF of Ukraine), taking into account current challenges and the experience of NATO member states. The article analyses the key issues that influence the process of recruiting personnel into the AF of Ukraine, identifies factors that reduce citizens' motivation to undergo military service, and offers practical recommendations to improve the effectiveness of manning.

The aim of the research is to identify systemic shortcomings in the mobilisation and contract-based enlistment system of the AF of Ukraine and to develop a comprehensive set of measures to improve personnel manning mechanisms. The research applies methods of structural analysis, statistical evaluation, and a comparative analysis of military models used by Ukraine's partner nations.

The results obtained may be used in the process of enhancing the state's military personnel policy, in forming a long-term strategy for manning the AF of Ukraine, and in developing recommendations for state authorities responsible for mobilisation and personnel management policy.

**Literature Review**

At present, many authors devote considerable attention to issues related to the manning of the Armed Forces of Ukraine (AF of Ukraine) and to the experience of other countries in engaging citizens for military service [1–11]. However, the experience of recent years remains insufficiently explored, and there is a notable lack of innovative solutions to address the identified problems.

**Methodological Framework**

This research applies methods of systems analysis, a structural-functional approach, and comparative analysis. It utilises statistical data on personnel strength, sociological surveys, and analytical reviews of international practices in military manning. SWOT analysis was also employed to assess the strengths and weaknesses of the current personnel acquisition system.

**Results**

Currently, the sources of personnel for the AF of Ukraine are conventionally divided into two categories:

the first category (primary) consists of citizens liable for military service who are called up to the ranks of the AF of Ukraine during mobilisation in a special period, in accordance with the requirements of Ukrainian legislation and applicable regulatory acts;

the second category includes individuals who have voluntarily expressed willingness and signed a contract for military service in the AF of Ukraine (including foreign nationals).

The aforementioned categories differ in terms of numerical indicators, motivation to carry out combat (special) tasks, and levels of morale and psychological resilience

At the same time, both categories of individuals are directly or indirectly influenced by their overall level of trust in the Ukrainian government, the Defence Forces of Ukraine, and the Armed Forces of Ukraine (AF of Ukraine) in particular.

Specifically, declining trust in the processes taking place prior to conscription, during it, and throughout the preparation for and execution of combat (special) tasks has led to a reduction in the overall number of individuals in the second category (the so-called volunteers). Among the first category (provisionally understood as the broader segments of the population), doubts arise regarding the necessity of fulfilling the legally defined obligation. As a result, individuals seek ways to evade mobilisation.

The immediate causes of reluctance to serve in the AF of Ukraine and the declining level of public trust in the overall manning system of the AF of Ukraine can be attributed to the following: systemic and organisational shortcomings; information and communication challenges; socio-economic factors; training and rotation issues; psychological aspects; and management deficiencies (see Fig. 1).

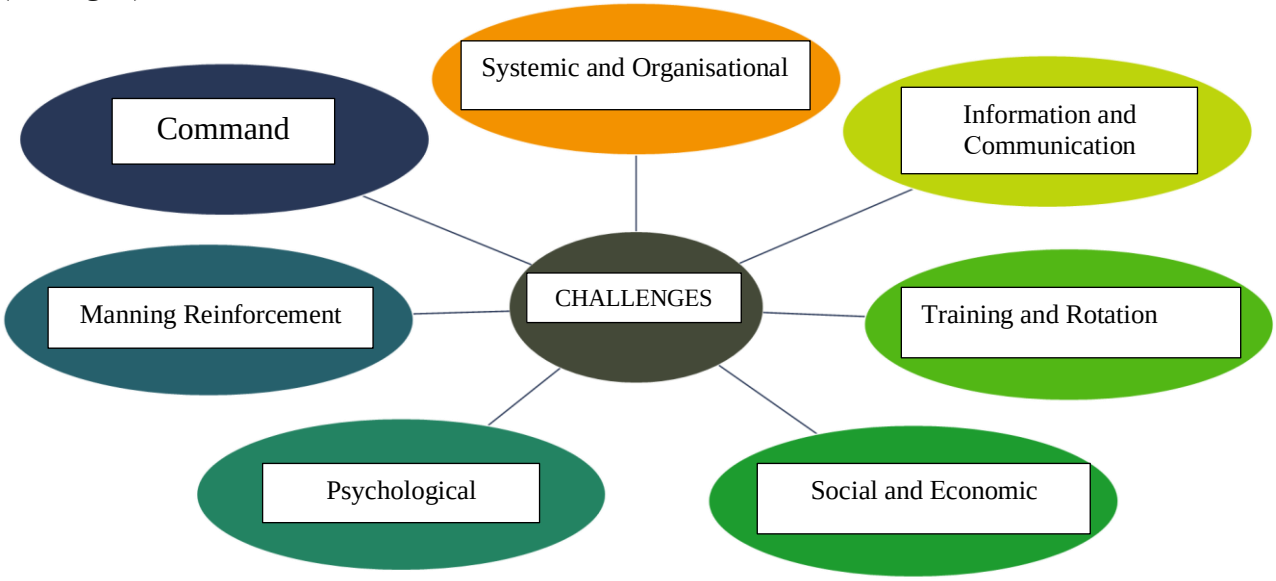



**Figure 1.** Main categories of issues in the organisation of manning within the AF of Ukraine

*Systemic and organisational problems:*

lack of proper motivation among citizens to fulfil their constitutional duty to defend the state, evasion of conscription for military service during mobilisation and special periods, and unwillingness to undertake contract-based military service;

low public trust in the functioning of Territorial Recruitment and Social Support Centres (TRC and SSC) due to numerous legal violations, as well as multiple cases of corruption involving personnel, particularly the leadership of certain TRC and SSCs, which have received widespread public attention in Ukrainian society;

failure of TRC and SSCs to meet planned targets for the conscription of individuals liable for military service during mobilisation and special periods, and to ensure their transfer to training military units (centres), higher military educational institutions, or training programmes at civilian higher education institutions, which hinders the replenishment of combat units to the required levels

using highly trained military personnel;

lack of adequate coordination between local authorities and TRC and SSCs, resulting in gaps in the organisation of notifications and ensuring the timely arrival of conscripts to TRC and SSCs.

*Information and communication challenges:*

insufficient public awareness regarding the opportunities and procedures for military service in the Armed Forces of Ukraine (AF of Ukraine), and the failure to refute, or untimely refutation of, distorted and manipulative information concerning the activities of the AF of Ukraine in the mass media and on internet platforms;

dissemination in society of information about the training inadequate duration and quality for newly recruited personnel of the AF of Ukraine, among other concerns.

*Social and economic factors:*

low levels of financial remuneration for AF of Ukraine service members due to the devaluation of the national currency and general inflation caused by the war;

in the perception of the civilian population, the system of benefits and entitlements for service members and veterans is disproportionate to the actual risks associated with military service.

*Training and rotation challenges:*

insufficient duration and quality of training for newly arrived service members negatively affects their willingness to serve in combat units, which ultimately impacts the combat readiness of these subunits;

extremely limited, and often absent, opportunities for the rotation of service members deployed in combat mission areas.

*Psychological aspects:*

the psychological unpreparedness of civilians to take part in combat operations;

the negative influence of disinformation from the russian federation on the Ukrainian population’s attitude towards mobilisation.

*Command challenges:*

the practice of transferring service members to other subunits and military units for continued military service without their consent, as well as filling vacant positions that are in high demand at a given stage with personnel whose military occupational specialities and experience are not relevant.

*Manning shortfalls:*

unfounded refusals (due to overly strict selection criteria) by representatives of military units to accept trained personnel from Training Centres (Recruitment and Personnel Centres);

unfounded refusals by representatives of combat military units (subunits) to accept service members assigned (transferred) from non-combat military units (subunits) of different branches (armed services) of troops within the AF of Ukraine.

In addition, the general level of public trust in the mobilisation process and the willingness to defend Ukraine is influenced by a range of state-level processes that have gained public attention. These processes are associated, on the one hand, with unequal compliance with current legislation among different population groups and categories, and on the other hand, with a strong societal demand for equality before the law, integrity, and transparency in procedures. At the same time, these issues lie beyond the remit of the Armed Forces of Ukraine and cannot be resolved by them.

According to the analysis results of the identified problems, a number of proposals have been made to enhance the efficiency of manning the AF of Ukraine with personnel (see Fig. 2).

*The work improvement at TRC and SSC (recruitment system):*

taking the necessary measures to ensure that TRC and SSC meet the planned indicators for calling up human mobilisation resources and directing them to training military units (centres), higher military educational institutions, and higher education institutions with military programmes;

increasing the role of unit commanders in recruitment efforts to engage citizens for military service under contract;

scaling up the existing system of Recruitment Centres, which enjoy greater trust among the civilian population;

intensifying the work of recruitment teams of subordinate military units and Recruitment Centres of branches (armed services) of troops in attracting citizens to contract-based military service;

digitalising most military registration processes in TRC and SSC to ensure mobilisation call-up measures during a special period, and organising and monitoring the execution of these measures by operational command headquarters;

strengthening efforts to enlist on contract those who apply in person or through online remote recruitment platforms such as “Lobby X”, “Work.ua”, “Robota.ua”, “OLX Robota”;

improving cooperation between TRC and SSC personnel and the civilian population. Conducting a thorough selection of personnel for TRC and SSC and checking their integrity. Creating specialised online courses in business communication, integrity, and the research of ethical standards for civil servants (service members), and sending TRC and SSC military personnel (employees) to these courses in stages.

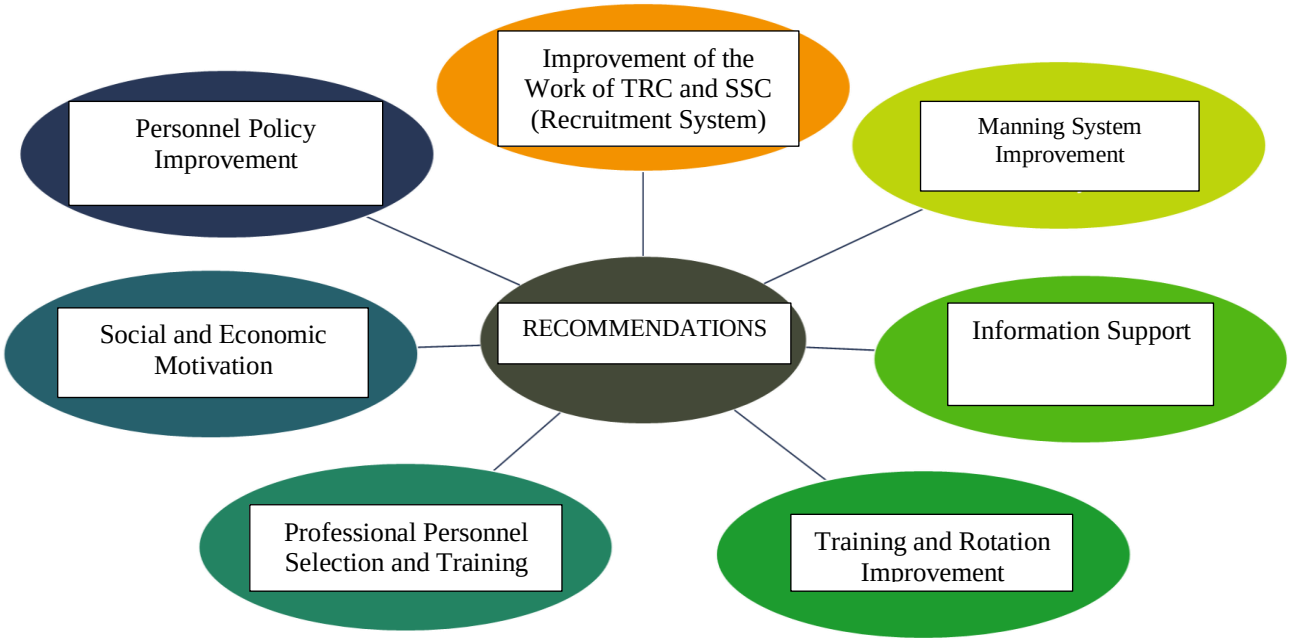



**Figure 2.** Key areas for enhancing the effectiveness of manning the Armed Forces of Ukraine with personnel

*The manning system improvement:*

ensuring the timely reception of trained military personnel from training centres (personnel training points) in the designated volumes; eliminating cases of unjustified refusals by representatives of military units to accept trained personnel. In the event of surplus trained resources, redistribution should be carried out to reinforce other combat military units;

eliminating cases of unjustified refusals by representatives of combat military units (subunits) to accept service members assigned (reassigned) for duty from non-combat military units (subunits);

organising personnel reinforcement of military units (subunits) to the levels and criteria defined in the order of the Commander-in-Chief of the AF of Ukraine dated 08.11.2024 No. 509/DSC, to achieve the “CAPABLE” rating;

granting the authority to officials responsible for enlisting contract personnel and assigning them to positions in accordance with the staffing nomenclature to conclude contracts with service-

eligible individuals selected for positions corresponding to their primary (related) Military Occupational Speciality (MOS) in military units not on the list of priority units, without requiring approval from the General Staff of the AF of Ukraine;

ensuring the fulfilment of training targets for personnel in accordance with the indicative volumes for the training of enlisted personnel, non-commissioned officers, and warrant officers;

ensuring priority in assigning personnel for training aimed at reinforcing the crews (teams) of combat military units.

*Personnel policy improvement:*

introduction of mandatory short-term specialised tactical-level military leadership courses for all platoon-company-battalion level commanders (for conscripts – prior to appointment to command positions; for current service members – during rotation or combat capability recovery);

conducting targeted scientific and practical research to assess the effectiveness of transferring service members to other subunits and military units without their consent (based on the experience of 2022–2024).

*Information support:*

implementation of measures to enhance citizens' motivation for military service, increase trust in the leadership of the AF of Ukraine, and improve the general perception of military service;

launching a nationwide advertising campaign to promote military service and foster its positive public image, along with initiatives to raise its prestige;

developing, at the state level, effective mechanisms for implementing national policy in the field of military-patriotic education, fostering active civic engagement and national and patriotic awareness among Ukrainian citizens;

conducting a continuous nationwide recruitment information campaign, presenting the opportunities, procedures, and prospects of military service in the AF of Ukraine. This campaign should target the broadest segments of the population, utilising all available state media and cooperating with private media outlets;

strengthening information space monitoring at all levels to detect any negative portrayal of the AF of Ukraine and ensuring timely and appropriate responses (rebuttals) to such content;

ensuring that up-to-date information on military service is accessible on the websites of recruitment centres, the Ministry of Defence of Ukraine, the Ministry of Education and Science, and via call centres as interactive web assistants or messenger bots;

limiting or cutting off channels through which enemy disinformation enters the Ukrainian information space. If this cannot be prevented entirely, such information must be swiftly and professionally rebutted in the public domain by recognised and trusted speakers.

*Social and economic motivation:*

increasing the financial remuneration level for service members of the Armed Forces of Ukraine (AF of Ukraine) in order to reduce the impact of inflation on the welfare of active service personnel and their families, as well as to enhance the competitiveness of the AF of Ukraine on the Ukrainian labour market in the eyes of the civilian population, including citizens with higher education and knowledge of modern information technologies;

introducing preferential state life insurance schemes;

ensuring free medical treatment for service members and their family members;

ensuring free higher education for the children of service members at an institution of their choice;

ensuring that family members of a fallen service member get access to preferential mortgage schemes for housing purchase;

implementing free vocational and higher education for veterans;

creating a nationwide loyalty programme (price reductions) for service members, veterans, and their families on consumer goods;

focusing efforts on achieving the maximum level of implementation of previously declared benefits and guarantees, expanding their application, and introducing new ones.

*Professional selection and personnel training:*

introducing modern testing methodologies to assess the physical, psychological, and moral qualities of candidates;

implementing specialised programmes for the training of junior and mid-level commanders;

deepening cooperation with military departments at civilian higher education institutions for the training of officer personnel.

*Training and rotation improvement:*

clearly defining rotation periods to reduce personnel fatigue and introducing a mandatory rotation schedule;

organising adaptation courses following return from combat operations, including psychological support and retraining;

ensuring an effective system for the retraining of service members after prolonged deployments.

*Additional measures:*

introducing and conducting, through the efforts of Recruiting Centres, special short-term courses in psychological readiness for national defence. These courses should be held in higher education institutions, vocational and technical education institutions, senior classes of general secondary education institutions, as well as within bodies and institutions.

The implementation of most of the aforementioned measures requires relevant decisions not only by the leadership of the Armed Forces of Ukraine but also by the political leadership of the state, including amendments to current legislation and other regulatory acts.

**Conclusion**

Manning the Armed Forces of Ukraine is a key factor in ensuring national security. The main challenges causing personnel shortages include significant combat losses, the demographic crisis, low citizen motivation for military service, and shortcomings in mobilisation organisation. The emigration of conscription-age men, weak social support for service members and their families, as well as the lengthy training period for specialists, further complicate the manning process.

To address these issues, a comprehensive approach is proposed, which includes:

- improving the social support system for service members, particularly housing programmes, life insurance, medical care, and veteran rehabilitation;
- implementing an effective recruitment system, including digital platforms, social media, and online resources;
- enhancing the quality of training in military training centres by engaging international instructors, with a special focus on modern military technologies (cybersecurity, unmanned systems);
- expanding contractual military service programmes with more attractive conditions;
- improving the national resistance system and involving civilian specialists on a contractual basis;
- optimising the ratio between combat and support units in line with NATO countries' experience;
- establishing a transparent career progression system and an effective personnel selection mechanism.

Therefore, modernising the approach to manning the Armed Forces of Ukraine must be based on increased motivation, improved recruitment, and enhanced social support for service members. The proposed measures will contribute to improving the personnel situation, ensuring combat readiness, and strengthening the long-term resilience of troops.

**Recommendations**

The findings of the research may be useful for military analysts, representatives of the Ministry of Defence of Ukraine, specialists in the field of military administration, as well as for scholars dealing with national security and military reform. The article may also be of interest to policymakers involved in shaping the strategy for defence sector development.

**References**

1. Gorbenko, S. (2024). Analysis of the experience of staffing the armed forces of the leading countries of the world with officers. *Collection of scientific papers of the Kharkiv National University of the Air Force, 2* (80), 153–157. https://doi.org/10.30748/zhups.2024.80.20.
2. Bukovsky, I. V. (2012). Historical experience of building professional armies of the leading countries of the world. *Bulletin of the National University of Lviv Polytechnic, 724*, 215–220. http://oldena.lpnu.ua/bitstream/ntb/14062/1/35_215-220_Vis724_Armiya.pdf.
3. Savynets, O. Yu. (2018). Foreign experience of staffing the armed forces. *Scientific Bulletin of Uzhhorod National University, 51* (2), 34–38.
4. Drok, L. V. (2021). *Recruiting officers of the Armed Forces of Ukraine (1991–2016): historical and statistical analysis*. National University of Defense of Ukraine.
5. Chernyshova, I. M. (2015). Analysis of foreign experience in the formation of a human mobilisation reserve. *Collection of scientific works of the Central Research Institute of the Armed Forces of Ukraine, 1* (71), 285–294.
6. Lebedenko, A., Semenenko, O., Smilyansky, O., Tsarynnyk, V., & Hovhannesyan, R. (2024). A promising model of recruiting and military service under a contract in the Armed Forces of Ukraine in wartime: an alternative to forced mobilisation. *Military Science, 2* (3), 6–20.
7. Cherep, V. L. (2023). Results of the analysis of the measures for staffing the Armed Forces of Ukraine and other military formations with mobilisation human resources during their mobilisation deployment in 2022. Problematic issues and ways to solve them. *Coll. Scientific Proceedings of the Central Research Institute of the Armed Forces of Ukraine, 1* (104), 105–116.
8. Pavlovsky, O. V. (2023). Results of the analysis of the number of mobilisation human resources of Ukraine at the beginning of 2023. *Coll. Scientific Proceedings of the Central Research Institute of the Armed Forces of Ukraine, 1* (104), 5–14.
9. *Lessons of the russian-Ukrainian war of 2022: military aspects: inf. material. Analysis of the conduct of mobilisation events in Ukraine in 2022*. (2022). Report No. 25. Central Research Institute of the Armed Forces of Ukraine.
10. Semenenko, O., Tsarynnyk, V., Hovhannesyan, R., Vodchyts, O., Remez, V., & Polyvoda, M. (2024). Methodological approach and models for organising research on increasing the effectiveness of mobilisation in Ukraine in wartime. *Social Development and Security, 14* (4), 70–90. https://doi.org/10.33445/sds.2024.14.4.6.
11. Semenenko, O., Koval, V., Dobrovolskyi, Y., Tsarynnyk, V., & Hovhannesyan, R. (2024). "Timeline" mobilisation – a path from coercion to the popularisation of military service in wartime: the right to choose – a way to effectively recruit human resources. *Military Science, 2* (2), 159–179. https://doi.org/10.62524/msj.2024.2.2.14.

The Central Research institute
of the Armed Forces of Ukraine
Military Science. Vol. 3 No. 2 (2025)

# Розроблення рекомендацій щодо підвищення ефективності комплектування Збройних Сил України особовим складом

**Анатолій Баргилевич**
кандидат військових наук
Генеральний інспектор Міністерства оборони України
Апарат Міністерства оборони України
03168, проспект Повітряних Сил, 6, Київ, Україна
e-mail: A.barhilevych@mil.ua
ORCID: 0000-0002-4799-0908

**Анотація.** Комплектування Збройних Сил України є одним із ключових аспектів обороноздатності держави, особливо в умовах тривалого збройного конфлікту. Зменшення мобілізаційного ресурсу, соціально-економічні виклики та низький рівень довіри до військових структур ускладнюють процес залучення особового складу. Стаття містить аналіз наявних проблем та шляхи їх вирішення і спрямована на розроблення рекомендацій, які можуть сприяти більш ефективному комплектуванню Збройних Сил України відповідно до сучасних викликів і стандартів НАТО.

У дослідженні застосовано методи системного аналізу, структурно-функціонального підходу та порівняльного аналізу. Використано статистичні дані щодо чисельності особового складу, соціологічні опитування та аналітичні огляди міжнародного досвіду комплектування армій. Застосовано також методи SWOT-аналізу для оцінювання сильних і слабких сторін наявної системи комплектування.

Мета дослідження полягає у виявленні системних проблем комплектування Збройних Сил України та розробленні ефективних шляхів удосконалення мобілізаційних і контрактних механізмів. Для цього застосовано структурний, статистичний та порівняльний аналіз із акцентом на досвід країн-партнерів.

У статті проаналізовано дві основні категорії джерел комплектування Збройних Сил України: мобілізаційний ресурс та контрактну службу. Виокремлено ключові проблеми, що негативно впливають на процес комплектування, серед яких: недостатня мотивація, проблеми управління, соціально-економічні фактори, інформаційні виклики та низький рівень підготовки новобранців. Запропоновано комплекс заходів для підвищення ефективності комплектування, зокрема покращення рекрутингу, цифровізація процесів військового обліку, підвищення соціального захисту військовослужбовців та удосконалення механізмів підготовки особового складу.

Майбутні дослідження мають бути зосереджені на розробленні механізмів адаптації системи комплектування до нових безпекових викликів, зокрема в умовах гібридної війни. Важливим аспектом є також аналіз міжнародного досвіду з метою імплементації найкращих практик до української моделі комплектування. Окремої уваги потребує дослідження впливу соціальних факторів на формування позитивного іміджу військової служби.

Результати дослідження можуть бути корисними для військових аналітиків, представників Міністерства оборони України, фахівців у сфері військового управління, а також для науковців, які займаються питаннями національної безпеки та військової реформи. Також стаття може зацікавити політиків, які формують стратегію розвитку оборонного сектору.

**Ключові слова:** Збройні Сили України, комплектування, співвідношення, рекрутинг, мобілізаційний ресурс, рівень укомплектованості.

The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 3 No. 2 (2025)

DOI: 10.62524/msj.2025.3.2.7

# Щодо оптимізації управління озброєнням у військах (силах)

**Олексій Шевченко**
кандидат історичних наук
заступник начальника Генерального штабу Збройних Сил України
Генеральний штаб Збройних Сил України
03168, проспект Повітряних Сил, 6, Київ, Україна
e-mail: shevchenko_om@asv.gov.ua
ORCID: 0000-0003-0734-6533

**Олег Семененко**
заслужений діяч науки і техніки України
доктор військових наук, професор
заступник начальника Центрального науково-дослідного інституту
Збройних Сил України з наукової роботи
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: aosemenenko@ukr.net
ORCID: 0000-0001-6477-3414

**Петро Закусило**
доктор військових наук, професор
провідний науковий співробітник
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: Zps20072017@gmail.com
ORCID: 0000-0003-0421-7736

**Василь Харченко**
кандидат військових наук
провідний науковий співробітник
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: vasaxar@ukr.net
ORCID: 0000-0001-7160-7385

**Володимир Мусієнко**
старший викладач кафедри військової підготовки, старший науковий співробітник
Військового інституту телекомунікацій та інформатизації імені Героїв Крут
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут
01011, вул. Острозьких Князів, 45/1, Київ, Україна
e-mail: volodymyr.musienko@viti.edu.ua
ORCID: 0000-0002-4909-6045

**Олег Мельничук**
викладач кафедри вогневої підготовки факультету логістики
Національної академії Національної гвардії України
Національна академія Національної гвардії України
61001, майдан Захисників України, 3, Харків, Україна
e-mail: melnichuk1973@gmail.com
ORCID: 0009-0002-4499-1902

**Анотація.** Забезпечення обороноздатності України значною мірою залежить від ефективної системи управління життєвим циклом озброєння. Однак чинне законодавство не забезпечує комплексного підходу до управління озброєнням, що охоплював би всі етапи життєвого циклу техніки: від планування потреб і розроблення до застосування за призначенням та утилізації. Відсутність єдиного регламенту у взаємодії Генерального штабу Збройних Сил України, Міністерства оборони та підприємств оборонного комплексу спричиняє дисбаланс у процесах закупівель, стандартизації, застосування, а також модернізації озброєння та військової техніки, що, своєю чергою, призводить до зростання рівня їхньої різнотипності у військах (силах).

Різнотипність озброєння та військової техніки створює низку проблем, зокрема ускладнюється організація і проведення технічного обслуговування та ремонту, зростають витрати на експлуатацію, унеможливлюється серійне виробництво та його масштабування, знижується оперативна сумісність як усередині Збройних Сил України, так і в контексті інтеграції до стандартів НАТО.

Мета статті – дослідити роль Генерального штабу Збройних Сил України у вдосконаленні системи управління життєвим циклом озброєння та військової техніки. Основна увага приділяється зменшенню різнотипності озброєння та військової техніки через стандартизацію та уніфікацію, аналізуючи нормативне, організаційне та управлінське забезпечення цих процесів.

Удосконалення системи управління життєвим циклом озброєння та військової техніки, яке б блокувало ці виклики, є необхідною умовою для зниження рівня різнотипності озброєння та військової техніки у Збройних Силах України.

З цією метою пропонується цілісний стратегічний підхід, який інтегрує всі етапи життєвого циклу озброєння та військової техніки в єдину систему управління з акцентом на уніфікацію, стандартизацію та оптимізацію. Такий підхід передбачає чітку взаємодію між ключовими органами військового управління (Міністерство оборони, Генеральний штаб Збройних Сил України, Командування видів (родів) військ (сил), Командування Сил логістики), врахування реальних потреб ефективного застосування з'єднань (частин) та раціонального використання виділених ресурсів, а також відповідність міжнародним стандартам, зокрема стандартам НАТО.

Практична значущість статті полягає у пропонуванні цілісного стратегічного підходу до удосконалення системи управління життєвим циклом озброєння в Україні, спрямованого на зниження різнотипності озброєння та військової техніки шляхом уніфікації, стандартизації та оптимізації взаємодії між ключовими органами військового управління відповідно до міжнародних стандартів.

**Ключові слова:** ефективність, життєвий цикл озброєння, закупівлі, Збройні Сили України, озброєння та військова техніка, потреби, різнотипність, стандартизація, система управління, уніфікація.

**Вступ (Introduction)**

В умовах збройної агресії росії забезпечення обороноздатності України потребує ефективної системи управління життєвим циклом озброєння (СУЖЦО), яка базується на стандартизації, уніфікації та стратегічному плануванні.

СУЖЦО у Збройних Силах України (ЗС України) перебуває у стані реформування, однак вона ще не досягла рівня, що відповідає сучасним викликам та стандартам, зокрема вимогам стандартів НАТО.

Наявна нормативна база, яка регулює окремі аспекти управління озброєнням, залишається фрагментарною та недосконалою. Крім того, нормативно-правові документи України не забезпечують комплексного підходу до управління озброєнням, що включав би всі етапи життєвого циклу техніки: від планування потреб і розроблення до утилізації.

Через відсутність єдиного регламенту взаємодії між Генеральним штабом (ГШ) ЗС України, Міністерством оборони та державними і приватними підприємствами оборонного комплексу виникають проблеми з координацією їхньої діяльності у сфері озброєння та військової техніки (ОВТ). Окремі законодавчі акти, нормативно-правові акти, що регламентують закупівлі (Закон України “Про оборонні закупівлі”), стандартизацію (Закон України “Про стандартизацію”), експлуатацію та утилізацію ОВТ, не узгоджені між собою та не утворюють єдиного регламенту для інтегрованої системи управління озброєнням.

Закон України “Про оборонні закупівлі” регламентує принципи конкурентності й прозорості, але його виконання на практиці часто призводить до закупівлі різнотипних зразків ОВТ (зразків-“аналогів”), що ускладнює стандартизацію процесу озброєння. Відсутність чітко визначених механізмів забезпечення уніфікації під час укладання контрактів на закупівлю ОВТ допускає постачання несумісних з наявними зразків, що знижує ефективність їх застосування та обслуговування у військах.

Генеральний штаб виконує ключову роль у стратегічному плануванні оборонних потреб, однак його взаємодія з Міністерством оборони та оборонними підприємствами нормативно не врегульована, що ускладнює процеси закупівлі, стандартизації, застосування за призначенням та модернізації ОВТ.

Проблема різнотипності ОВТ у ЗС України має декілька першопричин. Вона виникла внаслідок тривалого періоду несистемного підходу до комплектування військ, застосування застарілих зразків ОВТ радянського виробництва, надходження міжнародної технічної допомоги та необхідності закупівлі ОВТ від різних виробників в умовах війни [1]. Ця різноманітність суттєво ускладнює застосування ОВТ за призначенням, їхнє логістичне забезпечення, збільшує витрати ресурсів та негативно впливає на рівень боєздатності частин (підрозділів).

Використання ОВТ різних виробників із несумісними системами управління, калібрами боєприпасів та комплектуючими створює додаткові складнощі у їх технічному обслуговуванні та застосуванні.

Однією із ключових проблем є те, що ГШ ЗС України – основний орган військового управління ЗС України – не має достатніх повноважень для впливу на зменшення різнотипності ОВТ. Для розв’язання цієї проблеми необхідно забезпечити його взаємодію з Міністерством оборони, підприємствами оборонного комплексу та іншими суб’єктами сфери ОВТ.

Тому особливо актуальним є дослідження ролі ГШ ЗС України у вирішенні проблеми різнотипності ОВТ, оптимізації витрат на оборону, підвищенні боєготовності ЗС України та забезпеченні інтеграції України до міжнародної системи колективної безпеки.

**Огляд літератури (Literature review)**

В умовах широкомасштабного вторгнення росії в Україну, формування нового безпекового середовища в Європі велику увагу фахівці приділяють актуальним питанням щодо удосконалення системи управління життєвим циклом озброєння з метою привести у відповідність розвиток перспективних зразків озброєння до швидкоплинності військово-політичної та економічної обстановки. Зокрема, у [2] проведено аналіз сучасних тенденцій в СУЖЦО країн НАТО. Автори акцентують увагу на тому, що нормативним базисом, який визначає політику та принципи управління життєвим циклом озброєння в НАТО, є міжнародні стандарти. На базі аналізу запропоновані концептуальні погляди щодо реалізації Концепції створення в Україні СУЖЦО та відповідна Дорожня карта з урахуванням політики та підходів НАТО. Разом із тим, питання стосовно ролі ГШ ЗС України в цьому процесі автори статті не порушували.

У роботах [3–5] розглянуто підходи до аналізу воєнно-технічних і техніко-економічних аспектів життєвого циклу зразків ОВТ, проаналізовано основні управлінські проблеми та нові підходи до оборонного планування на основі спроможностей та забезпечення оптимального управління цільовими програмами розвитку ОВТ у структурі повного життєвого циклу озброєнь. У [6], [7] запропоновано підходи до орієнтування бізнес-процесів і процедур на взаємну узгодженість з метою ефективного використання і координації ресурсів, інформації та технологій протягом усього життєвого циклу ОВТ. Питання щодо зменшення різнотипності ОВТ, уніфікації та стандартизації ОВТ у роботах не розглядалися. Методичні підходи до обґрунтування вартості життєвого циклу носіїв спроможностей ЗС України досліджувались у [8], фінансово-економічні аспекти життєвих циклів складних високотехнологічних зразків ОВТ – у [9] і [10]. Проблемні питання, що стосуються науково-технічного супроводження процесу управління повним життєвим циклом складних зразків ОВТ та особливості побудови системи управління повним життєвим циклом ОВТ, детально розглянуто в [6]. При цьому питання щодо координації дій Міністерства оборони та ГШ ЗС України під час упровадження СУЖЦО в поєднанні з єдиним стратегічним підходом до стандартизації та уніфікації за етапами життєвого циклу озброєння не розглянуто.

Метою статті є дослідження ролі ГШ ЗС України в удосконаленні СУЖЦО з метою зменшення різнотипності ОВТ шляхом урахування питань стосовно стандартизації та уніфікації ОВТ. Для цього розглядаються питання щодо нормативного, організаційного та управлінського забезпечення процесів уніфікації та стандартизації ОВТ, а також можливі шляхи усунення проблем, пов’язаних із різнотипністю ОВТ.

**Результати (Results)**

Різнотипність ОВТ у ЗС України є системною проблемою, яка виникла внаслідок низки історичних, економічних, технологічних та організаційних факторів. Аналіз дозволяє виділити ключові проблеми:

– закупівля озброєння за типом, а не за конкретними зразками. Нормативно-правова база, яка регулює процеси закупівлі озброєння, допускає закупівлі за загальними технічними характеристиками, що призводить до значних відмінностей між зразками техніки;

– спадщина радянського періоду. Україна ще з часів радянського союзу успадкувала велику кількість озброєння, яке було виготовлене на різних заводах і за різними стандартами. Після розпаду срср постачання запчастин від багатьох підприємств стало неможливим, що змусило шукати альтернативні комплектуючі;

– відсутність єдиної довгострокової стратегії стандартизації озброєння. Протягом багатьох років через відсутність узгодженої національної стратегії уніфікації озброєння процес закупівель відбувався хаотично. Закупівлі ОВТ здійснювалися залежно від наявності фінансування або поточного стану ринку, а не на основі стратегічного плану. Через

недостатню координацію між Генеральним штабом, Міністерством оборони та державними підприємствами оборонного комплексу стандартизація ускладнювалась;

– множинність постачальників озброєння. Україна закуповує озброєння як у вітчизняних, так і у міжнародних постачальників. Це призводить до того, що вітчизняні та іноземні зразки ОВТ часто несумісні між собою. Різноманіття у системи озброєння додає також постачання озброєння в рамках міжнародної технічної допомоги від різних країн (наприклад, США, Великої Британії, Польщі).

Суттєва різнотипність ОВТ у військах залишається серйозною проблемою, що знижує боєздатність та ускладнює логістичне забезпечення частин (підрозділів), у тому числі збільшує витрати на технічне обслуговування та ремонт ОВТ. Причинами такого стану є відсутність єдиного стратегічного підходу до планування та закупівлі озброєння, неузгодженість функцій Міністерства оборони та ГШ ЗС України, фрагментарність нормативної бази, яка не враховує всі стадії життєвого циклу ОВТ, недостатня інтеграція стандартів взаємозамінності та уніфікації.

Зменшення різнотипності ОВТ є критичним фактором удосконалення СУЖЦО. Вона має не тільки реагувати на цей виклик, а й стати дієвим механізмом, що забезпечує ефективне управління всіма етапами життєвого циклу ОВТ.

Наразі нормативно-правовими актами не сформовано єдиної узгодженої системи управління ОВТ, яка б охоплювала всі етапи їхнього життєвого циклу. ГШ ЗСУ, Міністерство оборони, державні та приватні підприємства оборонного комплексу діють на основі різних нормативних документів, які не узгоджені між собою. Це призводить до дисбалансу у плануванні, закупівлі, стандартизації та координації розроблення ОВТ. Немає також механізму обмеження різнотипності ОВТ під час укладання контрактів. Нормативно-правові акти не забезпечують комплексного підходу до управління повним життєвим циклом ОВТ, що позначається на ефективності модернізації ОВТ, які нерідко залишаються поза стратегічними планами.

Координація між Міністерством оборони та ГШ ЗС України залишається одним із ключових викликів у системі управління життєвим циклом озброєння. Попри те, що ГШ ЗС України виконує визначальну роль у стратегічному плануванні оборонних потреб в ОВТ, нормативно-правові механізми його взаємодії з Міністерством оборони та підприємствами оборонного комплексу залишаються недостатньо ефективними. Це негативно впливає на процеси закупівлі, застосування за призначенням, стандартизації та модернізації ОВТ.

За таких умов СУЖЦО має бути інтегрованою системою, що забезпечує відповідність між стратегічними потребами ЗС України, оборонним бюджетом та спроможностями промисловості. Вона має включати організаційні, нормативно-правові, технічні та інформаційні механізми, що регламентують управління життєвим циклом ОВТ – від розроблення і виробництва до застосування за призначенням та утилізації.

Основними функціями такої системи мають стати:

– стандартизація та уніфікація озброєння для зменшення різнотипності й підвищення ефективності логістичного забезпечення ЗС України;

– координація дій між суб’єктами оборонного планування (ГШ ЗС України, Міністерством оборони, оборонними підприємствами) для усунення розбіжностей функцій та підвищення ефективності взаємодії з питань життєвого циклу ОВТ;

– інтеграція національної системи озброєння до міжнародних стандартів (зокрема стандартів НАТО);

– забезпечення оперативної сумісності між підрозділами;

– оптимізація витрат через серійне виробництво та масштабування, що знижує вартість закупівель і логістичного забезпечення.

Важливу роль в удосконаленні СУЖЦО має відігравати ГШ ЗС України як центральний орган координації системи управління життєвим циклом ОВТ, забезпечуючи її цілісність, ефективність та відповідність завданням оборони держави.

Його основні завдання в межах СУЖЦО мають стосуватися формування стратегічних та оперативно-тактичних вимог до ОВТ, прогнозів розвитку конфліктів та виявлення загроз, контролю відповідності закупівель стандартам ЗС України та оборонним цілям, що сприятиме уніфікації та оперативній сумісності ОВТ, необхідно спільно з Міністерством оборони формувати довгострокові програми розвитку ОВТ, враховуючи не лише потреби сьогодення, а й перспективи майбутніх конфліктів, а також здійснювати моніторинг ефективності всіх етапів життєвого циклу ОВТ, що дозволяє оптимізувати логістичне забезпечення військ (сил).

Хоча Міністерство оборони відповідає за формування військово-технічної політики, саме ГШ ЗС України визначає реальні потреби ЗС України в ОВТ та забезпечує їхню інтеграцію у систему стратегічного планування. Наприклад, на основі аналізу застосування військ (сил) ГШ ЗС України визначає критичні вимоги до ОВТ, які стають основою для розроблення стратегічних планів стандартизації та модернізації озброєння.

Варіант розподілу повноважень між Міністерством оборони та ГШ ЗС України під час формування та впровадження СУЖЦО представлено в табл. 1.

Для зменшення різнотипності озброєння у ЗС України необхідно розробити цілісний стратегічний підхід до управління життєвим циклом ОВТ, який інтегрує всі етапи життєвого циклу ОВТ (від формування потреби до утилізації) в єдину систему управління. Така система має бути спрямована на уніфікацію, стандартизацію та оптимізацію процесів, забезпечуючи взаємозв’язок між стратегічними цілями, оперативними потребами та економічною доцільністю.

**Таблиця1.** Розподіл повноважень між Міністерством оборони та Генеральним штабом під час формування та впровадження системи управління життєвим циклом озброєння

| Сфера діяльності | Міністерство оборони | Генеральний штаб ЗСУ |
|---|---|---|
| Формування політики у сфері управління озброєнням | Розробляє військово-технічну політику, яка включає обов’язкові вимоги до уніфікації та стандартизації озброєння | Визначає оперативні потреби ЗСУ, які враховують наявне озброєння та стратегічні цілі оборони держави |
| Стандартизація озброєння | Затверджує єдині стандарти озброєння відповідно до вимог НАТО | Формує детальні вимоги до ОВТ, унеможливлюючи закупівлю озброєння, що не відповідає стандартам |
| Планування закупівель | Затверджує програму закупівель із урахуванням необхідності уніфікації ОВТ | Подає запити на закупівлю ОВТ, що відповідає стандартам та потребам військ (сил) |
| Організація закупівель | Встановлює тендерні вимоги та обмеження на закупівлю несумісного ОВТ | Оцінює технічні пропозиції, підтверджує відповідність вимогам і стандартам |
| Контроль якості озброєння | Організовує сертифікацію ОВТ відповідно до стандартів | Контролює відповідність ОВТ вимогам та умовам їх уніфікації і стандартизації |
| Управління життєвим циклом озброєння | Координує модернізацію та оновлення ОВТ для зменшення різнотипності | Відповідає за планування експлуатації та обслуговування ОВТ |
| Зменшення різнотипності озброєння | Розробляє нормативні акти для обмеження різнотипності ОВТ | Проводить моніторинг закупівель і контролює відповідність стандартам |

Цілісний стратегічний підхід до управління життєвим циклом озброєння – це не просто набір окремих рішень, а інтегрована модель, що охоплює всі ключові етапи життєвого циклу:

– планування, розроблення та виробництво ОВТ (з урахуванням прогнозованих потреб);

– застосування за призначенням (експлуатацію) та модернізацію (з урахуванням реальної бойової ефективності ОВТ на полі бою);

– утилізацію та заміну (з урахуванням довгострокової економічної доцільності).

Цей підхід базується на трьох принципах: координація дій між основними органами управління; дотримання міжнародних стандартів (насамперед стандартів НАТО); врахування досвіду застосування ОВТ для підвищення ефективності застосування з'єднань і частин, а також раціонального використання ресурсів.

Ключовим елементом цілісного стратегічного підходу є ГШ ЗС України, який має виступати координаційним центром між органами військового управління, забезпечуючи інтеграцію стратегічного, оперативного й тактичного рівнів планування та управління. Саме ГШ ЗС України формує систему вимог до ОВТ, узгоджує їх із реальними потребами військ та контролює стандартизацію ОВТ.

Упровадження такого підходу дозволить зменшити різнотипність ОВТ у військах (силах) шляхом запровадження уніфікованих стандартів, підвищити ефективність застосування ЗС України за допомогою кращої сумісності ОВТ та оптимізувати витрати на логістичне забезпечення з'єднань і частин, у тому числі на технічне обслуговування та ремонт. Це дасть можливість створити більш ефективну, гнучку та уніфіковану систему ОВТ, яка відповідатиме сучасним і перспективним стандартам та викликам. Компоненти єдиного стратегічного підходу до зменшення різнотипності ОВТ наведено в табл. 2.

**Таблиця 2.** Компоненти єдиного стратегічного підходу до зменшення різнотипності ОВТ

| Компонент | Зміст | Очікуваний результат |
|---|---|---|
| 1. Формування стратегічних потреб | Визначення оперативних і бойових завдань ЗСУ з урахуванням довгострокових цілей розвитку | Озброєння відповідає реальним потребам військ |
| 2. Стандартизація та уніфікація | Упровадження єдиних національних і міжнародних стандартів, що регламентують взаємозамінність ОВТ | Скорочення різнотипності ОВТ, підвищення його сумісності |
| 3. Інтеграція управління життєвим циклом | Включення всіх етапів – від розроблення до утилізації – в єдину систему управління | Оптимізація процесів життєвого циклу ОВТ, зниження витрат |
| 4. Централізоване планування та контроль | Управління закупівлями, модернізацією та логістичним забезпеченням на основі єдиної стратегії | Уникнення дублювання функцій та оптимізація ресурсів |
| 5. Роль Генерального штабу | Формування вимог, участь у стандартизації, моніторинг сумісності | Закупівлі та модернізація ОВТ відповідно до реальних потреб військ |
| 6. Міжнародна інтеграція | Орієнтація на стандарти НАТО, співпраця з міжнародними партнерами та виробниками | Сумісність ОВТ з країнами-партнерами, посилення обороноздатності |
| 7. Економічна доцільність | Зниження витрат завдяки уніфікації, серійному виробництву та оптимізації логістичного забезпечення | Ефективне використання ресурсів, зменшення фінансового навантаження |
| 8. Інформаційні технології | Упровадження цифрових систем управління життєвим циклом ОВТ | Автоматизація процесів, прозорість і точність даних про стан ОВТ |

Ефективне впровадження інтегрованої моделі управління життєвим циклом ОВТ потребує комплексного підходу до стандартизації та уніфікації ОВТ, що забезпечує взаємозамінність та сумісність озброєння як у межах ЗС України, так і щодо міжнародних стандартів.

ГШ ЗС України відіграє ключову роль у формуванні вимог до ОВТ, зокрема в питаннях щодо оперативної сумісності, уніфікації та координації зусиль з Міністерством оборони та підприємствами оборонної промисловості.

Однією з основних проблем сьогодні є закупівля різнотипних зразків ОВТ, які не завжди відповідають реальним потребам військ (сил). Формально такі зразки можуть відповідати стандартам, але через неузгодженість нормативної бази вони часто не інтегруються з існуючими системами. Це ускладнює застосування ОВТ за призначенням у складі частин (підрозділів) і переобтяжує систему логістичного забезпечення військ (сил).

За цих умов ГШ ЗС України має забезпечити оперативну та стратегічну координацію в питаннях щодо стандартизації ОВТ, формуючи:

– перелік стандартних зразків ОВТ для застосування у видах (родах військ (сил);

– уніфікацію ключових параметрів, таких як калібри озброєння, системи зв'язку, базові платформи, що сприяє зниженню різнотипності ОВТ;

– контроль відповідності закупівель та модернізації ОВТ затвердженим стандартам.

Запровадження інтегрованої моделі управління життєвим циклом ОВТ на основі координації між ГШ ЗС України, Міністерством оборони та підприємствами оборонного комплексу дозволить зменшити різнотипність та підвищити рівень стандартизації ОВТ, оптимізувати витрати на логістичне забезпечення, у тому числі створення запасів, технічне обслуговування та ремонт, а також забезпечить сумісність ОВТ ЗС України з ОВТ країн – членів НАТО, що сприятиме інтеграції України в міжнародні оборонні ініціативи.

Варіант ролі ГШ ЗС України у питаннях стосовно стандартизації та уніфікації ОВТ, що є критично важливими для зменшення різнотипності озброєння та підвищення ефективності ЗС України, показано в табл. 3.

**Таблиця 3.** Роль ГШ ЗС України у питаннях щодо стандартизації та уніфікації ОВТ (варіант)

| Сфера діяльності | Роль ГШ ЗС України | Очікуваний результат |
|---|---|---|
| Формування потреб та пріоритетів | Визначення оперативно-стратегічних та оперативно-тактичних вимог до ОВТ | Закупівля та модернізація ОВТ відповідно до реальних потреб військ (сил) |
| | Аналіз існуючих зразків ОВТ та оцінювання необхідності уніфікації | Уникнення дублювання та зменшення різнотипності ОВТ |
| Розроблення стандартів | Визначення критеріїв сумісності та уніфікації | Єдині вимоги до ОВТ, відповідність стандартам НАТО |
| | Участь у міжвідомчих комісіях та робочих групах із розроблення стандартів | Включення оперативних вимог до стандартів на всіх стадіях їх розроблення |
| Оцінювання сумісності зразків ОВТ | Аналіз відповідності закупівель підтвердженим стандартам | Мінімізація проблем логістичного забезпечення |
| | Моніторинг сумісності нових зразків ОВТ із наявними системами | Оптимізація застосування ОВТ |
| Контроль виконання стандартів | Нагляд за дотриманням стандартів у процесах закупівлі, виробництва та експлуатації | Узгодженість нового озброєння зі стратегічними цілями ЗС України |
| | Оцінювання ефективності стандартів на основі бойового досвіду | Оновлення стандартів відповідно до реальних умов застосування ОВТ |

Завдяки такому підходу ГШ ЗС України може ефективно керувати стандартизацією, координацією та впровадженням уніфікованого підходу до життєвого циклу ОВТ, забезпечуючи єдність системи оборонного планування та бойового застосування ОВТ.

**Висновок (Conclusion)**

Отже, впровадження СУЖЦО в поєднанні з єдиним стратегічним підходом до стандартизації та уніфікації ОВТ є нагальною потребою для ЗС України. Такий підхід відкриває низку можливостей і дозволить вирішити проблемні питання, що стосуються різнотипності, шляхом уніфікації ОВТ. Це сприятиме скороченню витрат на їхнє логістичне забезпечення. Крім того, уніфіковані стандарти нададуть змогу ефективніше планувати закупівлі ОВТ, уникати дублювання видатків, а також спрямовувати ресурси на розроблення та модернізацію високопріоритетних зразків ОВТ. Упровадження таких ініціатив може стати ключовим кроком до інтеграції ЗС України з міжнародними оборонними стандартами, зокрема стандартами НАТО (STANAG). У перспективі це сприятиме підвищенню оперативної сумісності ЗС України з військами країн-партнерів.

Розроблені пропозиції можуть бути використані для формування державної політики у сфері управління озброєнням.

У подальшому напрямами досліджень можуть бути вивчення можливостей адаптації існуючих міжнародних моделей управління життєвим циклом озброєння до умов України, аналіз ризиків упровадження запропонованої системи в умовах обмежених ресурсів, дослідження шляхів прозорого та конкретного проведення оборонних закупівель в умовах уніфікації ОВТ.

**Використані джерела**

1. Танковий зоопарк: скільки десятків моделей та версій танків у ЗСУ вже зараз й очікується, та що з цим робити. *Defense Express*. https://defence-ua.com/army_and_war/tankovij_zoopark_skilki_desjatkiv_vidiv_tankiv_u_zsu_vzhe_zaraz_j_ochikujetsja_ta_scho_z_tsim_robiti-10448.html.
2. Кулагін, К. К., Солонець, О. І., Ведмідь, О. І., Квіткін, К. П., & Борисенко, М. В. (2022). Реформування національної системи управління життєвим циклом озброєння та військової техніки за стандартами НАТО. *Системи озброєння і військова техніка*, *3* (71), 24–34. https://doi.org/10.30748/soivt.2022.71.04.
3. Павловський, І. В., Чепков, І. Б., Борохвостов, В. К., & Рябець, О. М. (2017). Науково-методичні підходи до аналізу воєнно-технічних і техніко-економічних аспектів життєвого циклу зразків озброєння та військової техніки. *Наука і оборона, 2,* 43–51.
4. Кондратенко, Ю. В. (2020). Обґрунтування врахування життєвого циклу зразків ОВТ під час оборонного планування на основі спроможностей. *Зб. наук. пр. Центру воєнно-стратегічних досліджень Нац. ун-ту оборони України, 3* (70), 47–54.
5. Сіренко, В. Є., & Демченко, Є. Я. (2019). Повний життєвий цикл озброєння та військової техніки у якості критеріальної ознаки програмно-цільового планування їх розвитку. *Озброєння та військова техніка, 2* (22), 3–15.
6. Гриб, Д. А., Демідов, Б. О., Кулагін, К. К., & Хмелевська, О. О. (2020). Проблемні аспекти науково-технічного супроводження процесу управління повним життєвим циклом складних зразків озброєння та військової техніки. *Системи озброєння і військова техніка*, *2* (62), 129–140. https://doi.org/10.30748/soivt.2020.62.16.
7. Кулагін, К. К., Шевченко, І. І., Солонець, О. І., Шевченко, І. А., Кошель, А. В., & Петров, С. В. (2018). Проблеми створення системи державного гарантування якості оборонної продукції відповідно до стандартів НАТО. *Стандартизація, сертифікація, якість, 4* (111), 42–52.
8. Семененко, О., Чернишова, І., Онофрійчук, П., Мотрунич, І., Харитонов, К., & Демчук, Р. (2021). Методичний підхід до обґрунтування вартості життєвого циклу носіїв спроможностей Збройних Сил України (організаційних структур та органів управління). *Journal of Scientific Papers, 4* (11), 14–30.

9. Турінський, О. В., Демідов, Б. О., Гриб, Д. А., Хмелевський, С. І., & Хмелевська, О. О. (2020). Фінансово-економічні аспекти життєвих циклів складних наукоємних і високотехнологічних зразків озброєння і військової техніки. *Наука і техніка Повітряних Сил Збройних Сил України, 3* (40), 50–60. https://doi.org/10.30748/nitps.2020.40.06.
10. *Методичні рекомендації з фінансово-економічного обґрунтування вартості повного життєвого циклу спроможностей з урахуванням принципів та стандартів НАТО.* https://www.mil.gov.ua./content/oboron_plans/metod_recom_z_fin_ekon_life_ciklu_nato.pdf.
11. Міністерство оборони України. (2024, 11 квіт.). *Про затвердження Інструкції планування оборонних закупівель товарів, робіт і послуг на постачання (розроблення, модернізацію, ремонт) озброєння, військової та спеціальної техніки, ракет і боєприпасів, іншого військово-технічного майна і послуг в інтересах Збройних Сил України в умовах правового режиму воєнного стану (226/2024).* https://zakon.rada.gov.ua/rada/show/v0226322-24#n37.

**References**

1. Tank Zoo: How Many Dozens of Tank Models and Versions Are Already Expected in the Armed Forces of Ukraine, and What to Do About It. *Defense Express*. https://defence-ua.com/army_and_war/tankovij_zoopark_skilki_desjatkiv_vidiv_tankiv_u_zsu_vzhe_zaraz_j_ochikujetsja_ta_scho_z_tsim_robiti-10448.html.
2. Kulagin, K. K., Solonets, O. I., Vedmid, O. I., Kvitkin, K. P., & Borisenko, M. V. (2022). Reforming the National System of Lifecycle Management of Armaments and Military Equipment according to NATO Standards. *Armaments and Military Equipment, 3* (71), 24–34. https://doi.org/10.30748/soivt.2022.71.04.
3. Pavlovsky, I. V., Chepkov, I. B., Borokhvostov, V. K., & Ryabets, O. M. (2017). Scientific and methodological approaches to the analysis of military-technical and technical-economic aspects of the life cycle of weapons and military equipment samples. *Science and Defense, 2*, 43–51.
4. Kondratenko, Yu. V. (2020). Justification of taking into account the life cycle of weapons and military equipment samples during capabilities-based defense planning. *Collection of scientific papers of the Center for Military-Strategic Research of the National Defense University of Ukraine, 3* (70), 47–54.
5. Sirenko, V. Ye., & Demchenko, Ye. Ya. (2019). The full life cycle of weapons and military equipment as a criterion feature of program-targeted planning of their development. *Armaments and military equipment, 2* (22), 3–15.
6. Hryb, D. A., Demidov, B. O., Kulagin, K. K., & Khmelevska, O. O. (2020). Problematic aspects of scientific and technical support of the process of managing the full life cycle of complex weapons and military equipment. *Weapons systems and military equipment, 2* (62), 129–140. https://doi.org/10.30748/soivt.2020.62.16.
7. Kulagin, K. K., Shevchenko, I. I., Solonets, O. I., Shevchenko, I. A., Koshel, A. V., & Petrov, S. V. (2018). Problems of creating a system of state quality assurance of defense products in accordance with NATO standards. *Standardization, certification, quality, 4* (111), 42–52.
8. Semenenko, O., Chernyshova, I., Onofriychuk, P., Motrunych, I., Kharytonov, K., & Demchuk, R. (2021). Methodological approach to substantiating the life cycle cost of the capabilities of the Armed Forces of Ukraine (organizational structures and management bodies). *Journal of Scientific Papers, 4* (11), 14–30.
9. Turinsky, O. V., Demidov, B. O., Hryb, D. A., Khmelevsky, S. I., & Khmelevska, O. O. (2020). Financial and economic aspects of the life cycles of complex science-intensive and high-tech weapons and military equipment. *Science and Technology of the Air Force of the*

*Armed Forces of Ukraine, 3* (40), 50–60. https://doi.org/10.30748/nitps.2020.40.06.
10. *Methodological recommendations for financial and economic justification of the cost of the full life cycle of capabilities taking into account NATO principles and standards.* https://www.mil.gov.ua./content/oboron_plans/metod_recom_z_ fin_ekon_life_ciklu_nato.pdf.
11. Ministry of Defense of Ukraine. (2024, Apr. 11). *On approval of the Instructions for planning defense procurement of goods, works and services for the supply (development, modernization, repair) of weapons, military and special equipment, missiles and ammunition, other military-technical property and services in the interests of the Armed Forces of Ukraine under the legal regime of martial law (226/2024).* https://zakon.rada.gov.ua/rada/show/v0226322-24#n37.

## On optimization of weapons management in the armed forces

**Oleksii Shevchenko**
Candidate of Historical Sciences
Deputy Chief of the General Staff of the Armed Forces of Ukraine
General Staff of the Armed Forces of Ukraine
03168, Povitrianykh syl avenue, 6, Kyiv, Ukraine
e-mail:shevchenko_om@asv.gov.ua
ORCID: 0000-0003-0734-6533

**Oleh Semenenko**
Honoured Science and Technology Figure of Ukraine
Doctor of Military Sciences, Professor
Deputy Commandant of the Central Research Institute
of the Armed Forces of Ukrainefor scientific work
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh syl avenue, 28 B, Kyiv, Ukraine
e-mail: aosemenenko@ukr.net
ORCID: 0000-0001-6477-3414

**Petro Zakusylo**
Doctor of Military Sciences, Professor
Leading Research Fellow
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh syl avenue, 28 B, Kyiv, Ukraine
e-mail: Zps20072017@gmail.com
ORCID: 0000-0003-0421-7736

**Vasyl Kharchenko**
Candidate of Military Sciences (PhD)
Leading Research Fellow
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh syl avenue, 28 B, Kyiv, Ukraine
e-mail: vasaxar@ukr.net
ORCID: 0000-0001-7160-7385

The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 3 No. 2 (2025)

**Volodymyr Musiyenko**
Senior Lecturer at the Department of Military Training, Senior Research Fellow
Military Institute of Telecommunications and Information Technologies
Heroes of Kruty Military
Institute of Telecommunications and Information Technologies
01011, Knyaziv Ostrozkykh Street, 45/1, Kyiv, Ukraine
e-mail: volodymyr.musienko@viti.edu.ua
ORCID: 0000-0002-4909-6045

**Oleh Melnychuk**
Lecturer at the Department of Fire Training
Faculty of Logistics
National Academy of the National Guard of Ukraine
61001, Defenders of Ukraine Square, 3, Kharkiv, Ukraine
e-mail: melnichuk1973@gmail.com
ORCID: 0009-0002-4499-1902

**Abstract.** Ensuring Ukraine's defense capability largely depends on an effective weapons life cycle management system (WLMS). However, the current legislation does not provide a comprehensive approach to weapons management that would cover all stages of the equipment life cycle: from planning needs and development to intended use and disposal. The lack of a single regulation in the interaction of the General Staff of the Armed Forces of Ukraine (GSAF of Ukraine), the Ministry of Defense and defense complex enterprises causes an imbalance in the processes of procurement, standardization, use, and modernization of weapons and military equipment (WME), which in turn leads to an increase in the level of their heterogeneity in the troops (forces).

The diversity of AME creates a number of problems, in particular, it complicates the organization and conduct of maintenance and repair, increases operating costs, makes serial production and its scaling impossible, reduces interoperability both within the Armed Forces of Ukraine (AFU) and in the context of integration with NATO standards.

Improving the AME, which would block these challenges, is a necessary condition for reducing the level of diversity of AME in the AFU.

To this end, a holistic strategic approach is proposed that integrates all stages of the AME life cycle into a single management system with an emphasis on unification, standardization and optimization. Such an approach assumes clear interaction between key military management bodies (Ministry of Defense, General Staff of the Armed Forces of Ukraine, Command of the types (branches) of troops (forces), Command of the Logistics Forces), taking into account the real needs of the effective use of formations (units) and the rational use of allocated resources, as well as compliance with international standards, in particular NATO standards.

**Keywords:** efficiency, life cycle of weapons, procurement, Armed Forces of Ukraine, weapons and military equipment, needs, diversity, standardization, management system, unification.

The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 3 No. 2 (2025)

DOI: 10.62524/msj.2025.3.2.8

# Аналіз ризиків під час обґрунтування вимог до спроможностей складу військ (сил)

**Олександр Павлюк**
Командувач Сухопутних військ Збройних Сил України
Командування Сухопутних військ Збройних Сил України
04119, вулиця Дегтярівська, 19/7, Київ, Україна
e-mail: press.ksv@post.mil.gov.ua
ORCID: 0000-0002-6520-0797

**Володимир Дідіченко**
кандидат військових наук, старший науковий співробітник
старший науковий співробітник
Центральний науково-дослідний інститут ЗбройнихСил України
03049, проспект Повітряних Сил, 28Б, Київ, Україна
e-mail: DVP1951@ukr.net
ORCID: 0000-0002-0440-2299

**ВасильЧереп**
кандидат військових наук, старший дослідник
начальник науково-дослідного управління
Центральний науково-дослідний інститут Збройних Сил України
03049, 28Б проспект Повітряних Сил, 28Б, Київ, Україна
e-mail: vasya.cherep1976@gmail.com
ORCID: 0000-0003-3305-4518

**Степан Возняк**
кандидат технічних наук, старший науковий співробітник
начальник науково-дослідного відділу
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: step_voz@ukr.net
ORCID: 0000-0002-9015-813X

**Артем Ремез**
доктор філософії
старший викладач кафедри оперативного мистецтва
Національний університет оборони України
03049, проспект Повітряних Сил, 28, Київ, Україна
e-mail: remez.art.86@gmail.com
ORCID: 0000-0003-4970-1097

***“Ризик (англ. risk) – це ситуація, пов’язана з небезпекою; ймовірність (можливість) того, що станеться щось неприємне”.***

*(Оксфордський словник англійської мови)*

**Анотація.** Актуальність дослідження зумовлена необхідністю вдосконалення управління ризиками в процесах оборонного планування Міністерства оборони та Збройних Сил України, що здійснюються в умовах постійних змін і високої невизначеності безпекового середовища.

Мета статті полягає в аналізі ризиків, які виникають при визначенні вимог до спроможностей складу військ (сил), та у розробленні ефективних методологічних підходів до управління цими ризиками для підвищення результативності оборонного планування.

Під час дослідження застосовано комплексний підхід, що охоплює аналіз нормативно-правових актів, доктринальних і стратегічних документів, огляд сучасних наукових публікацій, а також використання передових міжнародних методик оцінювання і класифікації ризиків.

Основними результатами роботи є визначення ключових джерел виникнення ризиків у процесах оборонного планування, створення детальної семантичної моделі управління ризиками, формування чіткої структури та змісту реєстру ризиків, а також удосконалення класифікації ризиків за характером, ступенем їхнього впливу на процеси планування та визначення пріоритетності реагування. Практична значущість отриманих результатів полягає в можливості їх застосування для зменшення рівня невизначеності, мінімізації потенційних негативних наслідків ризиків, забезпечення оперативної адаптації до змін безпекової ситуації, підвищення ефективності використання ресурсів та поліпшення якості ухвалення стратегічних і тактичних рішень у сфері оборони. Матеріали статті будуть корисними для фахівців Міністерства оборони та Збройних Сил України у процесах формування перспективного складу сил оборони, а також науковців, які займаються питаннями управління ризиками й розвитку військових спроможностей.

**Ключові слова:** вимоги, оборонне планування, ризик, спроможність, управління ризиками.

## Вступ (Introduction)

Одним із основних завдань оборонного планування на основі спроможностей є: визначення вимог до спроможностей, структури, чисельності особового складу, кількісних та якісних показників озброєння та військової техніки, інших видів матеріально-технічних засобів, військової інфраструктури, підготовленості особового складу сил оборони (формування перспективного складу Збройних Сил України (ЗС України), який задовольняє вимогам щодо необхідних спроможностей з урахуванням можливостей держави задовольнити потреби оборони).

В основу визначення вимог до спроможностей військ (сил) покладаються: висновки з оцінювання середовища безпеки; цілі та завдання за ймовірними сценаріями та варіантами застосування ЗС України; вимоги до складу військ (сил) відповідно до завдань, які можуть бути покладені на ЗС України; кількісні показники типів зброї за сферами воєнних дій (суша, повітря, море, кіберпростір тощо).

За визначеними вимогами до кількості та якості систем озброєння, а також систем управління й логістики визначаються вимоги до спроможностей складу військ (сил) ЗС України, які необхідні для виконання кожного завдання на стратегічному, оперативному та тактичному рівнях.

З огляду на те, що склад військ (сил), визначений для виконання завдань, є сукупністю різних за оперативним (бойовим) призначенням з'єднань і військових частин видів і родів військ ЗС України, військ, що не входять до видів ЗС України, логістики, спроможності, які необхідні для виконання кожного завдання, будуть поєднувати спроможності всіх елементів (компонентів) визначеного складу військ (сил).

Аналіз типових завдань, які можуть бути покладені на війська (сили), свідчить про те, що до кожного елемента (компонента) визначеного складу військ (сил) висуваються свої, притаманні саме цьому елементу (компоненту) вимоги. Разом із тим, на різні за складом та призначенням військові формування, які мають на озброєнні різні типи, зразки, системи озброєння, можуть покладатися однакові завдання. Позбутися дублювання завдань та неекономного використання ресурсів, що виділяються для їх виконання, можливо завдяки раціональному використанню наявних сил та засобів. З цією метою висуваються вимоги до спроможностей для кожного елемента (компонента) складу військ (сил), визначеного для виконання конкретного завдання.

Оборонне планування здійснюється в умовах невизначеності. Тому ухвалення рішення та визначення пріоритетів формування складу військ (сил), здатного за своїми спроможностями виконати визначені завдання, пов'язано з ризиками неврахування чинників, які так чи інакше можуть впливати на визначення вимог до спроможностей складу військ (сил). Потреба в оцінюванні невизначеностей й управління ризиками з метою зменшення їхнього впливу зумовлює актуальність наукового завдання щодо аналізу ризиків під час обґрунтування вимог до спроможностей складу військ (сил).

**Методологічна основа (Methodological Framework)**

Аналіз публікацій та попередніх досліджень, довідкових та інформаційних матеріалів виявив, що питанню управління ризиками приділяється значна увага.

Невизначеність як неможливість оцінити майбутній розвиток подій із погляду як імовірності їхньої реалізації, так і виду їхнього прояву визначається у [1].

Н. Сарай [24] зазначає, що невизначеність – неповноцінність чи неточність інформації про умови реалізації проєктів або програм, зокрема пов'язаних із ними результатів. Невизначеність, пов'язана з можливістю виникнення несприятливих ситуацій і наслідків, характеризується наявністю ризику і потребує його оцінювання.

За В. Вітлінським, Г. Великоіваненко [2], невизначеність тісно пов'язана з ризиком та є його першопричиною. А ризик, у найширшому розумінні – це невизначеність стосовно здійснення тієї чи іншої події у майбутньому.

Ризик розглядають М. Д. Балджи, В. А. Карпов, А. І. Ковальов, О. О. Костусєв, І. М. Котова, Н. В. Сментина [1] як діяльність, що пов'язана з подоланням невизначеності в ситуації неминучого вибору, у процесі якого є можливість кількісно і якісно оцінити вірогідність досягнення передбаченого результату, невдачі та відхилення від мети.

Стаття Є. М. Пащенко, С. М. Іващенко [14] розглядає поняття ризику в трьох взаємопов'язаних аспектах, а управління ризиком як процес ухвалення рішень і здійснення заходів, спрямованих на зміну ризику. У контексті цієї статті ризик означає можливість виникнення небажаних подій або невдач, які можуть завадити досягненню поставлених цілей.

Найбільш детально питання оцінювання ризиків розглядається у [7], який призначено для того, щоб викласти належні сучасні методики вибирання та застосовування методів загального оцінювання ризику. У ньому не розглядають нові чи розроблювані концепції, щодо яких ще не досягнуто задовільного рівня професійного консенсусу. Він має загальний характер, тому може слугувати настановою для багатьох галузей і типів систем.

Загальні терміни, пов'язані з управлінням ризиками, визначено у [28].

У Доктрині "З оборонного планування у Збройних Силах України" [3] визначено мету управління ризиками оборонного планування, ознаки ризиків та суб'єкти управління ризиками.

Можливі підходи до створення та функціонування системи управління вимогами (СУВ) щодо розвитку спроможностей в органах управління як МО України та ЗС України, так й інших складових сил оборони (ССО) України висвітлено у В. Корендовича, А. Наливайко, А. Поляєва [9].

У І. С. Руснак, А. Г. Петренко, А. В. Яковенко, І. М. Романюк, В. Д. Кохно [23] зазначається, що перехід до планування на основі спроможностей потребує вирішення низки окремих проблемних питань, зокрема оцінювання ризиків, пов'язаних із вибором того чи іншого варіанта розвитку спроможностей залежно від наявного фінансового ресурсу.

Проблемні питання ідентифікації ризиків і загроз безпеці державного кордону та аналіз систем і моделей управління ризиками, кожна з яких досліджує ризики та загрози за визначеними параметрами (імовірність виникнення, можливі наслідки, їхня важкість тощо), розглядалися В. Никифоренко [12]. Зроблено висновок, що вдосконалення системи аналізу та оцінювання ризиків забезпечує ефективне реагування на виклики та загрози безпеці держави.

Комплексний метод визначення вимог до спроможностей збройних сил та інших складових сил оборони запропоновано О. Сурковим [26].

Міжнародний стандарт [19] містить принципи та рекомендації щодо управління ризиками, описує комплексний підхід до ідентифікації, аналізу, оцінювання, оброблення, моніторингу та звітування про ризики.

Досить ретельно управління ризиками оборонного планування розглянуто у Рекомендаціях з оборонного планування на основі спроможностей в Міністерстві оборони України та ЗС України [15], де визначено суб'єкти управління ризиками, процедури процесу управління ризиками, запропоновано методичні підходи до визначення ймовірності та істотності впливу виникнення конкретного ризику, побудови матриці ймовірності та впливу ризику, а також визначення способів реагування на ідентифіковані та оцінені ризики.

Використання процедур планування розвитку спроможностей військових формувань, що застосовують країни – члени НАТО, з урахуванням умов і набутого досвіду планування ЗС України, запропоновано [4].

Водночас, поза увагою залишаються питання аналізу та оцінювання невизначеностей та ризиків, які виникають або можуть виникнути під час визначення вимог до процедур оборонного планування, встановлення їхнього впливу на визначення вимог до спроможностей складу військ (сил).

**Результати і обговорення (Results and Discussions)**

Оборонне планування є важливим інструментом, який дозволяє прогнозувати та планувати дії для досягнення поставлених цілей. Здійснення оборонного планування характеризується певним ступенем невизначеності через відсутність необхідної інформації. У загальному сенсі "невизначеність" означає неможливість оцінити майбутній розвиток подій як з точки зору ймовірності їхньої реалізації, так і з точки зору видів їхнього прояву. Ступінь невизначеності залежить як від характеру невизначених параметрів, так і від терміну прогнозування (зростає зі збільшенням останнього).

Основними причинами виникнення невизначеності є недетермінованість процесів оборонного планування, що відбуваються; відсутність повної інформації; вплив суб'єктивних чинників на результати проведеного аналізу.

Уникнути невизначеності під час здійснення оборонного планування неможливо. Вона є елементом об'єктивної дійсності, тому що завжди існує аспект неоднозначності розвитку, неможливості точного прогнозування певних подій, неповної чи недостовірної інформації.

Невизначеність – це одна з причин виникнення ризику. Існування невизначеності під час здійснення оборонного планування є необхідною умовою виникнення ризиків, без яких неможливе ефективне планування.

Під "ризиком" І. В. Рішняк [18] розуміє можливість недосягнення поставленої мети, зумовлену необхідністю ухвалення рішення в умовах невизначеності.

Основними джерелами ризику визначення вимог до спроможностей складу військ (сил) є зовнішні та внутрішні невизначеності, пов'язані з імовірністю настання подій і явищ, які

впливають на оборонне планування у цілому та визначення вимог до спроможностей складу військ (сил) зокрема. Тобто є логічний зв'язок (рис. 1).




**Рисунок 1.** Логічний зв'язок для виникнення ризику

Іншими словами, ймовірність створює невизначеність, що призводить до ризику. Отже, ризик залежить від невизначеності – зменшення ризику можна досягти шляхом мінімізації невизначеності. Це зумовлює потребу в оцінюванні невизначеностей й управління ризиками з метою зменшення їхнього впливу на процедури оборонного планування.

У Рекомендаціях з оборонного планування на основі спроможностей в Міністерстві оборони України та ЗС України [15] визначено основні процедури оборонного планування: оцінювання середовища безпеки; планування сил; планування ресурсів; оцінювання ризиків; формування перспективної моделі (структури) ЗС України; підготовка програмних документів їхнього розвитку.

Вимоги є основою, внутрішнім змістом процедур оборонного планування. Саме вони визначають весь процес оборонного планування, забезпечуючи відповідність результату визначеним потребам.

Результат, отриманий на попередній процедурі оборонного планування, є основою, вихідними даними для визначення вимог та проведення наступної процедури (рис. 2).




**Рисунок 2.** Місце вимог до процедур оборонного планування

Оцінювання середовища безпеки є однією з основних процедур оборонного планування. Вихідні дані, сформовані за результатами оцінювання, є основою для здійснення подальших процедур оборонного планування, вони мають бути враховані під час визначення вимог до цих процедур. Повнота та достовірність вихідних даних забезпечується беззаперечним дотриманням визначених вимог до опису безпекового середовища (рис. 3).

Підготовка вихідних даних для подальших процедур оборонного планування передбачає виявлення та реагування на ризики вимог, які можуть виникнути в процесі оцінювання середовища безпеки (табл. 1).

На основі варіантів застосування ЗС України для виконання завдань, визначених сценаріями, здійснюється планування сил. Вимоги до цього процесу оборонного планування мають враховувати результати оцінювання середовища безпеки, зміст завдань за кожним зі сценаріїв, опис умов та критеріїв виконання завдань (рис. 4).

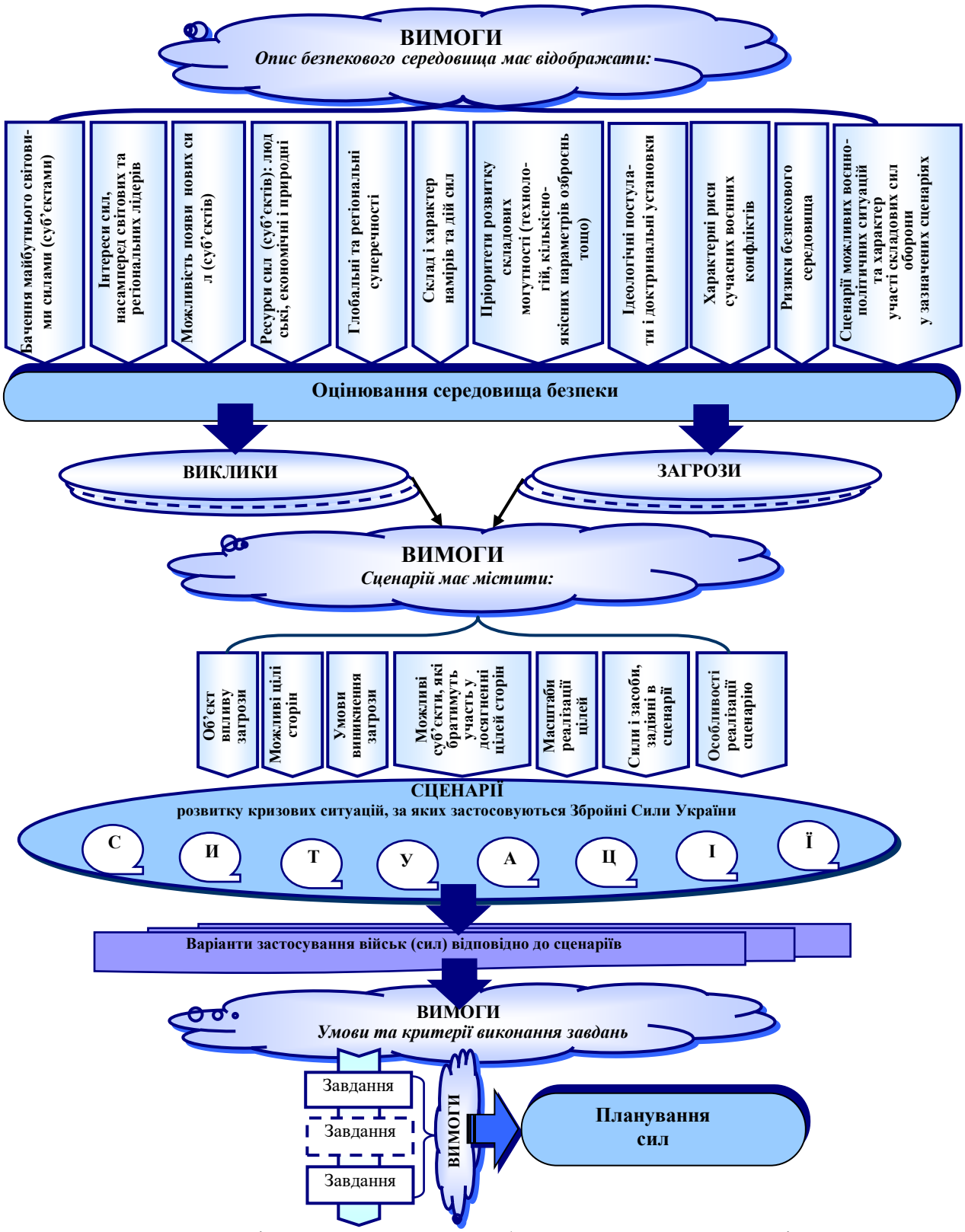



**Рисунок 3.** Сукупність вимог процедури оборонного планування "Оцінювання середовища безпеки"

Визначення вимог до спроможностей складу військ (сил) для виконання завдань за сценаріями є основною складовою процесу планування сил. Саме вимоги до спроможностей є основою:

- ❖ визначення необхідних спроможностей для виконання завдань за варіантами застосування;
- ❖ оцінювання наявних спроможностей та відповідності їх вимогам (здатності до виконання завдань за призначенням);
- ❖ визначення недостатніх та надлишкових спроможностей шляхом порівняння необхідних та наявних спроможностей;
- ❖ забезпечення формування перспективного складу ЗС України.

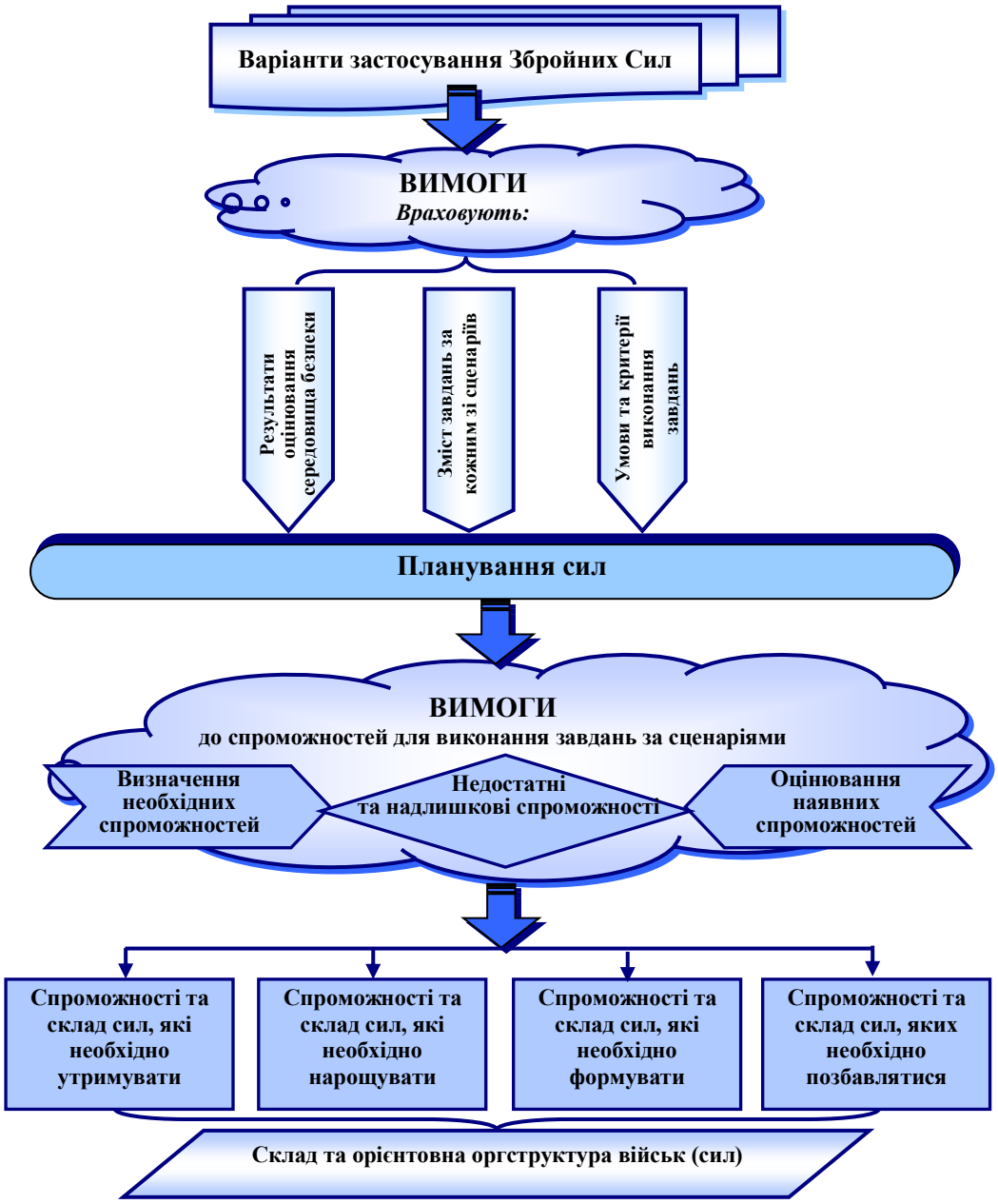



**Рисунок 4.** Сукупність вимог процедури оборонного планування “Планування сил”

**Таблиця 1.** Перелік можливих ризиків вимог процедури оборонного планування “Оцінювання середовища безпеки” (приклад)

| Процедура оборонного планування | Процес | Вимоги | Найменування ризику |
|---|---|---|---|
| **Оцінювання середовища безпеки** | Опис безпекового середовища | Бачення майбутнього світовими силами (суб’єктами) | Ризик недостатньої достовірності інформації щодо воєнно-політичної, воєнно-стратегічної та іншої обстановки; глобальних та регіональних суперечностей; бачення майбутнього світовими силами (суб’єктами); інтересів сил, насамперед світових та регіональних лідерів; можливості появи нових сил (суб’єктів) |
| | | Інтереси сил, насамперед світових та регіональних лідерів | |
| | | Можливість появи нових сил (суб’єктів) | |
| | | Глобальні та регіональні суперечності | |
| | | Ресурси сил (суб’єктів): людські, економічні та природні | Хибні висновки щодо ресурсів сил (суб’єктів): людських, економічних і природних |
| | | Склад і характер намірів та дій сил | Невизначеність складу і характеру намірів та дій сил |
| | | Пріоритети розвитку складових могутності (технологій, кількісно-якісних параметрів озброєнь тощо) | Недосконалість (відсутність) методичного апарату щодо визначення пріоритетів розвитку складових могутності (технологій, кількісно-якісних параметрів озброєнь тощо) |
| | | Ідеологічні постулати і доктринальні установки | Ризик неповної інформації щодо ідеологічних постулатів і доктринальних установок |
| | | Характерні риси сучасних воєнних конфліктів | Ризик хибних висновків щодо характерних рис сучасних воєнних конфліктів |
| | | Ризики безпекового середовища | Недосконалість (відсутність) методичного апарату щодо аналізу результатів оцінювання безпекового середовища |
| | | Сценарії можливих воєнно-політичних ситуацій та характер участі складових сил оборони у зазначених сценаріях | Недосконалість (відсутність) методичного апарату щодо визначення сценаріїв, можливих воєнно-політичних ситуацій та характеру участі складових сил оборони у зазначених сценаріях |
| | Визначення викликів та загроз | Об’єкт впливу загрози | Ризик хибного визначення об’єкта впливу загрози |
| | | Умови виникнення загрози | Ризик недостатньої достовірності інформації та хибні висновки щодо умов виникнення загрози |
| | | Тенденції розвитку викликів та загроз | Недосконалість (відсутність) методичного апарату щодо визначення викликів та загроз у сфері оборони та тенденції їх розвитку |
| | Формування сценаріїв та ситуацій | Можливі цілі сторін | Ризик хибного визначення можливих цілей сторін; суб’єктів, які братимуть участь у досягненні цілей сторін; сил і засобів, що мають бути задіяні в сценарії |
| | | Можливі суб’єкти, які братимуть участь у досягненні цілей сторін | |
| | | Сили і засоби, задіяні в сценарії | |
| | | Масштаби реалізації цілей | Недосконалість (відсутність) методичного апарату щодо визначення масштабу реалізації цілей |
| | | Особливості реалізації сценарію | Ризик визначення особливостей реалізації сценарію |
| | Визначення завдань | Умови виконання завдань | Ризик невизначеності умов виконання завдань. Недосконалість Переліку умов виконання завдань оборони |
| | | Критерії виконання завдань | Недосконалість (відсутність) методичного апарату щодо визначення критеріїв виконання завдань. |
| | | Перелік завдань | Недосконалість Єдиного переліку типових військових завдань |

Ризики вимог процесів, насамперед “Визначення складу та орієнтовної оргструктури військ (сил)”, процедури “Планування сил” (табл. 2) враховуються в процедурі оборонного планування “Планування ресурсів” під час визначення рівня задоволення потреб у ресурсах та обсягу й переліку необхідних ресурсів для формування, утримання, нарощування спроможностей та позбавлення від спроможностей.

Основним процесом процедури “Планування ресурсів” є оцінювання вартості необхідних та наявних спроможностей ЗС України для виконання завдань за сценаріями, метою є визначення ступеня відповідності та різниці між наявними та необхідними спроможностями. У результаті оцінювання визначається обсяг потреб у ресурсах для створення необхідних спроможностей (рис. 5).

**Таблиця 2.** Перелік можливих ризиків вимог процедури оборонного планування “Планування сил” (приклад)

| Процедура оборонного планування | Процес | Вимоги | Найменування ризику |
|---|---|---|---|
| **Планування сил** | Визначення змісту та умов виконання завдань | Результати оцінювання середовища безпеки | Неврахування результатів оцінювання середовища безпеки |
| | | Зміст завдань за кожним зі сценаріїв | Зміст завдань визначено не за всіма ситуаціями та сценаріями |
| | | Умови та критерії виконання завдань | Неповне визначення умов застосування військ (сил) при виконанні завдань за визначеними ситуаціями |
| | | | Недосконаліть методичного апарату щодо оцінювання завдань, до виконання яких мають бути готові (спроможні) складові сил оборони |
| | | | Недосконаліть (відсутність) методичного апарату щодо визначення ролі та відповідальності кожної зі складових сектора безпеки і оборони України за виконання завдань в рамках реалізації визначених сценаріїв |
| | Визначення спроможностей для виконання завдань за сценаріями | Визначення необхідних спроможностей | Не чітко визначені показники необхідних спроможностей за функціональними групами за всіма сценаріями застосування сил оборони |
| | | | Недосконаліть (відсутність) методичного апарату щодо оцінювання необхідних спроможностей за критеріями ефективності виконання завдань |
| | | Оцінювання наявних спроможностей | Поверхове оцінювання наявних спроможностей відповідно до їхньої здатності до виконання завдань в рамках визначених сценаріїв |
| | | Недостатні та надлишкові спроможності | Недосконаліть (відсутність) методичного апарату щодо здійснення порівняльного аналізу необхідних і наявних спроможностей за критеріями доцільності та пріоритетності( ) з метою формування Цільового пакета спроможностей сил оборони |
| | Визначення складу та орієнтовної оргструктури військ (сил) | Визначення типових організаційних структур ЗС України | Недосконаліть (відсутність) Переліку типових організаційних структур ЗС України та інших складових сил оборони |
| | | Визначення основних напрямів та завдань щодо планування сил | Недосконаліть нормативно-правових актів та методичних засад з питань визначення основних напрямів та завдань щодо планування сил |

Ризики вимог процесів процедури “Планування ресурсів” (табл. 3) враховуються під час оцінювання ризиків для процедури “Формування перспективної моделі та структури ЗС України (сил оборони), що відповідають прийнятим ризикам і збалансовані за завданнями складових сектора безпеки і оборони та ресурсами, розподіленими між складовими сектора безпеки і оборони”.

**Таблиця 3.** Перелік можливих ризиків вимог процедури оборонного планування “Планування ресурсів” (приклад)

| Процедура оборонного планування | Процес | Вимоги | Найменування ризику |
|---|---|---|---|
| **Планування ресурсів** | Визначення потреби у ресурсах для досягнення визначених необхідних спроможностей | Склад та орієнтовна оргструктура військ (сил) | Неповне оцінювання щодо визначення складу та структурних елементів |
| | | Потреба в ресурсах для досягнення визначених необхідних спроможностей | Поверхове оцінювання вартості необхідних спроможностей |
| | | Оцінювання ресурсів для забезпечення наявних спроможностей | Поверхове оцінювання вартості наявних спроможностей |
| | | Можливості залучення міжнародної технічної допомоги | Правова невизначеність порядку залучення міжнародної технічної допомоги |
| | | Щорічний рівень інфляції | Поверхове оцінювання рівня інфляції |
| | | Урахування зростання індексу цін | Поверхове оцінювання рівня зростання індексу цін |
| | | Визначення потреби у додаткових фінансових ресурсах для забезпечення розвитку критичних спроможностей | Недосконалість (відсутність) методичного апарату щодо оцінювання необхідних спроможностей за критеріями ефективності виконання завдань |
| | | Уточнення необхідних спроможностей для максимального збалансування їхньої вартості з прогнозними показниками фінансування | Поверхове оцінювання необхідних спроможностей відповідно до їхньої вартості |
| | | Законодавча та нормативно-правова база здійснення фінансування в особливий період | Відсутність та недосконалість нормативно-правових актів та методичних засад з питань здійснення фінансування в особливий період |

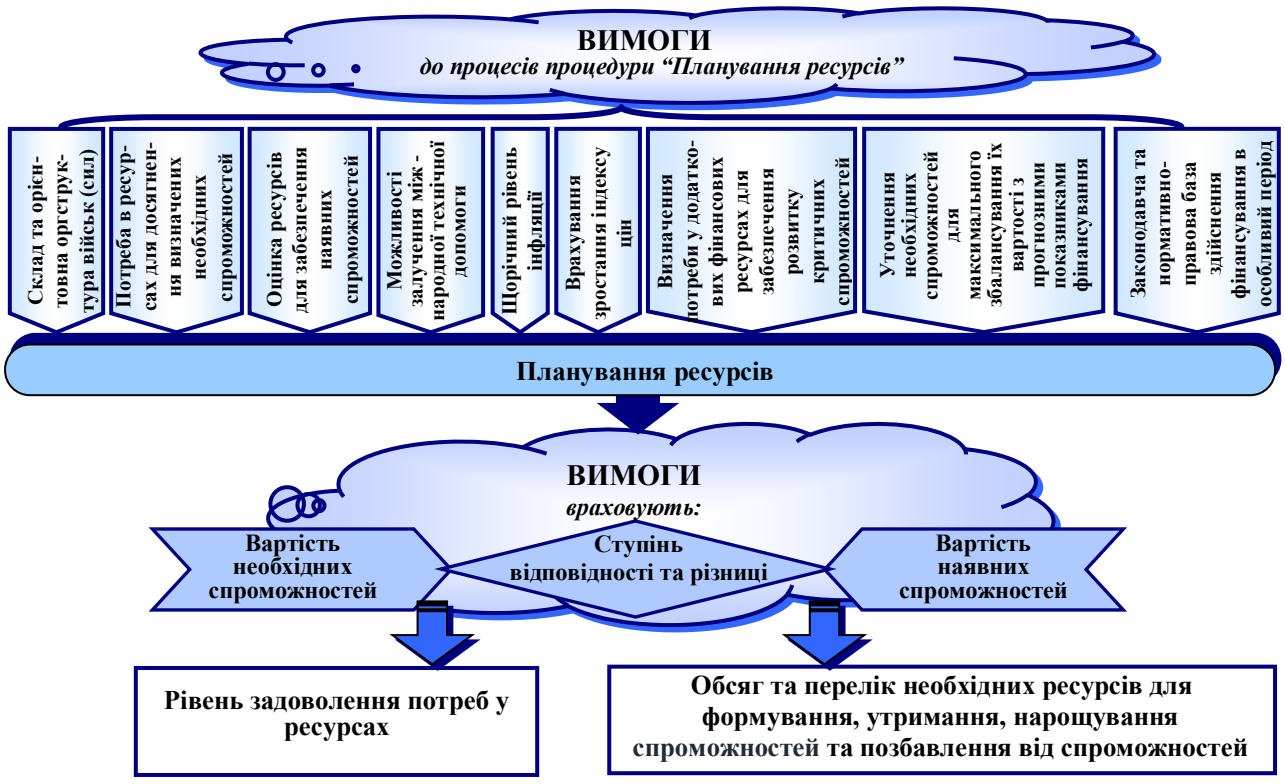



**Рисунок 5.** Сукупність вимог процедури оборонного планування “Планування ресурсів”

У Рекомендаціях з оборонного планування на основі спроможностей в МО та ЗС України [15] зазначається, що “формування перспективного складу Збройних Сил передбачає розроблення варіантів складу Збройних Сил та вибір оптимального варіанта на основі критерію “результат / вартість”. Процес вибору оптимального варіанта складу ЗС України передбачає оцінювання ефективності виконання визначених завдань кожним варіантом та вартості перетворення існуючого складу у перспективний. Ефективність виконання визначених завдань та вартість досягнення необхідних спроможностей є критерієм вибору оптимального варіанта перспективного складу Збройних Сил” (рис. 6).

Обов’язковою умовою вибору оптимального варіанта складу ЗС України є врахування ризиків, які можуть виникнути у разі ігнорування або недотримання вимог до оптимального складу ЗС України (табл. 4).

Вимоги зазвичай мають динамічний характер, оскільки вони постійно змінюються та розвиваються відповідно до змін безпекового середовища та мінливих потреб забезпечення оборони держави.

**Таблиця 4.** Перелік можливих ризиків вимог процедури оборонного планування “Формування перспективної моделі та структури ЗС України” (приклад)

| **Процедура оборонного планування** | **Процес** | **Вимоги** | **Найменування ризику** |
|---|---|---|---|
| **Формування перспективної моделі (структури) ЗС України** | **Вибір оптимального варіанта складу ЗС України** | Відповідність перспективного складу ЗС України завданням за сценаріями | Некоректність визначення складу та структурних елементів, які необхідно формувати та нарощувати |
| | | Своєчасність готовності перспективного складу ЗС України до виконання завдань за сценаріями | Недосконаліть (відсутність) методичного апарату щодо оцінювання готовності ЗС України до виконання завдань за сценаріями в умовах невизначеності |
| | | Уніфікація та сумісність ОВТ, МТЗ у складі сил оборони та для виконання спільних завдань | Несумісність основної номенклатури ОВТ, МТЗ ЗС України з іншими складовими сил оборони та з підрозділами іноземних держав |
| | | Здатність забезпечити належні соціальні стандарти для персоналу | Неможливість забезпечити належні соціальні стандарти для персоналу через відсутність відповідних коштів |
| | | Здатність складу до адаптації і виконання нових завдань | Некоректність визначення організаційно-штатної структури військових частин перспективного складу ЗС України |
| | | | Недосконаліть (відсутність) проведення аналізу визначеного складу та структури ЗС України за критерієм “результат / вартість |

Зважаючи на те, що оборонне планування здійснюється в умовах невизначеності, під час визначення вимог до спроможностей складу військ (сил) необхідно враховувати ризики впливу можливих помилкових припущень оцінки середовища безпеки та непередбачуваних змін у ньому, ситуацій, які потребуватимуть застосування ЗС України та сценаріїв застосування військ (сил), а також неповної інформації про структуру сил, спроможності та плани противника, можливості держави із забезпечення потреб ЗС України необхідними ресурсами (рис. 7)

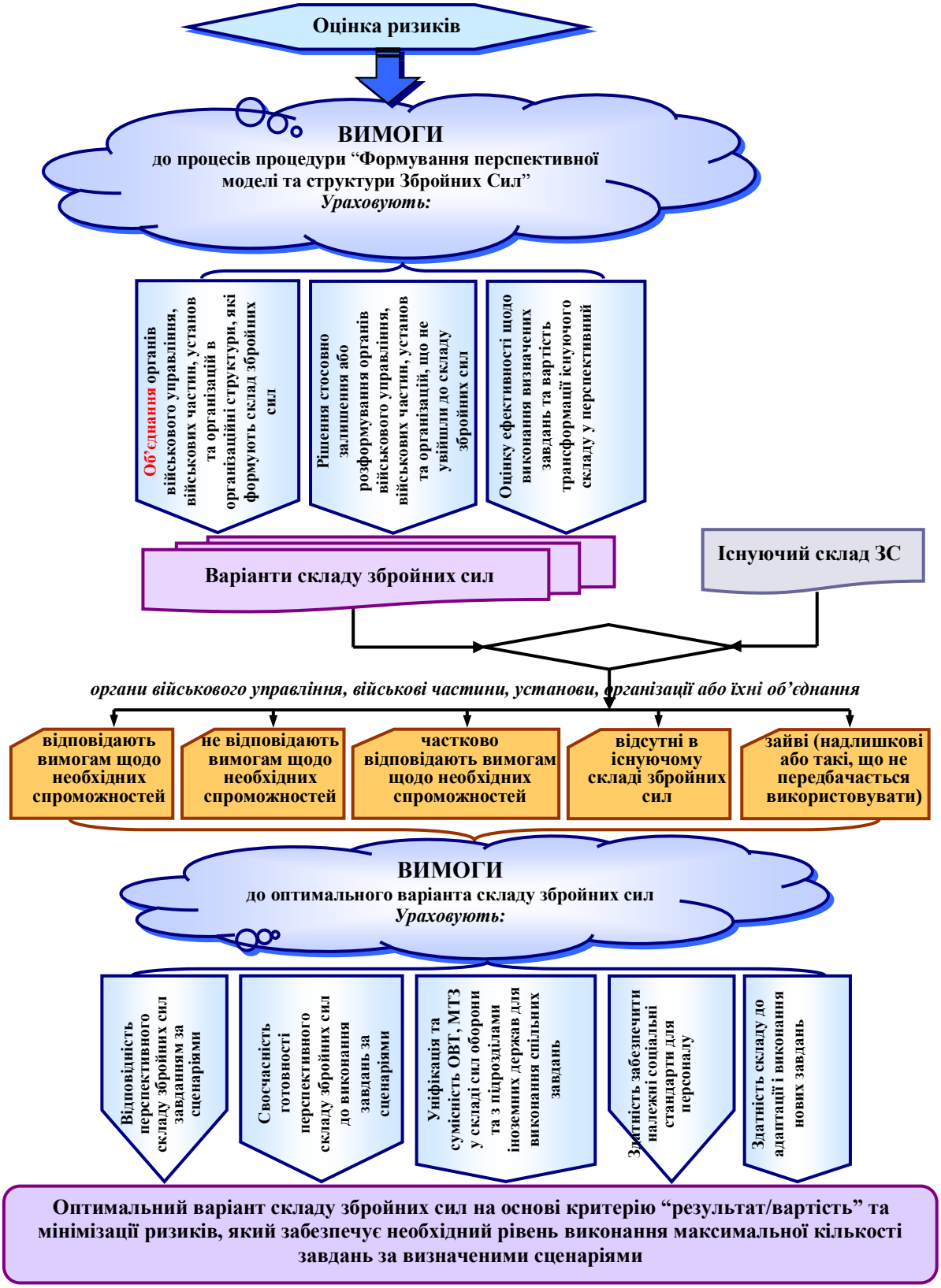



**Рисунок 6.** Сукупність вимог процедури оборонного планування "Формування перспективної моделі та структури Збройних Сил"

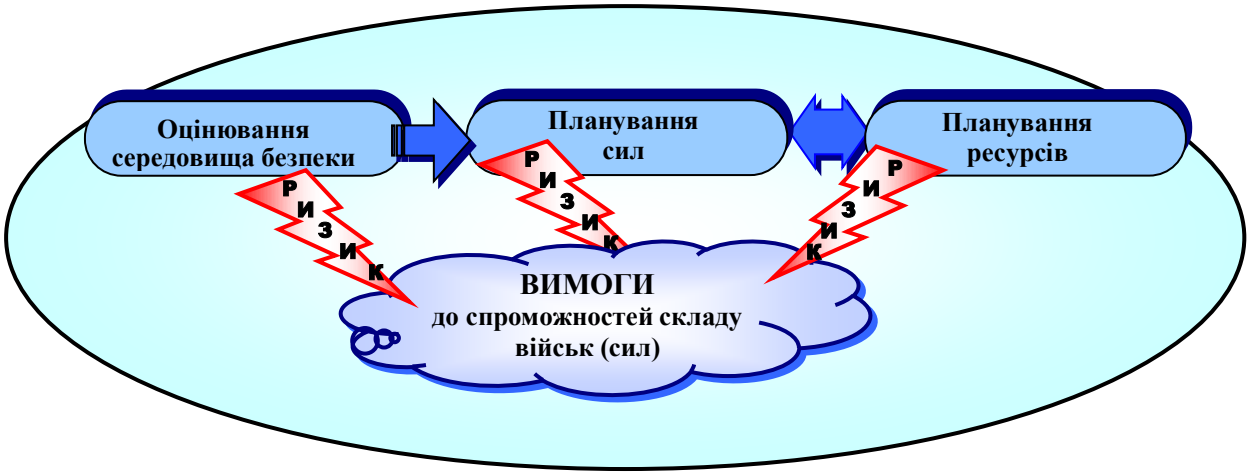



**Рисунок 7.** Зв'язок вимог до спроможностей військ (сил) із ризиками процедур

З метою зменшення потенційного негативного впливу виявлених ризиків постає необхідність проаналізувати їх та визначити їхню вірогідність і наслідки. Саме аналіз ризиків враховує потенційний вплив невизначеності, за якої здійснюється оборонне планування.

Аналіз ризиків є невід'ємною складовою процесу управління ризиками (рис. 8).

Управління ризиками відіграє ключову роль, забезпечуючи цілісність вимог та успішність результату оборонного планування.




**Рисунок 8.** Складові процесу управління ризиками

З метою узагальнення відомостей про принципи і підходи управління ризиками, які представлені у великій кількості стандартів [7], [8], [11], [19–22], пропонується використовувати модель у вигляді семантичної сітки, яка відображає структуру основних понять цієї предметної області (рис. 9) [31].

Як видно у запропонованій моделі, процес управління ризиками передбачає проведення 3 основних процедур:

- ❖ ідентифікація ризиків;
- ❖ аналіз ризиків;
- ❖ оцінювання ризиків.

**Ідентифікація ризику** – процес визначення елементів ризику, складання їхнього переліку, опису кожного елемента. Мета ідентифікації – складання переліку джерел ризику та

подій, які можуть вплинути на досягнення визначеної мети або унеможливити досягнення всіх цілей. Ідентифікація ризику передбачає встановлення:

- ризикової події;
- причини ризику;
- чинників ризику;
- ризикової ситуації;
- виду ризику;
- методів виявлення ризикової ситуації;
- наслідків;
- імовірності настання події;
- вірогідності, можливості настання події;
- тяжкості, міри впливу події;
- вразливості (рис. 10, табл. 5).




**Рисунок 9.** Структура основних понять управління ризиками

Результатом ідентифікації стане докладний опис ризиків – складання реєстру (рис. 11).

Реєстр ризиків необхідний, оскільки він дозволяє випереджати потенційні загрози, перш ніж вони виникнуть. Визначивши потенційні ризики, можна створити план дій для реалізації, якщо ризик будь-коли виникне.

Реєстр ризиків має містити опис кожного ризику, а також імовірність та вплив, який він може мати. Крім того, у реєстрі ризиків мають бути такі компоненти:

**Ідентифікація ризику:** назва ризику чи ідентифікаційний номер. Ці ідентифікаційні номери допомагають організувати ризики в різних категоріях, щоб їх було легше знаходити та відстежувати.

**Опис ризику:** короткий опис ризику і того, чому він є проблемою.

**Категорія ризику:** категоризація ризиків допомагає ідентифікувати ризик у реєстрі ризиків, що спрощує розуміння того, хто відповідатиме за пом'якшення наслідків.

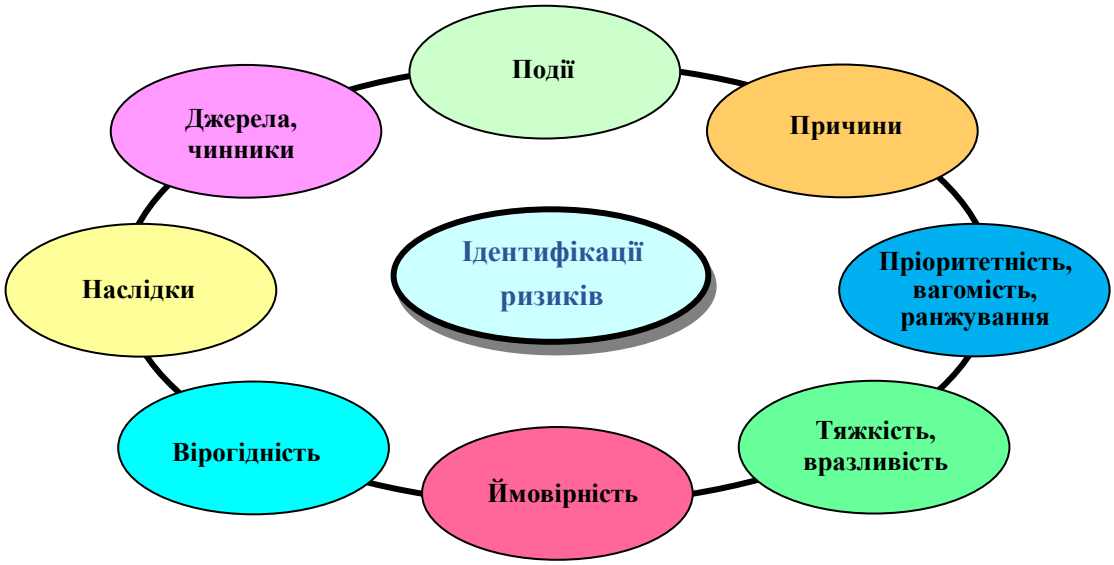



**Рисунок 10.** Головні складові ідентифікації ризиків

**Таблиця 5.** Характеристика елементів ідентифікації ризиків

| Елементи ідентифікації ризиків | Сутність і характеристика |
|---|---|
| Ризикова подія | Поява чи зміна певного явища чи сукупності обставин |
| Причини ризику | Джерело настання ризикової ситуації |
| Чинники ризику | Умови, за яких виявляються причини ризику, що спричиняють появу ризикових ситуацій |
| Ризикова ситуація | Подія, яка зумовлена причинами і чинниками ризику, що може призвести до негативних або позитивних наслідків |
| Вид ризику | Джерело настання ризикової ситуації (визначає, хто/що є ініціатором виникнення кризової ситуації |
| Метод виявлення | Спосіб встановлення ризикової ситуації |
| Наслідки | Результати ризикової ситуації у разі її реалізації |
| Імовірність | Кількісна міра вірогідності настання події (визначається числом від 0 до 1, де 0 – неможливість події, а 1 – її обов'язковість) |
| Вірогідність | Можливість настання події |
| Тяжкість | Міра впливу події |
| Вразливість | Внутрішня властивість, яка свідчить про чутливість до впливу, що спричиняється джерелом ризику, внаслідок чого може настати подія з наслідками |

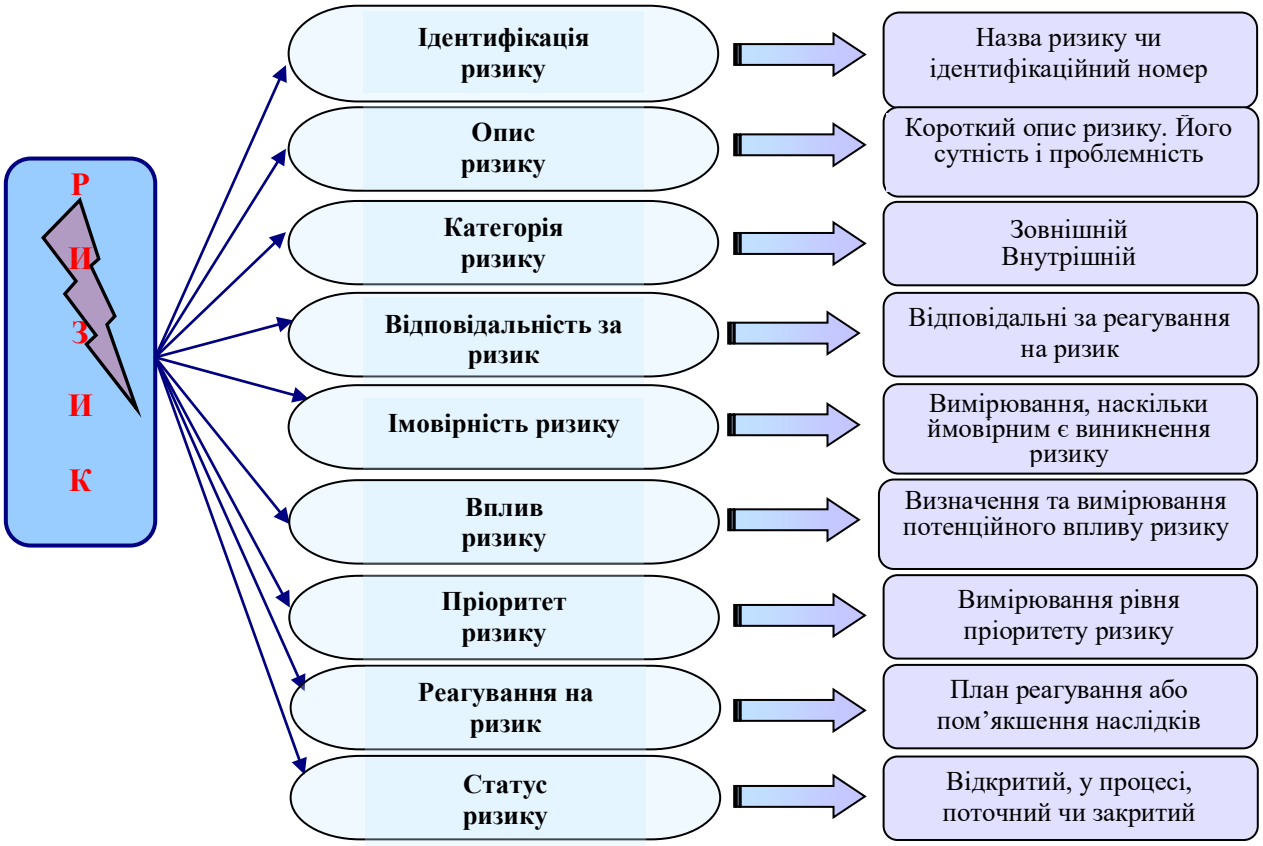



**Рисунок 11.** Структура та зміст реєстру ризиків

**Відповідальність за ризик:** особа чи особи, які відповідатимуть за управління та контроль реагування на ризик.

**Імовірність ризику:** вимір, наскільки ймовірним є виникнення ризику. За цим показником кожен ризик можна класифікувати як імовірність виникнення ризику дуже низька, низька, середня, висока, дуже висока. Можна також використовувати числову шкалу, де одиниця означає вкрай малоймовірний, а п'ять – дуже ймовірний.

**Вплив ризику:** виділяє та вимірює потенційний вплив ризику, допомагаючи зрозуміти, які ризики мають пріоритет. Під час оцінювання потенційного впливу використовується шкала, яка передбачає такі оцінки, як "украй низький", "низький", "середній", "високий" та "украй високий".

**Пріоритет ризику:** враховує можливість ризику та аналіз ризику для вимірювання рівня пріоритету ризику. Для оцінювання пріоритету використовується проста числова шкала: один означає украй низький, два – низький, три – середній, чотири – високий і п'ять – украй високий.

**Реагування на ризик:** план реагування або пом'якшення наслідків має містити докладний опис того, як планується впоратися з ризиком. Це ключовий компонент реєстру ризиків.

**Статус ризику:** поле реєстру ризиків містить статус ризику – відкритий, у процесі, поточний чи закритий – щоб допомогти визначити, був ризик оброблений чи ні.

Завдяки реєстру ризиків спрощується:

- виявлення та відстежування ризиків, які можуть вплинути на визначення вимог до процедур оборонного планування;
- ухвалення рішення, на які ризики варто звернути увагу (а на які ні);

- завчасне планування з усунення найбільших ризиків;
- реалізація планів пом'якшення наслідків, щоб зменшити ризик до прийнятного рівня.

**Аналіз ризиків** є важливим етапом процесу ухвалення рішення. Сутність аналізу ризиків полягає в оцінюванні невизначеностей з метою зменшення їхнього впливу на результати оборонного планування.

Під час аналізу ризику визначаються:

- джерела даних;
- засоби контролю;
- методи аналізу;
- наслідки реалізації ідентифікованої небезпечної події;
- імовірність настання ідентифікованої небезпечної події.

Аналіз ризику є фундаментальним процесом у ширшому контексті оцінювання ризику. Це передбачає поглиблене оцінювання виявлених небезпечних подій і ризиків, щоб зрозуміти їхній потенційний вплив, оцінити їхню ймовірність й ухвалити обґрунтовані рішення про те, як ними керувати або пом'якшувати.

Для визначення серйозності небезпечних подій (небезпеки) є різні критерії. Категорії серйозності небезпеки (табл. 6), представлені у (Міждержавний стандарт ГОСТ 27.310-95, 1995), встановлюють кількісне значення відносної серйозності ймовірних наслідків небезпечних умов (подій) залежно від характеру наслідків цієї небезпеки.

**Таблиця 6.** Категорії серйозності небезпек (приклад)

| Вид | Категорія | Опис небезпеки |
|---|---|---|
| Катастрофічна | IV | Небезпека, реалізація якої може швидко та з високою ймовірністю спричинити значний збиток |
| Критична | III | Небезпека, реалізація якої може з високою ймовірністю спричинити значний збиток |
| Гранична | II | Небезпека, реалізація якої може спричинити затримку виконання завдання |
| Незначна | I | Небезпека, у разі реалізації якої настають менш значні наслідки, ніж у категорії II |

Використання категорій серйозності небезпеки необхідно для визначення відносної важливості упереджувальних заходів зниження ризику.

Рівні ймовірності небезпеки (табл. 7) є якісним відображенням відносної ймовірності того, що відбудеться небажана подія, яка є наслідком не усунутої або непідконтрольної небезпеки.

Використовуючи водночас методики визначення серйозності та ймовірності небезпеки, можна визначити, вивчити небезпеки, віднести їх до певного класу і вирішити їх, виходячи з серйозності небезпеки, потенційно ймовірних наслідків та ймовірності того, що такі наслідки будуть мати місце.

**Таблиця 7.** Рівні ймовірності небезпеки (приклад)

| Вид | Рівень | Опис наслідків |
|---|---|---|
| Часта | A | Небезпека спостерігається постійно |
| Імовірна | B | Імовірно часте виникнення небезпеки |
| Можлива | C | Небезпека спостерігається кілька разів |
| Рідка | D | Малоймовірно, але можливе виникнення небезпеки хоча б раз |
| Практично неймовірна | E | Виникнення небезпеки настільки малоймовірне, що можна припустити, що вона ніколи не відбудеться |

Дані про наслідки та ймовірність подій використовують для оцінювання рівня ризику.

Встановивши буквено-цифрову систему оцінювання ризику для кожної категорії серйозності та кожного рівня ймовірності, можна глибше класифікувати та оцінювати ризик за ступенем припустимості. Використання такої матриці полегшує оцінювання ризику (табл. 8).

**Таблиця 8.** Матриця оцінювання ризику (приклад)

| **Частота, з якою відбувається подія** | **Категорія небезпеки** | | | |
|---|---|---|---|---|
| | IV<br>Катастрофічна | III<br>Критична | II<br>Гранична | I<br>Незначна |
| (A) Часто | 4A | 3A | 2A | 1A |
| (B) Імовірно | 4B | 3B | 2B | 1B |
| (C) Можливо | 4C | 3C | 2C | 1C |
| (D) Рідко | 4D | 3D | 2D | 1D |
| (E) Практично неможливо | 4E | 3E | 2E | 1E |
| **Індекс ризику небезпеки** | | | | |
| **Класифікація ризику** | **Критерії ризику** | | | |
| 4A,4B,4C,3A,3B,2A | Неприпустимий (надмірний) | | | |
| 4D,3C,3D,2B,2C | Небажаний (гранично допустимий) | | | |
| 4E,3E,2D,2E,1A,1B | Припустимий з перевіркою (прийнятний) | | | |
| 1C,1D,1E | Припустимий без перевірки (знехтуваний) | | | |

З метою якісного (бального) оцінювання рівня ризику зазвичай використовуються такі шкали (табл. 9, 10):

**Таблиця 9.** Шкала оцінювання наслідків ризику (приклад)

| **Наслідки (I), бали** | **Опис наслідків** | **Об'єкти впливу небезпечної події** |
|---|---|---|
| 5 | Катастрофічні наслідки | |
| 4 | Значні наслідки | |
| 3 | Помірні наслідки | |
| 2 | Невеликі наслідки | |
| 1 | Незначні наслідки | |

**Таблиця 10.** Шкала оцінювання ймовірності настання ризику (приклад)

| **Оцінка ймовірності (L), %** | **Опис імовірності** | **Якісна оцінка ймовірності** | **Бали** |
|---|---|---|---|
| 81–100 | Дуже висока | Дуже висока | 5 |
| 61–80 | Висока | Висока | 4 |
| 21–60 | Середня | Середня | 3 |
| 1–20 | Низька | Низька | 2 |
| Менше 1 | Дуже низька | Дуже низька | 1 |

Порівняльне оцінювання ризику містить зіставлення рівня ризику з критеріями ризику для визначення типу ризику та його значущості. Порівняльне оцінювання ризику використовує інформацію про ризик, отриману під час аналізу ризику. Результати порівняльного оцінювання ризику використовують для ухвалення рішення щодо майбутніх дій.

Аналіз ризиків є процесом не тільки кількісного оцінювання, а й класифікації ідентифікованих ризиків для забезпечення глибшого розуміння їхнього потенційного впливу. Класифікація ризиків – це систематизація сукупності ризиків на підставі яких-небудь ознак і критеріїв, що дозволяють об'єднати підмножини ризиків у загальні поняття (табл. 11).

**Таблиця 11.** Класифікація ризиків оборонного планування (приклад)

| Клас ризику | Вид ризику | Різновид ризику |
|---|---|---|
| **Ризики оцінювання середовища безпеки** | Ризики опису безпекового середовища | Ризик недостатньої інформації |
| | | Ризик хибних висновків |
| | | … |
| | Ризики викликів та загроз | Ризик визначення об’єкта впливу загрози |
| | | Ризик умов виникнення загрози |
| | | … |
| | Ризики сценаріїв та ситуацій | Ризик визначення можливих цілей сторін |
| | | Ризик визначення можливих суб’єктів, які братимуть участь у досягненні цілей сторін |
| | | … |
| | … | … |
| **Ризики планування сил** | | |
| **Ризики планування ресурсів** | | |
| **Оцінювання ризиків** | | |
| **Ризики формування перспективної моделі (структури) збройних сил** | | |

Необхідність класифікації ризиків є дуже важливою не лише з теоретичної точки зору, а й з практичної, оскільки саме від її точності залежить адекватність кількісних оцінок ризиків, правильність застосування методів уникнення та зниження ступеня ризику, а отже, й ефективність системи управління ризиками.

**Висновки (Conclusion)**

Ефективність оборонного планування в непередбачуваному зовнішньому середовищі є можливою за умови формування цілісної системи управління ризиками. Така система передбачає процеси ідентифікації, оцінювання та аналізу; добір та використання методів нейтралізації негативного впливу ризиків.

Аналіз ризиків є важливим етапом у процесі ухвалення рішень. Розуміючи та оцінюючи ризики, пов’язані з конкретним вибором, можливо ухвалювати більш обґрунтовані рішення з урахуванням потенційного впливу невизначеності.

Ефективне управління ризиками під час визначення вимог до спроможностей складу військ (сил) є наріжним каменем успішності оборонного планування. Використання аналізу ризиків підвищує обґрунтованість вимог до спроможностей складу військ (сил). Розуміючи потенційні ризики, оцінюючи їхній вплив та реалізуючи надійні стратегії пом’якшення наслідків, можна більш ефективно долати складнощі під час визначення вимог до спроможностей військ (сил). Ігнорування або несистемна реалізація процесу управління ризиками можуть негативно впливати на ефективність та результативність оборонного планування.

**Рекомендації (Recommendations)**

Матеріали статті може бути використано для обґрунтування вимог до процедур оборонного планування під час здійснення заходів оборонного планування. Стаття також може бути корисна науковцям, які займаються проблематикою оборонного планування й розвитком спроможностей, та фахівцям, які причетні до організації та здійснення оборонного планування.

**Використані джерела**

1. Балджи, М. Д., Карпов, В. А., Ковальов, А. І., Костусєв, О. О., Котова, І. М. & Сментина, Н. В. (2013). *Обґрунтування господарських рішень та оцінка ризиків.* ОНЕУ.
2. Вітлінський, В. В., & Великоіваненко, Г. І. (2004). *Ризикологія в економіці та підприємництві*. КНЕУ.
3. *Доктрина "З оборонного планування у Збройних Силах України"* (СП 5-00(67)01.01). (2020). Головне управління оборонного планування Генерального Штабу Збройних Сил України.
4. Дєнєжкін, М. М. (2021). Шляхи вирішення проблемних питань планування розвитку спроможностей військових формувань Збройних Сил України. *Наука і техніка Повітряних Сил Збройних Сил України, 1* (42), 28–33.
5. *Інтегрована модель управління ризиками (COSO ERM – Integrated Framework Enterprise Risk Management – Integrated Framework).* https://www.coso.org/documents/COSO_ERM_Executive Summary_Russian.pdf.
6. *Методичні рекомендації з організації та проведення оборонного огляду*. (2019). Затв. Міністром оборони України 7.06.2019. (Затв. МОУ 10.06.2019 № 9262/з). https://www.mil.gov.ua/diyalnist/reformi-ta-planuvannya-u-sferi-oboroni/plani-ukraina-2020/metodichni-rekomendaczii-z-organizaczii-ta-provedennya-oboronnogo-oglyadu-yaki-zatverdzheno-ministrom-oboroni-ukraini-7-chervnya-2019-roku-(zatverdzheni-mou-vid-10-chervnya-2019-%E2%84%96-9262/z).html
7. *Керування ризиком. Методи загального оцінювання ризику (ДСТУ IEC/ІБО 31010:2013).* (2015). Національний стандарт України. Мінекономрозвитку України. http://www.leonorm.com.ua/p/NL_DOC/UA/201301/Nak1469.htm
8. *Менеджмент ризиків. Принципи та керівні вказівки (ДСТУ ISO 31000:2014).* (2016). Національний стандарт України. Мінекономрозвитку України. http://www.dkrs.gov.ua/kru/uk/publish/article/106386.
9. Корендович, В. С., Наливайко, А. Д., & Поляєв, А. І. (2018). Підходи до створення та функціонування системи управління вимогами щодо розвитку спроможностей в органах управління складових сил оборони. *Зб. наук. пр. ЦВСД НАО України, 1* (62), 51–56.
10. Кабаченко, Д. В. (2017). Прийняття управлінських рішень в умовах невизначеності та ризику. *Economics Bulletin, 2*, 107–115.
11. *Надійність в техніці. Аналіз видів, наслідків та критичності відмов. Основні положення (ГОСТ 27.310-95).* (1995). Міждержавний стандарт.
12. Никифоренко, В. (2020). Современные риски и угрозы национальной безопасности в сфере охраны государственной границы. *Knowledge, Education, Law, Management, 3* (31), *vol. 2*, 120–125.
13. *Організація внутрішнього контролю та управління ризиками в обороні України.* (2022). Центр учбової літератури.
14. Пащенко, Є. М., & Іващенко, С. М. (2023). Поняття та принципи управління ризиками в Міністерстві оборони України та Збройних Силах України. *Науковий вісник Ужгородського Нац. ун-ту. Серія: Право. Вип. 77. Ч. 2*, 102–107.
15. *Рекомендації з оборонного планування на основі спроможностей в МО та ЗС України.* (2017). Затв. Міністром оборони України, № 5789/з/3. http://www.mil.gov.
16. ua/content/ other/Recommendationson_CBP_120617 pdf
17. *Рекомендації з порядку організації проведення оцінювання спроможностей у Збройних Силах України.* (2017). Затв. Міністром оборони України. https://www.mil.gov.ua/content/other/metod_recom_2019_2.pdf
18. Решетило, В. П., & Федотова, Ю. В. (2020). Невизначеність та ризик: співвідношення понять та специфіка прийняття рішень. *Економіка та управління підприємствами. Проблеми системного підходу в економіці, 3* (77)-2, 149–154.

19. Рішняк, І. В. (2003). Системний аналіз категорії ризику та невизначеності. *Вісник Нац. ун-ту "Львівська політехніка". Інформаційні системи та мережі*, *489*, 263–275.
20. *Ризик-менеджмент. Керівництво по здійсненню.* (*Risk Management. Guidelines for the implementation). (ISO /TR 31004:2013).* Міжнародний стандарт. https://www.iso.org/standard /56610.html
21. 20. *Ризик-менеджмент. Методи оцінки ризиків*. *(Risk Management. Risk assessment techniques). (IEC 31010:2009).* Міжнародний стандарт. https://www.iso.org/standard/51073.html.
22. *Ризик-менеджмент. Принципи та рекомендації. (Risk management. Principles and guidelines). (ISO 31000:2009).* Міжнародний стандарт. http://www.amu.kz/fotos-news/vstrecha_rectora_so_stud_31_oct/ ISO%2031000-2009.pdf.3.
23. *Ризик-менеджмент. Словник-керівництво з використання в стандартах. (Risk Management. Vocabulary. Guidelines for use in standards). (ISO Guide 73:2009).* Міжнародний стандарт. https://www.iso.org/obp/ui/#iso:std:iso:guide:73: ed-1:v1:en.
24. Руснак, І. С., Петренко, А. Г., Яковенко, І. М., & Кохно, В. Д. Оборонне планування на основі спроможностей: особливості та перспективи впровадження. *Наука і оборона, 2*, 3–10.
25. Сарай, Н. (2016). Невизначеність як першопричина ризику діяльності підприємств регіону. *Регіональні аспекти розвитку продуктивних сил України*, *21*, 34–39. http://nbuv.gov.ua/UJRN/rarpsu_2016_21_8
26. *Стандарти управління ризиками (Risk management standard). (RM, AIRMIC і ALARM (FERMA RMS).* Міжнародний стандарт. http://www.ferma.eu/app/uploads/2011/11/a-risk-management-standard-russian-version.pdf.
27. Сурков, О. О. (2022). Комплексний метод визначення вимог до спроможностей Збройних Сил та інших складових сил оборони. *East European Scientific Journal, 1* (77), 4–10.
28. *Управління ризиками. Керівні принципи. (ISO 31000:2018).* (2019). Міжнародний стандарт ДП "Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості" (ДП "УкрНДНЦ"). https://pqm-online.com/assets/files/pubs/translations/std/iso-31000-2018-(rus).pdf
29. *Управління ризиками. Словник*. (ISO 31073:2022). (2022). Міжнародний стандарт. https://ruk.at.ua/_ld/4/416_ISO_310073__.pdf
30. *Управління ризиками та FMEA. Вичерпний посібник*. https://visuresolutions.com/uk/Керівництво-fmea-з-управління-ризиками/
31. Якось, І. С. (2009). Ризик як міра невизначеності. *Економічний вісник Донбасу, 1* (15), 136–139.
32. Hayes, Adam. *Risk Analysis: Definition, Types, Limitations, and Examples.* https://www.investopedia.com/terms/r/risk-analysis.asp.

**References**

1. Baldzhi, M. D., Karpov, V. A., Kovalov, A. I., Kostusyev, O. O., Kotova, I. M., & Smentina, N. V. (2013). *Justification of business decisions and risk assessment*. ONEU. http://dspace.oneu.edu.ua/jspui/bitstream/123456789/550/1/
2. Vitlinskyi, V. V., & Velykoivanenko, G. I. (2004). *Riskology in Economics and Entrepreneurship*. KNEU.
3. *Doctrine "On Defense Planning in the Armed Forces of Ukraine"* (SP 5-00(67)01.01). (2020). Main Directorate of Defense Planning of the General Staff of the Armed Forces of Ukraine.
4. Denezhkin, M. M. (2021). Ways to address problematic issues of capability development planning for military formations of the Armed Forces of Ukraine. *Science and Technology of the Air Force of the Armed Forces of Ukraine,1* (42), 28–33.

5. *Integrated Risk Management Model (COSO ERM – Integrated Framework Enterprise Risk Management – Integrated Framework).* https://www.coso.org/documents/COSO_ERM_Executive Summary_Russian.pdf.
6. *Methodological recommendations for organizing and conducting defense review.* Approved by the Minister of Defense of Ukraine on June 7, 2019. https://www.mil.gov.ua/diyalnist/reformi-ta-planuvannya-u-sferi-oboroni/plani-ukraina-2020/metodichni-rekomendaczii-z-organizaczii-ta-provedennya-oboronnogo-oglyadu-yaki-zatverdzheno-ministrom-oboroni-ukraini-7-chervnya-2019-roku-(zatverdzheni-mou-vid-10-chervnya-2019-%E2%84%96-9262/z).html
7. *Risk Management. General Risk Assessment Methods (DSTU IEC/ISO 31010:2013).* (2015). National Standard of Ukraine. Ministry of Economic Development of Ukraine. http://www.leonorm.com.ua/p/NL_DOC/UA/201301/Nak1469.htm
8. *Risk Management. Principles and Guidelines (DSTU ISO 31000:2014).* (2016). National Standard of Ukraine. Ministry of Economic Development of Ukraine. http://www.dkrs.gov.ua/kru/uk/publish/article/106386.
9. Korendovych, V. S., Nalyvaiko, A. D., & Poliaiev, A. I. (2018). Approaches to creating and functioning a capability requirements management system in the management bodies of the defense forces. *Collection of Scientific Papers of the CVSD of NAO of Ukraine, 1* (62), 51–56.
10. Kabakhenko, D. V. (2017). Decision-making under uncertainty and risk. *Economics Bulletin, 2*, 107–115.
11. *Reliability in Technology. Failure Mode, Effects, and Criticality Analysis. Basic Provisions (GOST 27.310-95).* (1995). Interstate Standard.
12. Nikiforenko, V. (2020). Modern Risks and Threats to National Security in the State Border Protection Sector. *Knowledge, Education, Law, Management, 3 (31), vol. 2*, 120–125.
13. *Internal Control and Risk Management Organization in Ukraine's Defense Sector*. (2022). Center for Educational Literature.
14. Pashchenko, Ye. M., & Ivashchenko, S. M. (2023). Concept and Principles of Risk Management in the Ministry of Defense of Ukraine and the Armed Forces of Ukraine. *Scientific Bulletin of Uzhhorod National University. Law Series. Is. 77, Part 2*, 102–107.
15. *Recommendations on Capability-Based Defense Planning in the Ministry of Defense and the Armed Forces of Ukraine*. (2017). Approved by the Minister of Defense of Ukraine, No. 5789/z/3. http://www.mil.gov.ua/content/ other/Recommendationson_CBP_120617 pdf
16. *Recommendations on the Organization and Conduct of Capability Assessments in the Armed Forces of Ukraine.* (2017). Approved by the Minister of Defense of Ukraine. https://www.mil.gov.ua/content/other/metod_recom_2019_2.pdf
17. Reshetylo, V. P., & Fedotova, Yu. V. (2020). Uncertainty and Risk: The Relationship of Concepts and Decision-Making Specifics. *Economics and Enterprise Management. Systemic Approach Problems in Economics, 3* (77)-2, 149–154.
18. 18. Rishniak, I. V. (2003). Systemic Analysis of the Risk and Uncertainty Category. *Bulletin of the National University "Lviv Polytechnic". Information Systems and Networks, 489*, 263–275.
19. *Risk Management. Guidelines for Implementation. (ISO/TR 31004:2013).* International Standard. https://www.iso.org/ standard /56610.html
20. *Risk Management. Risk Assessment Techniques. (IEC 31010:2009).* International Standard. https://www.iso.org/standard/ 51073.html.
21. *Ризик-менеджмент. Принципи та рекомендації. (Risk management. Principles and guidelines). (ISO 31000:2009).* Міжнародний стандарт. http://www.amu.kz/fotos-news/vstrecha_rectora_so_stud_31_oct/ ISO%2031000-2009.pdf.3.
22. *Risk Management. Vocabulary. Guidelines for Use in Standards (ISO Guide 73:2009).* International Standard. https://www.iso.org/obp/ui/#iso:std:iso:guide:73: ed-1:v1:en.

23. Rusnak, I. S., Petrenko, A. G., Yakovenko, A. V., Romaniuk, I. M., & Kokhno, V. D. Capability-Based Defense Planning: Features and Implementation Prospects. *Science and Defense, 2*, 3–10.
24. Sarai, N. (2016). Uncertainty as the Primary Cause of Business Risks in the Region. *Regional Aspects of Productive Forces Development in Ukraine, 21*, 34–39. http://nbuv.gov.ua/UJRN/rarpsu_2016_21_8
25. *Risk Management Standards (Risk Management Standard). (RM, AIRMIC, and ALARM (FERMA RMS).* International Standard. http://www.ferma.eu/app/uploads/2011/11/a-risk-management-standard-russian-version.pdf.
26. Surkov, O. O. (2022). Comprehensive Method for Defining Capability Requirements of the Armed Forces and Other Defense Forces. *East European Scientific Journal, 1* (77), 4–10.
27. *Risk Management. Guidelines. (ISO 31000:2018).* (2018). International Standard. State Enterprise "UkrNDNC". https://pqm-online.com/assets/files/pubs/translations/std/iso-31000-2018-(rus).pdf
28. *Risk Management. Vocabulary*. (ISO 31073:2022). (2022). International Standard. https://ruk.at.ua/_ld/4/416_ISO_310073__.pdf
29. *Risk Management and FMEA. Comprehensive Guide*. https://visuresolutions.com/uk/Керівництво-fmea-з-управління-ризиками/
30. Yakos, I. S. (2009). Risk as a Measure of Uncertainty. *Economic Bulletin of Donbas, 1* (15), 136–139.
31. Hayes, Adam. *Risk Analysis: Definition, Types, Limitations, and Examples.* https://www.investopedia.com/terms/r/risk-analysis.asp

## Risk Analysis When Substantiating the Requirements for the Capabilities of Troops (Forces)

**Oleksandr Pavliuk**
Commander of the Land Forces of the Armed Forces of Ukraine
Command of the Land Forces of the Armed Forces of Ukraine
04119, Dehtiarivska Street, 19/7, Kyiv, Ukraine
e-mail: press.ksv@post.mil.gov.ua
ORCID: 0000-0002-6520-0797

**Volodymyr Didichenko**
Candidate of Military Sciences, Senior Research Fellow
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl Avenue 28 B, Kyiv, Ukraine
e-mail: DVP1951@ukr.net
ORCID: 0000-0002-0440-2299

**Vasyl Cherep**
Candidate of Military Sciences, Senior Researcher
Chief of the Research Directorate
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl Avenue 28 B, Kyiv, Ukraine
e-mail: vasya.cherep1976@gmail.com
ORCID: 0000-0003-3305-4518

**Stepan Vozniak**
Candidate of Technical Sciences, Senior Research Fellow
Chief of the Research Directorate
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl Avenue 28 B, Kyiv, Ukraine
e-mail: step_voz@ukr.net
ORCID: 0000-0002-9015-813X

**Artem Remez**
Doctor of Philosophy
Senior Lecturer at the Operational Art Chair
The National Defence University of Ukraine
03049, Povitrianykh Syl avenue, 28, Kyiv, Ukraine
e-mail: remez.art.86@gmail.com
ORCID: 0000-0003-4970-1097

***"Risk (eng. risk) – is a situation associated with danger; the probability (possibility) of something unpleasant happening".***
*(Oxford English Dictionary)*

**Abstract.** The relevance of the research is determined by the necessity to improve risk management in the defense planning processes of the Ministry of Defense and the Armed Forces of Ukraine, which are conducted under conditions of constant change and high uncertainty in the security environment. The aim of this article is to analyze risks emerging during the definition of capability requirements for military units (forces) and to develop effective methodological approaches for managing these risks, thus enhancing the effectiveness of defense planning. The study employs a comprehensive approach, including analysis of regulatory and legal acts, doctrinal and strategic documents, review of contemporary scientific publications, and application of advanced international methods for risk assessment and classification. The main results of the work include identifying key sources of risk in defense planning processes, developing a detailed semantic risk management model, establishing a clear structure and content of a risk register, and refining risk classification based on their nature, the degree of their impact on planning processes, and response prioritization. The practical significance of the obtained results lies in their potential use for reducing uncertainty, minimizing potential negative consequences of risks, ensuring operational adaptability to changes in the security situation, improving resource efficiency, and enhancing the quality of strategic and tactical decision-making in the defense domain. The materials of the article will be useful for specialists of the Ministry of Defense and the Armed Forces of Ukraine involved in developing prospective compositions of defense forces, as well as for researchers working on issues of risk management and military capability development.

**Keywords:** requirements, defence planning, risk, capability, risk management.

The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 3 No. 2 (2025)

DOI: 10.62524/msj.2025.3.2.9

# Defence Management Issues in Ukraine: The Economic Aspect

**Volodymyr Didichenko**
Candidate of Military Sciences, Senior Research Fellow
Senior Research Fellow
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl Avenue, 28 B, Kyiv, Ukraine
e-mail: DVP1951@ukr.net
ORCID: 0000-0002-0440-2299

**Vasyl Cherep**
Candidate of Military Sciences, Senior Researcher
Chief of the Scientific and Research Directorate
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl Avenue, 28 B, Kyiv, Ukraine
e-mail: vasya.cherep1976@gmail.com
ORCID: 0000-0003-3305-4518

**Polina Tolok**
Candidate of economic sciences (PhD)
Head of Defence Management chair
The National Defence University of Ukraine
03049, Povitrianykh Syl avenue, 28, Kyiv, Ukraine
e-mail: tolok100@meta.ua
ORCID: 0000-0002-2481-8152

**Valeriia Horhulenko**
Junior Research Fellow
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl Avenue, 28 B, Kyiv, Ukraine
e-mail: horhulenkovaleriia@gmail.com
ORCID: 0009-0009-1394-6325

**Mariia Yarmolchyk**
PhD
Head of Research Laboratory
The National Aviation University
03058, Liubomyra Huzara Avenue, 1, Kyiv, Ukraine
e-mail: LinkinFan357@ukr.net
ORCID: 0000-0001-9917-0189

**Abstract.** The relevance of the article is driven by the need for a comprehensive examination of the economic aspects of defence management in Ukraine. The study explores the economic aspects of defence management in Ukraine during the russian–ukrainian war, with a focus on the financial support for the Armed Forces of Ukraine, the specifics of defence procurement, the state of the defence-industrial complex, and the role of international support.

The aim of the article is to examine the key economic aspects of Ukraine's defence

management, particularly the financing of the Armed Forces of Ukraine, the reform of the procurement system, the state and development of the defence-industrial complex, as well as international support.

The article applies a systems approach, methods of economic and financial analysis, as well as a comparative analysis of NATO countries' experience.

Based on the analysis of budget expenditures, the study reveals an unprecedented increase in defence spending. The main challenges are identified, including a high level of budget deficit, corruption risks in the defence procurement system, limited production capacity of the defence-industrial complex, and dependence on external financial aid.

Specific recommendations are proposed to improve the system of financial planning and management of defence resources, ensure procurement transparency, intensify reforms of the defence-industrial complex, and strengthen international cooperation.

The results obtained have practical significance for the development of state policy in the field of defence management and may be used in educational and research institutions, as well as by government authorities and military structures involved in addressing defence management issues. Promising areas for further research include examining the place and role of the economic components of defence management in Ukraine's post-war recovery, the development of the Armed Forces of Ukraine, and exploring the prospects for overcoming the technological gap in the national defence-industrial complex.

**Keywords:** defence management, defence procurement, defence-industrial complex, international support, defence resource management.

## Introduction

The full-scale aggression of russia, launched in February 2022, has confronted Ukraine with unprecedented challenges in the field of defence management. The economic component plays a key role in ensuring national security, as financial resources determine the capabilities of the Armed Forces, the effectiveness of defence procurement, the development of the defence industrial complex (DIC), and the ability to attract international assistance. Under wartime conditions, the share of defence spending in Ukraine's budget has risen to record levels, reshaping the priorities of state policy. It is therefore highly relevant to analyse how the state finances defence, how procurement for the Armed Forces of Ukraine (AF of Ukraine) is organised, the current state of the national DIC, the role of international support, and the economic challenges faced by the security and defence sector. This paper examines these aspects based on the latest available data, providing specific examples, quantitative indicators, and factual information. This allows for an outline of the key economic challenges in defence management in Ukraine and possible solutions to address them.

## Methodological Framework

The methodological framework of the study is a comprehensive approach to analysing defence management in Ukraine, which includes economic analysis, a systems approach, and a comparative analysis of international experience. Methods of statistical and financial analysis were applied to examine data on state budget expenditures for defence, the structure of defence financing, procurement efficiency, and the state of the defence-industrial complex. For comparison, data on international support — particularly military and financial aid to Ukraine — were used. A significant role is also played by theoretical developments and empirical studies that highlight NATO countries' experience in defence planning and the financial management of defence resources. In particular, the works of N. M. Tkachuk (2020), A. M. Novytskyi et al. (2024), O. V. Soldatenko (2023), as well as studies on defence management in NATO member states by O. O. Surkov and Yu. V. Tsurko (2024), and A. Nalyvaiko and A. Poliaiev (2021), were used.

Thus, in (N. M. Tkachuk, 2020), the features of state defence expenditure financing were examined, along with the development of practical recommendations for their optimisation under current development conditions. The article by (A. M. Novytskyi, N. B. Novytska, D. V. Pryimachenko, 2024) is dedicated to the issues of organising control over the use of State Budget funds allocated for the needs of national security and defence. In the study by (O. V. Soldatenko, 2023), based on the analysis of the financing of the AF of Ukraine's needs, the main existing problems in the sphere of defence financing under martial law were identified, and certain directions for their resolution were proposed, taking into account Ukraine's Eurointegration development vector. The search for effective approaches to shaping a modern model for managing defence planning processes, adapting them to the current AF of Ukraine, as well as the principles and standards followed by the armies of developed NATO member states, was discussed in (P. V. Shchypanskyi, F. V. Sahaniuk, Yu. M. Mudrak, 2021). In their research, (H. Bukur-Marku, F. Fluri, T. Tagarev, 2010) explain the principles and approaches to the development and implementation of security and defence policy, present the results of relevant studies, and offer examples of best practices in transforming and managing security sector structures, organisational processes, and resources. An analysis of the functioning characteristics of the main defence management systems in the United States and an identification of differences in the implementation of capability-based defence planning within the Ministry of Defence of Ukraine (MoD of Ukraine) and the Armed Forces of Ukraine (AF of Ukraine) is provided in (O. O. Surkov, Yu. V. Tsurko, 2024). The article by (A. Koretskyi, V. Sotnyk, V. Mohylevska, R. Boiko, Ye. Kosaretskyi, 2023) is devoted to explaining the essence of the definitions “defence resources” and “defence resource management”, identifying key theoretical issues and proposing possible solutions. In (A. I. Poliaiev, 2020), the features of implementing defence management practices used in NATO member countries’ defence institutions are analysed. The concepts of “financial management of defence resources” and “defence resource financial management system” are clarified in (N. Pantieleeva, M. Khutorna, O. Honcharenko, 2024). The aim of the article by (A. Nalyvaiko, A. Poliaiev, 2021) was to develop approaches to forming a functional model of defence management using domestic experience alongside principles and approaches adopted in NATO member states, and to implement this model in the MoD of Ukraine, the AF of Ukraine, and other components of the Defence Forces. Significant contributions to developing the methodological foundations for defence resource management in the AF of Ukraine were made in (O. Semenenko, P. Onofriichuk, I. Chernyshova, O. Ostapets et al., 2021) and (O. Semenenko, O. Ostapets, P. Onofriichuk et al., 2021).

## Results and Discussions

**State Budget and Defence Share.** With the onset of the russian-ukrainian war, Ukraine’s defence expenditures have multiplied significantly. While the 2022 state budget had initially planned spending for national security and defence at approximately UAH 323 billion (≈6% of gross domestic product (GDP)), in reality, a colossal UAH 1.5366 trillion was allocated for these needs throughout the year, amounting to 32.5% of GDP [13]. For comparison, before the war, the share of defence spending in Ukraine’s GDP ranged between 2–3%. In 2023, the defence expenditures were set at UAH 1.141 trillion, or 18.2% of the projected GDP [13]. In fact, by the end of 2023, the total expenditures from the general fund of the state budget for the security and defence sector reached UAH 1.8438 trillion, which accounted for 60.8% of all state expenditures that year [14]. Thus, more than half of the wartime state budget was directed specifically toward defence (see Fig. 1).

In 2024, this trend persisted — the 2024 state budget law allocated nearly 50% of all expenditures (₴1.692 trillion, approximately 21.6% of GDP) to national security and defence [13]. For 2025, a further increase in defence spending is planned, reaching ₴2.223 trillion (26.3% of the projected GDP) [13]. This dynamic is unprecedented and reflects the prioritisation of defence under

wartime conditions (see Figure 1).

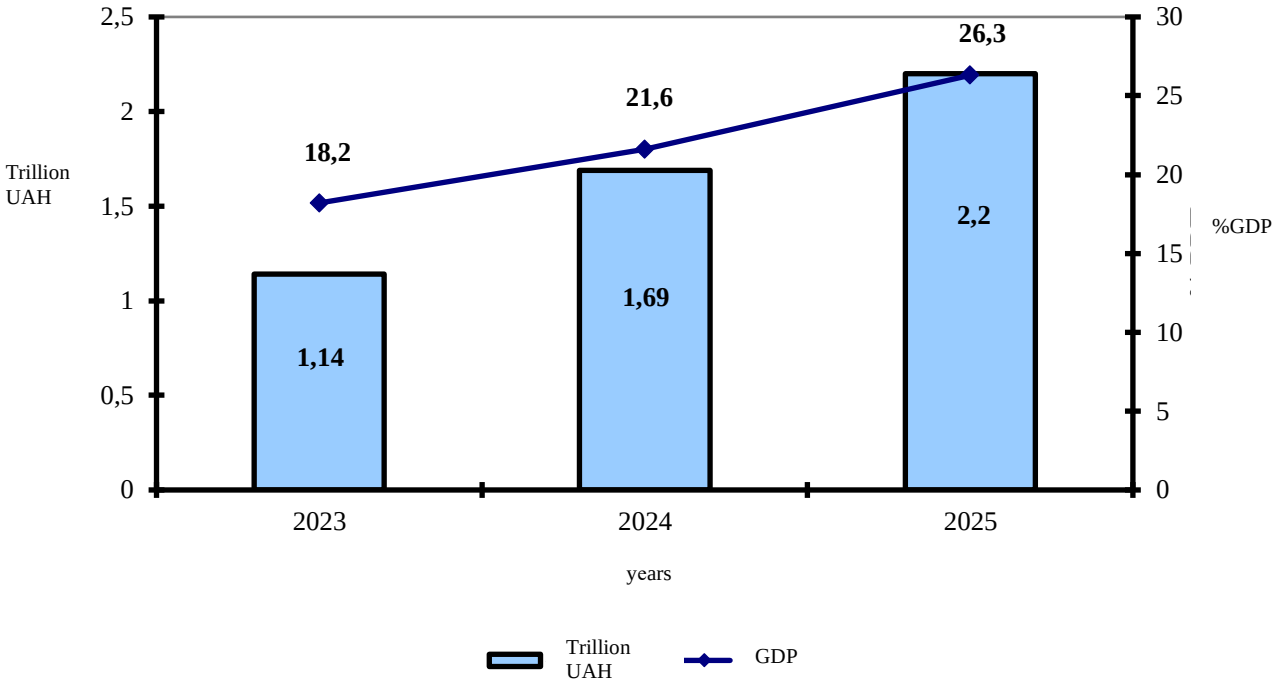



**Figure 1.** National Security and Defence Expenditures in 2023–2025

**Defence Budget Structure.** The substantial increase in appropriations is accompanied by changes in the structure of expenditures. The priority is the financial support of the Armed Forces of Ukraine (AFU), including salaries for service members, combat payments, and unit provisioning, as well as material support and procurement of weaponry. Thus, in 2023, out of the Ministry of Defence of Ukraine's budget (UAH 857.9 billion), the largest share – UAH 494.1 billion – was allocated to the maintenance and support of the AFU (including troop training, medical provision, and social benefits for veterans). A significant portion – over UAH 350 billion – was spent on the procurement and modernisation of weapons and military equipment [13]. Only small amounts were allocated for other needs (for example, UAH 136 million for the construction of housing for military personnel).

The structure of the wartime defence budget is characterised by the dominance of spending on personnel and material support for the Armed Forces, as well as substantial investments in new weaponry.

Figure 3 summarises the budget expenditure distribution by the Ministry of Defence of Ukraine in 2024 by main categories. According to this data, approximately 51% of the funds were spent on maintaining the army, around 42% on arms procurement, and the remainder on infrastructure and other programmes.

Figure 2 illustrates the share of the state budget allocated to defence and security..

It is worth noting that a significant portion of defence expenditure is financed through the state budget deficit. In 2022, a sharp increase in spending led to a deficit of over 20% of GDP, which was covered by monetary emission and external assistance [13].

Subsequently, the government soug to avoid excessive money issuance due to the risk of inflation, making international financial support critical. According to the Ministry of Finance, in 2023 Ukraine received USD 38.4 billion from its partners to finance the state budget (see Table 1) [15].

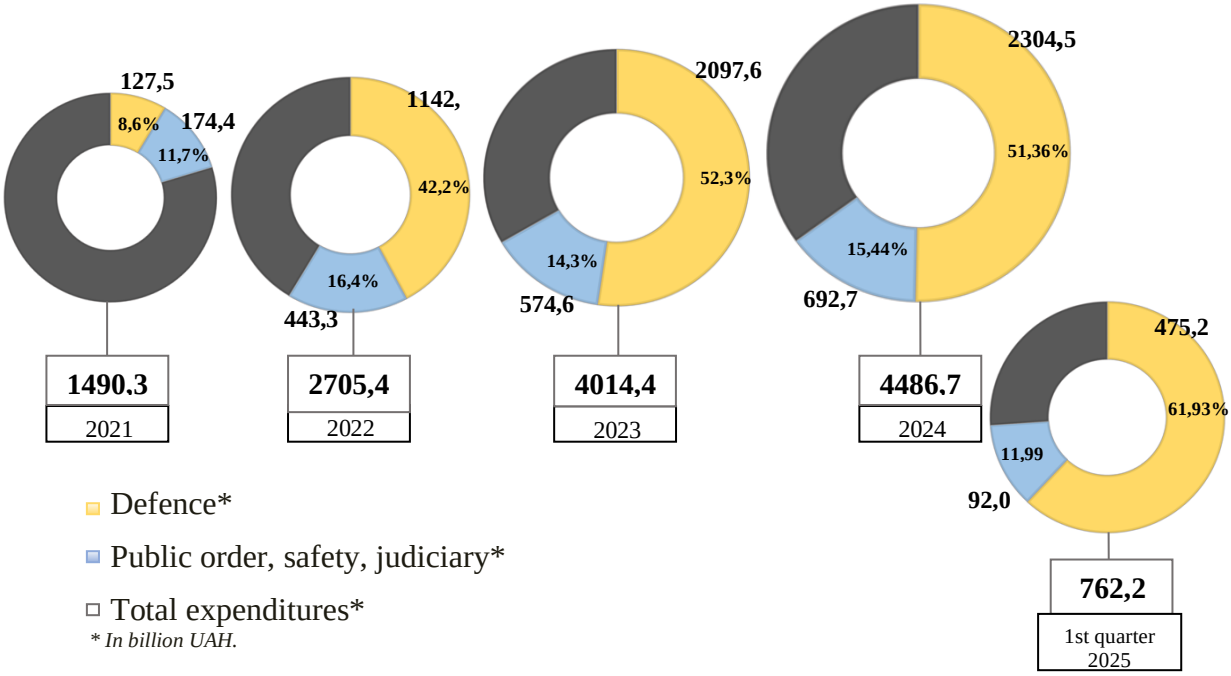
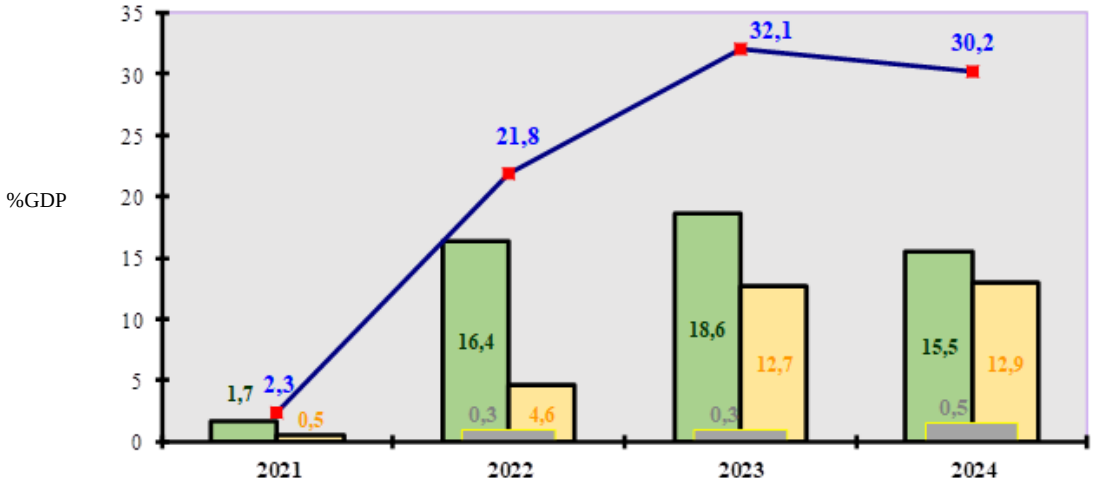



**Figure 2.** Growth of Ukraine's Defence Expenditure in 2021–2025




payment of service allowances, troop training, medical support
procurement, modernisation, development, and repair of weapons, equipment, and military hardware
State Special Transport Service
total defence

**Figure 3.** Budgetary Funding for Defence and Its Components in 2021–2024

Since the beginning of the full-scale aggression, Ukraine has received approximately €267 billion, or around €80 billion each year of the war in total. Of this total, 49% was military aid, 44% financial, and 7% humanitarian assistance [16].

**Table 1.** Contribution of Allies to Ukraine's Victory. Top 10 Countries

| Country | Aid from the Country, GDP % | Total Amount, USD Billion |
|---|---|---|
| Estonia | 1,26 | 0,54 |
| Latvia | 1,09 | 0,51 |
| Lithuania | 0,95 | 0,76 |
| Poland | 0,68 | 6,21 |
| Slovakia | 0,63 | 1,06 |
| Denmark | 0,51 | 3,01 |
| Netherlands | 0,44 | 7,24 |
| Finland | 0,44 | 1,97 |
| Bulgaria | 0,31 | 0,48 |
| Czech Republic | 0,36 | 1,57 |

The largest donors have become the European Union ($17.9 billion) and the United States ($10.9 billion) — these funds were spent on covering salaries, pensions, and other budgetary expenditures, allowing the state to allocate its own resources towards defence [15]. The share of each individual donor is extremely small when compared to the size of their respective economies. For instance, the United Kingdom, Germany, and the United States each allocated no more than 0.2% of their GDP to aid Ukraine. For France, Spain, and Italy, this figure is even lower — just 0.1%.%.

According to these estimates, the countries that have provided the most direct aid to Ukraine are:

Estonia – 2.2% of GDP;
Denmark – 2.17% of GDP;
Lithuania – 1.8% of GDP;
Latvia – 1.53% of GDP;
Finland – 0.98% of GDP;
Sweden – 0.92% of GDP;
Poland – 0.8% of GDP;
Netherlands – 0.78% of GDP;
Norway – 0.75% of GDP;
Slovakia – 0.65% of GDP.

In other words, the United States does not even feature in the top ten donors to Ukraine relative to the size of its economy.

During wartime, domestic budget revenues (taxes, internal borrowing) have also been mobilised to the maximum: military bonds have been introduced, and the government has significantly reduced civilian expenditure. As a result, defence spending is financed through both internal resources and external support. This enables Ukraine to maintain an army numbering in the hundreds of thousands and to equip it with the necessary weaponry, despite the sharp economic downturn in 2022 and significant GDP losses.

**Defence Procurement Needs**

***Defence Procurement System and Transparency.*** The urgent wartime needs required rapid and large-scale procurement for the army — ranging from food and uniforms to weapons and ammunition. Before 2022, procurement for the Armed Forces of Ukraine was mostly carried out through open tender procedures (the Prozorro system), in accordance with [17]. However, with the onset of the full-scale invasion, many tenders were classified or replaced by direct contracts due to the urgency of supply. On the one hand, this accelerated the provision of resources to the military; on the other, it created risks of abuse.

***Anti-Corruption Reforms in Procurement.*** In 2023, the Ministry of Defence of Ukraine introduced a new two-stage procurement mechanism for food supplies for the Armed Forces of

Ukraine. Firstly, ceiling prices were established for key food products for the Defence Forces in order to prevent procurement at deliberately inflated rates. Secondly, a two-tier procurement system was implemented: from now on, the newly established entity — the State Rear Operator — is responsible for directly concluding contracts with suppliers, while the Ministry of Defence of Ukraine determines the requirements and oversees the ceiling prices [18].

This model aligns with the practices of NATO member states. The State Rear Operator, headed by an expert in the field of anti-corruption, has taken over responsibility for supplying the troops (food, clothing, fuel, medical supplies), while the MoD of Ukraine has focused on policy-making and oversight. At the same time, a separate Defence Procurement Agency was established to centralise the acquisition of weapons and equipment [19]. Thus, crisis conditions have driven a profound restructuring of Ukraine's defence procurement system in line with NATO standards.

**The Defence-Industrial Complex of Ukraine (National DIC)**

***The State and Mobilisation of the Defence-Industrial Complex During Wartime.*** The Defence-Industrial Complex of Ukraine has historically possessed significant potential; however, prior to 2022, it was undergoing a prolonged reform process. The armed aggression required a sharp increase in the production of weapons and ammunition. At the onset of the war, Ukraine faced a shortage of domestic production capacity in several critical categories (particularly Soviet-calibre ammunition, missiles, modern drones, etc.). Nevertheless, by 2022–2023, the national DIC had undergone accelerated mobilisation. In 2023, production volumes continued to grow.

To support this process, the government adopted a decision obliging the Ministry of Defence of Ukraine to purchase all output from ammunition factories (within operational needs), and to turn to imports only in case of shortfalls［20]. This approach guarantees domestic manufacturers a secure market and incentives for ramping up production.

***Corporatisation and Sector Reforms.*** At the same time, the state continued reforming the structure of the Defence-Industrial Complex to enhance its efficiency. The main focus of the DIC reform was the transformation of the state-owned conglomerate Ukroboronprom, which united the country's key state defence enterprises. In June 2023, the conglomerate was officially dissolved as part of its conversion into a joint-stock company called Ukrainian Defence Industry ［19].

Despite the initiated transformation, by early 2024, the reform of the DIC had not yet been fully completed. Experts note that the delay in reform poses risks, particularly for the development of cooperation with Western partners［20］.

Another challenge lies in the personnel and technological modernisation of the Defence-Industrial Complex. Many highly qualified specialists have been lost, and part of the production facilities have been destroyed by hostilities or are now located in frontline areas. The response to these issues has been the establishment of cooperation with Western arms manufacturers on Ukrainian territory, as well as encouraging private Ukrainian companies to participate in defence production.

The large-scale development of high-tech weaponry requires substantial investment and technology transfer, which can only be secured through continued reform and active international cooperation.

**International Cooperation and Import Substitution.** Given its limited domestic resources, Ukraine is actively seeking opportunities to produce weapons jointly with foreign partners.

Import substitution of key components—previously supplied from russia or other countries—remains a challenge for the Defence-Industrial Complex of Ukraine. In recent years, Ukraine has managed to localise the production of gunpowder, explosives, and drone electronics. However, certain complex systems (e.g. turbojet engines for missiles) still require cooperation with Western manufacturers.

Due to russian strikes, which have repeatedly targeted defence enterprises, Ukraine has been forced to decentralise production and partially relocate it to underground or fortified facilities. This

complicates and increases the cost of manufacturing. However, despite all the challenges, Ukraine's defence industry is ramping up output: in 2023, production volumes of the Defence-Industrial Complex of Ukraine increased by 28% compared to 2021, and in certain areas (such as munitions and UAVs), output multiplied several times over [13]. This marks a significant achievement in economic aspects of defence management.

At this stage, there remains a shortage of funding for production capacities. Nevertheless, according to the Ministry of Defence of Ukraine, by 2023–2024 the domestic production of artillery systems, anti-tank weapons, armoured personnel carriers, and munitions had doubled. In 2025, the production capacity of Ukraine's Defence-Industrial Complex could reach 35 billion USD (compared to only 1 billion USD in 2022). In 2023, production volumes of defence products rose to 9 billion USD in domestic funds, supplemented by 1.5 billion USD in foreign investment, while in 2024 the figure already reached around 20 billion USD.

**International Aid**

***Scale and Significance of External Support.*** International military and financial aid has become a decisive factor in Ukraine's survival in this war. According to Pentagon estimates, as of early 2025, the total value of security aid provided to Ukraine by the United States exceeded USD 65 billion (see Figure 4) [16].

It is more than the military budget of most European countries. The European Union and its member states have jointly provided comparable volumes of support. According to analytical data, 47% of all international aid to Ukraine (in the broad sense, including financial and military) in 2022–2023 comes from EU countries, while the share of the United States is about 43% [15].

International aid has two main components: direct military aid (supply of weapons, ammunition, equipment, training of the military) and financial support (grants and loans that allow Ukraine to maintain macroeconomic stability and finance the wartime budget deficit). Both components are closely interconnected: external grants to the state budget ($38.4 billion to the general fund in 2023) make it possible for Ukraine to pay salaries to military personnel and pensions without resorting to excessive money issuance, while the deliveries of modern weaponry free of charge or on preferential terms significantly enhance the combat capabilities of the Armed Forces of Ukraine. Therefore, allied aid effectively compensates for Ukraine's economic weakness compared to the aggressor, levelling the situation in terms of resource provision for the Armed Forces of Ukraine.

**The Military Aid Structure.** During 2022–2024, Ukraine received a wide range of weaponry from more than 30 countries. The United States focused on supplying high-tech systems. European countries delivered a large quantity of heavy equipment of both Soviet and NATO origin: tanks (over 300 units, including ~100 Leopard 2 from various countries and dozens of other models), infantry fighting vehicles (thousands of units, including Marder, Bradley, CV90), artillery systems (PzH 2000 howitzers, CAESAR, Krab self-propelled guns, and others), air defence systems (SAMP/T, IRIS-T, Gepard), and so on (Figure 5).

United Kingdom, Germany, and Canada. Among international programmes, the European Peace Facility (EPF) stands out – the EU uses it to finance the procurement of weapons for Ukraine (its budget for Ukraine was increased to €5 billion per year by a 2023 decision).The Ukrainian military also received significant humanitarian aid of a military nature – equipment, medical supplies, gear, fuel, and more, delivered both by governments and through private initiatives.

One of the unique phenomena was the global wave of volunteer support: hundreds of millions of dollars were raised via foundations and platforms to purchase drones, vehicles, and thermal imagers for the Ukrainian army. While this lies outside the state management system, it significantly supplements official aid.

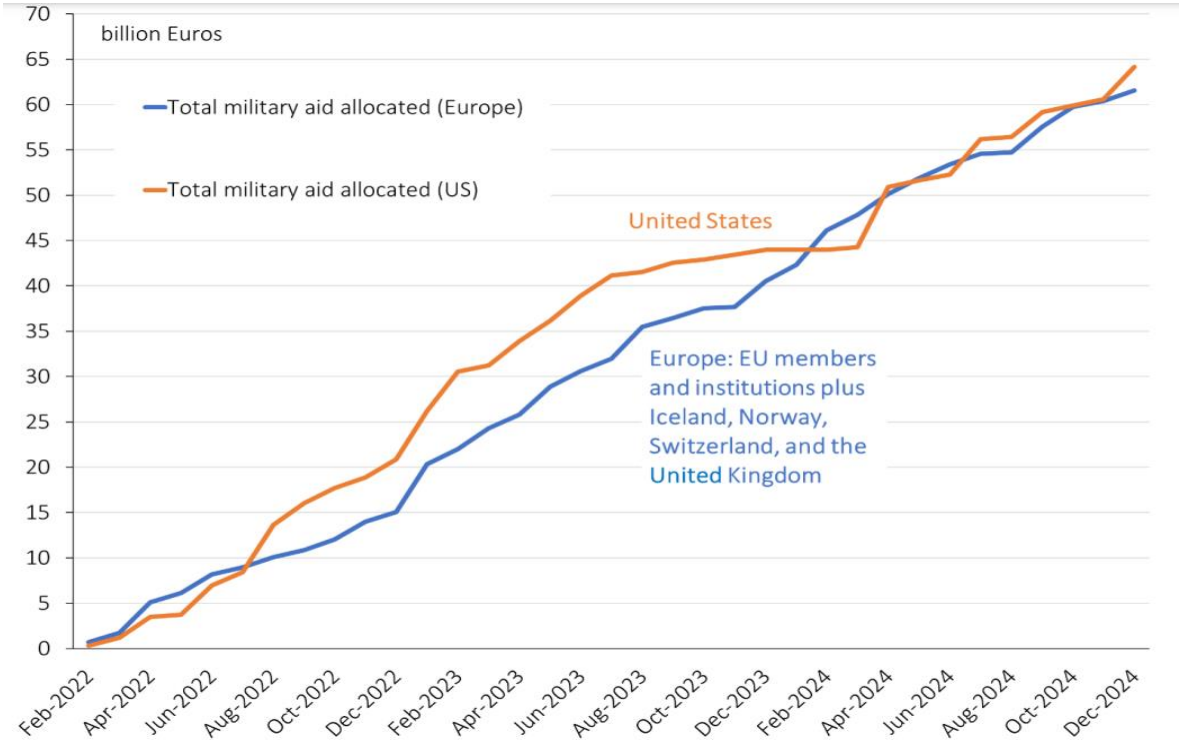



**Figure 4.** Estimated Military Aid Provided to Ukraine by the United States and European Countries. Infographic by the Kiel Institute




**Figure 5.** Weapons Received by Ukraine from Western Partners

**International Support Challenges.** Despite its considerable scale, international aid has certain problematic aspects. Firstly, it depends on the political will of donor countries, which may shift. For example, at the end of 2023, there was a pause in the new U.S. aid package worth approximately $60 billion due to political debates in Congress. In Europe, a change of government in Slovakia led to

statements about halting military aid to Ukraine, while the Hungarian authorities have systematically blocked certain joint EU programmes. Such factors create uncertainty regarding the sustainability of external support. Secondly, the logistics and speed of weapons delivery sometimes fail to match the pace of developments on the front line – decisions to provide modern tanks or fighter jets were made by partners after lengthy debates and with delays. Thirdly, there is a need for the effective integration of transferred systems into the structure of the Armed Forces of Ukraine: training of personnel abroad is required, as well as adaptation of infrastructure (for instance, the transition to NATO calibres demands the re-equipment of some arsenals and technical bases). All of these issues require a high level of coordination and strategic planning from Ukraine's defence management. In particular, the Government of Ukraine has developed a medium-term defence procurement plan, taking into account anticipated international aid to avoid duplication or shortages in specific areas. Additionally, Ukraine is making efforts to ensure accountability and transparency in the use of Western aid, fully understanding that donor trust is critical. In 2023, the "Logfas" weapons tracking system was introduced in line with NATO standards. It allows for tracking of every item of received equipment – thereby increasing partner confidence.

Thus, international aid has become an integral component of the economic support for Ukraine's defence. Without it, the country's own resources would not be sufficient to wage a prolonged and exhausting war. At the same time, the attraction of such aid poses a task for management: to use it effectively and to preserve the political support of allies. Ukraine is striving to demonstrate maximum effectiveness of the received resources on the battlefield, which, in turn, motivates partners to continue their support.

Analysis of the economic component of Ukraine's defence management during the wartime period reveals a number of systemic challenges. The **first** of these is the extreme budgetary burden. Defence spending exceeds the capacity of the national economy, leading to a massive budget deficit (over UAH 1 trillion in 2023) [14]. This makes Ukraine dependent on external funding and forces it to accumulate debt. In the long term, servicing this debt and rebuilding the economy after the war will be a separate challenge. The **second** challenge is maintaining a balance between the speed and transparency of defence procurement. Wartime circumstances demand immediate responses to the needs of the front, but at the same time, society expects proper control over public spending. Any corruption scandals undermine the trust of both citizens and foreign donors. Therefore, it is crucial to bring the initiated reforms to success — to ensure the full functioning of the State Rear Operator and the Defence Procurement Agency, to introduce electronic catalogues and open reporting wherever possible, without compromising secrecy.

The **third** set of problems is related to the limited internal production capacity. Despite gradual growth, the Ukrainian defence-industrial complex is still unable to fully meet the front's needs for critical types of weaponry (for example, air defence missiles, modern aircraft, etc.). The country must rely on imports and aid, which are not always predictable. A post-war strategy for the development of the defence industry needs to be devised, which should include the modernisation of enterprises, workforce training, and technology transfer from partner countries. The **fourth** challenge is both personnel-related and institutional. Waging war depletes not only material but also human resources. It is necessary to ensure adequate funding for military personnel pay to retain the army's human capital and prevent an outflow to the private sector or abroad after the war. At the same time, it is important to strengthen defence management institutions: to enhance the capacity of the Ministry of Defence of Ukraine and the General Staff of the Armed Forces of Ukraine to plan budgets and procurements based on the analysis of defence needs, to introduce modern ERP systems for resource management in the military, and to develop civil democratic oversight.

It is also worth highlighting the issue of the effective use of international aid. Ukraine must make the most efficient use of the resources provided in order to achieve a turning point in the war. A clear correlation is already visible: the reinforcement of armaments (artillery, armoured vehicles,

air defence systems) thanks to allied support enabled successful defensive and offensive operations in autumn 2022 and summer 2023. This serves as an argument for further investment in Ukraine's victory. Thus, part of defence management also includes diplomatic work, accountability to partners, and an information policy that demonstrates the effectiveness of the aid – for example, regular briefings showing how many targets were downed using donated air defence systems, how much territory was liberated with the support of Western tanks, and so on.

Finally, a **strategic challenge** lies in planning the post-war recovery of the security and defence sector. Once hostilities end, Ukraine will face the task of maintaining a combat-ready army while simultaneously reallocating part of its resources towards rebuilding the country. Experts are already discussing what level of military spending would be acceptable in peacetime and how to integrate the Ukrainian defence-industrial complex into the European arms market. The economic resilience of the defence sector will require the continuation of reforms – in particular, the introduction of medium-term defence budget planning, the establishment of stabilisation funds, and Ukraine's participation in joint European weapons procurement programmes.

**Conclusion**

The economic component of Ukraine's defence management during the russian–ukrainian war is marked by extreme pressure on resources alongside a large-scale transformation of the system for managing those resources. The analysis has shown that Ukraine sharply increased defence spending – the share of military expenditure in GDP rose to more than a quarter, and within the budget structure – to half or more [14]. This became possible due to the mobilisation of internal revenues and unprecedented international support. At the same time, these circumstances highlighted several problems: shortcomings of the old procurement system, the economy's vulnerability to shocks, and insufficient autonomy of the defence-industrial complex. In response, the state implemented a number of important reforms – from new defence procurement mechanisms (via the State Logistics Operator and the Defence Procurement Agency) to the corporatisation of defence enterprises and the involvement of foreign partners in weapons production. These steps have already yielded initial positive results in the form of improved support for the AF of Ukraine and reduced corruption risks.

However, significant challenges remain for defence management. It is necessary to ensure sustainable funding for the army in the context of economic decline, to maintain public trust through transparent and efficient spending of every hryvnia from the defence budget, and to continue strengthening domestic industrial capacity despite enemy strikes and technological limitations. Western support remains crucial – preserving the political will and unity of Western allies in assisting Ukraine until full victory. Economic aspects will also play a major role in the post-war period: the speed of recovery and Ukraine's place in the post-war architecture of European security will depend on how rationally current resources are used.

In conclusion, it can be stated that Ukraine withstood the first and most difficult blow thanks to the mobilisation of all available economic resources and the collective support of the international community. The further task of defence management is to shift from crisis response to strategic planning in order to ensure the long-term defence capability of the state based on sustainable economic development. Studying and taking into account the lessons of 2022–2024 will help strengthen Ukraine's institutional capacity to effectively manage the financial and industrial components of defence, which is an essential condition for achieving victory and preserving statehood.

**Recommendations**

The materials of the article may be used for the development of state policy in the field of defence management, as well as by educational and research institutions, public authorities, and military structures involved in addressing issues of defence management.

Promising areas for further research include studying the place and role of the economic components of defence management in the post-war recovery of Ukraine, the development of the AF of Ukraine, as well as examining the prospects for overcoming the technological lag of the national defence-industrial complex.

**References**

1. Tkachuk, N. M. (2020). *Specifics of financing defense expenditures in Ukraine*. http://baltijapublishing.lv/omp/index.php/bp/catalog/download/237/6438/13291-1?inline=1
2. Novytskyi, A. M., Novytska, N. B., & Pryimachenko, D. V. (2024). Organization of public-legal control over the utilization of Ukraine's state budget funds allocated for national security, defense, and small business support. *Legal Scientific Electronic Journal*, *1*, 430–433. http://www.lsej.org.ua/1_2024/101.pdf
3. Soldatenko, O. V. (2023). Funding the Armed Forces of Ukraine under martial law: Eurointegration vector. *Scientific Herald of Uzhhorod National University. Law Series*, *80* (1), 576–581. http://visnyk-pravo.uzhnu.edu.ua/article/view/297184/290100
4. Shchypanskyi, P. V., Sahaniuk, F. V., & Mudrak, Yu. M. (2021). Defense management: Approaches to managing defense planning processes. *Collection of Scientific Papers of the Center for Military and Strategic Studies, NDU of Ukraine*, *1* (71), 52–58. http://nbuv.gov.ua/UJRN/Znpcvsd_2021_1_10
5. Bucur-Marcu, H., Fluri, P., & Tagarev, T. (2010). *Defense management: An introduction. Geneva Centre for the Democratic Control of Armed Forces (DCAF). Security and Defense Management Series, 1*. https://www.dcaf.ch/sites/default/files/publications/documents/Book_Defense_ukr_final.pdf
6. Surkov, O. O., & Tsurko, Yu. V. (2024). Specifics of defense management in the U.S. Department of Defense. *Collection of Scientific Papers of the Center for Military and Strategic Studies, NDU of Ukraine*, *1* (80), 34–40. http://znp-cvsd.nuou.org.ua/article/view/305486/297089
7. Koretskyi, A., Sotnyk, V., Mohylevska, V., & Boyko, R., et al. (2023). Essential characteristics and the necessity of legal regulation of defense resource management mechanisms. *Social Development and Security*, *13* (1), 83–96. https://journals.indexcopernicus.com/api/file/viewByFileId/2013726
8. Poliaiev, A. I. (2020). Certain aspects of implementing defense management in defense agencies of NATO member states. *Collection of Scientific Papers of the Center for Military and Strategic Studies, NDU of Ukraine*, *3* (70), 70–74. http://znp-cvsd.nuou.org.ua/article/view/223664/223907
9. Pantelieieva, N. M., Khutorna, M. E., & Honcharenko, O. O. (2024). Financial management in national defense. *Testing and Certification*, *1* (3), 102–118. https://doi.org/10.37701/ts.03.2024.14
10. Nalyvaiko, A., & Poliaiev, A. (2021). Approaches to developing a functional model of defense management. *Social Development and Security*, *11* (3), 20–29. http://nbuv.gov.ua/UJRN/socdevsec_2021_11_3_4
11. Semenenko, O., Onofriichuk, P., Chernyshova, I., & Ostapets, O., et al. (2021). Methodological fundamentals of defense resource management in the Armed Forces of Ukraine. *Social Development and Security*, *11* (5), 98–110. https://media.neliti.com/media/publications/545556-methodological-fundamentals-of-defense-r-ee633546.pdf
12. Semenenko, O., Ostapets, O., Onofriichuk, P., & Moskalenko, I., et al. (2021). Modern features of formation and development of the defense resource management system in the Armed Forces of Ukraine. *Social Development and Security*, *11* (2), 125–140.

https://media.neliti.com/media/publications/543824-modern-features-of-formation-and-develop-10f61d1b.pdf
13. Sakhno, A. (2024). *Money for the strong: How Ukraine's defense budget has changed since the beginning of the war.* https://www.rbc.ua/rus/news/groshi-silnih-k-zminyuvavsya-oboronniy-byudzhet-1732120941.html
14. *How much state budget funding went to security and defense in 2023* – Ministry of Finance responded. (2024). https://suspilne.media/666746-aka-suma-vidatkiv-z-derzbudzetu-ukraini-jsla-na-bezpeku-j-oboronu-v-2023-roci-u-minfini-dali-vidpovid/
15. How much assistance and from whom Ukraine received in 2023. (2024). https://finance.ua/ua/goodtoknow/dopomoga-ukraini-2023
16. Nedashkivskyi, V. (2025). *How much aid Ukraine received from the US and other allies.* https://biz.censor.net/resonance/3537928/chy-diyisno-ssha-nadaly-ukrayini-350-500-milyardiv
17. Law of Ukraine (2020). "*On Defense Procurement"* (as amended). https://zakon.rada.gov.ua/laws/show/808-20#Text
18. Tsarevskyi, D. (2024). *Ministry of Defense of Ukraine introduced new procurement procedures after the "17 hryvnia eggs" scandal: what changed?* https://zaborona.com/mo-ukrayiny-vvelo-novu-proczeduru-zakupivel-pislya-skandalu-z-yajczyamy-po-17-grn-shho-zminylosya/
19. Ministry of Defense of Ukraine. (2023). *Procurement activities of the MoD*. https://mod.gov.ua/diyalnist/zakupivelna-diyalnist
20. Omelchenko, K. (2023). *Ukroboronprom plans to ramp up ammunition production.* https://rubryka.com/2023/05/15/ukroboronprom-planuye-narostyty-vyrobnytstvo-snaryadiv/
21. Kramarenko, D. (2023). *Corporation instead of a concern: What is known about Ukroboronprom's reform and why it is needed*. https://www.rbc.ua/rus/news/korporatsiya-zamist-kontsernu-shcho-vidomo-1688037575.html
22. Center for Army, Conversion, and Disarmament Studies (2024, 6 Decemb.). The issue of incomplete reforming of the state sector of the defense industry. *Defense Industry Courier*. https://opk.com.ua/проблема-незавершеного-реформування/#:~:text

## Проблеми оборонного менеджменту в Україні: економічний аспект

**Володимир Дідіченко**
кандидат військових наук, старший науковий співробітник,
старший науковий співробітник
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: DVP1951@ukr.net
ORCID: 0000-0002-0440-2299

**Василь Череп**
кандидат військових наук, старший дослідник
начальник науково-дослідного управління
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: vasya.cherep1976@gmail.com
ORCID: 0000-0003-3305-4518

**Поліна Толок**
кандидат економічних наук
начальник кафедри оборонного менеджменту
Національний університет оборони України
03049, проспект Повітряних Сил, 28, Київ, Україна
e-mail: tolok100@meta.ua
ORCID: 0000-0002-2481-8152

**Валерія Горгуленко**
молодший науковий співробітник
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: horhulenkovaleriia@gmail.com
ORCID: 0009-0009-1394-6325

**Марія Ярмольчик**
доктор філософії
начальник науково-дослідної лабораторії
Національний авіаційний університет
03058, проспект Любомира Гузара, 1, Київ, Україна
e-mail: LinkinFan357@ukr.net
ORCID: 0000-0001-9917-0189

**Анотація.** Актуальність статті зумовлена необхідністю комплексного розгляду економічних аспектів оборонного менеджменту в Україні. Досліджено економічні аспекти оборонного менеджменту в Україні в умовах російсько-української війни з акцентом на фінансове забезпечення Збройних Сил України, особливості оборонних закупівель, стан оборонно-промислового комплексу та роль міжнародної підтримки. Метою статті є дослідження ключових економічних аспектів оборонного менеджменту України, зокрема фінансування Збройних Сил України, реформування системи закупівель, стану та розвитку оборонно-промислового комплексу, а також міжнародної підтримки. У статті застосовано системний підхід, методи економічного і фінансового аналізу, а також порівняльний аналіз досвіду країн НАТО. На основі аналізу бюджетних видатків виявлено безпрецедентне зростання витрат на оборону. Визначено основні виклики, зокрема високий рівень дефіциту бюджету, ризики корупції у системі оборонних закупівель, обмеженість виробничих потужностей оборонно-промислового комплексу та залежність від зовнішньої фінансової допомоги. Запропоновано конкретні рекомендації щодо удосконалення системи фінансового планування та управління оборонними ресурсами, забезпечення прозорості закупівель, активізації реформ оборонно-промислового комплексу та посилення міжнародної співпраці. Отримані результати мають практичне значення для розроблення державної політики у сфері оборонного менеджменту та можуть використовуватися в освітніх і наукових закладах, а також органами державної влади та військовими структурами, причетними до вирішення питань, що стосуються оборонного менеджменту. Перспективними напрямами подальших досліджень є вивчення місця та ролі економічних складових оборонного менеджменту у післявоєнному відновленні України, розвитку Збройних Сил України, а також дослідження перспектив ліквідації технологічного відставання вітчизняного оборонно-промислового комплексу.

**Ключові слова:** оборонний менеджмент, оборонні закупівлі, оборонно-промисловий комплекс, міжнародна підтримка, управління оборонними ресурсами.

The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 3 No. 2 (2025)

DOI: 10.62524/msj.2025.3.2.10

# Recommendations on the Implementation of Defence Planning Measures for Acquiring and Developing Capabilities by the Prospective Cyber Forces of the Armed Forces of Ukraine Based on the DOTMLPFI

**Volodymyr Horbatiuk**
Deputy Chief of the General Staff of the Armed Forces of Ukraine
The General Staff of the Armed Forces of Ukraine
03168, Povitrianykh Syl Avenue, 6, Kyiv, Ukraine
e-mail: gorbvol@yahoo.com
ORCID: 0009-0009-9566-3168

**Vladyslav Horhulenko**
Adjunct of the Scientific and Organisational Department
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl Avenue, 28 B, Kyiv, Ukraine
e-mail: vladyslavhorhulenko@gmail.com
ORCID: 0000-0001-6382-5075

**Valeriia Horhulenko**
Junior Research Fellow
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl Avenue, 28 B, Kyiv, Ukraine
e-mail: horhulenkovaleriia@gmail.com
ORCID: 0009-0009-1394-6325

**Yuzef Dobrovolskyi**
Candidate of Technical Sciences, Associate Professor
Deputy Chief of the Military Education Department
for the Educational Work – Chief of the Educational Unit
The National Aviation University
03048, Medova Street, 1, Kyiv, Ukraine
e-mail: kataza@i.ua
ORCID: 0000-0002-1077-1402

**Maksym Samsonenko**
Educator of the Millitary Management Department
at the Institute of State Military Management of the National Defence University of Ukraine
National Defence University of Ukraine
03049, Povitrianykh Syl Avenue, 28, Kyiv, Ukraine
e-mail: samson8115@ukr.net
ORCID: 0009-0001-6264-6582

**Abstract.** Today, the development of the Ministry of Defence of Ukraine and its Armed Forces, in particular, is carried out based on the capabilities required, with a focus on existing and potential threats to national and military security. The experience of armed confrontation over the past decade has shown that one such threat is adversary aggression in cyberspace. Therefore, there is now

sufficient justification for establishing Cyber Forces as a separate branch of troops(Forces) within the Armed Forces of Ukraine, whose task shall be the preparation for and conduct of military measures for cyber defence. Effective execution of this task will be possible if the prospective Cyber Forces of the Armed Forces of Ukraine acquire the capabilities for conducting confrontation in cyberspace as defined in the Strategic Defence Bulletin. The aim of the article is to develop an implementation model for defence planning measures to acquire and develop capabilities by the prospective Cyber Forces of the AF of Ukraine, based on DOTMLPFI – one of the advanced methods (approaches, techniques) used in NATO countries.

During the course of the research, methods of systems analysis, generalisation, and systematisation were used, which collectively enabled the development of an implementation model for defence planning measures to acquire and develop capabilities by the prospective Cyber Forces of the Armed Forces of Ukraine based on DOTMLPFI. The developed model represents a description of capabilities for conducting confrontation in cyberspace for each of the eight fundamental DOTMLPFI components in the following format: the potential that can be achieved through the implementation of acquired capabilities; the current state (problem) of the capabilities; and possible measures to resolve the problem that will enable the potential to be realised. Thus, the implementation model for defence planning measures to acquire and develop capabilities by the prospective Cyber Forces of the Armed Forces of Ukraine covers such capability components for conducting confrontation in cyberspace as: doctrinal foundation (D), organisation (O), training (T), materiel support (M), leadership (L), personnel (P), infrastructure (F), and interoperability (I). The practical significance of the research results is revealed in the potential of the Armed Forces of Ukraine to acquire capabilities for conducting confrontation in cyberspace through the implementation of the proposed defence planning implementation model based on DOTMLPFI.

**Keywords:** cyber defence, cyberspace, cybersecurity, cyber confrontation, Cyber Forces, defence planning, capabilities, DOTMLPFI.

## Introduction

Defence planning activity plays a key role in ensuring state national security [1–3]. This activity requires constant dynamic development, adaptation, modernisation, and reform across the security sector, particularly within the armed forces, to maintain the state's ability to repel armed aggression. The complexity of the defence planning process lies in assessing this ability amidst uncertainty surrounding future armed aggression — including the scale of conflict, enemy weaponry, intentions, objectives, and other factors [4–6]. Accordingly, the level of readiness to repel aggression may fall short due to insufficient threat assessment, or exceed what is necessary and sufficient — leading to excessive defence spending from the state budget, which is unacceptable in countries with market economies and democratic systems. Under such conditions, a variety of defence planning approaches have emerged, including: top-down planning; resource-based; technology-based; risk-avoidance-based; sequential planning; historically driven; scenario-based; threat-oriented; and capability-based models. Ukraine currently adopts capability-based defence planning oriented towards threats. This model allows for consideration of threats to military security and their potential development scenarios, enabling the identification of tasks for Ukraine's Security and Defence Sector entities, as well as the capabilities required to fulfil them — capabilities that must be inherent in standard capability carriers [7–9].

Under the Law of Ukraine [10], the task of preparing and conducting cyber defence is assigned to the MoD of Ukraine and the General Staff of the AF of Ukraine. The Strategic Defence Bulletin [11] defines the list of components within the Security and Defence Sector of Ukraine required for capability development. Among these, the AF of Ukraine is the carrier of all the specified capabilities without exception. At the same time, the Cybersecurity Strategy of Ukraine [12] establishes the

formation of cyber troops within the system of the MoD of Ukraine. To implement this provision, a draft law [13] has been registered in the Verkhovna Rada of Ukraine, which proposes the establishment of Cyber Forces as a separate branch of troops(Forces) of the AF of Ukraine, whose main task shall be the execution of specifically military measures for the for state cyber defence. The relevance and urgency of forming Cyber Forces as a separate branch of troops(Forces) within the AF of Ukraine is further confirmed by the results of analysis and synthesis of advanced experience in conducting cyber warfare during contemporary armed conflicts [14], which indicate a threat to Ukraine's national and military security in the form of military cyber operations by the russian federation (rf) and highlight the dominance in cyberspace of states whose defence institutions include cyber troops. Under wartime conditions, the russian federation (rf) actively employs its own cyber forces, which influence the course of the war in Ukraine across the informational and cognitive dimensions. Unlike the United States, the rf has not formally declared the existence of cyber forces, but in practice they exist in the form of several structures, the main ones being: APT "Sandworm" under the Main Directorate of the General Staff of the Armed Forces of the rf, APT "Turla" under the Federal Security Service of the rf, and APT "Nobelium" under the Foreign Intelligence Service of the rf [14].

It would be entirely logical and rational for the prospective Cyber Forces to aggregate all required capabilities for conducting confrontation in cyberspace, as defined for the AF of Ukraine, with their acquisition enabling the formation of an integrated ability to conduct military measures for state cyber defence. At the same time, the use of modern methods, models, approaches, and techniques of defence planning during planning activity may significantly enhance the implementation model for capability development measures by the Cyber Forces [15–18].

The aim of the article is to develop an implementation model for defence planning measures to acquire and develop capabilities by the prospective Cyber Forces of the AF of Ukraine, based on DOTMLPFI – one of the advanced methods (approaches, techniques) used in NATO countries.

**Methodological Framework**

The methodological basis of the research is the application of DOTMLPFI principles to the process of acquiring and developing capabilities by Ukraine's prospective Cyber Forces through the development of a capability-based defence planning implementation model.

DOTMLPFI is based on eight fundamental components used for capability decomposition, namely:

1. Doctrine (D) – doctrinal foundation.
2. Organization (O) – organisation.
3. Training (T) – training.
4. Materiel (M) – materiel support.
5. Leadership (L) – command and leadership.
6. Personnel (P) – personnel.
7. Facility (F) – military infrastructure.
8. Interoperability (I) – interoperability.

Examples of applying the DOTMLPFI method in defence institutions of leading states provide a broader understanding of the strategy for the soft integration of Cyber Forces into the system of the MoD of Ukraine.

The DOTMLPFI system is based on NATO's defence capabilities. The NATO Alliance is a global leader in the field of cyber defence due to its well-considered strategy for protecting digital space, effective coordination among allies, and advanced cybersecurity infrastructure. As early as 2008, the North Atlantic Alliance recognised cyberspace as a separate theatre of operations, and since 2016, has equated it with the traditional domains of warfare – land, sea, air, and space. This demonstrates that NATO views cyberattacks not merely as a threat but as a serious challenge that may

have critical consequences for national security. The war waged by the rf against Ukraine has clearly demonstrated the impact of cyberattacks on Ukraine's cyberspace and information domain as a whole. The need for the AF of Ukraine to acquire capabilities for state cyber defence is fully justified.

It is proposed to develop an implementation model for defence planning measures aimed at acquiring and developing capabilities by the prospective Cyber Forces of the AF of Ukraine using a capability assessment methodology consisting of four stages [19]:

1. Preparatory stage
2. Requirement analysis
3. Gap analysis
4. Solution analysis

According to this methodology, the preparatory stage involves forming a working group in line with the subject of assessment. The requirement analysis stage focuses on identifying capability requirements, taking into account task specifics, conditions, assessment indicators, standards, and so forth. These two stages shall be considered completed, resulting in a defined set of capabilities required by the AF of Ukraine for conducting confrontation in cyberspace [12]. Accordingly, based on the implementation of the third and fourth stages of this methodology within the research, an implementation model for defence planning measures to acquire and develop capabilities by the prospective Cyber Forces of the AF of Ukraine will be developed using the DOTMLPFI framework.

Capabilities reflect and serve as indicators of the ability of capability carriers to achieve the desired outcome (effect) in military operations (combat actions) of troops (Forces) [1]. The following represent the capabilities of typical capability carriers of the AF of Ukraine for conducting confrontation in cyberspace (cyber defence) [11]:

the ability to conduct information measures for state defence;

creation of a cyber defence system for conducting confrontation in the information domain (including cyberspace);

the ability to ensure effective cyber protection of national information infrastructure (critical information infrastructure), conduct preventive actions to detect and respond to cyberattacks and cybersecurity incidents, eliminate their consequences under conditions of enemy cyber reconnaissance and intensive cyber influence (cyberattacks);

the ability to conduct cyber reconnaissance and cyber surveillance in information and telecommunication networks and systems of state, private, and military purpose (critical infrastructure targets) of the adversary, in order to obtain information about the adversary's cyber infrastructure, its function, location, technological processes, vulnerabilities, establish covert control, intercept and decrypt command and resource-related data and information;

the ability to prepare and carry out coordinated demonstrative cyber actions (cyber influence) in cyberspace to prevent the outbreak of armed conflicts, and to deter and repel military aggression in cyberspace;

the ability to organise training and conduct cyber actions (cyber influence, cyberattacks) using all types of cyber weapons, including seizure (disruption, takeover), infliction of damage (cascade effect), disruption of functioning of the adversary's critical and information infrastructure, while simultaneously concealing one's activity in cyberspace;

employment of cyber security hardware and software systems, cyber defence tools, and cyber weapons to fulfil cyber warfare tasks.

The process of acquiring and developing the listed capabilities by the prospective Cyber Forces of the AF of Ukraine may potentially lead to additional expenditures from the state budget. Therefore, when justifying the rationality of implementing particular defence planning measures in this area, it is proposed to use the return on investment indicator, known in English-language literature as ROI (*Return on Investment*). The $P_{ROI}$ indicator operates with the value of potential financial loss caused by adversary actions in cyberspace and the funds spent on cyber defence:

$$P_{ROI} = \frac{P_{loss} - P_{cost}}{P_{loss}}, \quad (1)$$

where, $P_{loss}$ – potential financial loss, UAH;

$P_{cost}$ – funds spent on cyber defence, UAH;

$0 < P_{cost} < P_{loss}$;

$0 \leq P_{ROI} \leq 1$.

That is, spending one million hryvnias on cyber defence, which protects cyber infrastructure from adversary's destructive actions that could potentially result in a financial loss of ten million hryvnias, would yield a $P_{ROI} = 0{,}9$ value. Based on the numerical value of the $P_{ROI}$, indicator, and knowing the criterion for rationality in implementing cyber defence measures, it is possible to assess the appropriateness of such measures. However, the justification of this rationality criterion constitutes a separate area of research.

**Results and Discussions**

The situation described above demonstrates the necessity of and confirms the course set out in the Cybersecurity Strategy of Ukraine for the establishment of Cyber Forces as a separate branch of troops (Forces) within the AF of Ukraine, enabling them to acquire the capabilities required to fulfil their assigned task of preparing for and conducting state cyber defence. In order to effectively carry out this task, the Cyber Forces of the AF of Ukraine, once (or if) established, must acquire the previously outlined capabilities for conducting confrontation in cyberspace.

The situation described above proves the necessity of and confirms the course declared in the Cybersecurity Strategy of Ukraine for establishing Cyber Forces as a separate branch of troops (Forces) within the AF of Ukraine, which would enable them to acquire the capabilities required to fulfil their assigned task of preparing for and conducting state cyber defence. In order to effectively perform this task, the Cyber Forces of the AF of Ukraine, once (or if) established, must acquire the previously outlined capabilities for conducting confrontation in cyberspace.

Taking into account that the first two stages of the selected capability assessment methodology [19] have been implemented directly in the form of a list of capabilities, the implementation model for defence planning measures to acquire and develop capabilities by the prospective Cyber Forces of the AF of Ukraine will be developed as the result of completing the stages of capability gap analysis and solution analysis. The implementation of these stages of the capability assessment methodology is proposed to be carried out for each of the eight fundamental components of DOTMLPFI. For this purpose, each of the eight fundamental components of the AF of Ukraine's capabilities for conducting confrontation in cyberspace will be described using the following structure:

the potential that can be achieved through the implementation of acquired capabilities;

the current state (problem) of capabilities;

measures to address the problem, which will allow the potential of capabilities to be achieved.

The structure of the implementation model for defence planning measures to acquire and develop capabilities by the prospective Cyber Forces of the AF of Ukraine may be conventionally presented as shown in Fig. 1 (for each fundamental DOTMLPFI capability component).

Proceeding to the direct presentation of the core content of the implementation model for defence planning measures to acquire and develop capabilities by the prospective Cyber Forces of the AF of Ukraine for conducting confrontation in cyberspace, it should be noted that this model is not a dogma, postulate, or directive for action. The aim of developing this model is to identify problem areas that require development and propose indicative measures in these areas that may be useful for achieving the potential of acquiring the specified capabilities.

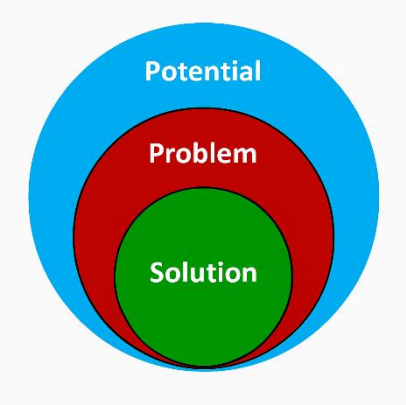



**Figure 1.** Structure of the implementation model for defence planning measures for each fundamental DOTMLPFI capability component

**Doctrinal foundation (D).** Ukraine's legislation and the doctrinal framework of the AF of Ukraine in the field of cybersecurity, cyber defence, and the conduct of military operations in cyberspace require further development (refinement) in the direction of unifying, systematising, and hierarchising the terminology, which is currently shaped by a range of legal acts and sectoral guidance documents. For today, the boundaries for the use of cyberspace for military purposes have not been clearly defined.

The definition of cyberspace provided in the Law of Ukraine [10] characterises it in a civilian context, without offering legal grounds to regard cyberspace as an operational environment. Cyber defence, for which the MoD of Ukraine and the General Staff of the AF of Ukraine are responsible in terms of preparation and execution, involves not only military but also economic, political, legal, social, and other measures. However, the mechanisms and algorithms for implementing the latter remain unclear. The doctrinal framework does not establish a link between cyber defence and cyber confrontation, despite recent studies on the relevant terminology [20] substantiating the need to introduce a clear relationship between these two concepts. Additionally, terms such as "cyber actions" and "actions in cyberspace" exist at the same level within the terminology system, although in practice they refer to the same concept. In other words, the doctrinal base contains a degree of duplication and substitution of terms.

The potential of improving and regulating the doctrinal framework lies in the ability to unambiguously interpret, describe, and classify actions in cyberspace and, as a result, to assess their effectiveness. Accordingly, the effectiveness of task execution by the prospective Cyber Forces of the AF of Ukraine, if established, will become one of the main criteria for evaluating the feasibility of this branch of troops (Forces). Without unifying the terminology in the fields of cyber defence, cybersecurity, and cyber confrontation, it is more than likely that there will be difficulties in clearly defining the tasks, authorities, and areas of responsibility within the Cyber Forces of the AF of Ukraine.

A possible solution to the problem of the doctrinal framework for realising the potential of acquiring capabilities for conducting confrontation in cyberspace by the prospective Cyber Forces of the AF of Ukraine is to carry out joint comprehensive research involving representatives from military, technical, and legal fields, at least within the scope of a research project. Such research should reformat Ukraine's doctrinal base in the part related to conducting confrontation in cyberspace and ensure clarity and unambiguity in the distribution of responsibilities among the components of the Security and Defence Sector of Ukraine regarding the provision of state cybersecurity.

**Organisation (O).** At present, the structure of the MoD of Ukraine includes military command bodies and military formations that perform assigned tasks related to Ukraine's cyber defence.

Specifically, these are the Main Directorate of Electronic and Cyber Warfare of the General Staff of the AF of Ukraine, the Main Directorate of Communications and Cybersecurity of the General Staff of the AF of Ukraine, and the AF of Ukraine's Communications and Cybersecurity Troops. The problem lies in the absence of a clearly defined division of tasks and responsibilities among these actors involved in ensuring state cyber defence, which creates uncertainty regarding accountability in this area of activity within the AF of Ukraine.

The potential of establishing the Cyber Forces of the AF of Ukraine as a separate branch of troops(Forces), tasked with carrying out military measures for preparing and conducting state cyber defence, lies in eliminating overlapping responsibilities among organisational structures within the MoD of Ukraine in this area, building a hierarchical cyber defence management system, and enabling scalability.

The solution to the organisational problem of the AF of Ukraine's capabilities for conducting confrontation in cyberspace is unequivocal – the formation of Cyber Forces as a separate branch of troops(Forces) within the AF of Ukraine, entrusted with the authority to carry out military measures for preparing and conducting state cyber defence.

**Training (T).** Training is an integral part of the system for ensuring state cyber defence. At present, the training cycle for military cybersecurity specialists and their targeted employment within the MoD of Ukraine and the AF of Ukraine remains incomplete. The leading military higher education institution that trains officers at the tactical level in the field of information technology, including cybersecurity, is the Military Institute of Telecommunications and Information Technologies named after the Heroes of Kruty. However, a common phenomenon is the assignment of graduates, upon completion of their studies and acquisition of the relevant qualification, to positions in related military occupational specialties, for example, as platoon commanders in mechanised (tank) battalions or battalion staff officers. Training for non-commissioned cybersecurity personnel exists only in a very generalised form, as the majority of specialised positions are officer roles.

At the same time, despite NATO's experience in establishing cyber ranges for simulating and modelling military operations in cyberspace, and a significant body of research in the field of cybersecurity that substantiates the relevance of introducing such experience into the training system of the AF of Ukraine, the training of military cybersecurity specialists is currently not conducted using cyber ranges. The relevance of integrating cyber ranges into the training system for cybersecurity specialists of the AF of Ukraine is reinforced by the rapid increase in the number of information and communication systems within the military command bodies of the AF of Ukraine and the complexity of their technical organisation.

The potential of establishing a closed-loop system for training military cybersecurity specialists and ensuring their targeted employment in relevant AF of Ukraine units, such as the prospective Cyber Forces of the AF of Ukraine, lies in maintaining a consistent level of unit proficiency and cohesion for conducting confrontation in cyberspace, as well as their ability to carry out assigned tasks related to the preparation for and execution of state cyber defence.

Given the persistent uncertainty of cyberspace and the processes occurring within it, military cybersecurity specialists must be trained on the basis of a creative approach to task execution, flexibility, and the ability to adapt and alter the nature of their actions depending on the operational environment. Cyber specialists of the AF of Ukraine must have fluent command of the applied information technology stack and be able to use it in practice without significant reliance on technical literature. In military higher education institutions, academic programmes in cybersecurity-related specialisations must be regularly updated to reflect emerging forms and methods of cyber confrontation and the advancement of information technologies. Cooperation with NATO in the training process is also essential, and participation in joint cyber defence exercises, such as Locked Shields and others, is necessary.

**Materiel support (M).** The acquisition and development of capabilities for conducting confrontation in cyberspace directly depend on the adequacy and quality of materiel support.

Currently, the existing units within the MoD of Ukraine and the AF of Ukraine responsible for preparing and conducting cyber defence possess certain types of antivirus software for combating malicious code, as well as software and hardware systems for scanning computer networks to detect and neutralise adversary intrusions into information and communication systems. At the same time, the process of equipping the AF of Ukraine with cyber weapons is at the stage of defining their tactical and technical requirements.

The potential of creating sufficient, high-quality, and technologically advanced materiel support for acquiring and developing capabilities to conduct confrontation in cyberspace by the prospective Cyber Forces of the AF of Ukraine lies in the ability to develop proprietary technologies and software solutions for cyber defence and cyber influence, engage in cyber defence cooperation with partner states, and utilise artificial intelligence technologies for attack analysis and cyber intelligence.

If a decision is made to establish Cyber Forces within the MoD of Ukraine, it will be essential to equip this branch of troops(Forces) with the most advanced equipment available on the market. In addition, considering the frequent cases of adversary intrusion into the cyber infrastructure of Ukraine's critical information infrastructure, caused by the use of software produced by non-resident companies, it is necessary to scale up Ukraine's own developments in the field of cybersecurity. The creation of domestic, internal software (or software-hardware) tools for cyber defence and cyber influence will enable the independent execution of actions or operations in cyberspace. In this regard, and to gain an advantage over the adversary in cyberspace, attention must be paid—during both the development and procurement of cyber weapons—to those systems equipped with artificial intelligence algorithms (technologies) for automated detection of enemy cyber reconnaissance (cyberattacks) and vulnerabilities within one's own cyber infrastructure. Today, the use of artificial intelligence in cybersecurity is one of the most relevant trends.

An equally important aspect of materiel support is financial provision. Since military cybersecurity specialists must have full command of the entire spectrum of applied information technologies, this makes them highly competitive on the labour market, while their financial remuneration in the AF of Ukraine does not differ significantly from that of service members in other armed services(branches) of troops(Forces)..

**Leadership (L).** Leadership is a driving fundamental component of any capability. Under conditions where the results of confrontation in cyberspace are directly dependent on knowledge and mastery of applied information technologies and the ability to implement them, ensuring the principles of unity of command and effective leadership becomes a complex task. This challenge is further compounded by the fact that military cybersecurity specialists are trained in military higher education institutions with a clear technical focus, while insufficient attention is paid to the development of methodological and leadership qualities necessary for command roles.

The potential of improving the leadership component within the capabilities for conducting confrontation in cyberspace by the prospective Cyber Forces of the AF of Ukraine lies in increasing the cohesion of relevant units, fostering healthy competition among personnel for career advancement, and building an effective command system for military operations in cyberspace.

At the same time, operations in cyberspace, like conventional military operations, require a clear hierarchical command structure. Therefore, a leader within the prospective Cyber Forces of the AF of Ukraine must possess both knowledge and practical skills in applying information technologies for cyber defence, as well as strong leadership qualities – to lead by example, inspire the team, and encourage top performers. A leadership-based approach presumes career advancement for the best and most motivated.

**Personnel (P).** The specifics of training and targeted employment of military cybersecurity specialists were considered during the analysis of the fundamental capability component "Training

(T)". However, there are certain issues related to the patriotic mindset and motivation of personnel who serve as carriers of capabilities for conducting confrontation in cyberspace. Motivation and patriotic commitment are often interrelated aspects. At the same time, such issues are present not only within the cyber defence units of the MoD of Ukraine but also in other organisational structures.

The potential of equipping the prospective Cyber Forces of the AF of Ukraine with qualified, patriotic, and motivated personnel who meet the defined requirements for capabilities to conduct confrontation in cyberspace lies in preventing a personnel shortage within this branch of troops(Forces) and ensuring that units are capable of fulfilling their designated tasks through careful candidate selection.

To realise this potential, it is necessary to select candidates for service in the prospective Cyber Forces of the AF of Ukraine based on professional competence, to maintain continuous motivation of personnel, and to strengthen the patriotism of units by creating attractive service conditions and ensuring fairness in managerial decisions.

A separate area for improving the provision of qualified personnel is the involvement of civilian cybersecurity specialists—of whom there are many in Ukraine—during a special period or under martial law, to perform tasks related to Ukraine's cyber defence as an alternative to their mobilisation on general grounds into general military formations. An example of this is the CyberGuard programme in the United States, which enables IT experts from the private sector to work with military units.

**Military infrastructure (F).** The level of military infrastructure for conducting confrontation in cyberspace can be assessed based on the availability and condition of facilities, individual structures and associated communications, as well as land designated for ensuring the preparation and conduct of state cyber defence, their location, suitability for supporting daily functioning and training.

The potential of providing military infrastructure is revealed in the ability to adequately prepare units and military formations to carry out state cyber defence measures and in enhancing the effectiveness of cyber weapons with which they will be equipped.

At present, the AF of Ukraine lacks a network of cyber ranges, which complicates the training process for cybersecurity specialists. In addition, to enable the acquisition and development of capabilities by the prospective Cyber Forces of the AF of Ukraine, it is necessary to expand military infrastructure for their deployment and performance of designated measures, ensuring that it meets all technical requirements of this branch of troops(Forces). Such facilities must be compatible with the weaponry of the Cyber Forces.

Ukraine is already expanding state data centres for information protection, and backup server projects have been created to safeguard state data. However, a critical issue remains the heavy dependence on civilian infrastructure (commercial cloud services).

**Interoperability (I).** At present, the problem of interoperability lies in the decentralisation of responsibility for Ukraine's cyber defence among military command bodies. Different tasks and responsibilities for conducting confrontation in cyberspace are assigned to various organisational structures that are not subordinated to one another. Moreover, interoperability among the entities of Ukraine's National Cybersecurity System is limited; in addition to the MoD of Ukraine, this system includes the State Service of Special Communications and Information Protection of Ukraine, the Security Service of Ukraine, and several other agencies. A separate issue is achieving interoperability between the prospective Cyber Forces of the AF of Ukraine and NATO cyber defence units, given Ukraine's course toward joining the Alliance.

The potential of enhancing interoperability in conducting confrontation in cyberspace lies in enabling the AF of Ukraine to carry out joint, coordinated, effective, and result-oriented actions aimed at achieving tactical, operational, and strategic objectives of cyber defence.

To address the issue of interoperability, Ukraine must scale up the ongoing integration into NATO's cyber network, define clear tasks and limits of authority for the prospective Cyber Forces of

the AF of Ukraine in conducting confrontation in cyberspace, and establish effective mechanisms for interaction between this branch of troops(Forces) and other organisational structures of the MoD of Ukraine whose activities involve cybersecurity, cyber protection, and cyber defence.

To fully address and summarise this issue, the key points of the implementation model for defence planning measures aimed at acquiring and developing capabilities by the prospective Cyber Forces of the AF of Ukraine should be presented in the form of Table 1.

**Conclusion**

Thus, the article proposed recommendations for implementing defence planning measures to acquire and develop capabilities by the prospective Cyber Forces of the AF of Ukraine based on the DOTMLPFI framework. The developed model presents a description of each of the eight fundamental capability components of the AF of Ukraine for conducting confrontation in cyberspace, following the structure: the potential that can be achieved through the implementation of acquired capabilities; the current state (problem) of capabilities; and the measures to resolve the problem that will enable the potential to be realised. The implementation and adoption of this model will constitute a significant step towards strengthening Ukraine's national security, enabling effective preparation for and conduct of cyber defence, and countering aggression in the digital domain.

**Table 1.** Key provisions of the implementation model for defence planning measures

| | Potential | Problem | Solution |
|---|---|---|---|
| **D** | – clarity in the interpretation, description, classification, and evaluation of the effectiveness of actions in cyberspace;<br>– unified terminology in the fields of cyber defence, cybersecurity, and cyber confrontation;<br>– clear definition of tasks, authorities, and area of responsibility of the prospective Cyber Forces | – ambiguity in the terminology;<br>– duplication of terms and substitution of concepts within the system of legal acts and guidance documents;<br>– lack of clear distribution of tasks for preparing and conducting state cyber defence;<br>– absence of a unified military doctrine on cyber defence;<br>– low level of integration of cyber strategy into the overall concept of warfare | – reformatting the doctrinal framework in the part related to conducting confrontation in cyberspace to ensure clarity and unambiguity in the distribution of responsibilities among the components of the Security and Defence Sector of Ukraine regarding the provision of state cybersecurity |
| **O** | – elimination of overlapping responsibilities among organisational structures of the MoD of Ukraine in the field of cyber defence;<br>– establishment of a hierarchical cyber defence management system and the possibility of its scalability | – lack of clearly defined distribution of tasks and responsibilities among the entities responsible for state cyber defence;<br>– uncertainty in accountability for state cyber defence | – formation of the Cyber Forces of the AF of Ukraine as a separate branch of troops(Forces);<br>– aggregation by the Cyber Forces of all defined capabilities for conducting confrontation in cyberspace |
| **T** | – consistent level of proficiency and cohesion among units designated for conducting confrontation in cyberspace;<br>– capability to carry out assigned tasks for preparing and conducting state cyber defence | – incompleteness of the training cycle for military cybersecurity specialists and their targeted employment within the military education system | – high-quality training of military cybersecurity specialists based on a creative approach and adaptability;<br>– regular updating of academic programmes in cybersecurity-related specialisations in military higher education institutions; cooperation with NATO in the training process and joint exercises |

**Table 1 continued.** Key provisions of the implementation model for defence planning measures

| | | | |
|---|---|---|---|
| **M** | – possibility of developing proprietary technologies and software solutions for cyber defence and cyber influence;<br>– cooperation in the field of cyber defence with NATO partner states;<br>– use of artificial intelligence technologies for attack analysis and cyber reconnaissance | – the process of equipping the AF of Ukraine with cyber weapons is at the stage of defining their tactical and technical requirements | – equipping the prospective Cyber Forces of the AF of Ukraine with the most advanced equipment;<br>– scaling up Ukraine's own developments in the field of cybersecurity;<br>– use of artificial intelligence algorithms (technologies) for automated detection of adversary cyber reconnaissance (cyberattacks) and vulnerabilities in cyber infrastructure;<br>– adequate financial provision for military cybersecurity specialists |
| **L** | – increased cohesion among cyber defence units;<br>– healthy competition among personnel for career advancement in the field of cyber defence;<br>– establishment of an effective command system for military operations in cyberspace | – difficulty in ensuring the principles of unity of command and leadership in the domain of confrontation in cyberspace;<br>– predominantly technical focus in the training of military cybersecurity specialists;<br>– low level of methodological and leadership skills | – enhancement of leadership abilities among military cybersecurity specialists;<br>– career advancement for the best and most motivated personnel in cyber defence units;<br>– adoption of NATO leadership practices in cyber defence units |
| **F** | – possibility of proper preparation of units and military formations for carrying out state cyber defence measures;<br>– increased effectiveness in the use of cyber weapons | – absence of a cyber range system for simulating and modelling confrontation in cyberspace | – expansion of military infrastructure for deployment and execution of cyber defence measures;<br>– alignment of military infrastructure with the needs of the prospective Cyber Forces of the AF of Ukraine;<br>– compatibility of military infrastructure facilities with Cyber Forces weaponry |
| **I** | – enabling the AF of Ukraine to conduct joint, coordinated, effective, and result-oriented actions to achieve tactical, operational, and strategic objectives of cyber defence | – decentralisation of responsibility for Ukraine's cyber defence among military command bodies;<br>– low interoperability among the entities of Ukraine's National Cybersecurity System | – scaling up the ongoing integration into NATO's cyber network;<br>– defining clear tasks and authorities for conducting confrontation in cyberspace;<br>– establishing effective mechanisms of interaction with other MoD of Ukraine structures involved in cybersecurity, cyber protection, and cyber defence;<br>– interoperability with cyber defence units of NATO member states |

## References

1. Deniezhkin, M. M., Nalyvaiko, A. D., & Polyayev, A. I. (2017). Features of Defense Planning in NATO Member States Based on Capabilities. *Collection of Scientific Papers of the Center for Military-Strategic Studies, National Defense University of Ukraine, 2* (60), 34–38. https://doi.org/10.33099/2304-2745/2017-2-60/34-38.
2. Nalyvaiko, A. D., Polyayev, A. I., & Nalyvaiko, L. P. (2019). Theoretical Foundations of Building a Functional Model of the Defense Planning Process for Defense Forces. *Collection*

*of Scientific Papers of the Center for Military-Strategic Studies, National Defense University of Ukraine, 2* (66), 35–41. https://doi.org/10.33099/2304-2745/2019-2-66/35-41.

3. Nalyvaiko, A. D., & Polyayev, A. I. (2021). Approaches to Developing a Functional Defense Management Model. *Social Development and Security, 11* (3), 20–29. https://doi.org/10.33445/sds.2021.11.3.2.
4. Pavlikovsky, A., Frolov, V., & Saghanyuk, F. (2020). *Defense Reform: A Systematic Approach to Defense Management.* (Edited by A. Syrotenko). National University of Defense of Ukraine.
5. Valtonen, I., Rautio, S., & Salmi, M. (2022). Capability Development in Hybrid Organizations: Enhancing Military Logistics with Additive Manufacturing. *Progress in Additive Manufacturing. 7*, 1037–1052. https://doi.org/10.1007/s40964-022-00280-z.
6. Korendovych, V. S., & Chirikalov, O. S. (2020). The Problem of Decentralization of Command and Control in Hybrid Warfare. *Development of Theory and Methodology, 3* (12), 32–40. https://doi.org/10.33099/2618-1614-2020-12-3-32-40.
7. Shchipansky, P. V., Saghanyuk, F. V., & Mudrak Y. M. (2021). Defense Management: Approaches to Managing the Defense Planning Process. *Collection of Scientific Papers of the Center for Military-Strategic Studies, National Defense University of Ukraine*, *1* (71), 52–58. https://doi.org/10.33099/2304-2745/2021-1-71/52-58.
8. Nalyvaiko, A. D. (2024). Justification of Directions for Improving Strategic Planning in the Defense Sector. *Collection of Scientific Papers of the Center for Military-Strategic Studies, National Defense University of Ukraine*, *1* (80), 27–33. https://doi.org/10.33099/2304-2745/2024-1-80/27-33.
9. Lutsyk, Y. O., Parkhomenko P. P., Demeniev O. M., & Alimov D. I. (2023). Analysis of the Defense Planning System Based on Capabilities, Considering the Leading Experience of NATO Member States. *Modern Economics*, *41*, 73–78. https://doi.org/10.31521/modecon.V41(2023)-11.
10. Law of Ukraine *"On the Basic Principles of Cybersecurity Provision in Ukraine"* No. 2163-VIII (2017, 05 Aug. 10): as of June 28, 2024. https://zakon.rada.gov.ua/laws/show/2163-19
11. President of Ukraine. (2021). *On the Decision of the National Security and Defense Council of Ukraine of August 20, 2021 "On the Strategic Defense Bulletin of Ukraine"* (473/2021). https://zakon.rada.gov.ua/laws/show/473/2021#Text
12. President of Ukraine. (2021). *On the Decision of the National Security and Defense Council of Ukraine of May 14, 2021, "On the Cybersecurity Strategy of Ukraine"* (447/2021). https://zakon.rada.gov.ua/laws/show/447/2021#Text
13. *Draft Law on Cyber Forces of the Armed Forces of Ukraine.* https://itd.rada.gov.ua/billinfo/Bills/Card/45453
14. Horhulenko, V. A. (2024). Cyber Warfare in Modern Conflicts: Advanced Experience, Trends, and Development Patterns. *Modern Information Technologies in Security and Defense*, *2* (50), 11–28. https://doi.org/10.33099/2311-7249/2024-50-2-11-28.
15. Krykun, P., Pavlenko, V., Korendovych, V., Yasenko, S., & Tkach, M. (2024). Development of the National Defense Planning System of Ukraine Based on Euro-Atlantic Principles: Military-Historical Analysis. *Social Development and Security*, *14* (3), 14–32. https://doi.org/10.33445/sds.2024.14.3.2.
16. Fediienko, O. P. (2024). Modern Trends in Normative Support for Institutional Formation of Cyber Forces (Cyber Troops): The Experience of Some NATO Countries. *Information and Law*, *1* (48), 150–161. https://doi.org/10.37750/2616-6798.2024.1(48).300800.
17. Nagy, J., Foltin, P., & Ondryhal, V. (2022). Use of Big Data Analysis to Identify Possible Sources of Supply Chain Disruption through the DOTMLPFI Method. *LogForum*, *18* (3), 309–319. http://doi.org/10.17270/J.LOG.2021.731.

18. Llopis Sanchez, S., Sandoval Rodriguez-Bermejo, D., Daton Medenou, R., Pasqual de Riquelme, R., Torelli, F., & Maestre Vidal, J. (2022). Tackling Verification and Validation Techniques to Evaluate Cyber Situational Awareness Capabilities. *Mathematics, 10*, 2617. https://doi.org/10.3390/math10152617.
19. Tkach, M. Y., & Korendovych, S. A. (2024). *Basics of Defense Management*. National University of Defense of Ukraine.
20. Horhulenko, V. A. (2024). Military-Theoretical Justification of Recommendations for the Development of Terminological Apparatus in the Field of Cyber Warfare. *Modern Information Technologies in Security and Defense, 3* (51). https://doi.org/10.33099/2311-7249/2024-51-3-41-50.

## Рекомендації щодо реалізації заходів оборонного планування для набуття й розвитку спроможностей перспективними Кіберсилами Збройних Сил України на основі DOTMLPFI

**Володимир Горбатюк**
заступник начальника Генерального штабу Збройних Сил України
Генеральний штаб Збройних Сил України
03168, проспект Повітряних Сил, 6, Київ, Україна
e-mail: gorbvol@yahoo.com
ORCID: 0009-0009-9566-3168

**Владислав Горгуленко**
ад'юнкт науково-організаційного відділу
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: vladyslavhorhulenko@gmail.com
ORCID: 0000-0001-6382-5075

**Валерія Горгуленко**
молодший науковий співробітник
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: horhulenkovaleriia@gmail.com
ORCID: 0009-0009-1394-6325

**Юзеф Добровольський**
кандидат технічних наук, доцент
заступник начальника кафедри військової підготовки
з навчальної роботи – начальник навчальної частини
Національний авіаційний університет
03048, вулиця Медова 1, Київ, Україна
e-mail: kataza@i.ua
ORCID: 0000-0002-1077-1402

**Максим Самсоненко**
викладач кафедри військового управління
Інституту державного військового управління
Національного університету оборони України
Національний університет оборони України
03049, проспект Повітряних Сил, 28, м. Київ, Україна
e-mail: samson8115@ukr.net
ORCID: 0009-0001-6264-6582

**Анотація.** Сьогодні розвиток Міністерства оборони України та її Збройних Сил зокрема здійснюється на основі необхідних для набуття спроможностей, з орієнтуванням на існуючі та потенційні загрози національній і воєнній безпеці держави. Досвід збройного протистояння останнього десятиліття показав, що однією з таких загроз є агресія противника у кіберпросторі. Тому наразі існують достатні підстави для формування Кіберсил як окремого роду військ (сил) Збройних Сил України, завданням якого має стати підготовка та ведення військових заходів з кібероборони. Ефективне виконання покладеного завдання є можливим у разі набуття перспективними Кіберсилами Збройних Сил України визначених у Стратегічному оборонному бюлетені необхідних спроможностей з ведення протиборства у кіберпросторі.

Під час проведення дослідження було використано методи системного аналізу, узагальнення та систематизації, які за сукупністю дозволили розробити модель реалізації заходів оборонного планування для набуття й розвитку спроможностей перспективними Кіберсилами Збройних Сил України на основі DOTMLPFI.

Метою цієї статті є розроблення моделі впровадження заходів оперативної безпеки для формування та розвитку потенціалу перспективних Кіберсил Збройних Сил України, використовуючи DOTMLPFI – передовий підхід, що застосовується в країнах-членах НАТО.

Розроблена модель являє собою опис спроможностей щодо ведення протиборства у кіберпросторі за кожним із восьми базових компонентів DOTMLPFI у формі: потенціал, якого можна досягнути, реалізувавши набуті спроможності; існуючий стан (проблема) спроможностей; можливі заходи для вирішення проблеми, які дозволять досягнути потенціалу спроможностей. Отже, модель реалізації заходів оборонного планування для набуття й розвитку спроможностей перспективними Кіберсилами Збройних Сил України охоплює такі компоненти спроможностей з ведення протиборства у кіберпросторі як: доктринальна база (D), організація (O), підготовка (T), ресурсне забезпечення (M), управління та лідерство (L), персонал (P), інфраструктура (F), взаємосумісність (I).

Практична значимість результатів дослідження розкривається у потенціалі набуття Збройними Силами України спроможностей з ведення протиборства у кіберпросторі шляхом впровадження запропонованої моделі реалізації заходів оборонного планування на основі DOTMLPFI.

**Ключові слова:** кібероборона, кіберпростір, кібербезпека, кіберборотьба, Кіберсили, оборонне планування, спроможності, DOTMLPFI.

The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 3 No. 2 (2025)

DOI: 10.62524/msj.2025.3.2.11

# Situational conditions at the state border as a factor influencing the staffing of border guard units' headquarters with managerial personnel

**Olena Kushnir**
Doctor of Philosophy in State Border Security,
Senior Lecturer at the General Military Disciplines Department
Bohdan Khmelnytskyi National Academy
of the State Border Guard Service of Ukraine
29000, Shevchenka St, 46, Khmelnytskyi, Ukraine
e-mail:lena.kysh@ukr.net
ORCID 0000-0001-6445-5248

**Liliia Semenenko**
Senior lecturer
The National University of Defence of Ukraine
03049, Povitrianykh Syl Ave, 28, Kyiv, Ukraine
e-mail: selin-ua@ukr.net
ORCID: 0000-0002-5628-3586

**Abstract.** Modern challenges in the state border protection (SBP) require improved approaches to staffing the headquarters of border guard units with management personnel.

Managerial activities have a pronounced intellectual component, as they involve the development, adoption and implementation of managerial decisions in a changing situation. This requires a high level of adaptability and flexibility, as solutions must be effective and capable of changing the course of operations or battles, as well as influencing the mindset and behaviour of troops or forces in the course of performing tasks.

The article deals with the specifics of managerial activities in the units of the State Border Guard Service of Ukraine (SBGS) in the context of modern hybrid warfare.

The purpose of this article is to analyze how situational conditions at the state border affect the staffing of managerial personnel in border guard unit headquarters.

The authors pay special attention to the asymmetry of the actions of the russian federation, which is actively using new methods of warfare, in particular the use of strategic and tactical incommensurability between goals and resources, which in turn creates new challenges for border guard units.

Taking this context into account has led to the need to analyse the graphical cause-and-effect relationships of the risks associated with changes in the situation in the border area and to identify the types of tasks that need to be implemented to effectively counter threats. An important aspect is also the definition of criteria for assessing the operational efficiency of border guard unit headquarters, which should take into account the specific conditions of the situation.

It is concluded that the organisation of service in border guard units occurs under conditions of constant change and uncertainty. This requires appropriate, specific decisions to be made, which must be implemented in light of the current situation.

The managerial capacity of the border guard units' headquarters should be focused on a prompt and flexible response to changes in the situation. To achieve this, the headquarters' capability to make quick, accurate decisions in critical situations must be ensured.

The assessment of headquarters performance should take into account the ability of personnel to analyse the conditions of service, clearly define the necessary tasks, and properly allocate available resources. This includes not only professionalism but also the ability to work under conditions of high uncertainty and limited time.

The asymmetric actions used by russia require the search for innovative approaches to the organisation of managerial processes that enable not only to counter traditional threats but also to respond effectively to various forms of aggression.

The procedure for selecting candidates for senior positions in the headquarters of border guard units should include specific criteria that determine the ability of applicants to analyse and make effective decisions in a changing situation. This should include an assessment of their operational thinking, their ability to manage crises and their ability to effectively organise interaction with other units.

The article provides a practical framework for assessing how situational conditions at the state border directly impact the staffing needs of border guard headquarters. Its findings can be used to optimize personnel management decisions and improve the operational readiness of border units.

**Keywords:** border guard unit, situational conditions, risks, threats, tasks for units, staffing, selection of candidates for senior headquarters positions.

**Introduction**

Russia's armed aggression against Ukraine with the support of belarus began on 24 February 2022 and became a new stage in the russian-Ukrainian war. The full-scale invasion was made possible by a significant build-up of russian troops along the border with Ukraine and in the occupied territories, which had been ongoing since November 2021.

The aggression of russia, supported by belarus, included not only ground attacks, but also missile and air strikes. At the same time, all attempts by russian officials to deny their aggressive intentions were aimed at disorienting and reducing Ukraine's defence readiness.

The military resistance organised by the Ukrainian defence forces from the first day of the invasion caused the russian army to suffer significant losses. It is already known that russia's losses in manpower and equipment are among the largest in recent history. This also demonstrates the effectiveness of new tactical approaches to defence, in which the State Border Guard Service of Ukraine has played a significant role.

The analysis of combat operations and the effectiveness of managerial decisions of border guard units in wartime conditions is important for further improvement of management activities and training of future managerial personnel to ensure national security.

**Analysis of recent research and publications.** A number of specialists and scholars studied the issues of assessment and selection of managerial personnel. Paying tribute to their scientific achievements, it should be noted that the studies do not fully take into account the specifics and peculiarities of the management activities of the border guard detachment headquarters under different conditions.

**The purpose of the article** is to substantiate the relationship between the situational conditions at the state border and the specifics of the decisions that should be made at the headquarters of a border guard unit. The research aims to substantiate the need to adapt the personnel policy in the Border Guard Service to current challenges and threats, which will help improve management efficiency and strengthen national security.

**Methodological Framework**

**Presentation of the main research material**

On 24 February 2022, a heroic period began for Ukraine, when our country's statehood entered into an unprecedented struggle against the aggression of the russian federation and its allies. This period is characterised by numerous heroic deeds that resulted from the determination and dedication of both military personnel and civilians who sacrificed their lives and health for Ukraine's independence. Despite the heavy losses suffered by both the army and the civilian population, the heroism of Ukrainians became a powerful factor that caused shock and confusion among the enemy. This situation was effectively used by the Ukrainian authorities to organise numerous military operations aimed at liberating the occupied territories.

From late February to early July 2022, Ukraine's military command was forced to make a number of decisions aimed at manoeuvrable defence. Military and border guard units quickly adapted to new challenges, using available resources and forces to effectively counter the occupiers.

Since the first days of the war, the State Border Guard Service of Ukraine (SBGS) has been implementing a set of measures to counter the invasion of the russian federation across Ukraine's state border. After submitting relevant information reports on the shelling of border crossing points and places of permanent deployment of border guard divisions and detachments, decisions were made to organise surveillance of the enemy's activities (directions of movement of convoys and their numbers, nature of actions, etc.), organise retreats to alternate positions, and set up fire ambushes and observation posts. The next stage was the decision to ‘merge’ the linear border guard units into units of the National Guard of Ukraine and the Armed Forces of Ukraine and to continue fulfilling the tasks assigned to the border guards by the military command of the defence forces. Separate mobilisation activities were carried out, resulting in the formation of rapid response border commands, combat border detachments (e.g. ‘Steel Border’), reserves of the Head of the SBGS, and other units that reinforced the regular SBGS units.

Nowadays, there are many facts of heroic deeds of border guards during their participation in the combined defence units, which contribute to the overall result of confronting the aggressor and liberating the territories from invaders.

It was the operations of the national defence forces, international military and technical assistance, as well as the activities of the civilian population and the volunteer movement that made it possible to liberate parts of the northern and eastern borders from the invaders and take control of the state border in those areas.

After the de-occupation of certain territories of Ukraine, the tasks performed by the SBGS units should be divided into two separate groups: direct participation in defensive and assault operations (warfare) and control of the state border in the de-occupied territories (operational and military activities).

As for the first group, its very name reveals its essence.

As for the second group, it is appropriate to reveal its essence more broadly. Given the enemy's criminal activities in the occupied territories, the use of prohibited means of warfare, and the negative attitude towards the local population and the Ukrainian nation as a whole, there are issues of secure implementation of tasks by border guard units in these territories. In these circumstances, the SBGS leadership faced the challenge of organising and implementing state border control tasks in the de-occupied territories. It is logical that it is impossible to carry out such tasks in everyday conditions or during an escalation of the situation as in peaceful sectors of the border. The enemy is constantly disturbing the border areas and intensively using unmanned aerial vehicles for aerial reconnaissance and means of remote fire strikes on manpower, equipment of the national defence forces and border infrastructure, using sabotage and reconnaissance groups with wide involvement of collaborators from the local population. In addition, during the withdrawal from our territory, the enemy widely used mines and explosives to counter Ukrainian advancing forces and create sabotage against the

civilian population, disrupt sowing works, destroy economic infrastructure, and damage logistics routes, etc.

These and other conditions revealed the need to search for new forms and methods of organising the protection (control) of the state border, using regular border units and forming temporary units with specific tasks to be implemented under the aforementioned conditions. As for the regular border guard units that were used to perform tasks of controlling the state border, they were provided with attached forces from rapid response border commands, which made it possible to increase the potential of the forces to counter the enemy's sabotage reconnaissance groups.

At the same time, the need for the formation and further use of joint special forces detachments (JSFDs) was identified. The main tasks of these units were local border tasks, which are not typical for regular units.

As for the JSFDs:

A JSFD should perform tasks using operational and military means in the de-occupied territories in conditions where the enemy, in various ways, opposes the access of regular border units to the state border line from its side;

It is advisable to form a JSFD from servicemen who have special training, experience in organising and implementing operational and service activities at the tactical level, and stable moral, psychological and physical indicators;

A JSFD should be equipped with appropriate weapons, technical means, vehicles that allow to perform tasks in a mobile and autonomous manner at any time of the year, at any sector of the land part of the border, time of day, and ensuring the reduction of the risk to the life and health of the detachment's servicemen;

A JSFD should provide the ability to perform tasks both as the entire unit and by small tactical groups;

The intensity of the deployment of JSFDs should be ensured by the necessary staffing of personnel.

The main tasks for the JSFD should be considered as follows:

1. Conducting reconnaissance and search activities;
2. Detecting possible enemy hiding places;
3. Conducting aerial reconnaissance of the border area, border line and enemy borders to a depth of 3-5 km;
4. Counteracting enemy UAVs;
5. Reconnaissance of the minefield situation;
6. Organising countermeasures against the enemy's sabotage reconnaissance groups;
7. Organising fire ambushes;
8. Organising watch posts;
9. Identifying possible places of service and routes of movement for border details from regular units to them;
10. Reconnaissance of the condition of border crossing points of regular units.
11. Protection and defence of convoys on the march;
12. Counteracting enemy convoys;
13. Implementation of operational information on the detention of border violators in areas liberated from enemy occupation;
14. Inspecting and reconnoitring border settlements (clearing);
15. Work with the local population, detention of persons;
16. Organisation and implementation of interaction with regular border guard units, the Armed Forces of Ukraine, the National Guard of Ukraine and other entities ensuring national security and protection of the areas of responsibility in the area of the JSFDs;

17. Organisation and implementation of joint operations with interacting units in the area of operations.

These and other tasks, which should be assigned to the SBGS units during military operations and in the context of organising the protection (control) of the state border in the de-occupied territories, can become an effective tool to counteract the enemy's asymmetric activities in the border areas of our country.

In general, the signs of asymmetric activities are difficult to understand, which leads to difficulties in the promptness and adequacy of countermeasures. Asymmetric activities involve the use of non-traditional, fundamentally new concepts using incommensurability (lack of correlation) between the goals of adversaries or between the resources spent and the effect obtained.

The asymmetry of the enemy's activities justifies the need to find adequate countermeasures to be implemented across all spheres of Ukraine's national security (including border security).

As for the border sphere of national security, asymmetric activities can manifest both in everyday conditions and during the escalation of the situation, military operations, and the organisation of the protection (control) and defence of the state border in the de-occupied territories. Based on the above, to illustrate the essence of the issue under consideration, it is necessary to reproduce the cause-and-effect graphical relationship of the risks associated with changes in the situation in the border area and the scope and types of tasks that need to be performed to counteract them (threats) (see Fig. 1).

The ordinate axis represents the levels of escalation (conditions) of the situation (DC, AS, and MO). The organisation of state border (SB) protection and defence in the de-occupied territories can also be attributed to the level of MO, considering the peculiarities of the service.

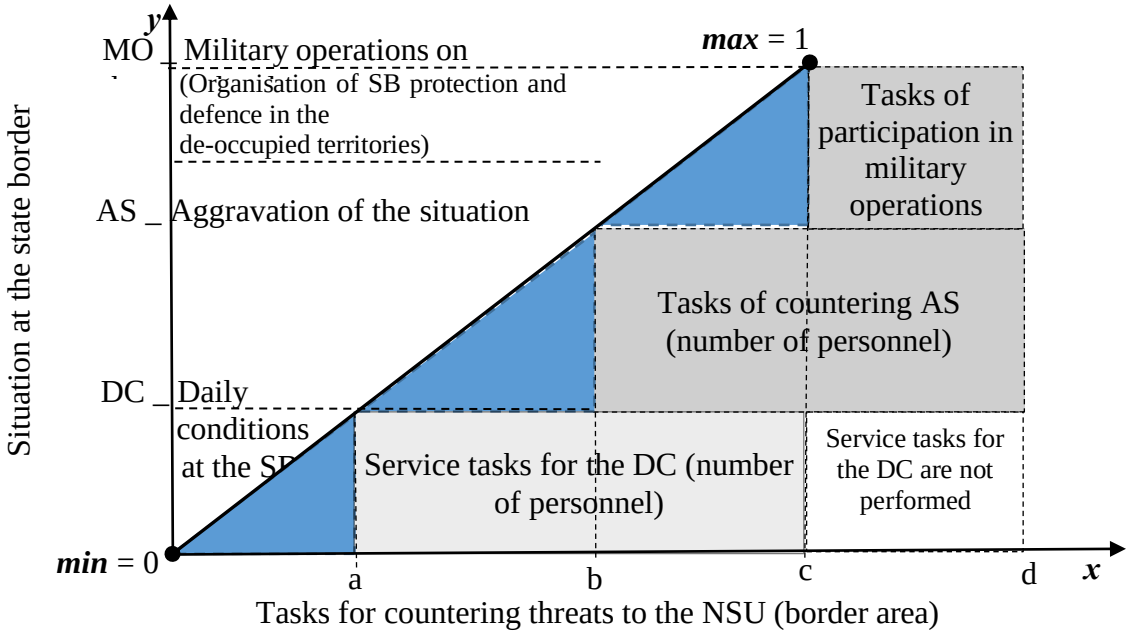



**Figure 1.** Graphical representation of the dependence of the substantive and quantitative characteristics of the tasks assigned to a BG body and the situational conditions at the state border

The transition from one level to another is carried out according to the senior officer's order based on the results of a risk analysis, which can be accepted as a normative requirement for subordinate units to organise and implement tasks that are carried out in these (normative) conditions of service. Of course, the transition from one regulatory state to another may have different functional dependencies, which should be investigated in the future. In our case, it is enough to state that there

is a regulatory requirement that allows the headquarters of a BG body to switch from one form of organisation of the protection and defence of the state border in the area of responsibility to another (which is projected accordingly on the number and specificity of tasks for line units and all personnel of the BG body). In Fig. 1, the following options are shown graphically. For example, the abscissa axis represents the points ‘a - c’. At point ‘b’, the normative transition of the BG body from ‘DC’ to ‘AS’ takes place. At the same time, the protection of the SB is implemented in ways both in the ‘DC’ and additionally personnel can be involved to perform specific tasks aimed at neutralising the threats that contributed to the introduction of the ‘AS’. That is, in this variant, a set of tasks similar to those in daily conditions is implemented, and additionally tasks aimed at neutralising threats that contribute to the aggravation of the situation.

At point ‘c’, upon receipt of a normative instruction from the headquarters of a BG body, the line units switch to performing tasks under ‘MO’ conditions. In this scenario, border guard units are transferred to the operational subordination of the Defence Forces and perform the relevant tasks in combat zones. In addition, a certain number of tasks are implemented by line units in ways that are also used to neutralise threats that led to the aggravation of the situation at the stage of transition to the ‘AS’ level. The tasks performed by the line units in the ‘DC’ during this period in the combat zone are not implemented (see Fig. 1).

It is worth noting that the graphically considered processes to achieve the research goal can be represented as a direct dependence between the critical values (point min = 0 [transparent borders and no border guard units] and point max = 1 [start of combat operations on the border]).

The area bounded by the system of lines: the abscissa axis; a straight line that passes through the ‘DC’ (y = ‘DC’) and x = ‘a’ and x = ‘b’ can be interpreted as the area whose output parameters are the list of tasks and the costs of their implementation (labour costs) during the ‘DC’ at the SB. Other areas can be defined in the same way. However, the above is also the subject of separate studies.

In order to determine the normative moments of transitions from one state of task performance organisation to another, it is advisable to use a proven methodology for determining the values of the risk indicator of the corresponding state [Instruction 2-4].

This Instruction defines the organisation of risk analysis in the State Border Guard Service in the field of state border security, taking into account the common integrated risk analysis model of the EU member states and national experience.

Risk analysis is a set of procedures and methods for processing information in order to identify existing and potential risks in the sphere of state border security. Risk analysis is an integral part of integrated border management: impact is the likely (predictable) consequences of the realisation of a threat or the occurrence of other phenomena and factors that do not pose a threat but may affect the sphere of the state border security;

A threat is an existing and potentially possible phenomenon or factor that negatively affects the sphere of state border security;

Risk indicator is a feature or a set of features with specified parameters, the use of which makes it possible to identify an object that poses a risk; vulnerability is a problem in the state border protection system that prevents this system from adequately counteracting threats.

Risk analysis is carried out by the structural units of the Administration of the State Border Guard Service, regional directorates, border guard bodies, maritime guard detachments and officials of border guard units whose competence includes the issues that are the subject of analysis.

Risk analysis in the State Border Guard Service is divided into:

1) according to the level of conduct: strategic; operational; tactical;

2) according to the purpose of conduct: periodic; thematic; situational.

Risk analysis is carried out in the following sequence:

Depending on the level of risk analysis, the following types of threats are identified:

local threats that are limited to the territory of one or two regions (separate areas of temporary

assignment);

regional threats that are limited to the areas of responsibility of one or two regional directorates;

national threats that affect the entire state border or its individual sections, which can lead to negative consequences;

global national threats that extend beyond the borders of Ukraine.

Threat assessment is carried out by analysts separately for each threat or group of identical threats.

At the initiative of analysts, officials of the State Border Guard Service whose competence includes the issues that are the subject of the threat assessment may be involved in the threat assessment with the consent of the relevant managers.

Based on the results of the threat assessment, external and internal factors that negatively affect (impact on) the state border security are identified (hereinafter - impact factors).

The determination of influence factors is based on a four-level system of control over the entry and stay of foreigners and stateless persons in Ukraine:

in the countries of origin of irregular migrants;

in the countries bordering Ukraine;

at border crossing points and beyond them (during border control and ensuring the protection of the state border beyond the border crossing points);

in Ukraine (compliance with the terms of temporary stay of foreigners and stateless persons in Ukraine).

Based on the results of the quantitative and qualitative characteristics, the following levels of threats are determined: low, moderate, and high.

Terrorist threat levels are determined in accordance with the Regulation on the Unified State System of Prevention, Response and Suppression of Terrorist Acts and Minimisation of Their Consequences, approved by Resolution of the Cabinet of Ministers of Ukraine No. 92 of 18 February 2016;

2) conducting a vulnerability assessment, during which:

problems in the state border protection system, their causes, as well as the capacity (capabilities) of the bodies and units of the State Border Guard Service to adequately counteract current and potential threats in the sphere of state border security are identified.

Vulnerability assessments are carried out on the components of the state border protection system, as well as on the factors that attract threats.

The determination of the capabilities (capacities) of the SBGS bodies and units is carried out by the structural units of the SBGS bodies and officials of the border guard units within their competence, separately for each threat or group of identical threats.

Assessment of factors that attract threats involves determining the existing internal and external factors in the sphere of state border security that influence the increase in the level of threat.

The results of the vulnerability assessment are provided to analysts for summarisation within the timeframe established for the specific risk analysis.

Based on the results of the vulnerability assessment for each of the identified threats, the following vulnerability levels are determined: low, moderate, and high.

The result description of the vulnerability assessment is followed by the conclusion on the capabilities of the state border protection system to adequately counteract threats;

3) conducting an impact assessment, during which:

the consequences of the state border security threat are determined, including the consequences that affect the crossing of the state border by persons, vehicles and cargo, the procedure for organising the service of border details, etc.

An impact assessment is a study of the aggregate of estimates of immediate impacts, impacts that may increase over time, and individual events that are not significant but that, in aggregate, may reach a level that could have negative consequences.

Based on the results of the impact assessment for each of the identified threats or other phenomena and factors that do not pose a threat but may affect the security of the state border, the following levels of impact are determined: low, moderate, and high;

4) determining risk levels.

The risk level is defined as a function of threat, vulnerability and exposure.

The risk level is determined by analysts using qualitative and quantitative assessments of the threshold value of the established risk levels.

Depending on the results of the risk analysis, the following risk levels are set:

low - for insignificant levels of threat, vulnerability and impact;

moderate - for a low or moderate level of impact, when the level of threat exceeds the level of vulnerability;

acceptable - for a low or moderate level of impact, when the level of vulnerability corresponds to the level of threat;

high - for a moderate or high level of impact, when the level of vulnerability exceeds the level of threat;

critical - for high levels of threat, vulnerability and impact.

In other cases, risk levels are set depending on the quantitative and qualitative characteristics of the threat, vulnerability and impact.

In order to conduct risk analysis, the State Border Guard Service applies the risk analysis methods used in the Common Integrated Risk Analysis Model (CIRAM). The selection of the appropriate risk analysis method (or combination of methods) depends on the specific risk.

The organisation of the application of these methods is entrusted to the Administration of the State Border Guard Service.

The sources of information on risk analysis are the data received by the SBGS Administration, regional directorates and border guard bodies in the course of operational activities, and from international organisations, border guard and other authorised bodies of foreign countries, in accordance with international agreements, mass media, including the Internet, and other sources, as well as the results of strategic criminal analysis and own analytical developments.

If it is necessary to use information (data) of an intelligence, operational and investigative nature during the risk analysis, the risk analysis is carried out with the involvement of the relevant officials of the structural unit of the border guard body.

**Results**

Based on the above material (see Fig. 1), it became possible to analyse the impact of different situational conditions on the content and scope of tasks to be performed by border guard units, which requires appropriate decisions to be made by the headquarters of the border guard units. The above substantiates the need to consider the issue of qualitative staffing for managerial positions in the relevant units of the Border Guard Service, and the search for new parameters and an integral indicator to assess the ability of applicants to hold relevant managerial positions in the headquarters of a BG body.

**Conclusions**

Thus, from the material presented, it can be concluded that the organisation of service in border guard units takes place in different conditions, which reveals the need to implement appropriate tasks specific to the situation with the involvement of adequate forces and facilities, which in turn requires direct consideration of this fact when forming a headquarters that is potentially capable of making

these decisions. The selection procedure should take this fact into account and use appropriate indicators and criteria for evaluating applicants in terms of their ability to analyse the conditions of service, clearly define the required list of tasks, allocate the available forces and facilities of a BG body, etc. with due regard to ensuring the required values of the parameters for assessing the quality of functioning of the headquarters of a BG body.

It is necessary to further develop practical recommendations for the assessment and selection of managerial personnel, maintaining the required level of their professionally important qualities for managerial activities. To develop a toolkit that will make it possible to assess the psychological and professional suitability of applicants for managerial positions with further assessment of the quality of the decision and the time spent on decision-making, which, when used in conjunction with the developed operational apparatus, will make it possible to determine the relevance of the decision and, as a result, to build a rating of applicants for managerial positions in the headquarters of a BG body.

These results will be a certain guarantee of confidence in the professional capability of the headquarters of a BG body to make decisions in any situation, which is an integral part of ensuring the specified efficiency of accomplishing the tasks of operational and service activities (operational and service tasks) by border guard units.

**References**

1. Possible areas of application of the special purpose unit during the war. (2022). *Nauka pid chas viiny : chasopys*, pp. 100–106. URL: https://nadpsu.edu.ua/naukova-diyalnist/naukovi-napryamy/.
2. Instructions for carrying out risk analysis in the State Border Service of Ukraine. (2017). *Nakaz Ministerstva vnutrishnikh sprav Ukrainy vid 11 hrudn, 1007*. URL: https://zakon.rada.gov.ua/laws/show/z0091-18#Text.
3. Skazhynska, K. & Navrotski, D. (2015). Guide to risk analysis based on the Ciram 2.0 model for analysts of the State Border Service of Ukraine, 133. URL : http:// www.frontex.europa.eu.
4. General integrated model of risk analysis. (2012). *Yevropeiske ahentstvo z upravlinnia operatyvnym spivrobitnytstvom na zovnishnikh kordonakh Derzhav-Chleniv Yevropeiskoho Soiuzu (Frontex)*, pp. 100-124. URL : http:// www.frontex.europa.eu).
5. Advisor on the organization of management bodies of the State Border Service of Ukraine in crisis situations of a military nature. (2019). *Nakaz Administratsii Derzhavnoi prykordonnoi sluzhby Ukrainy vid 07 veresn. 2019 r. no. 37t. Kyiv*, pp. 9–147.
6. Kushnir, O. M., Litvin, L. Y., & Kyrylenko, V. A. (2022). Justification of the structural and logical scheme of the method of selection of managerial personnel for the formation of the headquarters of the state border protection body. *Zbirnyk naukovykh prats Natsionalnoi akademii Derzhavnoi prykordonnoi sluzhby Ukrainy, 1-2*(87), pp. 73–84.
7. Kushnir, O. M. & Kyrylenko, V. A. (2023). Substantiating the influence of situational conditions at the state border and the specific tasks on the content of decision quality assessment by the headquarters of border guard units. *Zbirnyk naukovykh prats Natsionalnoi akademii Derzhavnoi prykordonnoi sluzhby Ukrainy, 1*(90), pp. 53–61.

The Central Research institute
of the Armed Forces of Ukraine
Military Science. Vol. 3 No. 2 (2025)

# Ситуаційні умови на державному кордоні як фактор впливу на укомплектування управлінського складу штабів прикордонних підрозділів

**Олена Кушнір**
доктор філософії з безпеки державного кордону,
викладач кафедри загальновійськових дисциплін
Національна академія Державної прикордонної служби України
імені Богдана Хмельницького
м. Хмельницький, Україна
e-mail: lena.kysh@ukr.net
ORCID 0000-0001-6445-5248

**Лілія Семененко**
старший викладач кафедри іноземних мов
Національний університет оборони України
03049, проспект Повітряних Сил, 28, Київ, Україна
e-mail: selin-ua@ukr.net
ORCID: 0000-0002-5628-3586

**Анотація.** Актуальність статті полягає у тому, що сучасні виклики в охороні державного кордону (ОПД) вимагають удосконалення підходів до комплектування керівного складу штабів підрозділів охорони державного кордону.

Управлінська діяльність має яскраво виражену інтелектуальну складову, оскільки передбачає розробку, прийняття та реалізацію управлінських рішень в умовах зміни ситуації. Це потребує високого рівня адаптивності та гнучкості, оскільки рішення мають бути ефективними та здатними змінювати хід операцій чи боїв, а також впливати на мислення та поведінку військ чи сил під час виконання завдань.

У статті розглядається специфіка управлінської діяльності підрозділів Державної прикордонної служби України (ДПСУ) в умовах сучасної гібридної війни.

Метою цієї статті є аналіз того, як ситуаційні умови на державному кордоні впливають на укомплектованість керівним складом штабів підрозділів прикордонної служби.

Автори звертають особливу увагу на асиметричність дій російської федерації, яка активно застосовує нові методи ведення війни, зокрема використання стратегічної і тактичної неспівмірності цілей і ресурсів, що в свою чергу створює нові виклики для підрозділів охорони кордону.

Врахування цього контексту призвело до необхідності аналізу графічних причиново-наслідкових зв'язків ризиків, пов'язаних зі зміною ситуації в прикордонній зоні, та визначення типів завдань, які необхідно виконувати для ефективної протидії загрозам. Важливим аспектом є також визначення критеріїв оцінки ефективності діяльності штабів прикордонних підрозділів, які повинні враховувати конкретні умови обстановки.

Зроблено висновок, що організація служби в підрозділах охорони кордону відбувається в умовах постійних змін і невизначеності. Для цього потрібні відповідні, конкретні рішення, які мають бути реалізовані з урахуванням поточної ситуації.

Управлінський потенціал штабів прикордонних підрозділів має бути спрямований на оперативне та гнучке реагування на зміни обстановки. Для досягнення цього необхідно забезпечити здатність штабу приймати швидкі та точні рішення в критичних ситуаціях.

Оцінка діяльності штабу повинна враховувати здатність особового складу аналізувати умови служби, чітко визначати необхідні завдання та правильно розподіляти наявні ресурси.

Це не тільки професіоналізм, але й здатність працювати в умовах високої невизначеності та обмеженого часу.

Асиметричні дії, які використовує росія, вимагають пошуку інноваційних підходів до організації управлінських процесів, які дозволяють не тільки протистояти традиційним загрозам, але й ефективно реагувати на різноманітні форми агресії.

Порядок відбору кандидатів на керівні посади в штабах прикордонних підрозділів повинен містити конкретні критерії, які визначають здатність претендентів аналізувати та приймати ефективні рішення в умовах зміни ситуації. Це має включати оцінку їхнього оперативного мислення, здатності керувати кризами та здатності ефективно організовувати взаємодію з іншими підрозділами.

У статті представлено практичну модель оцінювання того, як ситуаційні умови на державному кордоні безпосередньо впливають на потреби в кадровому забезпеченні штабів прикордонних підрозділів. Отримані результати можуть бути використані для оптимізації управлінських рішень у сфері персоналу та підвищення бойової готовності прикордонних формувань.

**Ключові слова:** прикордонний підрозділ, ситуаційна обстановка, ризики, загрози, завдання підрозділам, комплектування, відбір кандидатів на керівні штабні посади.

The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 3 No. 2 (2025)

DOI: 10.62524/msj.2025.3.2.12

# Високоточне авіаційне озброєння класу “повітря – поверхня” провідних країн: стан і тенденції розвитку

**Дмитро Соломатін**
кандидат військових наук, старший науковий співробітник, начальник відділу
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail:dmit73@ukr.net
ORCID:0009-0009-6864-173X

**Андрій Седляр**
кандидат військових наук, старший науковий співробітник,
провідний науковий співробітник
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: saa66ua@ukr.net
ORCID: 0009-0008-6816-2459

**Вадим Пасічник**
кандидат військових наук, провідний науковий співробітник
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: wws1@ukr.net
ORCID:0009-0007-6183-2731

**Олександр Луцевят**
старший науковий співробітник
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: lucevyat@i.ua
ORCID:0009-0001-2435-5434

**Марина Слюсаренко**
кандидат технічних наук, старший дослідник
старший науковий співробітник
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: slusarenko.m@gmail.com
ORCID:0000-0003-4165-3908

**Сергій Ільницький**
науковий співробітник
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: anastx85@icloud.com
ORCID:0009-0009-3000-9034

**Анотація.** Досвід війн останнього десятиліття та активної фази російсько-української війни, отриманий протягом 2022–2024 років, свідчить про те, що однією з основних рис ведення бойових дій (операцій) на сучасному етапі є завдавання масованих ракетно-авіаційних ударів високоточними балістичними, аеробалістичними та крилатими ракетами, протирадіолокаційними ракетами й керованими авіаційними бомбами, безпілотними літальними апаратами, що зумовлює відповідні зміни у характері ведення збройної боротьби, формах та способах застосування військ (сил). Зважаючи на відсутність сучасного високоточного озброєння вітчизняного виробництва на озброєнні Повітряних Сил Збройних Сил України та обмеження, які накладають партнери щодо застосування наданої високоточної зброї іноземного виробництва, питання щодо розвитку такої зброї набуває особливої актуальності та ваги. Насамперед це стосується зразків озброєння та військової техніки, які здатні забезпечити надійне ураження об'єктів противника в оперативній та оперативно-стратегічній глибині й завдяки цьому відіграють значну роль у досягненні успіху операції (бойових дій). Цим обумовлена актуальність дослідження.

Метою статті є дослідження розвитку високоточного авіаційного озброєння класу "повітря – поверхня" провідних країн світу для боротьби із наземними цілями, а також розгляд стану і тенденцій розвитку цього озброєння.

Основним методом для дослідження зазначених тенденцій є метод аналізу, що дозволяє їх комплексно розглянути та обґрунтувати. Виявлено основні тенденції розвитку високоточного озброєння класу "повітря – поверхня" збройних сил провідних країн світу, що є підґрунтям для подальшого розроблення оперативно-тактичних вимог до перспективних зразків (комплексів, систем) високоточного озброєння Збройних Сил України. Матеріали статті становлять практичну цінність для виробників, які мають досвід розроблення такої зброї.

**Ключові слова:** високоточне озброєння, засоби ураження класу "повітря – поверхня", оперативно-тактичні вимоги, тенденції розвитку, провідні країни.

## Вступ (Introduction)

Постійний розвиток форм і способів застосування військ (сил), надходження на оснащення багатьох армій світу нових, більш ефективних засобів збройної боротьби зумовлюють необхідність впровадження адекватних заходів щодо підтримання бойової могутності Збройних Сил України (ЗС України) за рахунок оновлення наявного парку озброєння та військової техніки (ОВТ). Оновлене озброєння має бути спроможним не тільки ефективно протидіяти сучасним засобам збройної боротьби противника, а й мати відповідний модернізаційний потенціал для забезпечення подальшого нарощування бойових можливостей військ (сил). Забезпечення такої спроможності визначається рівнем розвитку науково-технічного потенціалу держави та її фінансовими можливостями зі створення (закупівлі) систем (комплексів, зразків) ОВТ, характеристики яких мають відповідати певним вимогам.

Обґрунтованість вимог до ОВТ здебільшого визначається повнотою врахування низки факторів, що впливають на їх розроблення. До переліку основних із них належать: застосування систем (комплексів, зразків) ОВТ у сучасних збройних конфліктах, розвиток ОВТ ЗС України, а також основні тенденції розвитку ОВТ провідних країн світу. На наш погляд, відсутність глибокого аналізу будь-якого із цих факторів негативно відбивається на обґрунтованості сформованих вимог до ОВТ і є однією з проблем, яка потребує вирішення. При цьому визначення тенденцій розвитку ОВТ, до переліку яких, зокрема, належить високоточне озброєння класу "повітря – поверхня", є важливим для провідних країн світу.

На підставі результатів проведеного аналізу виявлено останні дослідження та публікації, які стосуються тенденцій розвитку ОВТ.

Аналіз наявного методичного апарату для визначення тенденцій розвитку озброєння та військової техніки розглядається авторами у [1]. Аналіз підходів та методику визначення

пріоритетних тенденцій розвитку систем озброєнь ЗС України наведено у [2].

У роботах (Кравець О. П.), [3] та (Седляр А. А.) [4, 5] здійснено достатньо ґрунтовний аналіз сучасних тенденцій розвитку систем (комплексів, зразків) ОВТ авіації та протиповітряної оборони (ППО) збройних сил передових з воєнного погляду країн світу. Конструктивні особливості, тактико-технічні характеристики та переваги сучасних і перспективних зразків авіаційних керованих засобів ураження малого калібру, а також основні тенденції розвитку цього класу зброї аналізують автори [6]. Аналіз сучасного стану та перспективи розвитку високоточних авіаційних засобів ураження пропонують автори у [7]. У роботі [8] визначено основні напрями розвитку ОВТ авіації та ППО ЗС України.

Детально проаналізовано призначення та характеристики високоточного озброєння класу “повітря – поверхня” провідних країн світу у [9], [10]. Щодо зарубіжних публікацій, то можна зазначити, що у [11] автор пропонує аналітичний огляд, у якому висвітлено сучасні тенденції розвитку ракетних технологій, які впливають на швидкість та точність ракет і збільшення дальності їх ураження. Автори у [12] розглядають майбутні тенденції ракетного озброєння у системах протиповітряної оборони. Фахівці у [13] пропонують аналітичний матеріал, у якому досліджено перспективи розвитку гіперзвукових ракет та їхній вплив на сучасні військові стратегії. У дослідженні [14] аналізується роль високоточної зброї у повітряних операціях, але не зосереджується увага на тенденціях її розвитку.

Водночас, практично поза увагою авторів цих робіт залишився аналіз основних тенденцій розвитку конкретних систем (комплексів, зразків) ОВТ провідних країн світу як одного із ключових факторів, які слід ураховувати, формуючи вимоги до ОВТ ЗС України.

З огляду на зазначене проведення більш глибокого аналізу стану та тенденцій розвитку високоточного озброєння класу “повітря – поверхня” збройних сил провідних країн світу є актуальним науковим завданням.

**Методологічна основа (Methodological Framework)**

Високоточне озброєння класу “повітря – поверхня” продовжує динамічно розвиватися під впливом новітніх технологій, змін у військових доктринах та зростаючих вимог до ефективності бойових дій.

Сьогодні одними із пріоритетних зразків високоточного озброєння збройних сил провідних країн світу є авіаційні керовані засоби ураження класу “повітря – поверхня”, застосування яких не потребує входження літаків-носіїв у зону ППО противника, що дозволяє максимально уникнути ризику їх ураження під час виконання бойових завдань. Досвід ведення збройних конфліктів кінця XX – початку XXI століть та широкомасштабної війни рф проти України свідчить про те, що питома вага такої зброї у повітряних ударах зросла до 90%. Провідні країни світу реалізують програми з удосконалення високоточних засобів ураження з наданням переваги насамперед порівняно недорогим системам. При цьому основні зусилля спрямовуються на підвищення ефективності їх застосування і зменшення витрат на виконання типового завдання. Практичні заходи здійснюються одночасно із проведенням науково-дослідних робіт зі створення новітніх стратегічних і тактичних пілотованих або безпілотних носіїв. Також здійснюються заходи з адаптації наявних зразків літаків до новітніх та перспективних авіаційних засобів ураження.

Високоточні авіаційні керовані засоби ураження класу “повітря – поверхня” з’явилися як варіант більш точного та ефективного застосування некерованих засобів ураження і згодом утворили новий клас високоточної зброї. Розвиток цих засобів зумовлений насамперед завданнями, які на них покладаються у сучасних війнах і війнах майбутнього, та технологічними можливостями розробників. При цьому весь шлях еволюції цих засобів характеризується постійним підвищенням ефективності їх застосування завдяки збільшенню точності, потужності бойових частин, дальності ураження та зниженню ймовірності впливу

противника.

Визначено, що на сучасному етапі перевага надається системам наведення комбінованого типу (інерціальній з коригуванням за даними систем супутникової навігації у комбінації з удосконаленими головками самонаведення, що можуть працювати у декількох діапазонах (радіолокаційному, оптичному, інфрачервоному) залежно від умов, у яких застосовуються).

Проведений аналіз показав, що до основних характеристик сучасних зразків високоточного озброєння класу “повітря – поверхня” належать: широкий діапазон дальності застосування (від 250 км до 1500 км) та швидкостей польоту (від дозвукових до надзвукових та гіперзвукових); низька ефективна поверхня розсіювання (на рівні 0,01–0,1 м$^2$); висока точність влучання у ціль (кругове імовірне відхилення до 5 м); достатньо значна вага бойової частини (на рівні 400–500 кг); змінюваність траєкторії польоту (зокрема з огинанням рельєфу місцевості на гранично малих висотах); висока перешкодозахищеність.

Зазначені характеристики зумовлюють достатньо високу ефективність цих зразків високоточного озброєння щодо ураження широкого переліку об’єктів (цілей) (з імовірністю на рівні 0,8–0,98) та подолання системи ППО противника (з імовірністю на рівні 0,95).

Сучасні засоби ураження класу “повітря – поверхня” мають модульність та гнучкість конструкції, що дає можливість здійснювати їхню подальшу модернізацію та адаптацію під широкий спектр виконуваних завдань, забезпечує високу надійність під час зберігання та експлуатації (з гарантійним та призначеним терміном експлуатації не менше 10 та 25 років відповідно), а їхні масогабаритні характеристики відповідають технічним можливостям і конструктивним особливостям літаків-носіїв. При цьому більшість із цих засобів можуть застосовуватися з різноманітних носіїв (винищувачів, бомбардувальників, штурмовиків) включно із транспортними літаками.

Розглянемо більш детально, як відбувається розвиток високоточного озброєння класу “повітря – поверхня” у провідних країнах світу, що прагнуть досягти технологічної переваги на полі бою, на прикладі США, Китаю, росії, Європи та Ізраїлю (табл. 1).

**Таблиця 1**. Розвиток високоточного озброєння класу “повітря – поверхня” у провідних країнах світу

| Країни | Основні тенденції | Примітки |
|---|---|---|
| США | 1. Розвиток гіперзвукових ракет | – **AGM-183A ARRW** – гіперзвукова ракета з дальністю понад 1000 км, розробляється для B-52H;<br>– Програма **HACM** (Hypersonic Attack Cruise Missile) – перспективна гіперзвукова ракета для винищувачів |
| | 2. Удосконалення стелс-технологій | – **AGM-158 JASSM** та її модифікація JASSM-ER (дальність 980 км) мають малопомітний корпус;<br>– **LRASM** – протикорабельна ракета, що може запускатися з літаків |
| | 3. Універсалізація та модульність | – **GBU-53/B StormBreaker** – планерувальна бомба, що може вражати рухомі цілі в будь-яку погоду |
| | 4. Штучний інтелект (ШІ) та автономність | – розвиток **“роєвої тактики”** для взаємодії між високоточними боєприпасами |

**Продовження таблиці 1.** Розвиток високоточного озброєння класу “повітря – поверхня” у провідних країнах світу

| | | |
|---|---|---|
| Китай | 1. Гіперзвукові технології | – **DF-ZF** (гіперзвуковий планерувальний блок) може бути адаптований для авіаційних платформ |
| | 2. Аналоги американських систем | – **KD-63, KD-88** – аналоги JASSM, мають дальність 200–300 км;<br>– **YJ-12** – потужна надзвукова ракета для боротьби з кораблями |
| | 3. Безпілотні носії озброєння | – Китай активно працює над бойовими дронами-“камікадзе” та розробляє системи рою дронів |
| росія | 1. Гіперзвукові ракети | – **“Кинжал”** – аеробалістична ракета (дальність понад 2000 км), базується на винищувачах МіГ-31К;<br>– розробка **Х-95** – перспективної гіперзвукової ракети |
| | 2. Розширення арсеналу крилатих ракет | – **Х-101/Х-102** – крилаті ракети з дальністю до 5000 км;<br>– оновлення **Х-59МК2** – аналога американського JASSM |
| | 3. Розвиток тактичного озброєння | – керовані авіабомби **КАБ-250/КАБ-500** – аналог JDAM, що використовує супутникове й лазерне наведення |
| Європа (Франція, Британія, Велика Німеччина) | 1. Створення уніфікованих ракет для НАТО | – **Storm Shadow/SCALP-EG** – крилата ракета (дальність 550 км), використовується Британією, Францією, Італією;<br>– **Taurus KEPD 350** (Німеччина) – дальність понад 500 км, розробляється спільно з Іспанією |
| | 2. Безпілотні носії озброєння | – Проєкт **FCAS** (Future Combat Air System) передбачає інтеграцію штучного інтелекту та дронів у бойові операції |
| | 3. Модернізація керованих авіаційних бомб | – Франція та Німеччина активно розвивають **AASM Hammer**, який може запускатися з літаків Rafale |
| Ізраїль | 1. Компактні ракети для тактичної авіації | – **SPIKE N** |

Визначимо основні метрики для візуалізації процесу розвитку високоточного озброєння класу “повітря – поверхня” у провідних країнах світу: основні характеристики (рис. 1 та рис. 4); тенденції розвитку (рис. 2); обсяги коштів, які держави вкладають (рис. 3).

Як видно, сучасні тенденції розвитку високоточного озброєння класу “повітря – поверхня” провідних країн світу орієнтовані на розширення дальності, впровадження ШІ, підвищення точності та зниження вразливості до засобів протидії. Варто очікувати подальшого розвитку гіперзвукових технологій, збільшення ролі безпілотних платформ та інтеграції боєприпасів у єдині бойові системи.

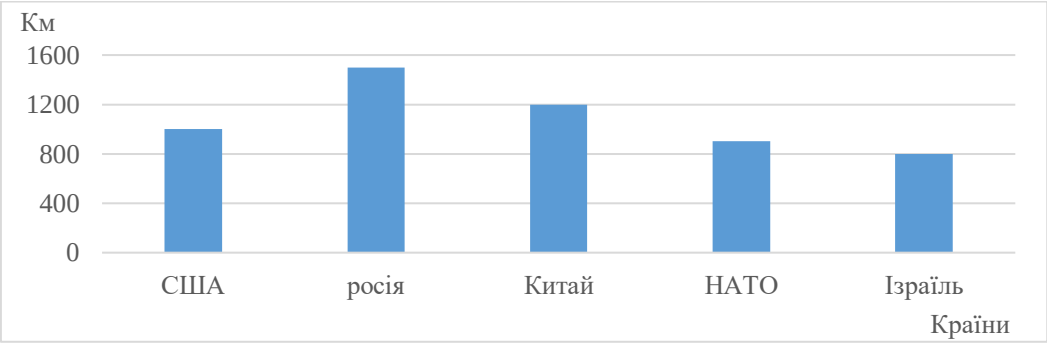



**Рисунок 1.** Дальність ураження, км

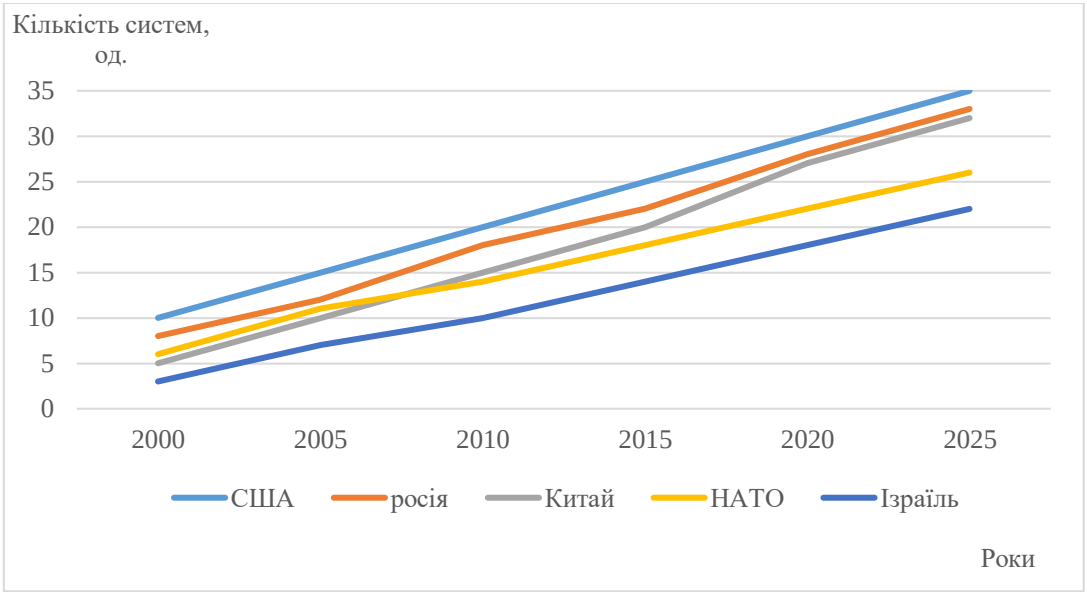



**Рисунок 2.** Темпи розроблення високоточного озброєння провідних країн світу

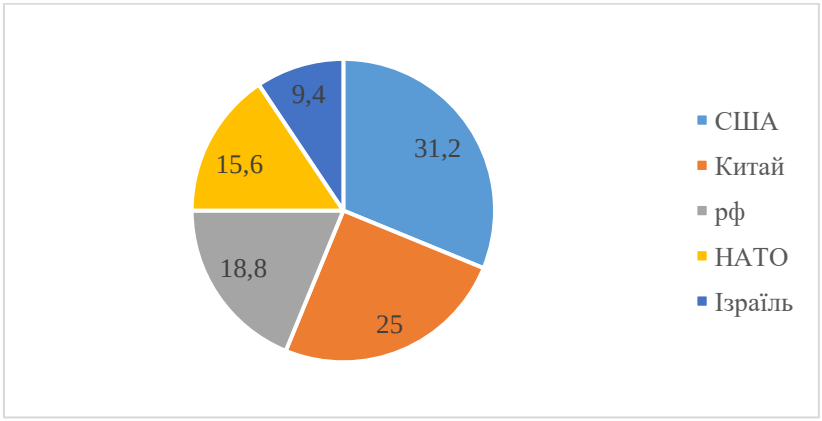



**Рисунок 3.** Фінансування високоточного озброєння у провідних країнах світу, %

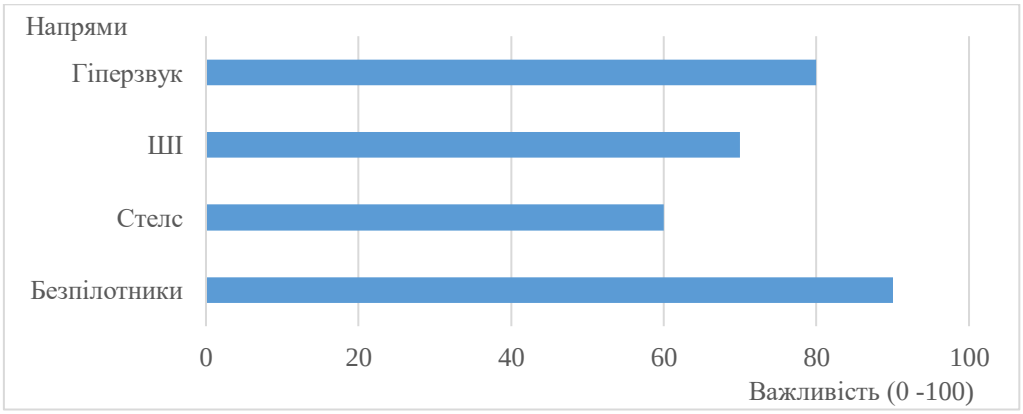



**Рисунок 4.** Ключові технологічні напрями розвитку високоточного озброєння

За результатами проведеного аналізу визначено, що до основних тенденцій розвитку високоточного озброєння класу “повітря – поверхня” провідних країн світу належать:

оптимізація аеродинамічних схем, удосконалення систем наведення, бортового обладнання та двигунів для досягнення необхідних показників точності, дальності польоту,

надійності роботи та технологічності;

адаптація керованих засобів ураження під широку номенклатуру носіїв повітряного, наземного та морського базування;

збільшення потужності бойових частин ракет та дальності їхнього польоту за рахунок використання ефективного хімічного складу вибухових речовин та порохів (рідин);

оснащення ракет турбореактивними двигунами та гіперзвуковими прямоточними повітряними реактивними двигунами для забезпечення їхньої надзвукової та гіперзвукової швидкості;

забезпечення можливості використання зовнішніх джерел інформації (насамперед безпілотних літальних апаратів) для уточнення місцеположення об’єктів удару та здійснення цілевказань по них на кінцевій ділянці польоту ракет;

побудова ракет на основі модульної конструкції з відкритою архітектурою для забезпечення можливості встановлення бойових частин різного типу (зокрема касетної бойової частини із самонавідними боєприпасами та бойової частини некінетичної дії);

оснащення ракет сучасними системами навігації (типу DSMAC, TERCOM), які порівнюють завантажені у бортовий комп’ютер цифрові дані про рельєф місцевості з даними від датчиків ракети, що підвищує ефективність їх застосування у цілому;

інтелектуалізація головок самонаведення ракет для забезпечення можливості автоматичного вибору найбільш ефективного каналу (режиму роботи) на кінцевій ділянці траєкторії (залежно від умов бойового застосування та параметрів цілі, що уражається), а також ураження цілей у найменш захищеній зоні й із виконанням маневру, що дозволяє використати весь потенціал бойової частини ракети;

забезпечення електромагнітної сумісності бортової апаратури систем управління ракет для їх спільного застосування з ракетами інших комплексів;

підвищення перешкодозахищеності бортової апаратури систем управління ракет (зокрема за допомогою селекції сигналів, відбитих від хибних цілей (зокрема від дипольних хмар, надувних кутових відбивачів) та використання аперіодичних зондувальних сигналів зі змінюванням частоти за випадковим законом);

зменшення радіолокаційної та теплової помітності завдяки використанню сучасних поглинаючих покриттів;

забезпечення можливості автоматичного вибору висоти польоту на кінцевій ділянці траєкторії польоту залежно від рельєфу місцевості (стану поверхні моря).

**Результати (Results)**

Авторами з’ясовано, що сучасні тенденції розвитку високоточного озброєння класу “повітря – поверхня” провідних країн світу орієнтовані на розширення дальності, впровадження ШІ, підвищення точності та зниження вразливості до засобів протидії. У перспективі варто очікувати подальшого розвитку гіперзвукових технологій, збільшення ролі безпілотних платформ та інтеграції боєприпасів у єдині бойові системи.

Під час дослідження тенденцій розвитку високоточного озброєння класу “повітря – поверхня” також визначено, що на сучасному етапі з’явились уточнені вимоги щодо концепції його застосування. Встановлено, що принцип застосування “вистрілив і забув”, який передбачає повну автоматизацію процесів управління на всіх етапах польоту до цілі, доповнено вимогою щодо забезпечення можливості здійснення контролю за ракетою у процесі польоту та перенацілювання її після пуску за допомогою організації двосторонньої лінії

обміну інформацією з літаком-носієм (або іншим пунктом управління). Ця вимога зумовлена швидкоплинністю змінювання обстановки на полі бою, коли може виникати потреба у призначенні іншої цілі для ураження, а також бажанням операторів та розробників високоточного авіаційного озброєння інтегрувати його в автоматизовану систему керування полем бою та систему ситуаційної обізнаності.

**Обговорення (Discussions)**

Зацікавленість цією тематикою виявляють дослідники всього світу. Автори у [15] розглядають інтеграцію західних авіаційних засобів ураження, таких як крилаті ракети та керовані бомби, у літаки радянського виробництва (МіГ-29, Су-27, Су-25, Су-24). Дослідження [16] присвячено аналізу трансформації авіаційної техніки ЗС України, зокрема проблемам модернізації та інтеграції сучасного озброєння. Прогноз ринку авіаційних систем озброєння на 2024–2034 роки надається у [17]. Інтеграцію штучного інтелекту в системи озброєння розглядають автори у [18] та [19]. Яким чином РЕБ впливає на високоточну зброю, досліджує автор у [20].

Наступні публікації надають глибоке розуміння поточних розробок і тенденцій у сфері високоточного авіаційного озброєння класу “повітря – поверхня” у Великій Британії та США [21], [22].

**Висновки (Conclusion)**

Отже, на підставі результатів проведеного аналізу визначено основні тенденції розвитку високоточного озброєння класу “повітря – поверхня” збройних сил передових з воєнного погляду країн світу. Ці тенденції є одним із ключових факторів, що мають враховуватися під час розроблення вимог до перспективних ОВТ ПС ЗС України для підвищення їхньої обґрунтованості.

Результати зазначеного аналізу підтверджують актуальність подальшого розвитку в нашій державі високоточного озброєння класу “повітря – поверхня” та нарощування його кількості. При цьому одним із пріоритетних напрямів має бути створення високоточних авіаційних керованих ракет, які здатні ефективно уражати наземні (морські) цілі з великих відстаней та можуть запускатися з носіїв поза зонами ураження засобів ППО великої та середньої дальності.

Перспектива подальших досліджень вбачається у визначенні аналогічних тенденцій для ОВТ іншого типу.

**Рекомендації (Recommendations)**

Матеріали статті становлять практичну цінність для виробників, які мають досвід розроблення такої зброї.

**Використані джерела**

1. Потьомкін, М. М., Кравець, О. П., & Седляр, А. А. (2021, 24 жовт.). Аналіз існуючого методичного апарату для визначення тенденцій розвитку озброєння та військової техніки. У Зб. мат. постійно діючого наук.-практ. семінару, *Актуальні проблеми будівництва Збройних Сил, їх застосування та всебічного забезпечення. Вип. 2 (31).* (С. 142–151). ЦНДІ ЗС України.
2. 2. Потьомкін, М. М., Кравець, О. П., & Седляр, А. А. (2021). Аналіз підходів до визначення тенденцій розвитку озброєння та військової техніки. *Зб. наук. пр. ЦНДІ ЗС України, 4* (99), 177–182.

3. Потьомкін, М. М., Кравець, О. П., Седляр, А. А. (2022). Методика визначення пріоритетних тенденцій розвитку систем озброєнь Збройних Сил України. З*б. наук. пр. ЦНДІ ЗС України, 1* (100), 194–202.
4. *Робочі матеріали НДР шифр "Спеціалізація"* (Етап 1). (2017). ЦНДІ ЗС України.
5. Седляр, А. А. (2021, 20 квіт.). Аналіз світових тенденцій розвитку озброєння та військової техніки авіації та протиповітряної оборони. У Зб. мат. постійно діючого наук.-практ. семінару, *Актуальні проблеми будівництва Збройних Сил, їх застосування та всебічного забезпечення. Вип. 1 (22).* (С. 252–259). ЦНДІ ЗС України.
6. Сєряков, І., Пономарьов, О., & Бабкін, С. (2021). Аналіз тенденцій розвитку авіаційних керованих засобів ураження малого калібру. *Зб. наук. пр. ДНДІА, 17* (24), 153–158. https://znp.dndia.org.ua.
7. Нікітченко, В. І., Кірдей, Л. М., & Гордєєв, С. М. (2019). Аналіз сучасного стану та перспективи високоточних авіаційних засобів ураження. *Зб. наук. пр. Держ. наук.-досл. ін-ту випробувань та сертифікації озброєння та військової техніки, 1* (1), 129–134. https://dndivsovt.com.
8. Потьомкін, М. М., Кравець, О. П., Седляр, А. А., & Соломатін, Д. О. (2019). Основні напрямки розвитку озброєння та військової техніки авіації та протиповітряної оборони Збройних Сил України. *Зб. наук. пр. ЦНДІ ЗС України, 4* (90), 210–219.
9. *Звіт про оперативне завдання шифр "Простір"*. (2024). ХНУПС ім. Івана Кожедуба.
10. *Звіт про виконання оперативного завдання шифр "Простір"*. (2024). НУО України.
11. Barrie, D. (2024). Trend sin missile tech no logiest. *Jane's Defence Weekly.* https://www.iiss.org/people/defence-and-military-analysis/douglas-barrie/.
12. Upendra Dwivedi, Dinesh Kumar Tripathi, Singh A. P. Future Trendsin Army Air Defence Systems. *SP's Land Forces.*(2022) https://www.spslandforces.com.
13. *The Future of Hypersonic Missiles. Аналітичний матеріал від TE Connectivity.* (2024). https://www.linkedin.com.
14. Vivek Kapur. (2020). Precision Weaponsin Aerial Warfare. *Дослідження від Institute for Defence Studies and Analyses.* https://idsa.in.
15. Каплюк, О., Гончаренко, Є., Печененко, О., & Чернов, С. (2024). Адаптація літаків тактичної авіації Повітряних Сил ЗСУ для застосування іноземних авіаційних засобів ураження класу "повітря-поверхня". *Повітряна міць України, 1* (6), 63–72. https://sap.nuou.org.ua/article/view/300646.
16. Шостак, В. Г., Пащенко, С. В., Кубарь, С. В., & Мавренков, О. Є. (2024). Розвиток авіаційної техніки авіації Збройних Сил України: ретроспектива та сьогодення, проблеми і шляхи їх розв'язання. *Наука і оборона, 3,* 11–17. https://nio.nuou.org.ua.
17. Fact. MR. (2024). *Airborne weapon systems market forecast 2024–2034.* https://www.factmr.com/report/airborne-weapon-system-market.
18. Kania, E. B. (2019). *The weaponization of AI: Strategic risks and responses. arXiv.* https://arxiv.org/abs/1905.03899.
19. Feldman, P., Dant, A., & Massey, A. (2020). *Integrating Artificial Intelligence into Weapon Systems.* https://arxiv.org/abs/1905.03899.
20. Seldin, M. (2024). Russian electronic warfare keeps beating US precision weapons. *Business Insider.* https://www.businessinsider.com/russian-cheap-electronic-warfare-keeps-beating-us-precision-weapons-2024-4.
21. *Airforce Technology. UK revises SPEAR 3 baseline, to be finalised in 2026*. (2025). https://www.airforce-technology.com/news/uk-revise-spear-3-baseline-to-be-finalised-in-2026/.
22. *Aviacionline. Lockheed Martin introduces AGM-158 XR: the evolution of JASSM-ER, but with longer range.* (2024). https://www.aviacionline.com/lockheed-martin-introduces-agm-158-xr-

the-evolution-of-jassm-er-but-with-longer-range.

**References**

1. Potemkin, M. M., Kravets, O. P., & Sedlyar, A. A. (2021, October 24). Analysis of the existing methodological apparatus for determining trends in the development of weapons and military equipment. In Proceedings of the permanent scientific and practical seminar, *Actual problems of the construction of the Armed Forces, their application and comprehensive support. Issue 2 (31).* (pp. 142-151). Central Research Institute of the Armed Forces of Ukraine.
2. Potemkin, M. M., Kravets, O. P., & Sedlyar, A. A. (2021). Analysis of approaches to determining trends in the development of weapons and military equipment. *Collection of scientific papers of the Central Research Institute of the Armed Forces of Ukraine, 4 (99)*, 177-182.
3. Potemkin, M. M., Kravets, O. P., & Sedlyar, A. A. (2022). Methodology for determining priority trends in the development of weapons systems of the Armed Forces of Ukraine. *Collection of scientific papers of the Central Research Institute of the Armed Forces of Ukraine*, 1 (100), 194-202.
4. *Working materials of the research and development program "Specialization"* (Stage 1). (2017). Central Research Institute of the Armed Forces of Ukraine.
5. Sedlyar, A. A. (2021, April 20). Analysis of world trends in the development of weapons and military equipment of aviation and air defense. In Proceedings of the permanent scientific and practical seminar, *Actual problems of the construction of the Armed Forces, their application and comprehensive support. Issue 1 (22).* (pp. 252-259). Central Research Institute of the Armed Forces of Ukraine.
6. Seriakov, I., Ponomarev, O., & Babkin, S. (2021). Analysis of trends in the development of small-caliber aircraft guided munitions. *Collection of Scientific Papers of the State Research Institute of Air Defense, 17 (24)*, 153-158. https://znp.dndia.org.ua.
7. Nikitchenko, V. I., Kirdey, L. M., & Gordeev, S. M. (2019). Analysis of the current state and prospects of high-precision aviation weapons. *Collection of scientific papers of the State Research Institute for Testing and Certification of Arms and Military Equipment, 1 (1)*, 129-134. https://dndivsovt.com.
8. Potemkin, M. M., Kravets, O. P., Sedlyar, A. A. & Solomatin, D. O. (2019). The main directions of development of weapons and military equipment of aviation and air defense of the Armed Forces of Ukraine. *Collection of scientific papers of the Central Research Institute of the Armed Forces of Ukraine, 4 (90)*, 210-219.
9. *Report on the operational task cipher "Space"* (2024). KhNUPS named after Ivan Kozhedub.
10. *Report on the implementation of the operational task cipher "Space"* (2024). National Defense University of Ukraine.
11. Barrie, D. (2024). Trend sin missile tech no logiest. *Jane's Defence Weekly.* https://www.iiss.org/people/defence-and-military-analysis/douglas-barrie/.
12. Upendra Dwivedi, Dinesh Kumar Tripathi, Singh A. P. Future Trendsin Army Air Defence Systems. *SP's Land Forces.*(2022) https://www.spslandforces.com.
13. *The Future of Hypersonic Missiles. Analytical material from TE Connectivity. (2024).* https://www.linkedin.com.
14. Vivek Kapur. (2020). Precision Weaponsin Aerial Warfare. *A study by the Institute for Defense Studies and Analyses.* https://idsa.in.
15. Kapliuk, O., Honcharenko, E., Pechenenko, O., & Chernov, S. (2024). Adaptation of tactical aircraft of the Air Force of Ukraine for the use of foreign air-to-surface weapons. *Air Power of Ukraine*, 1 (6), 63-72. https://sap.nuou.org.ua/article/view/300646.
16. Shostak, V. G., Pashchenko S. V., Kubar, S. V., & Mavrenkov, O. E. (2024). Development of

aviation equipment of the aviation of the Armed Forces of Ukraine: retrospective and present, problems and ways of their solution. *Science and Defense, 3*, 11-17. https://nio.nuou.org.ua.
17. Fact. MR. (2024). *Airborne weapon systems market forecast 2024–2034.* https://www.factmr.com/report/airborne-weapon-system-market.
18. Kania, E. B. (2019). *The weaponization of AI: Strategic risks and responses. arXiv*. https://arxiv.org/abs/1905.03899.
19. Feldman, P., Dant, A., & Massey, A. (2020). *Integrating Artificial Intelligence into Weapon Systems.* https://arxiv.org/abs/1905.03899.
20. Seldin, M. (2024). Russian electronic warfare keeps beating US precision weapons. *Business Insider.* https://www.businessinsider.com/russian-cheap-electronic-warfare-keeps-beating-us-precision-weapons-2024-4.
21. *Airforce Technology. UK revises SPEAR 3 baseline, to be finalised in 2026*. (2025). https://www.airforce-technology.com/news/uk-revise-spear-3-baseline-to-be-finalised-in-2026/.
22. *Aviacionline. Lockheed Martin introduces AGM-158 XR: the evolution of JASSM-ER, but with longer range.* (2024). https://www.aviacionline.com/lockheed-martin-introduces-agm-158-xr-the-evolution-of-jassm-er-but-with-longer-range.

## High-precision air-to-surface weapons of leading countries: state of the art and development trends

**Dmytro Solomatin**
Candidate of Military Science, Senior Researcher
Head of the Division
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl avenue, 28 B, Kyiv, Ukraine
e-mail: dmit73@ukr.net
ORCID: 0009-0009-6864-173X

**Andrii Sedliar**
Candidate of Military Science, Senior Researcher
Leading Research Fellow
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl avenue, 28 B, Kyiv, Ukraine
e-mail: saa66ua@ukr.net
ORCID: 0009-0008-6816-2459

**Vadim Pasichnyk**
Candidate of Military Science
Leading Research Fellow
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl avenue, 28 B, Kyiv, Ukraine
e-mail: wws1@ukr.net
ORCID: 0009-0007-6183-2731

**Aleksandr Lutsevyat**
Senior Researcher
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl avenue, 28 B, Kyiv, Ukraine
e-mail: lucevyat@i.ua
ORCID: 0009-0001-2435-5434

**Maryna Sliusarenko**
Candidate of Technical Sciences, Senior Researcher
Senior Research Fellow
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl avenue, 28 B, Kyiv, Ukraine
e-mail: slusarenko.m@gmail.com
ORCID: 0000-0003-4165-3908

**Serhii Ilnytskyi**
Junior Research Fellow
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl avenue, 28 B, Kyiv, Ukraine
e-mail: anastx85@icloud.com
ORCID:0009-0009-3000-9034

**Abstract.** The experience of the wars of the last decade and the active phase of the Russian-Ukrainian war, gained in 2022-2024, shows that one of the main features of combat operations at the present stage is the infliction of massive missile and air strikes with high-precision ballistic missiles, aeroballistics and cruise missiles, anti-radar missiles and guided aircraft bombs, unmanned aerial vehicles, which leads to corresponding changes in the nature of armed struggle, forms and methods of using troops (forces). Given the absence of modern high-precision weapons of domestic production in the inventory of the Air Force of the Armed Forces of Ukraine and the restrictions imposed by partners on the use of foreign-made high-precision weapons, the issue of developing such weapons is of particular relevance and importance. First of all, this concerns the types of weapons and military equipment that are capable of providing reliable destruction of enemy targets in operational and operational-strategic depth and thus play a significant role in achieving the success of an operation (combat operations). This determines the relevance of the study.

The article is aimed at studying the development of high-precision air-to-surface weapons of the leading countries of the world for combating ground targets, and the status and trends of development are considered.

The main method for studying these trends is the method of analysis, which allows them to be comprehensively considered and substantiated.

The article identifies the main trends in the development of air-to-surface precision weapons of the armed forces of the world's leading countries, which is the basis for further development of operational and tactical requirements for advanced models (complexes, systems) of precision weapons of the Armed Forces of Ukraine.

The materials of the article are of practical value for manufacturers who have experience in developing such weapons.

**Keywords:** precision weapons, air-to-surface weapons, operational and tactical requirements, development trends, leading countrie.

The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 3 No. 2 (2025)

DOI: 10.62524/msj.2025.3.2.13

# The Post-War Development Strategy of Ukraine: Assessment of the Global Security Environment

**Volodymyr Komarov**
Laureate of the Borys Paton National Prize
Doctor of Military Sciences, Professor
Leading Research Fellow of the branch at the Military Intelligence Research Institute
Military Intelligence Research Institute
04050, Yurii Illienka Street, 81, Kyiv, Ukraine
e-mail: komarvlad@ukr.net
ORCID: 0000-0003-2873-8261

**Serhii Baranov**
Head of the Main Directorate of the General Staff of the Armed Forces of Ukraine
General Staff of the Armed Forces of Ukraine
03168, Povitrianykh syl avenue, 6, Kyiv, Ukraine
e-mail: sharada3699@gmail.com
ORCID: 0000-0002-3306-943X

**Denys Grazion**
Candidate of Military Sciences, Senior Researcher
Scientific Secretary
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh syl avenue, 28 B, Kyiv, Ukraine
e-mail: denion@ukr.net
ORCID 0000-0001-9319-0736

**Abstract.** The structure of the Strategy for the Development of Ukraine draft in the Post-War Period envisages the implementation of five main stages, the justification of which in terms of structure and content has been described in previous studies. The first stage – the assessment of the strategic situation (the global security environment) – is decisive. It lays the foundation for ensuring Ukraine's security guarantees, primarily in the military sphere, in both the short and long term, based on the analysis of the transformation of security processes at the global and regional levels.

The relevance of the article is driven by the necessity of forming an adequate assessment and forecast of the further development of the current security environment at both the global and regional levels in order to implement the subsequent stages of the development of the draft Strategy for Ukraine's Development in the Post-War Period.

The aim of the article and its direction is to conduct an assessment of the current security environment and its impact on resolving the issue of providing military security guarantees to Ukraine.

The main results of the article is the consideration of possible formats for providing military security guarantees to Ukraine (bilateral, multilateral, and/or alliance-based), based on an analysis of the current security environment, with the aim of identifying and developing effective mechanisms for ending the russian-Ukrainian war with minimal losses.

The practical significance of the article's results lies in the attempt to assess the current strategic situation (the global security environment), which will contribute to the identification and formulation of Ukraine's long-term strategic development goals in the field of national security and defence, as well as in other areas of the state's living activity.

**Keywords**: military security guarantees, global security environment, russian-Ukrainian war, post-war development strategy of Ukraine.

## Introduction

The full-scale armed aggression of the russian federation against Ukraine has continued for the fourth year with the aim of restoring the "russian empire" on the territory of the former Soviet Union. The plans of the putin regime have not changed – the destruction of Ukraine as an independent state, its return under russian geopolitical influence, the occupation of its territory, and the deprivation of the Ukrainian population of its national identity.

Taking into account the position of the United States regarding forcing the russian federation to cease fire and end the russian-Ukrainian war, China's expansionist plans concerning Taiwan and North Korea's concerning South Korea, Iran's nuclear ambitions in the Middle East, Israel's permanent war with Palestinian militants, and other negative factors in the transformation of the global security environment, the urgency of addressing the issue of adequately assessing the situation and forecasting its further development is increasing.

The development of criteria for such an assessment will contribute to determining and implementing priority and subsequent steps in all areas of the state's functioning and to enshrining the relevant decisions in long-term documents that define its further development.

The relevance of the article is due to the need to form an adequate assessment and forecast of the further development of the current security environment at both the global and regional levels for the implementation of the next stages in the development of the post-war Strategy for the Development of Ukraine.

## Literature review

Much attention has been paid to the issue of providing military security guarantees to Ukraine. Since 2023, numerous meetings of partner countries have taken place, during which the issue of providing military security guarantees to Ukraine after the end of the russian-Ukrainian war was discussed. Possible actors and mechanisms for forming a "security umbrella" have been considered in many analytical studies (reports) by both domestic and foreign institutions, information and analytical agencies, well-known politicians, and individual experts [1, 2]. Reports by research centers such as the RAND Corporation, Hudson Institute, Atlantic Council, CSIS, RUSI, and others have outlined the United States's strategic vision regarding russia through the lens of ending the russian-Ukrainian war, the United States's interests in Europe and globally, as well as possible scenarios for shaping the post-war future for all parties and building a new security environment [3–6]. The definition of the actors and mechanisms for providing military security guarantees to Ukraine largely depends on the global struggle to uphold the geopolitical interests of the world's centers of power — the United States and China — and on the relations each of them maintains with russia, which claims the status of a center of power and rejects a bipolar world order that leaves no place for it.

It should be noted that most materials present possible formats for providing military security guarantees that have been proposed at high-level international meetings; however, forecasts regarding the mechanisms and timelines for their implementation remain cautious and restrained [7–10]. This indicates a certain uncertainty still present regarding the issue of guaranteeing military security to Ukraine after the end of the russian-Ukrainian war.

The above highlights the urgent need to address the task of assessing the global security environment as the foundation for developing the post-war Strategy for the Development of Ukraine.

## Methodological Framework

The development of the draft Strategy for the Development of Ukraine in the post-war period involves the implementation of five main stages [11].

At the first stage, the global situation is assessed as a basis for determining Ukraine's place in the global security environment in the post-war period, based on a comprehensive analysis of available information, namely:

the impact of changes in the world order on the timeline for ending the russian-Ukrainian war and the positions of the world's centers of power (country alliances) on this issue;

possible scenarios for ending the russian-Ukrainian war, changes in the security environment that create conditions for refining these scenarios in accordance with the situation, and their impact on global and regional security [12, 13];

the most effective strategies for ending the war [14, 15];

factors, risks, and threats that influence the state, changes, and further development of the security environment at global and regional levels, as well as the military-strategic situation around Ukraine;

actors and mechanisms through which they will provide military security guarantees to Ukraine in the post-war period, and other related aspects.

**Results and Discussions**

The assessment of the global security environment indicates that the new world order is being formed under conditions of unresolved contradictions between the leading geopolitical actors (global centers of power), which they are attempting to resolve, in particular, through the use of military force. The existing global security architecture, based on all countries' adherence to universally recognized principles and norms of international law, enshrined in relevant treaties, and on the operation of international control regimes, has become ineffective.

The intensification of the aggressive policies of authoritarian states—such as China, Iran, russia, North Korea—as well as transnational terrorist groups and organizations, is leading to the disregard of traditional mechanisms and processes for resolving emerging conflicts, the fundamental principles of international humanitarian law, and a refusal to recognize the right of neighboring countries to sovereignty and independence.

The onset and course of the open phase of the russian-Ukrainian war, along with the assistance provided to russia by other authoritarian regimes, demonstrate that they have formed a geopolitical axis to confront the so-called "collective West" and to limit its influence. This constitutes a real and growing challenge aimed at dismantling the liberal-democratic world order and the American-centric model of global security. The formation of this "axis of evil" was finalized at the beginning of 2025, after the ratification in April 2025 by the State Duma of the treaty on strategic partnership with Iran and the signing of the corresponding law by the president of russia. Prior to that, in November 2024, the treaty on comprehensive strategic partnership between russia and North Korea was ratified, and in May 2024, during putin's visit to China, a decision was made and a memorandum signed on strengthening cooperation between the countries' defence ministries.

The unsuccessful course of the full-scale invasion of Ukraine for russia and the disregard for its geopolitical ambitions indicate the gradual loss of russia's subjectivity. The russian president views the partial occupation of Ukraine and the creation of a buffer zone of tension ("managed chaos") on NATO's eastern flank as the foundation for building the future, which, in his opinion, would make russia the third pole of the world and break the bipolar model of the global order "USA – China" that is currently taking shape. russia is employing the logic of the Nazi dichotomy from the Second World War – either russia defeats the "collective West," or it ceases to exist and loses its former pre-war status as one of the centers of power in the global world.

The open armed aggression of russia against Ukraine is combined with the intensification of hybrid influence measures across various spheres. At the beginning of the full-scale invasion, russia was effectively in political isolation, with belarus as its only ally. Currently, however, russia is reactivating pro-russian politicians in the West. Its destructive activity in African countries amidst a

provoked food crisis deserves attention, as it aims to gain allies in these regions. Additionally, russia is covertly implementing manipulative measures aimed at escalating "frozen" and smouldering conflicts around the world. The hybrid component of russia's aggression is aimed at reducing support for Ukraine, diverting attention from the russian-Ukrainian war, and restoring its pre-war status after the failure of the blitzkrieg in the so-called "special military operation".

In the bipolar world order model of "USA – China," russia will become a vassal of one of the two hegemons, with no right to act as an independent global power center. Aware of this, russia is using every possible tool to prevent the loss of its former status. To this end, so-called "signals" are emerging in the Western press about russia's alleged readiness for pseudo-peacemaking activities and cessation of hostilities on Ukrainian territory, while retaining the occupied territories along the current line of contact at the time of negotiations. "Peacekeeping" proposals and initiatives are also appearing within the European and US establishments. These measures are a façade for gaining a pause to accumulate necessary resources, continue the "creeping" advance to seize Ukrainian territory, restore lost combat capabilities, conduct covert or open mobilisation, and exploit the "fatigue" from the russian-Ukrainian war. Considering the possible split in NATO, triggered by statements from D. Trump after phone conversations with putin, russia seeks to obtain a carte blanche to realise its imperial ambitions in Europe.

China plays a significant role in shaping the future world order, as one of the global centers of power and a major rival to the United States. Its position remains far from clearly defined regarding the violation of international law and the use of military force in the russian-Ukrainian war, yet it is becoming increasingly assertive concerning Taiwan and the Philippines. China also has its own geopolitical interests in the armed confrontation between Pakistan and India in the disputed regions of Jammu and Kashmir, aiming to gain control over Tibet.

The development of relations between China and the United States, as global actors, will be decisive in forming the new world order, as well as in resolving the main contradictions driven by their national interests and a range of regional and global issues. However, it must be considered that the United States and China are situated on opposing political poles, and each is pursuing its own strategy. Therefore, the United States's expectations that China might use its influence on russia and North Korea to promote a peace-oriented stance on Ukraine, as well as on Iran regarding its actions in the Middle East, appear rather pessimistic.

China and russia are strengthening their influence and international standing in the political domain by forming an anti-Western coalition as an element of geopolitical confrontation with the United States, and the BRICS summit serves as one of the platforms to demonstrate such a stance. At the latest 16th summit held on 22–24 October 2024, its membership was expanded (Ethiopia, Egypt, Iran, and the UAE were added).

A telling factor indicating the growing convergence of russia, China, and Iran in the military domain—and the emerging threat of a new global alliance against the United States and NATO—is the joint military exercise Security Bond. These exercises have been held annually since 2019, but under the current geopolitical circumstances, they take on particular significance: russia seeks to demonstrate its military power against the backdrop of the war in Ukraine and Western sanctions pressure; China continues to expand its military presence in the Indian and Pacific Oceans, aiming to challenge the United States; Iran strives to strengthen its military ties with russia and China to cement its role in opposing the West. Previously, China and russia had already conducted large-scale joint exercises in the Arctic and Pacific Oceans and coordinated their actions in the Mediterranean and Baltic Seas.

Further evidence of the deepening military rapprochement between russia and China includes the sale of russian military aviation equipment and modern air defence systems, as well as the probable transfer of submarine production technologies, the use of which would provide China with

a degree of parity in potential military conflicts with the United States and its allies in the Indo-Pacific region.

Western analysts view these exercises as a show of force against the United States and its allies. However, Donald Trump sees no reason for concern.

The ongoing russian-Ukrainian war, in which russia is gradually losing its military and economic potential, contributes to the achievement of the United States' geopolitical goals. Therefore, continued support for Ukraine by the United States—even through the transfer of outdated military equipment and weapons—on the one hand, enhances Ukraine's ability to inflict irreparable losses on russia, and on the other hand, the allocated appropriations for the implementation of these measures remain within the United States and are directed toward strengthening the military potential of the U.S. Army. This is of great significance if, in the near future, the United States faces the threat of an escalating armed conflict with both russia and China simultaneously [14, 15].

The return to power of Donald Trump at the beginning of 2025 drastically altered the strategy for ending the russian-Ukrainian war that had been developed in 2024 by partner countries led by the United States. All hopes for a swift agreement on a ceasefire and an end to the war remained unfulfilled. The issue of ending the war had been a grand pre-election promise of Donald Trump, which left the new Administration of the United States facing two very significant problems: first—the inheritance of the russian-Ukrainian war, which is reaching a "dead end" with no way to end it "within 24 hours"; second—the lack of a clear vision or plan on how to achieve this.

After Donald Trump's election victory, several options for ending the russian-Ukrainian war were developed within his team and were made public through the media. However, all of them, in various interpretations, envisaged a "freezing" of the current front lines, a postponement of Ukraine's NATO membership in the near future, and an undefined mechanism for providing military security guarantees to Ukraine.

A particularly unexpected move was Donald Trump's demand that Ukraine repay funds for the military assistance provided by signing a minerals agreement, his messaging about a potential United States's withdrawal from NATO, the necessity for European countries to increase their defence spending, as well as the launch of a "tariff war." Even during his first presidential term, Donald Trump was sceptical about NATO as a collective force capable of ensuring security in the North Atlantic. He believed that European defence expenditures were insufficient and that these countries were taking advantage of U.S. security guarantees as the Alliance's most powerful member. He considered the possibility of the United States leaving NATO. Donald Trump insisted that European Alliance members allocate 2% of GDP to defence.

On the eve of his second presidential term, Donald Trump reiterated the same narratives regarding the European members of the Alliance. Although five of them increased their defence spending to 3% of GDP during the russian-Ukrainian war, he argued that it should be raised to 5%. He suggested that the United States might not defend NATO allies who do not meet his target spending benchmarks as part of the Alliance's reorganization. Donald Trump also does not support Ukraine's NATO membership but is interested in a strong and well-armed Ukrainian defence force after the end of active hostilities. He believes that Europe should play the leading role in protecting, supporting, and providing military security guarantees to Ukraine, taking into account the 27 security agreements signed—with seven G7 countries, the European Union, and 19 states that have joined the G7 declaration.

Based on this position of the United States, the European NATO countries anticipate the beginning of a new security era amid the geopolitical changes in the world [16]. For decades, the former Soviet Union sought to "disconnect" the United States from Europe and "break apart" NATO, which was restraining Soviet military expansion in Europe. However, today, the President of the United States Donald Trump is doing what the former Soviet Union could not achieve over many years of the Cold War.

The response to Donald Trump's campaign statements was a series of provocative actions by the russian federation during missile strikes on Ukraine, when missiles and attack UAVs violated the airspace of NATO countries and even fell on their territories. With such acts, the russian federation was testing the resolve and political will of NATO member states regarding the protection of their own borders (airspace) and the possibility of a consolidated response to these provocations. These instances of border violations of NATO countries during massive air attacks on Ukraine by the aggressor's forces, without an adequate reaction from the Alliance, are becoming systematic. All of this indicates that NATO's military-political leadership clearly understands the real threat posed by the russian federation and its own inability to respond decisively to provocations, while the russian federation increasingly feels impunity for its actions.

In this situation, Europe is concerned by the growing realization of the urgent need for rapid rearmament and the shift in American security ideology, which could lead to a split in NATO. At this stage, Europe must determine what in Donald Trump's actions is political maneuvering, and what represents a long-term reorientation of the United States toward authoritarianism.

Against the backdrop of Trump's statements, French President Emmanuel Macron warned of "irreversible changes" in relations with the United States and called for strengthening the European army. He proposed extending France's nuclear "umbrella" to its allies and emphasized that the end of russian aggression must not come at the cost of Ukraine's capitulation.

In Germany, the situation caused particular tension. The country, which was rebuilt after World War II with the United States's support, is now forced to rethink its security policy, taking into account the decline of the post-war world order. Germany's new Chancellor, Friedrich Merz, stated that the absolute priority is to strengthen Europe as quickly as possible in order to gradually achieve independence from the United States. Germany is also considering the expansion of France's nuclear deterrent and a significant increase in defense spending.

Europe has realized that Donald Trump's flirtation with Putin could trigger new waves of aggression, because the russian federation sees Ukraine as an intermediate stage in a global strategy to destabilize NATO and the EU. The ultimate goal of this strategy is, together with China, North Korea, and Iran, to bring an end to the dominance of the collective West, American hegemony, and the U.S. dollar in the world economy.

The above indicates that ensuring their own military security has become a top priority for European NATO members. Therefore, the process of identifying actors and developing effective formats and mechanisms for providing military security guarantees to Ukraine may be somewhat slowed.

In addition, the swift preparation and conduct of negotiations on terms favorable to Ukraine is impossible because the russian federation must be forced into this — placed under extremely unfavorable and harsh conditions not only through heavy losses on the front line and the imposition of effective sanctions negatively affecting its economy, but also through constant political pressure from the world's leading countries. Donald Trump's threats do not have the intended effect or influence. Visits by representatives of the U.S. establishment to russia only contribute to the restoration of diplomatic relations and russia's exit from political isolation. Promises by the russian dictator to the President of the United States regarding future mutually beneficial economic relations only increase the United States's disinterest in participating in negotiations and leave Ukraine and Europe face-to-face with russia. In such a situation, the russian federation shows complete unwillingness to negotiate a ceasefire agreement, as it is achieving success in its "creeping" seizure of Ukrainian territory, despite heavy losses.

The Easter "ceasefire" during the military parade in Moscow on May 9 served as a security guarantee for russia and ensured the absence of strikes from Ukraine's defence forces, as well as an opportunity for russian occupation troops to improve the tactical situation and logistics along the line of contact and in the "grey zones".

The outcomes of the May negotiations in Turkey with the russian delegation regarding a ceasefire clearly demonstrate Putin's unwillingness to end the russian-Ukrainian war.

A ceasefire alone is not enough to achieve lasting peace in Europe — it is merely the first step in applying a comprehensive approach that must include resolving a number of key issues: the full termination of the russian-Ukrainian war, military security guarantees and Ukraine's recovery, the status of the occupied territories, compensation for Ukraine's losses during russia's armed aggression, the diplomatic return of temporarily occupied territories, the return of prisoners of war, children, and civilians, and so on.

It should be taken into account that a ceasefire in the russian-Ukrainian war has an ambiguous impact on European security — it may temporarily reduce the risk of further conflict spreading to neighbouring countries in Eastern Europe and the Baltics. However, the relevance of the real threat of aggression from the russian federation remains high.

The negative impact may be caused by the following factors:

during the war, European countries significantly increased defence spending and strengthened cooperation within NATO, but a ceasefire may slow down this process, which would pose a risk in the event of a renewed armed aggression by the russian federation not only against Ukraine but also against European countries;

the restoration of the offensive potential of the russian armed forces during a ceasefire is a realistic condition for possible aggression against the Baltic states (the Suwałki Corridor on the border of Poland and Lithuania, occupation of the Baltic countries);

the joint support of Ukraine during the war became a catalyst for the consolidation of European and Euro-Atlantic structures, but a ceasefire may weaken political unity on issues of military aid to Ukraine and strengthening sanctions against the russian federation;

the retention by the russian federation of the occupied territories of Ukraine in the event of a ceasefire would become a dangerous precedent that would undermine trust in international law and encourage other authoritarian countries to commit aggression in the future;

the easing of sanctions (as one of the possible conditions of the russian federation) without significant concessions on the part of the russian federation regarding the restoration of Ukraine's territorial integrity would nullify trust in the European policy of deterrence;

a ceasefire may stabilise the supply of gas and oil to Europe (against the backdrop of D. Trump's statements about the possible restoration of the "Nord Streams"), but dependence on the russian federation would remain a risk if Europe's energy diversification is not completed;

a ceasefire would contribute to active efforts by the russian federation to divide the European countries of the Alliance, in particular through pro-russian agents of influence in Europe;

the shift of the United States's geopolitical interests to the Indo-Pacific region, where escalation of actions by China regarding Taiwan and by North Korea regarding South Korea is possible;

a possible reduction in the presence of American troops in the European region as one of the possible conditions of the russian federation for concluding a ceasefire agreement.

The positive impact lies in the following:

bringing (modernising) the armed forces of the European member states of the Alliance up to the technological and technical standards defined by the experience of the russian-Ukrainian war, and in developing an alternative plan for protecting European countries from the russian threat;

increasing the capacities of the defence industries of the European NATO members to produce ammunition, air defence systems, artillery systems, armoured fighting vehicles, other weaponry, and military and special equipment;

conducting a future peacekeeping mission of European countries in Ukraine (with the consent of the russian federation), which would allow multinational units to better prepare for joint armed struggle under modern conditions;

the need to improve the mechanism of military assistance provision by the United States to the

European members of the Alliance and mutual assistance in the event of possible russian armed aggression in Europe;

providing military security guarantees for Ukraine, which would strengthen its position as a future member of the EU and NATO.

The signing of a ceasefire agreement brings to the forefront the issue of conducting a peacekeeping mission in Ukraine within the future buffer zone. European countries discussed the matter initiated by the President of France regarding the possibility of deploying troops to Ukraine in the event of a ceasefire or a peace agreement between Ukraine and the russian federation. This is due to the fact that the President of the United States Donald Trump, during negotiations with the Presidents of France and Ukraine in December 2024, ruled out the possibility of U.S. troops participating in ensuring the ceasefire and insisted that this task be carried out independently by European countries. During the discussion of this issue, a number of disagreements emerged regarding the possible objectives and mandate of such a mission in Ukraine: whether the future European mission will fulfil a traditional peacekeeping role (monitoring the ceasefire line), or whether it will ensure reliable deterrence of any potential future attacks by the russian federation. The question remains unresolved as to which countries will be involved, what role the United States will play in supporting this agreement, and whether the russian federation will consent to the participation of NATO countries' troops in the peacekeeping mission.

One of the options considered was a European mission aimed at supporting Ukraine's economic recovery and reconstruction. The reconstruction security forces could include troops from EU countries or a special coalition, which, together with Ukraine's defence forces, would be deployed in designated industrial zones far from the line of contact to minimise security risks. Given the remoteness of these zones, the russian federation would have to understand that the mission is not intended to support any potential military actions. Armed with air defence and early warning systems, the forces would be mandated to protect areas of economic activity, including reconstruction projects involving European companies, from russian aerial attacks. However, unfortunately, the issue of deploying a peacekeeping contingent from European countries to Ukraine remains unresolved as of the end of April 2025 and is still under consultation.

The current situation regarding the organization of negotiations to conclude a ceasefire agreement and end the russian-Ukrainian war is being used by Donald Trump to divide spheres of influence among the world's power centers. The shaping of the future outline of the United States's security environment in negotiations with russia—without the participation of Europe's leading countries and Ukraine—is being compared by the European political elite to the Yalta Conference of 1945, where the postwar future of Eastern Europe was decided without its involvement. If the agreements between the United States and russia are implemented, then, considering russia's growing influence on the domestic politics of the Czech Republic, Slovakia, Bulgaria, and Romania, Eastern Europe will be left at the mercy of future russian expansion and drawn back into russia's geopolitical orbit. Central Asia may also become a zone of rivalry between russia and China.

If the agreements between the United States and russia on ending the russian-Ukrainian war are not implemented, russia's dependence on China will increase. However, after the start of the "tariff war," China may move closer to Europe economically, which would potentially weaken russia's position, especially considering that China was the one to prevent the collapse of russia's military-industrial complex by meeting its needs for strategic raw materials, electronics, critical electronic components, dual-use goods, and more.

In any case, the terms for ending the russian-Ukrainian war are one of the most important factors in the further division of spheres of influence between the United States, russia, and China.

Taking the above into account, the issue of determining the mechanisms and actors for providing military security guarantees to Ukraine in the postwar period can only be resolved during the preparation of the ceasefire agreement and the end of the russian-Ukrainian war, and should be

enshrined in corresponding bilateral or multilateral agreements as an alliance treaty with specific commitments from the guarantor states.

**Conclusion**

In conclusion, the following can be stated.

1. An assessment of the global security environment, the strategies of further action by the leading actors regarding the distribution of spheres of influence in the world, the financial, economic, and military-technical capabilities of partner countries in countering russian aggression, as well as the current state of the russian-Ukrainian war, indicates that the issue of a ceasefire through the implementation of a negotiation process with russia—with the participation of Ukraine and the mediation of the United States and leading European countries—is becoming the only way out of the war. The key element in resolving this issue lies in the terms of the ceasefire and war termination agreement, as well as in the mechanisms and actors responsible for providing military security guarantees.

However, negotiations without specific deadlines—with no timeframe for the preparation and signing of the relevant memorandum—provide russia with an opportunity to buy time and concentrate its forces for a summer offensive.

The divergence between the positions of the United States and leading European countries regarding a ceasefire and the end of the russian-Ukrainian war is expected to reach its peak at the G7 Summit in Canada (15–17 June 2025) and the NATO Summit in the Netherlands (24–26 June 2025).

2. A new world order is taking shape amid unresolved contradictions between the leading geopolitical actors (global centers of power), which they are trying to resolve, including through the use of military force. Therefore, the emergence of a multipolar world presents a growing challenge aimed at dismantling the liberal-democratic world order and the America-centric model of global security. This complicates the process of resolving the issue of providing military security guarantees in the postwar period.

3. By using the ceasefire, russia will restore its offensive capabilities for further aggression in Europe, the aim of which is to advance its imperial geopolitical interests. These will be pursued based on the principles of conducting “hybrid warfare” across all domains, as well as through the application of a “carrot and stick” policy toward specific European countries, namely: energy blackmail, influence over global food supply chains, large-scale cyberattacks, global disinformation campaigns, irresponsible nuclear rhetoric, threats to global stability and security, and more. In other words, while a ceasefire may reduce the immediate risks of escalation, it will create new challenges associated with the long-term stability of the European region. The upcoming joint russian-belarusian military exercise “Zapad-2025,” scheduled for September 2025 on the territory of the Republic of Belarus, serves as a compelling argument in support of this assertion.

4. A shift in the United States’ strategic direction in the military sphere may lead to the weakening of NATO, which would pose a threat to Eastern Europe from russia and require the rapid build-up of military potential and the development of new effective mechanisms of military mutual assistance to replace Article 5 of the Washington Treaty.

5. The terms of the ceasefire and the end of the war will serve as an indicator for the countries of the “axis of evil” – russia, China, Iran, and North Korea. If, under U.S. mediation, conditions dictated by russia are imposed on Ukraine and the occupied territories remain under russian control along the line of contact, this would set a dangerous precedent, undermining trust in international law and encouraging other authoritarian states to commit acts of aggression in the future – for example, China toward Taiwan, or North Korea toward South Korea.

6. Military security guarantees are needed by our state both after the end of the russian-Ukrainian war and in the medium- and long-term perspective. The format of these guarantees may vary – either within NATO or outside of it. Although the President of the United States does not

support Ukraine's accession to the Alliance in the near future and this issue is not being considered in the upcoming agreement on ending the russian-Ukrainian war, Ukraine's foreign policy course toward European integration and NATO membership is clearly defined in the foundational documents of our state's further development.

Ukraine's security orientation may focus on the European members of the Alliance, considering the 27 signed security agreements – with seven G7 countries, the European Union, and 19 states that have joined the G7 declaration. The mechanism for concluding bilateral agreements proposed at the Vilnius Summit exists, but it is progressing very slowly and does not provide the necessary efficiency for their implementation. Additionally, security guarantees outside of NATO can be obtained through the creation of military-political alliances with leading countries and regional powers that support Ukraine. One possible option for implementing such a format could be the establishment of a Baltic-Black Sea belt. At the same time, the agreement between Ukraine and the United States on natural resources is expected to strengthen the strategic partnership within the framework of post-war reconstruction of Ukraine after the end of the russian-Ukrainian war. The presence of the American side at reconstruction sites would provide protection against attempts by russia to carry out strikes with high-precision weapons on the Ukrainian territory.

7. The russian-Ukrainian war must become a significant impetus for the global elites to reconsider the role of Ukraine and the West in building a new format of relations and communication regarding Ukraine's contribution to global security.

Regardless of when and under what conditions the russian-Ukrainian war ends, Ukraine will remain a central element of European security for decades to come. A strong Ukraine has a positive impact on European security today and will be an integral part of it in the future.

**Recommendations**

The materials presented in this article will be useful to public administration specialists, developers of long-term foundational documents in all spheres of life of our state, as well as to instructors, postgraduate students, and students of higher educational institutions in this field.

**References**

1. Taranenko, A. (n. d.). *Transformation of the international security system and Ukraine's further role*. ADASTRA. https://adastra.org.ua/blog/transformaciya-sistemi-mizhnarodnoyi-bezpeki-i-podalsha-rol-ukrayini
2. *Dmytro Kuleba: Ukraine created three new alliances in the Baltic-Black Sea region to strengthen security*. (n. d.). Ministry of Foreign Affairs of Ukraine. https://mfa.gov.ua/news/dmitro-kuleba-ukrayina-stvorila-3-novi-alyansi-u-balto-chornomorskomu-regioni-zadlya-zmicnennya-bezpeki
3. Gressel, G. (2024, Jan. 31). *Ukraine's survival: Three scenarios for the war in 2024*. European Council on Foreign Relations. https://ecfr.eu/article/ukraines-survival-three-scenarios-for-the-war-in-2024/
4. *Ukraine's most plausible security guarantee will not come from the U.S.* (2025). Crisis Group. https://www.crisisgroup.org/europe-central-asia/eastern-europe/ukraine-united-states-europe-central-asia/ukraines-most-plausible-security-guarantee
5. *Episode 53: How can Ukraine's security be guaranteed?* (n. d.). RUSI. https://www.rusi.org/podcasts/global-security-briefing/episode-53-how-can-ukraines-security-be-guaranteed
6. Charap, S., & Priebe, M. (2023). *Avoiding a long war: U.S. policy and the trajectory of the russia-Ukraine conflict*. RAND Corporation. https://www.rand.org/pubs/perspectives/PEA2510-1.html

7. *Postwar Ukraine: Planning for a successful and secure recovery*. (2024). RAND Corporation. https://www.rand.org/pubs/articles/2024/postwar-ukraine-planning-for-a-successful-and-secure.html
8. Coffey, L., & Rough, P. (2024, Apr. 11). *A strategy of courage: The next phase of the russia-Ukraine war*. Hudson Institute. https://www.hudson.org/defense-strategy/strategy-courage-next-phase-russia-ukraine-war-peter-rough-luke-coffey
9. Binnendijk, H., & Kramer, F. D. (2023). *Providing long-term security for Ukraine: NATO membership and other security options*. Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/providing-long-term-security-for-ukraine-nato-membership-and-other-security-options/
10. *A winning strategy to end russia's war against Ukraine*. (2024). Atlantic Council. https://www.atlanticcouncil.org/blogs/new-atlanticist/a-winning-strategy-to-end-russias-war-against-ukraine/
11. Romanov, O. M., & Komarov, V. S. (2024). Strategy for Ukraine's development: Forming views on the state's role and place in the post-war period. *Military Science, 2* (3), 194–205.
12. Budanov, K. O., Zaitsev, V. V., Romanov, O. M., & Komarov, V. S. (2023). Possible scenarios for ending the russian-Ukrainian war. Ukraine's role and place in the post-war order at global and regional levels. *Science and Defense, (3)*, 10–15.
13. *Five security scenarios on russian war in Ukraine for 2024–2025: Implications and policy recommendations to Western partners*. (2023, Nov.). GLOBSEC. https://www.globsec.org/sites/default/files/2023-12/Ukraine%20scenarios%20report%202024-2025.pdf
14. *The high price of losing Ukraine*. (n. d.). Institute for the Study of War. https://www.understandingwar.org/backgrounder/high-price-losing-ukraine
15. *The high price of losing Ukraine: Part 2 – The military threat and beyond*. (n. d.). Institute for the Study of War. https://www.understandingwar.org/backgrounder/high-price-losing-ukraine-part-2-%E2%80%94-military-threat-and-beyond
16. Kramer, A. E. (2025, Mar. 8). Trump, Putin and the future of Europe. *The New York Times*. https://www.nytimes.com/2025/03/08/world/europe/trump-putin-russia-europe.html

## Стратегія розвитку України у повоєнний час: оцінка глобального безпекового середовища

**Володимир Комаров**
Лауреат Національної премії імені Бориса Патона
доктор військових наук, професор
провідний науковий співробітник відділу
Науково-дослідний інститут воєнної розвідки
04050, вул. Юрія Іллєнка, 81, Київ, Україна
e-mail: komarvlad@ukr.net
ORCID: 0000-0003-2873-8261

**Сергій Баранов**
начальник Головного управління Генерального штабу Збройних Сил України
Генеральний штаб Збройних Сил України
003168, проспект Повітряних Сил, 6, Київ, Україна
e-mail: sharada3699@gmail.com
ORCID: 0000-0002-3306-943X

**Денис Гразіон**
кандидат військових наук, старший дослідник
вчений секретар
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: denion@ukr.net
ORCID 0000-0001-9319-0736

**Анотація.** Структура проєкту Стратегії розвитку України в повоєнний час передбачає реалізацію п’яти основних етапів, обґрунтування структури та змісту яких описано в попередніх дослідженнях. Перший етап – оцінка стратегічної ситуації (глобального безпекового середовища) – є визначальним, він закладає основу забезпечення безпекових гарантій України, насамперед у воєнній сфері, у найближчій та подальшій перспективі на підставі результатів проведеного аналізу трансформації безпекових процесів світового та регіонального рівнів.

Актуальність статті обумовлена необхідністю формування адекватної оцінки та прогнозу подальшого розвитку сучасного безпекового середовища на глобальному та регіональному рівнях для реалізації наступних етапів розроблення проекту Стратегії розвитку України в повоєнний час.

Метою статті та її спрямованістю є проведення оцінювання поточного безпекового середовища та його впливу на вирішення питання надання гарантій воєнної безпеки Україні.

Основним результатом статті є розглянуті можливі формати надання гарантій воєнної безпеки Україні (двосторонній, багатосторонній та/або блоковий) на основі аналізу поточного безпекового середовища для визначення та відпрацювання дієвих і ефективних механізмів завершення російсько-української війни з найменшими втратами.

Практична значимість результатів статті полягає у спробі оцінки поточної стратегічної ситуації (глобального безпекового середовища), яка стане в нагоді для визначення та формування довгострокових стратегічних цілей розвитку Держави у сфері національної безпеки і оборони та інших сферах її життєдіяльності.

**Ключові слова**: гарантії воєнної безпеки, глобальне безпекове середовище, російсько-українська війна, стратегія розвитку України в повоєнний час.

The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 3 No. 2 (2025)

DOI: 10.62524/msj.2025.3.2.14

# Аналіз наявних підходів до оцінювання та прогнозування рівня воєнно-економічної безпеки держави: закордонний та вітчизняний досвід

**Іван Гаврилюк**
кандидат військових наук, старший дослідник
перший заступник Міністра оборони України
Міністерство оборони України
e-mail: ivan_havryliuk@ukr.net
ORCID: 0000-0002-3514-0738

**Анотація.** Актуальність дослідження підходів до оцінювання та прогнозування рівня воєнно-економічної безпеки держави зумовлена зростанням глобальних загроз, гібридних війн і економічного тиску, що перетворюють традиційні уявлення про національну безпеку. У цьому контексті особливої ваги набуває порівняльний аналіз закордонного та вітчизняного досвіду, що дозволяє виявити ефективні методологічні підходи та інструменти для зміцнення безпекового потенціалу держави. Вивчення міжнародних практик дозволяє адаптувати перевірені моделі забезпечення воєнно-економічної безпеки до українських реалій, підвищуючи здатність держави своєчасно реагувати на загрози та забезпечувати стабільність у критичних умовах.

Методологічною основою дослідження стали системний, функціональний, стратегічний, інституційний, діалектичний та міждисциплінарний підходи. Для аналізу залучено сценарне моделювання, індикативний моніторинг, емпіричні методи (контент-аналіз, статистичний аналіз, порівняльні дослідження). Це забезпечило комплексне бачення структури воєнно-економічної безпеки та чинників, що впливають на її стійкість.

Мета статті – здійснити аналіз наявних підходів до оцінювання та прогнозування рівня воєнно-економічної безпеки України в умовах трансформаційної економіки та тривалої воєнної агресії, виявити основні загрози, визначити структурні дисбаланси та обґрунтувати доцільність створення інтегрованої системи управління воєнно-економічною безпекою на основі стратегічного прогнозування, інноваційного розвитку та міжнародної кооперації.

Результати дослідження свідчать про доцільність інтеграції вітчизняного та закордонного досвіду в оцінюванні та прогнозуванні рівня воєнно-економічної безпеки держави. Виявлено, що українські моделі краще враховують реалії гібридної війни, тоді як міжнародні практики відзначаються технологічною досконалістю та методологічною структурованістю. Проведений аналіз дозволив визначити переваги системного підходу, мультидисциплінарного аналізу та моделювання сценаріїв як основи для формування адаптивних стратегій воєнно-економічної безпеки.

У висновках зроблено акцент на необхідності зміцнення інституційної спроможності держави, модернізації законодавчої бази та налагодженні партнерських зв’язків з державами – членами НАТО та ЄС. Розроблено практичні рекомендації щодо оптимізації оборонних витрат, стимулювання національного виробництва та підвищення ефективності використання міжнародної допомоги.

Практична цінність роботи полягає у можливості застосування результатів дослідження при формуванні державної політики в сфері національної безпеки, розробленні стратегій воєнно-економічної стійкості та ухваленні управлінських рішень в умовах воєнного стану та постконфліктного відновлення.

**Ключові слова:** воєнно-економічна безпека, національна безпека, трансформаційна економіка, стратегічне управління, оборонно-промисловий комплекс, ризики, сценарне моделювання, безпекова політика.

**Вступ (Introduction)**

У сучасних умовах безпекової нестабільності, зумовленої широкомасштабною агресією проти України, питання воєнно-економічної безпеки набуває критичного значення. Надійна оцінка поточного стану та ефективне прогнозування загроз є необхідними елементами системи національної безпеки. Сьогодні актуальними є дослідження, що поєднують як вітчизняний, так і закордонний досвід у сфері стратегічного планування оборонного сектору [1].

Вітчизняна наукова думка сформувала низку підходів до оцінювання воєнно-економічної безпеки. Наприклад, у роботах О. Барановського [2] запропоновано методологічні основи фінансової безпеки, що є основою для ширших оцінок воєнно-економічного потенціалу держави. В. Башинський та ін. [3] розробили модель прогнозування воєнних загроз, що враховує імовірні сценарії розвитку подій у регіоні.

Іншою вагомою складовою є розроблення індикаторів воєнно-економічної безпеки. І. Бабець підкреслює важливість стратегічного підходу до економічного співробітництва між Україною та ЄС, що створює додатковий рівень захисту в умовах глобальної нестабільності [4]. Системний аналіз структур безпеки, запропонований З. Гбур, зосереджується на ролі державного управління у формуванні стійкості національної економіки [5].

Міжнародний досвід також заслуговує на окрему увагу. У звітах НАТО аналізують підходи до економічної оцінки в сфері оборони, що ґрунтуються на принципах багатофакторного аналізу та адаптивного планування [6]. Подібну методику використовує Велика Британія у своїй національній стратегії безпеки з акцентом на стратегічну гнучкість і економічну витривалість [7].

Окрему увагу варто звернути на інтегровані підходи, які поєднують оцінку оборонних ресурсів, потенціалу ЗСУ та прогнозування ризиків. У праці В. Коваля та ін. проаналізовано як вітчизняну, так і закордонну практику управління оборонними ресурсами з урахуванням сучасних загроз [8]. Ці підходи дозволяють моделювати не лише поточний стан, а й варіанти розвитку безпекової ситуації у майбутньому.

Загалом, аналіз наявних підходів демонструє необхідність комплексного бачення воєнно-економічної безпеки. Поєднання кількісних методів оцінки з якісним аналізом ризиків дозволяє сформувати гнучку та адаптивну систему воєнно-економічної безпеки держави. Такий підхід відповідає викликам сьогодення та сприяє зміцненню національного потенціалу України [9]; [10].

**Методологічна основа (Methodological Framework)**

Методологічну основу дослідження воєнно-економічної безпеки України в умовах трансформаційної економіки складає системний підхід, який передбачає комплексне вивчення об’єкта в усій сукупності його взаємозв’язків, структурних компонентів та зовнішніх впливів. Воєнно-економічна безпека розглядається як багатокомпонентна система, що функціонує в складному середовищі воєнних загроз, соціально-економічної нестабільності та зовнішньополітичного тиску. Такий підхід дозволяє ідентифікувати не лише прямі, а й опосередковані чинники ризику та вразливості.

У процесі аналізу використовувалися елементи *функціонального аналізу*, що дало змогу визначити ключові функції складових системи воєнно-економічної безпеки (державного управління, оборонно-промислового комплексу, економічної політики, міжнародної взаємодії) та оцінити їхню ефективність. Для порівняльного аналізу залучено *систему*

*індикативного моніторингу*, що ґрунтується на оцінці критичних економічних і соціальних показників, які впливають на безпекову ситуацію (рівень ВВП, оборонні витрати, індекси стабільності, енергетична незалежність тощо).

Методика дослідження спирається на принципи *сценарного моделювання*, що дозволяє прогнозувати розвиток подій у коротко- та середньостроковій перспективі. Зокрема, використовувалися моделі аналізу ризиків та загроз із урахуванням факторів невизначеності, динаміки бойових дій, зміни структури економіки та поведінки зовнішніх акторів. Такий підхід забезпечив можливість розробити стратегічні варіанти реагування на потенційні виклики.

Застосовано також *діалектичний підхід*, що дозволив ураховувати суперечливу природу соціально-економічних процесів в умовах війни та перехідного періоду. Дослідження проводилося з позицій *інституційного аналізу*, що дав змогу оцінити роль державних інститутів, законодавчого забезпечення та управлінських практик у зміцненні безпеки. Особлива увага приділялася й *стратегічному підходу*, що передбачає формування довгострокового бачення цілей воєнно-економічного розвитку та їх досягнення в умовах кризових обмежень.

Методологія ґрунтується на *міждисциплінарному підході*, що охоплює економічні, політичні, військові, соціальні та технологічні аспекти безпеки. Це забезпечило комплексний аналіз проблеми та врахування широкого спектру факторів, які впливають на стійкість економіки держави в умовах війни. Теоретичним підґрунтям слугували наукові праці українських і зарубіжних фахівців, аналітичні звіти урядових структур, публікації провідних міжнародних організацій (OECD, NATO, IMF, World Bank).

З метою верифікації аналітичних висновків та рекомендацій у дослідженні застосовано *емпіричні методи*: контент-аналіз стратегічних документів, статистичний аналіз динаміки показників, порівняльний аналіз досвіду інших країн (зокрема( ) Ізраїлю, Польщі, Литви). Це дозволило обґрунтувати наукові положення роботи на практичному матеріалі та адаптувати теоретичні концепції до реалій українського безпекового простору.

Отже, методологічний підхід до дослідження воєнно-економічної безпеки України є комплексним, багаторівневим і адаптивним до динамічного середовища. Він дозволяє забезпечити об’єктивність оцінки, стратегічну орієнтацію дослідження та практичну значущість сформульованих рекомендацій.

**Результати (Results)**

Воєнно-економічна безпека України в сучасних умовах є ключовим чинником національної стабільності, особливо в контексті воєнного стану, що значно ускладнює традиційні підходи до її забезпечення. Воєнний конфлікт створює нові виклики, що мають як безпосередній вплив на економічні процеси, так і довготривалі наслідки для розвитку держави. Протистояння вимагає комплексного підходу, який поєднує військові, політичні та економічні стратегії для мінімізації загроз [3]-[9]. Важливо відзначити, що воєнно-економічна безпека не обмежується лише внутрішніми аспектами, а також передбачає зовнішньо-економічні ризики, зокрема вплив світових економічних тенденцій. У цьому контексті актуальним є врахування міжрегіонального співробітництва, що може посилити стійкість економіки. Аналіз сучасних загроз показує необхідність адаптації методологічних підходів до нових реалій воєнного часу [4]; [10]; [12].

Фінансова безпека України традиційно розглядається як одна з базових складових економічної безпеки, яка забезпечує стабільність функціонування економічної системи в цілому [2]. Особливої актуальності цей аспект набуває в умовах воєнного конфлікту, де державні фінансові ресурси перебувають під значним тиском. Важливою складовою є

прогнозування джерел фінансових ризиків, що дозволяє завчасно розробляти заходи реагування. Одночасно впровадження сучасних інформаційних технологій сприяє більш оперативному моніторингу та аналізу загроз. Дослідження також підкреслюють роль системи державного управління у підтримці фінансової безпеки, особливо в кризових ситуаціях. Отже, інтеграція фінансової безпеки у загальну систему національної безпеки залишається пріоритетом державної політики [5]; [13]-[15].

У контексті воєнного конфлікту важливим є не лише аналіз загроз, а й розроблення моделей прогнозування для мінімізації негативних наслідків. Прогнозування воєнних загроз передбачає врахування як традиційних військових аспектів, так і економічних параметрів, що безпосередньо впливають на безпеку держави. Такі моделі допомагають адаптувати оборонні стратегії до реальних викликів, сприяючи збереженню економічної стабільності. Застосування комплексних підходів до оцінювання ризиків дозволяє більш ефективно управляти ресурсами і забезпечувати цілісність економічної системи. Важливо, що ці підходи мають враховувати динаміку розвитку конфлікту та глобальні тенденції світової економіки. Тільки так можна забезпечити своєчасне реагування на потенційні загрози [1]; [3]; [9]; [16]; [17].

Проблематика забезпечення воєнної безпеки України тісно пов’язана із забезпеченням воєнно-економічної безпеки, адже обидва ці напрями взаємопов’язані [10]. Військові дії безпосередньо впливають на інвестиційний клімат, виробничі потужності та логістичні ланцюги, що в цілому створює ризики для економіки. Відповідно управління воєнно-економічними ресурсами в умовах війни потребує особливої уваги до захисту критичних галузей. Сучасні методики оцінювання рівня воєнної небезпеки дозволяють враховувати не лише військові, а й соціально-економічні чинники, що посилює комплексність підходу. Оцінка ризиків має бути оперативною та динамічною, що дасть змогу ухвалювати своєчасні управлінські рішення. Цей процес вимагає тісної співпраці між військовими та економічними структурами держави [8]; [13]; [18]; [19].

Значну роль у підтримці воєнно-економічної безпеки відіграє міжнародне співробітництво, зокрема з країнами Європейського Союзу. Інтеграція в європейський оборонно-промисловий простір створює додаткові можливості для підвищення обороноздатності та воєнно-економічної стабільності. Водночас це потребує узгодження нормативно-правової бази та адаптації національних стандартів до європейських. Міжнародна підтримка в оборонній сфері допомагає посилити ресурси для забезпечення безпеки країни. Однак для ефективної взаємодії необхідно також підвищувати рівень внутрішньої економічної стабільності. Цей баланс між зовнішніми та внутрішніми чинниками є ключовим у стратегії воєнно-економічної безпеки [16]; [20]-[22].

Важливим елементом у системі національної безпеки є державне управління економічною безпекою, що ґрунтується на теоретичних засадах і практичних інструментах. Ефективне управління потребує чіткого визначення пріоритетів, системи моніторингу і аналізу загроз. Також потрібно інтегрувати різні рівні управління – від місцевого до державного – для координації дій у сфері безпеки. Крім того, важливо враховувати специфіку воєнного стану, що змінює пріоритети та структуру управління. Адміністративні механізми мають бути гнучкими і швидко адаптуватися до змінної ситуації. Це дозволить своєчасно реагувати на нові виклики та мінімізувати їхній вплив [1]; [5]; [11]; [15]; [23].

Як зазначає В. Коваль, аналіз військових і економічних загроз свідчить про необхідність розвитку системи оборонних ресурсів, що є важливою складовою забезпечення воєнної безпеки [8]. Сучасні підходи до управління ресурсами передбачають їх ефективне розподілення та раціональне використання в умовах

обмеженості. Особливо важливою є прозорість та контроль над використанням ресурсів для запобігання корупційним ризикам. В. Горбулін підкреслює, що воєнно-економічна безпека в таких умовах не може бути забезпечена без чіткого планування і координації оборонних зусиль [15]. Відповідні механізми мають передбачати оцінку ефективності та постійне оновлення планів. Такий системний підхід дозволить зберегти баланс між військовими потребами та воєнно-економічною стабільністю.

Одним із викликів є гібридна агресія, що поєднує військові дії з економічним, інформаційним і політичним тиском. У таких умовах традиційні методи забезпечення воєнно-економічної безпеки вимагають суттєвих коректив. Необхідно розробляти комплексні моделі, які враховують мультидисциплінарний характер загроз і дозволяють швидко адаптувати стратегії. Крім того, важливо впроваджувати нові технології моніторингу та аналізу інформації. Це забезпечує своєчасне виявлення потенційних загроз та їхню нейтралізацію. Тільки комплексний підхід дозволить зберегти стійкість економіки і безпеку держави в цілому [3]; [13].

Іноземні підходи до оцінювання воєнно-економічної безпеки грунтуються на комплексних методиках, що поєднують економічний аналіз з безпековим контекстом. Зокрема, у країнах НАТО застосовують системний підхід до аналізу ресурсів, який враховує як фінансові, так і людські, технологічні та матеріальні складові обороноздатності [6]. Акцент робиться на прогнозуванні ризиків, що можуть впливати на економічну стабільність держави в умовах конфліктів. Британська національна стратегія безпеки підкреслює необхідність інтеграції економічних показників у загальну систему оцінювання безпеки для забезпечення оперативного реагування. Цей підхід дозволяє більш гнучко адаптуватися до змін у глобальному безпековому середовищі та враховувати довгострокові тенденції. Водночас у зарубіжних дослідженнях значну увагу приділяють застосуванню математичних моделей і сценарного аналізу для передбачення можливих кризових ситуацій [7]; [24].

Вітчизняні дослідники також розробляють комплексні моделі оцінки воєнно-економічної безпеки, адаптовані до специфіки національного контексту. Зокрема М. Биченков [9] пропонує інтегровану модель, що поєднує економічні, військові та політичні чинники з урахуванням сучасних викликів воєнного часу. Такі моделі забезпечують системний аналіз загроз та вразливостей, що виникають у результаті військових дій та економічних санкцій. Дослідження О. Семененка [1] фокусуються на індикаторах воєнно-економічної стабільності, які можна оперативно вимірювати та прогнозувати, що сприяє підвищенню ефективності державного управління. Цей підхід передбачає оцінку логістичних можливостей, фінансової стійкості та ресурсної бази оборонних структур. Водночас українські науковці В. Коваль, А. Тристан та ін. визнають необхідність інтеграції досвіду міжнародних партнерів для удосконалення власних методик [8].

Особливістю українських підходів є значна увага до контексту гібридної війни, що накладає специфічні вимоги на систему оцінювання безпеки. Я. Базилюк, С. Давиденко та Д. Венцковський [25] підкреслюють, що в умовах гібридної агресії важливо не лише враховувати традиційні економічні параметри, а й інформаційні та політичні аспекти, що впливають на стійкість держави. Аналіз ризиків передбачає оцінку впливу санкцій, блокад і кібератак, що суттєво ускладнює прогнозування. Застосування мультидисциплінарних підходів допомагає створити більш адекватну картину сучасної безпеки. Такий досвід є важливим для побудови адаптивних моделей, здатних враховувати динаміку військових конфліктів. Водночас підкреслюється роль національної економічної стабільності як фундаменту воєнної безпеки [2].

Закордонні практики оцінювання безпеки часто базуються на застосуванні таксономічних методів, що дозволяють систематизувати та ранжувати потенційні загрози. С. Газонянц, П. Грицай та О. Шапран [13] пропонують методику, що передбачає комплексну класифікацію факторів воєнної небезпеки за допомогою статистичних і комп'ютерних інструментів. Це сприяє підвищенню точності прогнозування і своєчасному виявленню кризових тенденцій. О. Соломицький наголошує, що в міжнародній практиці велика увага приділяється моделюванню сценаріїв розвитку подій із залученням експертних оцінок [19]. Крім того, інтеграція геополітичного аналізу з воєнно-економічними індикаторами розширює можливості прогнозування та планування оборонних заходів. Такий підхід забезпечує більш цілісне бачення безпекової ситуації [10].

Вітчизняні методики також використовують комплексний підхід, але з більшим акцентом на управлінські аспекти державної політики. З. Гбур [5] визначає державне управління економічною безпекою як ключовий елемент забезпечення стійкості національної оборони. Це включає систематичний моніторинг економічних параметрів, оцінку потенціалу оборонної промисловості та координацію з іншими секторами безпеки. Активне впровадження стратегічного планування, за словами В. Горбуліна та А. Качинського [15], сприяє узгодженню економічних ресурсів із потребами військового сектору. Важливим є також аналіз зовнішніх факторів, що впливають на внутрішню безпеку, таких як міжнародні санкції та геополітичні ризики. Такий підхід підвищує здатність держави до оперативного реагування на виклики сучасності.

Порівняльний аналіз показує, що іноземні країни більш широко використовують цифрові технології та великі дані для оцінювання безпеки, що дозволяє більш швидко реагувати на зміни. Українські науковці, зокрема Д. Кошиков [12], вказують на необхідність розвитку відповідної інфраструктури для збирання та оброблення інформації. Це особливо актуально в умовах воєнного конфлікту, коли ситуація може змінюватися миттєво. Водночас вітчизняні розробки С. Марчевського, Н. Моргуна, О. Шевчука спрямовані на оптимізацію методів аналітичної роботи, зокрема шляхом залучення міждисциплінарних команд [22]. Удосконалення цих процесів дозволить підвищити якість ухвалення управлінських рішень у сфері безпеки. Відповідність сучасним стандартам є важливою складовою реформування системи національної безпеки України.

Питання прогнозування воєнно-економічної безпеки вимагає використання інтегрованих моделей, які здатні враховувати взаємозв'язок політичних, економічних і військових чинників. О. Іляш та П. Блохін [18] акцентують на необхідності оцінки впливу збройних конфліктів на регіональну економіку, особливо у тимчасово окупованих територіях. Прогнозування в таких умовах має враховувати не лише безпосередні втрати, а й довгострокові соціально-економічні наслідки. Це дозволяє створювати більш реалістичні сценарії розвитку подій і розробляти ефективні заходи реагування. В. Богданович зауважує, що в зарубіжній практиці широко застосовуються моделі кризового менеджменту, що дають змогу адаптувати стратегії у реальному часі [14]. Такий підхід є перспективним для України в контексті постійних викликів безпеці.

Аналіз наявних методик свідчить, що як закордонний, так і вітчизняний досвід мають суттєві переваги та недоліки, які потребують інтеграції для підвищення ефективності. Українські розробки часто краще враховують специфіку внутрішніх ризиків і воєнного конфлікту, тоді як міжнародні забезпечують більш глибокий теоретичний та технологічний базис. Поєднання цих підходів дозволить створити більш універсальні й адаптивні інструменти оцінки. Крім того, розвиток міжнародної співпраці та обмін досвідом сприятимуть удосконаленню методик і підвищенню обороноздатності

держави. Важливо також розвивати систему моніторингу та своєчасного реагування на нові загрози, що виникають у воєнно-економічній сфері. Цей комплексний підхід є ключем до забезпечення стійкості національної безпеки в умовах сучасних викликів [21].

У таблиці 1 наведено порівняльний аналіз основних підходів до оцінювання та прогнозування рівня воєнно-економічної безпеки держави на основі закордонного та вітчизняного досвіду, що дозволяє виокремити ключові методологічні та практичні відмінності між ними.

**Таблиця 1.** Порівняльний аналіз підходів до оцінювання та прогнозування рівня воєнно-економічної безпеки: закордонний та вітчизняний досвід

| Параметр | Закордонний досвід | Вітчизняний досвід |
|---|---|---|
| **Основний підхід** | Системний підхід із застосуванням комплексного аналізу ресурсів, ризиків та стратегічних загроз | Комплексний підхід із урахуванням військово-політичних, економічних та інформаційних загроз |
| **Методи оцінювання** | Використання математичних моделей, сценарного аналізу, методів великої кількості даних (Big Data) | Інтегровані методики, що поєднують експертні оцінки, таксономічні та статистичні методи |
| **Основні показники** | Фінансово-економічні ресурси, технологічний рівень, оборонні потужності, людський капітал | Фінансова стійкість, логістична забезпеченість, оборонний потенціал, адаптивність до гібридних загроз |
| **Прогнозування** | Моделювання декількох сценаріїв розвитку подій з урахуванням зовнішніх і внутрішніх факторів | Оцінка впливу військових дій, санкцій, політичної нестабільності з використанням експертних та аналітичних методів |
| **Технології та інструменти** | Штучний інтелект, системи підтримки ухвалення рішень, аналітика великих даних | Оперативний аналіз ризиків, воєнно-економічні прогнози, інструменти оцінки кризових сценаріїв |
| **Основні виклики** | Швидкі зміни глобальної безпеки, нові технології ведення війни, кіберзагрози | Гібридна війна, економічна нестабільність, інформаційні та кіберзагрози |
| **Приклади країн** | США, Велика Британія, НАТО, країни ЄС | Україна, з урахуванням поточної військової агресії та економічних викликів |
| **Роль міжнародної підтримки** | Активна участь у системах колективної безпеки, обмін інформацією, координація ресурсів | Важлива роль зовнішньої допомоги та кооперації із західними партнерами |
| **Особливості впровадження** | Висока технологічність, широке застосування цифрових технологій | Орієнтація на швидку адаптацію та інтеграцію в систему національної безпеки |
| **Перспективи розвитку** | Розширення застосування штучного інтелекту та автоматизації аналізу безпекових загроз | Посилення ролі аналітики та прогнозування у реальному часі з урахуванням нових гібридних загроз |

У таблиці 2 наведено порівняльний аналіз основних методів оцінювання воєнно-економічної безпеки, що застосовуються у вітчизняній та зарубіжній практиці, з виділенням їх сильних і слабких сторін. Аналіз сильних та слабких сторін цих підходів дає змогу краще зрозуміти їх потенціал та обмеження.

Вітчизняні методи, зокрема кількісний аналіз, мають перевагу у врахуванні специфіки національної економіки та оборонної сфери. Це дозволяє формувати оцінки, які максимально відповідають реальним умовам країни. Водночас обмеженість індикаторів і недостатня їх актуалізація створюють ризик отримання застарілої або неповної інформації. Метод експертної оцінки, що широко застосовується в Україні, дозволяє включати в аналіз якісні аспекти, що важко формалізувати. Проте через

суб'єктивність оцінок та залежність від досвіду експертів результати можуть бути нестабільними та варіюватися залежно від обраної експертної групи.

**Таблиця 2.** Порівняння методів оцінювання воєнно-економічної безпеки держави: вітчизняні та зарубіжні підходи

| Метод | Сильні сторони | Слабкі сторони |
|---|---|---|
| Вітчизняний метод кількісного аналізу | Врахування специфіки національної економіки та оборони | Обмежена кількість індикаторів, які часто не оновлюються |
| Вітчизняний метод експертної оцінки | Можливість врахування якісних аспектів безпеки | Суб'єктивність оцінок, залежність від кваліфікації експертів |
| Закордонний метод системного аналізу | Комплексний підхід із використанням багатьох показників | Висока складність та вартість впровадження |
| Закордонний метод моделювання ризиків | Гнучкість і адаптивність до різних сценаріїв | Не завжди підходить для специфічних національних умов |

Зарубіжні підходи, такі як метод системного аналізу, відзначаються комплексністю та широким використанням різноманітних показників. Такий підхід забезпечує глибокий та всебічний аналіз безпекових процесів, але його впровадження потребує значних ресурсів та спеціалізованих знань. Метод моделювання ризиків характеризується високою гнучкістю, що дає змогу адаптувати оцінку до різних сценаріїв розвитку подій. Однак цей підхід не завжди може врахувати унікальні національні особливості, що обмежує його ефективність у певних контекстах.

Отже, кожен із розглянутих методів має свої переваги й недоліки. Вітчизняні моделі краще пристосовані до національних умов, але потребують модернізації і розширення інструментарію. Закордонні методи більш універсальні та гнучкі, проте вимагають значних ресурсів і адаптації до локальних реалій. Оптимальним шляхом є інтеграція найкращих практик з обох підходів для створення ефективної системи оцінювання воєнно-економічної безпеки, здатної своєчасно реагувати на сучасні виклики.

З метою комплексного аналізу підходів до оцінювання рівня воєнно-економічної безпеки доцільним є застосування SWOT-методології. Вона дозволяє виявити сильні та слабкі сторони кожного з методів, а також можливості їх подальшого вдосконалення та потенційні загрози при практичному застосуванні. Такий аналіз сприяє обґрунтованому вибору або поєднанню підходів для конкретних умов безпеки держави (таблиця 3).

Як видно з таблиці 3, кожен метод має свої переваги й обмеження. Кількісні підходи забезпечують точність, але потребують якісної статистики. Експертні оцінки враховують специфіку ситуації, однак страждають від суб'єктивності. Системний аналіз забезпечує цілісність розгляду, але є складним в реалізації. Моделювання ризиків зосереджене на попередженні загроз, тоді як комбіновані підходи дозволяють досягти балансу, хоча і потребують значних ресурсів. Вибір конкретного підходу залежить від контексту, ресурсного забезпечення та стратегічних цілей державної політики безпеки.

Підсумовуючи, воєнно-економічна безпека України у воєнний час потребує системного підходу, який передбачає прогнозування загроз, ефективне управління ресурсами, міжнародну співпрацю та розвиток методик оцінювання. Важливо, щоб усі ці компоненти працювали у взаємозв'язку, адаптуючись до швидкозмінних умов воєнного конфлікту [12]. Забезпечення такої цілісності системи є запорукою не лише стабільності, а й подальшого розвитку України [15]. Особливу увагу слід приділяти розвитку людського потенціалу та технологічних інновацій. Збалансована стратегія дасть змогу

мінімізувати економічні втрати і підвищити рівень національної безпеки [22]. Тільки на основі таких підходів Україна зможе ефективно протистояти зовнішнім і внутрішнім викликам.

**Таблиця 3.** SWOT-аналіз методів оцінювання воєнно-економічної безпеки

| Метод | Сильні сторони (Strengths) | Слабкі сторони (Weaknesses) | Можливості (Opportunities) | Загрози (Threats) |
|---|---|---|---|---|
| **Кількісний аналіз** | Висока точність за умови якісних даних; формалізація показників для порівняння між країнами | Ігнорування контексту та людського фактора; уразливість до статистичних похибок | Розвиток Big Data та аналітики; автоматизація процесів оцінювання | Нестача відкритих даних у воєнний період; можливі маніпуляції цифрами |
| **Експертна оцінка** | Можливість швидкої реакції; гнучкість у врахуванні політичних та соціальних змін | Висока суб'єктивність; залежність від репутації експертів | Міжнародна співпраця експертів; комбінування з кількісними методами | Людський фактор, емоційність; вплив політичних інтересів |
| **Системний аналіз** | Інтеграція багатьох сфер (економіка, безпека, демографія); моделювання сценаріїв розвитку ситуації | Складність розроблення моделей; високі обчислювальні вимоги | Впровадження штучного інтелекту; створення динамічних систем моніторингу | Ризик спрощень у моделюванні; складність адаптації до нових загроз |
| **Моделювання ризиків** | Акцент на прогнозування загроз; виявлення критичних точок системи | Потребує точного обліку чинників; ризик хибних сценаріїв | Розвиток сценарного аналізу; інтеграція з GIS та цифровими картами | Зміна вихідних умов веде до помилок; модель може втратити актуальність |
| **Комбіновані підходи** | Найбільш комплексний і адаптивний; зниження похибки шляхом крос-перевірки | Висока складність реалізації – Необхідність кваліфікованих кадрів | Підвищення достовірності оцінок; гнучке використання в кризових умовах | Висока вартість реалізації; неузгодженість даних із різних джерел |

**Обговорення (Discussions)**

В умовах гібридної війни та збройної агресії проти України актуалізується потреба у вдосконаленні методів оцінювання та прогнозування рівня воєнно-економічної безпеки. Вітчизняні дослідники акцентують( ) на важливості адаптації наявних методичних підходів до сучасного контексту загроз, що динамічно змінюються. Наприклад, у роботі С. Газонянца та ін. обґрунтовано застосування таксономічних методів для оцінювання рівня воєнної небезпеки, що дозволяє сформувати кількісні індикатори загроз та ризиків [13].

Водночас необхідність врахування багатовимірності безпекового середовища зумовлює використання комплексних моделей. У цьому контексті важливою є розробка М. Биченкова, що пропонує інтегративний підхід до моделювання воєнно-економічної безпеки на основі взаємозв'язку економічних та воєнних чинників [9]. Цей підхід дозволяє забезпечити цілісне розуміння загроз та визначити критичні зони економічної вразливості держави. Крім того, методичні розробки В. Башинського та колег дозволяють прогнозувати джерела воєнних

загроз із використанням інструментів ситуаційного аналізу [3], що підвищує ефективність управлінських рішень у сфері безпеки.

Іноземний досвід також свідчить про перевагу інтегрованих стратегій безпеки. Зокрема, у Національній стратегії Великої Британії наголошується на взаємозв'язку економічних, політичних та воєнних чинників у системі національної безпеки [7] НАТО, зі свого боку, активно застосовує економічний аналіз для оцінювання потенціалу держав-членів та рівня їхньої обороноздатності [6]. Ці підходи ґрунтуються на системному моніторингу індикаторів економічної стійкості та наявності стратегічних резервів, що є актуальним і для України в умовах довготривалої війни.

Попри наявність значного наукового доробку, вітчизняна система прогнозування воєнно-економічної безпеки все ще стикається з проблемами методологічної несумісності та фрагментарності. Наприклад, у дослідженні О. Семененка та ін. відзначається, що більшість наявних моделей ґрунтуються на статистичних даних мирного часу, що не враховують специфіку воєнного стану [1]. Крім того, як зауважує Д. Кошиков, для ефективного впровадження зарубіжних підходів в українських реаліях необхідна адаптація з урахуванням політичної, економічної та соціальної нестабільності [12].

Отже, обговорення свідчить про необхідність синтезу національного і зарубіжного досвіду з метою створення уніфікованої методології оцінювання та прогнозування воєнно-економічної безпеки. Цей підхід дозволить не лише підвищити стійкість національної безпекової системи до зовнішніх і внутрішніх загроз, а й створити ефективний інструмент стратегічного планування в умовах невизначеності. Подальші дослідження мають бути спрямовані на формалізацію індикаторів ризиків та створення динамічних моделей, які враховують як воєнно-політичні сценарії, так і економічні тренди.

**Висновок (Conclusion)**

Аналіз наявних підходів до оцінювання та прогнозування рівня воєнно-економічної безпеки свідчить про багатогранність проблематики та потребу в комплексному підході до формування відповідної державної політики. Вітчизняні дослідники акцентують( ) на необхідності врахування як економічних, так і воєнно-політичних чинників у контексті постійно змінюваного безпекового середовища. У цьому контексті особливого значення набуває розробка адаптивних методик та моделей, здатних оперативно реагувати на новітні виклики та загрози.

Закордонний досвід, зокрема підходи, застосовувані у НАТО та країнах ЄС, демонструє переваги стратегічного планування, аналітичного моделювання та міжвідомчої взаємодії у сфері воєнно-економічної безпеки. Такі підходи можуть бути частково імплементовані в українські реалії за умови врахування національної специфіки, зокрема загрози широкомасштабної війни та обмеженості ресурсів.

Особливу цінність становлять розробки щодо методик прогнозування джерел воєнних загроз, побудовані на системному аналізі та використанні таксономічних методів. Вони створюють підґрунтя для підвищення ефективності рішень у сфері оборонного планування та економічного управління в умовах воєнного стану.

Вітчизняні науковці також наголошують на потребі в інституціоналізації системи оцінювання воєнно-економічної безпеки, яка б поєднувала державні, академічні та оборонні структури в єдину аналітичну мережу. Лише така інтеграція може забезпечити ефективне прогнозування загроз і формування превентивних стратегій.

Отже, забезпечення належного рівня воєнно-економічної безпеки України вимагає синтезу кращих національних і міжнародних практик, удосконалення нормативно-методичної бази, а також формування гнучкої системи стратегічного реагування. Перспективним напрямом подальших досліджень є побудова динамічних моделей, які дозволять не лише

оцінювати поточний стан, а й прогнозувати довгострокові сценарії розвитку подій з урахуванням багатофакторного ризику.

**Рекомендації (Recommendations)**

Для підвищення ефективності управління воєнно-економічною безпекою в Україні доцільно розробити єдину інтегровану методику оцінювання, яка передбачатиме як кількісні, так і якісні індикатори. Така методика має враховувати специфіку гібридних загроз, динаміку зовнішньої агресії та вплив внутрішньоекономічних чинників. Створення відповідного інструментарію сприятиме своєчасному виявленню критичних дисбалансів та ухваленню превентивних рішень.

Необхідно розробити ефективну систему координації між державними органами, яка б дозволила уникати дублювання функцій та забезпечити цілісне управління воєнно-економічною безпекою. Така система має ґрунтуватися на чітко визначених повноваженнях, стандартизованих процедурах взаємодії та прозорих механізмах контролю. Забезпечення ефективної комунікації між органами виконавчої влади, силовими структурами та регіональними адміністраціями дозволить оперативно реагувати на нові виклики та загрози.

Особливу увагу слід приділяти вдосконаленню законодавчої бази у сфері воєнно-економічної безпеки. На сьогодні багато нормативних актів є застарілими або не відповідають сучасним умовам війни та глобалізаційних викликів. Доцільно провести системний аудит чинного законодавства та гармонізувати його з європейськими стандартами, забезпечивши при цьому правову гнучкість у кризових ситуаціях.

Важливо також розширити інструменти стратегічних комунікацій, які спрямовані на формування суспільної стійкості. Населення має бути проінформоване про основні загрози, напрями державної політики у сфері безпеки та механізми власної участі у її забезпеченні. Це сприятиме зростанню довіри до інституцій та мобілізації громадянського потенціалу на підтримку обороноздатності держави.

В умовах тривалого військового конфлікту особливої актуальності набуває розвиток воєнної економіки як окремого напряму економічної політики. Йдеться про стимулювання внутрішнього виробництва озброєння, модернізацію оборонно-промислового комплексу, розвиток подвійних технологій та локалізацію виробничих потужностей. Такий підхід дозволить зменшити залежність від імпорту та забезпечити потреби Збройних Сил України у стратегічній перспективі.

Доцільно розробити регіональні програми зміцнення безпеки, які враховуватимуть особливості прикордонних територій, зон підвищеної загрози та тимчасово окупованих регіонів. Такий децентралізований підхід дозволить адаптувати загальнодержавну політику до локальних умов і підвищити ефективність реалізації заходів безпеки на місцях.

Варто налагодити системну взаємодію з вітчизняним бізнесом, зокрема шляхом запровадження державно-приватного партнерства у сфері безпеки. Бізнес-структури можуть брати участь у забезпеченні критичної інфраструктури, кіберзахисті, логістиці та фінансуванні оборонних ініціатив. Для цього потрібно створити стимули та гарантії участі приватного сектору в реалізації безпекових програм.

У перспективі необхідно ініціювати створення Національної стратегії воєнно-економічної безпеки, яка б охоплювала всі ключові напрями: оборону, економіку, інфраструктуру, енергетику, інформаційний простір. Такий стратегічний документ має бути результатом консолідованої роботи всіх гілок влади, наукового середовища, громадянського суспільства та міжнародних партнерів, із чітким визначенням пріоритетів, ресурсів і механізмів контролю за її реалізацією.

**Використані джерела**

1. Семененко, О., Бойко, Р., Воронченко, І., & Таран, О. (2023). Оцінювання рівня воєнно-економічної безпеки країн світу та України. *Збірник наукових праць Центру воєнно-стратегічних досліджень ЗС України*, 2(79), 62–72. https://znp-cvsd.nuou.org.ua/article/view/267215.
2. Барановський, О. І. (2004). *Фінансова безпека в Україні (методологія оцінки та механізм забезпечення)*. Київ: Київський національний торговельно-економічний університет.
3. Башинський, В. Г., Клят, Ю. О., & Тристан, А. В. (2022). Методичний підхід до прогнозування джерел воєнних загроз для забезпечення воєнної безпеки України. *Теорія і практика управління соціальними системами*, (2), 13–21. https://dndivsovt.com/index.php/ts/article/view/487.
4. Бабець, І. Г. (2013). Концептуальні засади стратегії економічної безпеки інтеррегіонального співробітництва України з країнами ЄС. *Науковий вісник Львівського державного університету внутрішніх справ. Серія економічна*, (1), 3–13.
5. Гбур, З. В. (2018). *Державне управління економічною безпекою України: теорія та практика*. Кам'янець-Подільський: ТОВ «Друкарня «Рута».
6. NATO. (n.d.). Economic analysis at NATO. http://www.nato.int/cps/en/natohq/topics_400.htm.
7. HM Government. (2010). A strong Britain in an age of uncertainty: The national security strategy. Ministry of Defence of the United Kingdom. http://www.official-documents.gov.uk.
8. Коваль, В. В., Тристан, А. В., Скуріневська, Л. В., & Щерблюк, С. Л. (2023). Моделі та методи в управлінні оборонними ресурсами: монографія. Київ: Генеральний штаб Збройних Сил України.
9. Биченков, М. В. (2022). *Комплексна модель економічної безпеки України* (магістерська дисертація). КПІ ім. Ігоря Сікорського. https://ela.kpi.ua/items/4cf5f20a-afe6-4d9a-bad6-8ba88a0fd20d.
10. Богданович, В., Муженко, В., & Луцький, О. (n.d.). Концепція забезпечення воєнної безпеки України на основі оцінювання та прогнозування ризиків реалізації кризових сценаріїв. *Збірник наукових праць. Серія: Військові та технічні науки НАДПСУ*, 4–19.
11. Актуальні виклики та загрози економічній безпеці України в умовах воєнного стану. (2023). *Національний інститут стратегічних досліджень*. https://niss.gov.ua/publikatsiyi/analitychni-dopovidi/aktualni-vyklyky-ta-zahrozyekonomichniy-bezpetsi-ukrayiny-v.
12. Кошиков, Д. О. (2021). Зарубіжний досвід оцінювання економічної безпеки: основні підходи та можливості для України. *Вісник Харківського національного університету внутрішніх справ*, 3(94), 75–83. https://dspace.univd.edu.ua/items/119140b9-6be2-4875-a8f8-0d4e477ab5d1.
13. Газонянц, С. Ю., Грицай, П. М., & Шапран, О. О. (2019). Загальні положення методики оцінювання рівня воєнної небезпеки на основі таксономічних методів. *Сучасні інформаційні технології у сфері безпеки та оборони*, 34(1), 29–36. https://doi.org/10.33099/2311-7249/2019-34-1-29-36.
14. Богданович, В. Ю. (2003). *Воєнна безпека України: методологія дослідження та шляхи забезпечення*. Київ: Тираж.
15. Горбулін, В. П., & Качинський, А. Б. (2023). *Стратегічне планування: вирішення проблем національної безпеки*. Київ: НІСД.
16. Коваленко, Т. (2022). *Роль міжнародної підтримки в забезпеченні обороноздатності України*. Київ: Видавництво Національної академії наук України.
17. Болтян, О. (2023, June 27). Світ озброюється: три фактори, що вплинуть на глобальну та українську економіки. https://zn.ua/ukr/macroeconomics/svit-ozbrojujetsja-tri-faktori-shcho-

vplinut-na-hlobalnu-ta-ukrajinsku-ekonomiki.html.
18. Іляш, О. І., & Блохін, П. В. (2021). Емпіричне оцінювання впливу збройного конфлікту на стан економічної безпеки тимчасово окупованих Донецької та Луганської областей. http://www.econom.stateandregions.zp.ua/journal/2021/4_2021/5.pdf.
19. Соломицький, О. І. (кер.). (2024). *Імовірні сценарії та прогнозування дій російської федерації у війні на період до 2027 року: звіт про оперативне завдання (заключний)*. ЦНДІ ЗС України.
20. Горбулін, В. П., Шеховцев, В. С., & Шевцов, А. І. (2015). Входження ОПК України в європейський оборонно-промисловий простір. *Стратегічні пріоритети*, (4), 5–11.
21. Центр досліджень армії, конверсії та роззброєння. (n.d.). *Потенціали співробітництва України з ЄС у сфері безпеки*. https://www.kas.de/c/document_library/get_file?uuid=3c38095e-4b0b-26e6.
22. Марчевський, С. В., Моргун, Н. С., & Шевчук, О. О. (2023). Зарубіжний досвід забезпечення економічної безпеки держави правоохоронними органами. *Вісник Ужгородського національного університету. Серія: Право*, 73(1), 102–108. https://visnyk-pravo.uzhnu.edu.ua/article/view/268579.
23. Богма, О. С. (2016). Діалектика та синергетика у дослідженні категорій “безпека” та “економічна безпека”. *Економічний вісник Запорізької державної інженерної академії*, (4)1, 7–10.
24. Мунтіян, В. І. (1998). *Економіка та оборонні витрати: аналіз зарубіжних досліджень і український шлях розвитку*. Київ: Науково-дослідний фінансовий інститут при Міністерстві фінансів України.
25. Базилюк, Я. Б., Давиденко, С. В., & Венцковський, Д. Ю. (2017). *Економічна безпека України в умовах гібридної агресії: аналітична доповідь*. Київ: НІСД.

**References**

1. Semenenko, O., Boiko, R., Voronchenko, I., & Taran, O. (2023). Assessment of the level of military-economic security of countries around the world and Ukraine. *Collection of Scientific Works of the Center for Military-Strategic Studies of the Armed Forces of Ukraine*, *2*(79), 62–72. https://znp-cvsd.nuou.org.ua/article/view/267215.
2. Baranovs'kyi, O. I. (2004). *Financial security in Ukraine (assessment methodology and assurance mechanism)*. Kyiv: Kyiv National University of Trade and Economics.
3. Bashynskyi, V. H., Kliat, Yu. O., & Trystan, A. V. (2022). Methodological approach to forecasting sources of military threats for ensuring military security of Ukraine. *Theory and Practice of Social Systems Management*, (2), 13–21. https://dndivsovt.com/index.php/ts/article/view/487.
4. Babets, I. H. (2013). Conceptual foundations of the economic security strategy for interregional cooperation between Ukraine and EU countries. *Scientific Bulletin of Lviv State University of Internal Affairs. Economic Series*, (1), 3–13.
5. Hbur, Z. V. (2018). *State management of economic security of Ukraine: theory and practice*. Kamianets-Podilskyi: Ruta Printing House LLC.
6. NATO. (n.d.). Economic analysis at NATO. http://www.nato.int/cps/en/natohq/topics_400.htm.
7. HM Government. (2010). *A strong Britain in an age of uncertainty: The national security strategy*. Ministry of Defence of the United Kingdom. http://www.official-documents.gov.uk.
8. Koval, V. V., Trystan, A. V., Skurinevska, L. V., & Shcherbliuk, S. L. (2023). *Models and methods in defense resource management: monograph*. Kyiv: General Staff of the Armed Forces of Ukraine.
9. Bychenkov, M. V. (2022). *Comprehensive model of economic security of Ukraine* (Master's thesis). Igor Sikorsky Kyiv Polytechnic Institute. https://ela.kpi.ua/items/4cf5f20a-afe6-4d9a-

bad6-8ba88a0fd20d.
10. Bohdanovych, V., Muzhenko, V., & Lutskyi, O. (n.d.). Concept of ensuring military security of Ukraine based on assessing and forecasting risks of crisis scenarios implementation. *Collection of Scientific Works. Series: Military and Technical Sciences of NADPSU*, 4–19.
11. *Current challenges and threats to economic security of Ukraine in conditions of martial law*. (2023). National Institute for Strategic Studies. https://niss.gov.ua/publikatsiyi/analitychni-dopovidi/aktualni-vyklyky-ta-zahrozyekonomichniy-bezpetsi-ukrayiny-v.
12. Koshykov, D. O. (2021). Foreign experience in assessing economic security: main approaches and opportunities for Ukraine. *Bulletin of Kharkiv National University of Internal Affairs*, *3*(94), 75–83. https://dspace.univd.edu.ua/items/119140b9-6be2-4875-a8f8-0d4e477ab5d1.
13. Hazoniants, S. Yu., Hrytsai, P. M., & Shapran, O. O. (2019). General provisions of the methodology for assessing the level of military danger based on taxonomic methods. *Modern Information Technologies in Security and Defense*, *34*(1), 29–36. https://doi.org/10.33099/2311-7249/2019-34-1-29-36.
14. Bohdanovych, V. Yu. (2003). *Military security of Ukraine: research methodology and ways of ensuring*. Kyiv: Tyrazh.
15. Horbulin, V. P., & Kachynskyi, A. B. (2023). *Strategic planning: solving national security problems*. Kyiv: NISD.
16. Kovalenko, T. (2022). *The role of international support in ensuring Ukraine's defense capability*. Kyiv: Publishing House of the National Academy of Sciences of Ukraine.
17. Boltyan, O. (2023, June 27). *The world is arming: three factors that will affect the global and Ukrainian economies*. https://zn.ua/ukr/macroeconomics/svit-ozbrojujetsja-tri-faktori-shcho-vplinut-na-hlobalnu-ta-ukrajinsku-ekonomiki.html.
18. Iliash, O. I., & Blokhin, P. V. (2021). *Empirical assessment of the impact of armed conflict on the economic security of the temporarily occupied Donetsk and Luhansk regions*. http://www.econom.stateandregions.zp.ua/journal/2021/4_2021/5.pdf.
19. Solomytskyi, O. I. (superv.). (2024). *Probable scenarios and forecasting of the actions of the Russian Federation in the war for the period until 2027: report on the operational task (final)*. CSDI AF of Ukraine.
20. Horbulin, V. P., Shekhovtsev, V. S., & Shevtsov, A. I. (2015). Ukraine's defense industry integration into the European defense-industrial space. *Strategic Priorities*, (4), 5–11.
21. Center for Army, Conversion and Disarmament Studies. (n.d.). *Potentials of Ukraine's cooperation with the EU in the security sphere*. https://www.kas.de/c/document_library/get_file?uuid=3c38095e-4b0b-26e6.
22. Marchevskyi, S. V., Morhun, N. S., & Shevchuk, O. O. (2023). Foreign experience in ensuring economic security of the state by law enforcement agencies. *Bulletin of Uzhhorod National University. Series: Law*, *73*(1), 102–108. https://visnyk-pravo.uzhnu.edu.ua/article/view/268579.
23. Bohma, O. S. (2016). Dialectics and synergetics in the study of categories "security" and "economic security". *Economic Bulletin of Zaporizhzhia State Engineering Academy, (4)1*, 7–10.
24. Muntian, V. I. (1998). *Economy and defense expenditures: analysis of foreign research and Ukrainian path of development*. Kyiv: Research Financial Institute under the Ministry of Finance of Ukraine.
25. Bazyliuk, Ya. B., Davydenko, S. V., & Ventskovskyi, D. Yu. (2017). *Economic security of Ukraine in conditions of hybrid aggression: analytical report*. Kyiv: NISD.

The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 3 No. 2 (2025)

# Analysis of Existing Approaches to Assessing and Forecasting the Level of Military-Economic Security of the State: Foreign and Domestic Experience

**Ivan Havryliuk**
Candidate of Military Sciences, Senior Researcher
First Deputy Minister of Defence of Ukraine
Ministry of Defence of Ukraine
e-mail: ivan_havryliuk@ukr.net
ORCID: 0000-0002-3514-0738

**Abstract.** The relevance of studying approaches to assessing and forecasting the level of military-economic security of the state is due to the growth of global threats, hybrid wars and economic pressure, which transform traditional ideas about national security. In this context, a comparative analysis of foreign and domestic experience becomes particularly important, as it allows for the identification of effective methodological approaches and tools to strengthen the state's security potential. The study of international practices allows us to adapt proven models of ensuring military-economic security to Ukrainian realities, increasing the state's ability to respond to threats in a timely manner and ensure stability in critical conditions.

The methodological basis of the study was the systemic, functional, strategic, institutional, dialectical and interdisciplinary approaches. Scenario modeling, indicative monitoring, empirical methods (content analysis, statistical analysis, comparative studies) were used for the analysis. This provided a comprehensive vision of the structure of military-economic security and the factors affecting its stability.

The purpose of the article is to analyze existing approaches to assessing and forecasting the level of military-economic security of Ukraine in the conditions of a transformational economy and prolonged military aggression. In addition, to identify the main threats, determine structural imbalances and justify the feasibility of creating an integrated system of military-economic security management based on strategic forecasting, innovative development and international cooperation.

The results of the study indicate the feasibility of integrating domestic and foreign experience in assessing and forecasting the level of military-economic security of the state. It was found that Ukrainian models better take into account the realities of hybrid warfare, while international practices are distinguished by technological perfection and methodological structuring. The analysis made it possible to determine the advantages of a systemic approach, multidisciplinary analysis and scenario modeling as the basis for the formation of adaptive strategies of military-economic security.

The conclusions emphasize the need to strengthen the institutional capacity of the state, modernize the legislative framework and establish partnerships with NATO and EU member states. Practical recommendations have been developed to optimize defense spending, stimulate national production and increase the efficiency of the use of international aid.

The practical value of the work lies in the possibility of applying the results of the study in the formation of state policy in the field of national security, the development of strategies for military-economic stability and the adoption of management decisions in conditions of martial law and post-conflict recovery.

**Keywords:** military-economic security, national security, transformational economy, strategic management, defense-industrial complex, risks, scenario modeling, security policy.

The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 3 No. 2 (2025)

DOI: 10.62524/msj.2025.3.15

# Кібертехнології та математичне моделювання для пришвидшення петлі Джона Бойда в асиметричній війні

**Світлана Зварич**
кандидат технічних наук, старший дослідник
провідний науковий співробітник
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: zvarych.ss@gmail.com
ORCID: 0000-0002-0636-250X

**Руслан Хомчак**
доктор військових наук, старший дослідник
перший заступник секретаря РНБОУ
01014, вулиця Петра Болбочана, 8, Київ, Україна
e-mail: khomchakk@ust.hk.com.cn
ORCID: 0000-0002-8492-7510

**Анатолій Зварич**
кандидат військових наук, старший дослідник
провідний науковий співробітник
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: zvarych_ao@ukr.net
ORCID: 0000-0002-7136-0295

**Наталя Коркіна**
старший науковий співробітник наукового центру
Військова академія (м.Одеса)
65009, Фонтанська дорога, 10, Одеса, Україна
e-mail: natakorkina1978@gmail.com
ORCID: 0009-0004-8920-0363

**Анотація.** Актуальність статті обумовлена тим, що російсько-українська війна за всіма ознаками є асиметричною і досягти перемоги у ній виключно стандартним силовим протистоянням на полі бою неможливо. Для виграшу у такій війні стороні, що поступається у людських і технічних ресурсах, необхідно застосовувати нові стратегії і тактики, нові технологічні рішення. Одним із таких рішень є застосування кібертехнологій та математичного моделювання для пришвидшення проходження петлі Бойда в асиметричні війни.

Метою статті є висвітлення напрямів використання кібертехнологій та математичного моделювання для пришвидшення проходження петлі Джона Бойда в асиметричній війні.

Основним підходом до розгляду цієї проблеми визначено дослідження на основі концепції Джона Бойда якості управління військами, яка дає можливість найкраще використовувати свої переваги та зменшувати значущість переваг ворога.

У статті розглянуто напрями використання кібертехнологій, а також систем математичного моделювання, на всіх етапах “петлі Бойда”, а саме: спостереження, орієнтації, рішення, дії. Зазначено, що на етапі спостереження варто використовувати системи збирання,

зберігання та передавання значних обсягів інформації, які можна використовувати для аналізу та структурування інформації. Такий підхід дозволить на етапі орієнтації (за рахунок зекономленого часу і використовуючи кібертехнології та математичне моделювання) сформувати сукупність альтернативних варіантів раціонального вирішення завдання замість одного, що підвищить якість рішення, яке буде прийняте в подальшому.

На етапі прийняття рішень варто використовувати системи підтримки прийняття рішень різного рівня (тактичний, оперативний, стратегічний). Важливо, щоб математичні моделі, закладені в такі системи різного рівня, були узгоджені між собою за вхідними і вихідними даними, завданнями і часом їх вирішення. Такий підхід дасть можливість розробляти в прийнятні терміни каскад узгоджених рішень (на різних рівнях), які уточнюватимуть та доповнюватимуть одне одного. На етапі дій забезпечується виконання рішення (каскаду рішень). Використання кібертехнологій на цьому етапі допоможе скоротити час між прийняттям рішення та його реалізацією.

У статті наведено перелік програмних продуктів, які уже використовуються у Збройних Силах України на всіх зазначених вище етапах, і вказано на їхню несумісність між собою та відсутність інтеграції з автоматизованими системами управління, що використовуються на оперативному і стратегічному рівнях.

Результати статті доцільно використати під час створення нових та удосконалення наявних систем підтримки прийняття рішень різного рівня (тактичний, оперативний, стратегічний) та автоматизованих систем управління. У перспективі доцільно об’єднати наявні програмні продукти в єдину систему (та нарощувати її), в якій усі математичні моделі мають бути сумісними між собою, користуватись єдиними протоколами оброблення даних, обміну ними, стандартами збереження тощо та готувати (синтезувати) характеристики й управляючі параметри одні для одних.

**Ключові слова**: асиметрична війна, петля Джона Бойда, кібертехнологія, математичне моделювання, система ситуаційної обізнаності, система підтримки прийняття рішення.

**Вступ (Introduction)**

російсько-українська війна за всіма ознаками підпадає під визначення асиметричної: ми значно поступаємось росії як у людських, так і в технічних ресурсах.

Специфіка асиметричної війни передбачає необхідність нестандартних дій та використання новітніх технологій для перемоги над супротивником. Значно поступаючись противнику в силі, неможливо виграти асиметричну війну виключно стандартним військовим протистоянням на полі бою. Тут важливу роль відіграють стратегії, які б компенсували цю різницю: дезінформація, дезорганізація ворога, диверсії, таємні спецоперації, нестандартні дії та ін. В останні десятиріччя асиметрія набула нових рис завдяки технічному прогресу: використання дронів різного базування та призначення, інформаційних і кібертехнологій, систем математично моделювання. Раз за разом супротивники використовують нові стратегії й тактики, застосовують нові технологічні рішення. Загалом аналіз досвіду ведення бойових дій під час відсічі збройній агресії рф проти України свідчить про здійснення трансформації форм та способів бойового застосування військ (сил) і зброї (бойових засобів). Така трансформація і широке використання новітніх технологічних та інноваційних рішень обумовлюють необхідність фундаментального перегляду вимог щодо управління**.** Це стосується насамперед необхідності забезпечення оперативного управління сукупністю динамічних процесів, що взаємопов’язані між собою та мають розподілений характер.

Отже, дослідження впливу сучасних технологій, зокрема кібертехнологій та математичного моделювання, на ефективність управління в асиметричної війни є актуальним науковим завданням.

**Методологічна основа (Methodological Framework)**

Дослідники з давніх часів задавались питанням: чому в деяких асиметричних конфліктах виграє слабша, з точки зору матеріальної та людської сили, сторона [1].

Ключовим у відповіді на це питання, на думку науковців Інституту стратегічних досліджень США [2], є "вміння діяти, організовувати свою діяльність та мислити відмінним від опонентів чином з метою максимізації власних переваг та використання вразливих місць опонента, захоплення ініціативи чи забезпечення простору для маневрування".

Американський військовий теоретик Джон Бойд ще у 1995 році довів, що у великій війні причина поразки або перемоги – це не набір матеріальних або моральних факторів самих по собі, не загальна кількість людей, зброї, ресурсів, не психологічний стан або соціальні умови. Передусім – це якість управління, яка дає можливість використати свої переваги та зменшувати значущість переваг противника, тобто діяти швидше та компетентніше за ворога [3].

Згідно з концепцією Д. Бойда [4] усі процеси, які відбуваються на полі бою, здійснюються у безперервному циклі, відомому як "петля Бойда" або цикл СОРД (Спостереження-Орієнтація-Рішення-Дія), постійно взаємодіють із навколишнім середовищем і враховують його зміни, зокрема дії противника. Кожна зі сторін, які вступають у воєнний конфлікт, діє і приймає свої рішення в межах своєї петлі Бойда. Знаючи цей принцип та прогнозуючи можливі дії противника (його петлі Бойда під час управління), можна досягти перемоги, зробивши свої цикли дій швидшими або покращивши якість своїх рішень. У першому випадку ми можемо діяти на випередження та змусити противника реагувати на наші дії (у тому числі, добитись погіршення його рішень через нестачу часу). У другому випадку – прийняти рішення, які краще відповідають даній ситуації, ніж рішення противника, або добитися погіршення рішень з його боку.

Приймаючи рішення на випереджувальні дії, завжди слід мати на увазі, що швидкі, але неадекватні або погано прораховані дії можуть призвести до негативних наслідків. Водночас, найкращі рішення, але прийняті запізно, не допоможуть нам досягти своїх цілей. Отже, постійно потрібно тримати під контролем як якість рішень, що приймаються, так і час їх прийняття та виконання. У цьому може допомогти застосування кібертехнологій та математичного моделювання на всіх етапах циклу СОРД.

Під кібертехнологіями мають на увазі сукупність цифрових, інформаційних та комунікаційних технологій, що забезпечують збирання, оброблення, зберігання, передавання та захист інформації в кіберпросторі.

Етап спостереження передбачає збирання ключової інформації, необхідної для прийняття рішень в конкретному випадку. Найчастіше це дані про стан та розміщення військ (сил): як противника, так і своїх. Джерела інформації можуть бути внутрішніми та зовнішніми, можуть мати різноманітну фізичну природу. Як наслідок й інформація може бути описовою, цифровою або логічною. Немає значення, в якому вигляді надійшла інформація, важливо, щоб після оброблення вона була доступна та зрозуміла для тих, хто її потребує, на всіх рівнях. Для цих цілей варто використовувати системи збирання, зберігання та передавання інформації, користувачі якої об'єднані в єдину мережу. У такому випадку дані, оновлені одним із користувачів або засобів, миттєво стають доступними іншим. Це значно прискорить прийняття узгоджених рішень з урахуванням швидких змін інформації. Наприклад, використання дронів для спостереження за пересуванням ворожих колон дозволяє передавати дані на командний пункт практично миттєво.

Етап орієнтації, як правило, поділяють на два підетапи: аналізу та синтезу. Аналіз даних та створення ситуаційної обізнаності як про стан та можливості своїх військ, так і противника, дають можливість прогнозувати та планувати подальший розвиток подій. Наприклад, алгоритми штучного інтелекту можуть прогнозувати ймовірні напрямки атаки противника на

підставі аналізу його попередніх маневрів. Якщо за допомогою використання додаткових модулів процес аналізу даних об'єднати з етапом їх спостереження, то, маючи постійне оновлення даних про ситуацію на полі бою, можна миттєво структурувати інформацію та аналізувати зміни. Зекономлений час дасть змогу на етапі синтезу рішення сформувати сукупність альтернативних варіантів раціонального вирішення завдання замість одного, що підвищить якість рішення, яке буде прийняте у подальшому.

Етап прийняття рішення передбачає вибір альтернатив і планів на базі їхньої сукупності, яку було розроблено на етапі орієнтації. Критерії вибору залежать від мети конкретної операції (бою). На цьому етапі доцільно використовувати системи підтримки прийняття рішення (СППР), вхідними даними для яких є інформація, отримана на попередніх двох етапах. Важливо, щоб СППР (математичні моделі, що в них закладені) на різних рівнях (тактичний, оперативний, стратегічний) були узгоджені між собою. Це означає, що потрібно мати не просто набір різних математичних моделей, а систему моделей, які як вихідні дані використовують ідентичну інформацію і готують одні для одних необхідні характеристики та управляючі параметри. Такий підхід дозволить здійснювати прискорений аналіз великої кількості варіантів розвитку подій і розробляти в прийнятні терміни каскад узгоджених рішень (на різних рівнях), які уточнюватимуть та доповнюватимуть одне одного.

Етап дій передбачає забезпечення виконання рішення (каскаду рішень). Використання автоматизованих систем управління, кібертехнологій на цьому етапі допоможе скоротити час між прийняттям рішення та його реалізацією.

Використання кібертехнологій і математичного моделювання на всіх етапах дасть змогу забезпечити формування єдиного інформаційного середовища і досягти стану ситуаційної обізнаності на нашу користь та суттєво покращити процеси узагальнення, актуалізації, генерування, розподілу та доведення інформації, підвищити її якість та достовірність. Це сприяє досягненню інформаційної переваги і дає змогу результативно координувати дії підлеглих військ (сил) для підвищення ефективності процесів управління та в цілому досягнення мети проведення операції (бойових дій) в умовах відсутності стратегічної переваги у силах і засобах.

**Результати (Results)**

Застосування кібертехнологій та (або) математичного моделювання на кожному з етапів петлі Дж. Бойда в асиметричній війні може значно зменшити їхню тривалість, покращити якість прийнятих рішень та їх виконання. Для найкращого ефекту доцільно мати та використовувати взаємопов'язані системи збирання, аналізування, зберігання та передавання даних, а також систему математичних моделей різного рівня й призначення, які використовують підготовлені дані.

**Обговорення (Discussions)**

Більше десятка програмних продуктів та автоматизованих систем управління різного походження та з різними можливостями вже зараз допомагають нашим військам якісно виконувати свої завдання на полі бою та краще планувати операції у штабах (див. рис. 1).

Штаби та окремі посадові особи використовують ті програми, які більше підходять для їхніх завдань. Зокрема, "Кропива" зайняла нішу на тактичному рівні [9]. Завдяки їй у нас одна з найточніших артилерій у світі. GisArta із офлайн-карти переросла у систему ситуаційної обізнаності. "Броня" – система ураження цілей із закритих позицій, дозволяє стріляти без прямої видимості ворога.

Система "Віраж-планшет" є автоматизованою системою, яка збирає, аналізує та узагальнює інформацію про повітряну та надводну обстановку в інтересах підрозділів протиповітряної оборони Збройних Сил України [14].




**Рисунок 1.** Програмні продукти, що використовуються українськими військами

**Джерело:** Forbes [5]

Система ситуаційної обізнаності Delta [11] – збирає інформацію з різноманітних джерел, таких як безпілотники, знімки супутників, радіоперехоплення та чат-боти, які можуть наповнюватись будь-ким. Також вона може приймати розвіддані з системи ситуативної обізнаності НАТО.

Усі волонтерські програми розроблялися за принципом "знизу вгору", швидко реагуючи на запити військових. Тому наявні автоматизовані інформаційні системи та системи управління значно допомагають прискорити прийняття рішень та покращити їхню якість на всіх етапах циклу СОРД тактичного рівня.

Таке різноманіття та децентралізація програмних продуктів для армії мають як свої плюси, описані вище, так і мінуси. Системи, як правило, покривають проблеми тактичного рівня, допомагають військовим швидше та точніше виконувати завдання безпосередньо на полі бою. Проте Україні також потрібна система для штабів оперативного та стратегічного рівнів, до якої б стікалась інформація з усіх військ. Сьогодні на таку роль претендують система ситуаційної обізнаності Delta та прийняті на озброєння автоматизовані системи управління "Дзвін АС" [12], "Ореанда ПС".

Однак системи, якими користуються на тактичному рівні, не сумісні між собою та з тими, що використовуються у штабах. Це призводить до неможливості обміну даними та проведення моделювання операцій (бойових дій) в єдиному інформаційному середовищі. Для вирішення цієї та інших проблем сумісності необхідні єдині правила для всіх: протокол шифрування даних, обміну ними, стандарти щодо збереження даних тощо. Кожна система має бути ідентифікована і мати можливість щодо інтеграції (спільної роботи) за єдиними правилами з основною системою – ядром найвищого рівня.

Також мають бути розроблені методики, у тому числі з використанням штучного інтелекту, які б дозволяли, аналізуючи та узагальнюючи накопичену інформацію з поля бою, отримувати необхідні характеристики (коефіцієнти) та управляючі параметри для моделей (аналітичні, Ланчестеровські, масового обслуговування, на базі рівнянь Колмогорова), які використовуються у системах підтримки прийняття рішень штабів оперативного та стратегічного рівня.

Комплексне використання зазначених і нових систем створює передумови для технологічної переваги в ситуаційній обізнаності та досягнення синергетичного ефекту від застосування сучасних інтегрованих систем математичного моделювання й автоматизованих систем управління. [5–14]. Більшість цих продуктів розроблені волонтерами, але є й ті, які офіційно стоять на озброєнні.

**Висновок (Conclusion)**

В Україні є значні можливості для використання кібертехнологій та математичного моделювання для пришвидшення проходження петлі Джона Бойда в асиметричній війні з рф. На цей час найбільше вони задіяні на тактичному рівні. Проте необхідно мати не набір розрізнених інформаційних програм та автоматизованих систем, а їхню систему. У такій системі всі складові мають бути сумісними між собою, користуватись єдиними протоколами шифрування даних, обміну ними, стандартами збереження тощо та виробляти (синтезувати) характеристики й управляючі параметри одні для одних.

**Рекомендації (Recommendations)**

У перспективі доцільно створити організаційні структури для забезпечення експлуатації автоматизованих систем та використання систем моделювання, продовжувати створювати та розширювати державні стандарти щодо розроблення моделюючих програм (інформаційно-управляючих систем) у військовій сфері, які б дозволяли різноманітним системам бути сумісними, але водночас не обмежували б використання під час їх розроблення нових технологічних можливостей.

**Використані джерела**

1. Леонов, В. В. & Воровичˌ Б. О. (2016). Парадокс асиметрії в сучасних міжнародних збройних конфліктах. *Збірник наукових праць Центру воєнно-стратегічних досліджень НУОУ, 1* (56), 29–34.
2. Steven, Metz, & Douglas, Jonson. (2001). P. 5. *Asymmetry and US Military Strategy: Definition Background and Strategic Concepts*. Strategic Studies Institute.
3. Angerman, W. S. (2004). *Coming full circle with Boyd`s OODA loop ideas: an analysis of innovation diffusion and evolution.* Air Force Institute of Technology.
4. Ian T. Brown. (2018). *A new conception of war*. Quantico, VA.
5. Мельник, Т. (2022*). IT-хаос на службі ЗСУ*. Forbes. http://forbes.ua/innovations/it-khaos-na-sluzhbi-zsu.
6. Іванова, К. (2024). *DELTA, "Кропива" та "Віраж-планшет": які системи стали найпопулярнішими у військових.* https://speka.media/delta-kropiva-i-virazh-planshet-yaki-sistemi-stali.
7. *"Секретна система" допомагає ЗСУ отримувати інформацію про російські дрони та літаки*. (2023). Фокус. https://focus.ua/uk/digital/569874-sekretna-sistema-dopomagaye-zsu.
8. *Інновації для армії. Система "Кропива" та карти Армії SOS*. (2015). https://life.pravda.com.ua/society/2015/08/11/198416.
9. *Бойова система управління тактичної ланки "Кропива".* Конструкторське бюро "Логіка". https://logica.ua/avtomation-systems.
10. Мельник, Т. (2022). *Жалюча "Кропива". Як українське програмне забезпечення для артилеристів впливає на перебіг війни.* https://forbes.ua/innovations/zhalucha-kropiva-yak-ukrainske-programne.
11. Мельник, Т. (2023*). Військовий софт Delta тепер офіційно у ЗСУ.* Forbes. http://forbes.ua/innovations/twitter-dlya-zsu-viyskoviy-soft-delta.
12. *"Дзвін" на практиці: командувачі Сухопутних військ та ОК "Північ" оцінили роботу нової АСУВ.* (2020). Defense Express. https://web.archive.org/web/20200528030700/https://defence-ua.com.
13. *Бойова система управління тактичної ланки "Кропива" на службі ЗСУ та НГУ*. (2020). Defense Express. https://web.archive.org/web/20200708072928/https://defence-ua.com.
14. *Методичні рекомендації використання спеціалізованого програмного забезпечення "Віраж-планшет" під час підготовки бойових обслуг підрозділів зенітних ракетних військ Повітряних сил Збройних Сил України.* (2019). Центр оперативних стандартів і методики підготовки Збройних Сил України спільно з командуванням Повітряних Сил Збройних Сил України.

**References**

1. Leonov, V. V. & Vorovych, B. O. (2016). Paradoks asymetrii v suchasnykh mizhnarodnykh zbroinykh konfliktakh. *Zbirnyk naukovykh prats Tsentru voienno-stratehichnykh doslidzhen NUOU, 1* (56), 29–34.
2. Steven, Metz, & Douglas, Jonson. (2001). P. 5. *Asymmetry and US Military Strategy: Definition Background and Strategic Concepts.* Strategic Studies Institute.
3. Angerman, W. S. (2004). *Coming full circle with Boyd`s OODA loop ideas: an analysis of innovation diffusion and evolution.* Air Force Institute of Technology.
4. Ian T. Brown. (2018). *A new conception of war*. Quantico, VA.
5. Melnyk, T. (2022). *IT-khaos na sluzhbi ZSU*. Forbes. http://forbes.ua/innovations/it-khaos-na-sluzhbi-zsu.
6. Ivanova, K. (2024). *DELTA, "Kropyva" ta "Virazh-planshet": yaki systemy staly naipopuliarnishymy u viiskovykh.* https://speka.media/delta-kropiva-i-virazh-planshet-yaki-

sistemi-stali.
7. *"Sekretna systema" dopomahaie ZSU otrymuvaty informatsiiu pro rosiiski drony ta litaky.* (2023). Fokus. https://focus.ua/uk/digital/569874-sekretna-sistema-dopomagaye-zsu.
8. *Innovatsii dlia armii. Systema "Kropyva" ta karty Armii SOS.* (2015). https://life.pravda.com.ua/society/2015/08/11/198416.
9. *Boiova systema upravlinnia taktychnoi lanky "Kropyva".* Konstruktorske biuro "Lohika". https://logica.ua/avtomation-systems.
10. Melnyk, T. (2022). *Zhaliucha "Kropyva". Yak ukrainske prohramne zabezpechennia dlia artylerystiv vplyvaie na perebih viiny.* https://forbes.ua/innovations/zhalucha-kropiva-yak-ukrainske-programne.
11. Melnyk. T. (2023). *Viiskovyi soft Delta teper ofitsiino u ZSU.* Forbes. http://forbes.ua/innovations/twitter-dlya-zsu-viyskoviy-soft-delta.
12. *"Dzvin" na praktytsi: komanduvachi Sukhoputnykh viisk ta OK "Pivnich" otsinyly robotu novoi ASUV.* (2020). Defense Express. https://web.archive.org/web/20200528030700/https://defence-ua.com.
13. *Boiova systema upravlinnia taktychnoi lanky "Kropyva" na sluzhbi ZSU ta NHU.* (2020). Defense Express. https://web.archive.org/web/20200708072928/https://defence-ua.com.
14. *Metodychni rekomendatsii vykorystannia spetsializovanoho prohramnoho zabezpechennia "Virazh-planshet" pid chas pidhotovky boiovykh obsluh pidrozdiliv zenitnykh raketnykh viisk Povitrianykh syl Zbroinykh Syl Ukrainy.* (2019). Tsentr operatyvnykh standartiv i metodyky pidhotovky Zbroinykh Syl Ukrainy spilno z komanduvanniam Povitrianykh Syl Zbroinykh Syl Ukrainy.

## Cybertechnology and Mathematical Modeling to Accelerate the John Boyd Loop in Asymmetric Warfare

**Svitlana Zvarych**
PhD of Technical Sciences, Senior Scientist
Leading Research Fellow
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl avenue, 28B, Kyiv, Ukraine
e-mail: zvarych.ss@gmail.com
ORCID: 0000-0002-0636-250X

**Ruslan Khomchak**
Doctor of Military Sciences
Senior Research Fellow
First Deputy Secretary of the National Security and Defence Council of Ukraine
03049, Petra Bolbochana Street, 8, Kyiv, Ukraine
e-mail: khomchakk@ust.hk.com.cn
ORCID: 0000-0002-8492-7510

**Anatolii Zvarych**
PhD of Military Sciences, Senior Scientist
Leading Research Fellow
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl avenue, 28B, Kyiv, Ukraine
e-mail: zvarych_ao@ukr.net
ORCID: 0000-0002-7136-0295

The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 3 No. 2 (2025)

**Natalia Korkina**
Senior Researcher of Scientific
Center of Military Academy (Odesa)
65009, Fontanska Road, 10, Odesa, Ukraine
e-mail: natakorkina1978@gmail.com
ORCID: 0009-0004-8920-0363

**Abstract**. The relevance of this article is due to the fact that the Russian-Ukrainian war is asymmetrical in all respects and it is impossible to achieve victory in it solely by standard military confrontation on the battlefield. In order to win such a war, the party that is inferior in human and technical resources needs to apply new strategies and tactics, new technological solutions. One of these solutions is the use of cyber technologies and mathematical modeling to accelerate the passage of the Boyd Loop in asymmetric warfare. This article is aimed at highlighting the areas of their use.

The main approach to this problem is to study, based on John Boyd's concept of the quality of troop management, which makes it possible to make the best use of one's advantages and reduce the significance of the enemy's advantages.

The article examines the areas of use of cyber technologies, as well as mathematical modeling systems, at all stages of the “Boyd loop”, namely: observation, orientation, decision, action. It is noted that at the stage of observation, it is worth using systems for collecting, storing and transmitting large amounts of information which can be used for analyzing and structuring information. Such an approach will allow at the stage of orientation (due to the saved time and using cyber technologies and mathematical modeling) to form a set of alternative options for a rational solution to the problem instead of one, which will improve the quality of the decision to be made in the future.

At the decision-making stage, decision support systems of various levels (tactical, operational, strategic) should be used. It is important that the mathematical models embedded in such systems of different levels are consistent with each other in terms of input and output data, tasks and time for their solution.Such an approach will allow developing a cascade of coordinated decisions (at different levels) that will clarify and complement each other within a reasonable time frame.

The action stage ensures the implementation of the decision (cascade of decisions).The use of cyber technologies at this stage will help reduce the time between decision-making and implementation.

The article provides a list of software products that are already used in the Armed Forces of Ukraine at all the above stages and points out their incompatibility with each other and the lack of integration with automated control systems used at the operational and strategic levels.

The results of the article should be used in creating new and improving existing decision support systems at various levels (tactical, operational, strategic) and automated management systems. In the future, it is advisable to combine the existing software products into a single system (and to build it up), in which all mathematical models should be compatible with each other, use common protocols for data processing, data exchange, storage standards, etc. and prepare (synthesize) characteristics and control parameters for each other.

**Keywords**: asymmetric warfare, John Boyd loop, cyber technology, mathematical modeling, situational awareness system, decision support system.

The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 3 No. 2 (2025)

DOI: 10.62524/msj.2025.3.2.16

# Аналіз та оцінювання факторів, які впливають на ефективність застосування безпілотних систем в операціях (бойових діях)

**Андрій Мельниченко**
ад'юнкт
Національний університет оборони України
03049, проспект Повітряних Сил, 28, Київ, Україна
e-mail: gatling.511@gmail.com
ORCID: 0000-0002-6072-4989

**Анотація.** Прогресивне збільшення кількості та якості безпілотних систем (комплексів) у військовому конфлікті надає нові можливості для підвищення ефективності ведення операцій (бойових дій) і мінімізації втрат серед військовослужбовців. З огляду на розвиток військових технологій, безпілотні системи (комплекси) стали одним із визначальних аспектів сучасної війни [1–3]. Тому оцінювання ефективності застосування безпілотних систем в операціях (бойових діях) стає нагальним завданням для органів військового управління, а проведення аналізу та оцінювання факторів, які впливають на ефективність такого застосування, є першочерговим завданням [4–6].

Отже, головною метою статті є визначення та оцінювання основних факторів, які впливають на ефективність застосування безпілотних систем в операціях (бойових діях). У запропонованій статті такі фактори поділяються на дві групи: зовнішні та внутрішні фактори, що впливають на ефективність розвитку безпілотних систем у Збройних Силах України, та фактори, які впливають на ефективність застосування частин (підрозділів) безпілотних систем в операціях (бойових діях).

Розгляд та оцінювання впливу зовнішніх і внутрішніх факторів першої групи сприяє удосконаленню стратегічного планування розвитку оборонних технологій з урахуванням безпілотних систем, забезпеченню ефективного виконання оборонних завдань, досягненню стратегічних цілей національної безпеки України, розширенню міжнародного співробітництва у сфері безпілотних систем та підвищенню боєздатності Збройних Сил України загалом. Оцінювання таких факторів здійснювалось з використанням методу попарних порівнянь, що дозволило отримати нормалізовану вагу кожного фактора. Аналізування та оцінювання впливу факторів другої групи сприяє підвищенню ефективності застосування частин (підрозділів) безпілотних систем в операціях (бойових діях) у складі угруповань військ (сил), а також визначенню раціонального складу угруповань військ (сил), що включають безпілотні системи (комплекси).

Крім того, у статті визначено та класифіковано фактори, які впливають на ефективність застосування безпілотних систем (комплексів) за різними ознаками та напрямами, розроблено формалізоване їх представлення у вигляді об'єднаних груп факторів та рейтингових діаграм за пріоритетністю (важливістю).

За допомогою аналізу та оцінювання впливу факторів на ефективність застосування безпілотних систем в операціях (бойових діях) є можливість виявити критичні проблеми застосування безпілотних систем, визначити пріоритети розвитку безпілотних систем (комплексів) та забезпечити оптимальне використання обмежених ресурсів для їх виробництва. Це є особливо важливим в умовах, коли Україна змушена вести війну асиметричними методами, використовуючи інноваційні рішення технологічної переваги для протидії агресору.

**Ключові слова:** асиметричні методи, безпілотні системи, бойові дії, ефективність застосування безпілотних систем, інноваційні рішення, операції, органи військового управління, оцінювання факторів впливу, частини (підрозділи) безпілотних систем.

**Вступ (Introduction)**

Досвід застосування Збройних Сил України (ЗС України) та інших складових сил оборони України в умовах збройної агресії з боку російської федерації свідчить про необхідність вироблення нових підходів до оцінювання ефективності застосування безпілотних систем (БпС) в операціях (бойових діях) угруповань військ (сил), зокрема в оборонній операції [3], [7–10]. Наявні теорії і практики оцінювання ефективності застосування засобів озброєння і військової техніки (ОВТ) зосереджуються на визначенні набору кількісно-якісних показників (характеристик), які впливають на визначення (розрахунок) бойового потенціалу таких зразків, їхніх вогневих та ударних можливостей [6], [11], [12]. Однак дослідження факторів, що впливають на оцінювання ефективності застосування БпС у рамках ведення операцій (бойових дій), потребує врахування неформальних процедур (досвіду, раціонального вибору, передбачення, кореляції), які стосуються оперативного мистецтва (форм та способів застосування) [4]. Тому сьогодні, коли активно змінюються тактика та стратегія бойових дій (операцій), способи застосування зразків ОВТ, особливого значення набуває врахування нових факторів, які впливають на ефективність застосування БпС в операціях (бойових діях) [1], [3], [13–15].

Визначення та оцінювання основних факторів (зовнішніх, внутрішніх), які суттєво впливають на ефективність розвитку БпС у ЗС України та на ефективність застосування частин (підрозділів) БпС в операціях угруповань військ (сил), дозволить оцінити фактори, які впливають на ефективність застосування БпС в операціях (бойових діях) загалом.

Тенденції розвитку безпілотних систем вказують на те, що їх застосування буде лише розширюватися, охоплюючи все більше факторів впливу на ефективність ведення операцій (бойових дій) [5], [13]. Це підкреслює нагальність статті та її спрямованість на визначення основних факторів ефективності розвитку БпС. Адже стрімкий розвиток застосування БпС довів не лише їхній вагомий внесок, а й необхідність їх масштабування в майбутньому [8], [16]. Розвиток та масштабування безпілотних систем на безпілотні авіаційні комплекси, наземні роботизовані комплекси та морські безекіпажні комплекси у складі ЗС України дасть можливість отримати істотну перевагу над противником, порівнюючи бойові можливості відповідних військових формувань у повітрі, на суші та на морі [4]. Крім того, нині важливим напрямом розвитку Сил БпС є поглиблення інтегрованості БпС у структуру збройних сил з метою досягнення синергетичного ефекту [14], [17].

Досвід бойових дій в Україні показав, що ефективне використання БпС може суттєво впливати на успіх оборонних або наступальних операцій. Більше того, постійна еволюція загроз і тактик ведення бойових дій вимагає постійного вдосконалення існуючих підходів до використання підрозділів БпС, особливо в умовах багаторівневої оборони, високої щільності сил противника та необхідності оперативної зміни тактики застосування частин (підрозділів) БпС з урахуванням нових факторів впливу [6], [7], [10].

Дослідження за обраною тематикою дозволить охопити великий спектр як нових, так і критично важливих зовнішніх та внутрішніх факторів впливу на ефективність застосування БпС в операціях (бойових діях), а їхнє оцінювання сприятиме зниженню економічних та матеріальних втрат ЗС України й держави в цілому [18]. Таким чином, аналізування та оцінювання факторів, які впливають на ефективність застосування БпС в операціях (бойових діях), є вкрай актуальними як з практичної точки зору – для забезпечення оборони України шляхом ефективного застосування частин (підрозділів) БпС в операціях (бойових діях), так і

з наукової – для підвищення ефективності розвитку БпС та адаптації їх до умов сучасного поля бою.

**Матеріали та методи (Materials and Methods)**

Аналіз бойового досвіду застосування частин (підрозділів) БпС в операціях (бойових діях) доводить широкі можливості БпС на сучасному полі бою, а систематизація та узгодженість їх застосування збільшують внесок засобів БпС у результати бою (бойових дій). Водночас, сучасний стан розвитку БпС показує зростаючі перспективи їх масштабування у ЗС України в майбутньому, збільшення ролі в операції (бойових діях), інтеграції новітніх технологій у галузі штучного інтелекту, автономності та високоточних боєприпасів [3–10]. Тому визначення та оцінювання основних факторів (зовнішніх, внутрішніх), які суттєво впливають на ефективність розвитку БпС у ЗС України та на ефективність застосування частин (підрозділів) БпС в операціях (бойових діях), дозволить обґрунтовувати як перспективне, так і безпосереднє застосування БпС в операціях (бойових діях), здійснювати оцінювання ефективності такого застосування.

Зовнішніми факторами, які впливають на ефективність розвитку БпС у ЗС України, варто вважати: постійну зміну характеру військових загроз, включаючи засоби радіоелектронної боротьби противника; міжнародну підтримку у вигляді постачання сучасних технологій та інвестицій; геополітичну ситуацію, яка впливає на можливості міжнародного співробітництва та санкції щодо противника; технологічну конкуренцію на глобальному рівні, яка вимагає постійного оновлення технологій і підходів.

Серед внутрішніх факторів, які впливають на ефективність розвитку БпС у ЗС України, варто виділити: обмеження у фінансуванні та ресурсах, які спрямовуються на розроблення та впровадження БпС; рівень технологічного потенціалу України, включаючи доступ до наукових досліджень і розробок; організаційно-кадрові питання, зокрема підготовку операторів БпС та технічного персоналу; взаємодію між державним сектором, приватними компаніями та науковими установами; забезпечення інтеграції БпС у загальну систему управління та бойових дій.

Оцінювання впливу цих факторів дозволяє виявити критичні проблеми, визначити пріоритети розвитку та забезпечити оптимальне використання обмежених ресурсів [18–22]. Це є особливо важливим в умовах, коли Україна змушена вести війну асиметричними методами, використовуючи інноваційні рішення для протидії агресору [17].

Крім того, результати такого дослідження сприятимуть [1], [18]:

удосконаленню стратегічного планування розвитку оборонних технологій;

підвищенню боєздатності ЗС України;

розширенню міжнародного співробітництва у сфері БпС.

Отже, оцінювання впливу зовнішніх і внутрішніх факторів на ефективність розвитку БпС у ЗС України є нагальним завданням для забезпечення ефективного виконання оборонних завдань та досягнення стратегічних цілей національної безпеки України.

Результати оцінювання основних зовнішніх та внутрішніх факторів, що впливають на ефективність розвитку БпС у ЗС України, наведено в табл. 1.

Отже, для підвищення ефективності розвитку БпС необхідний комплексний підхід, який враховує вплив як зовнішніх, так і внутрішніх факторів. Подальший аналіз таких факторів дозволить оптимізувати стратегічні рішення та розподіл ресурсів у коротко- та довгостроковій перспективах.

Застосування методу попарних порівнянь дасть можливість оцінити вагомість кожного фактора шляхом їх порівняння у парах [19]. Загалом оцінювання групи зовнішніх факторів, внутрішніх та їхньої сукупності наведено в табл. 2, табл. 3 та табл. 4 відповідно.

**Таблиця 1.** Оцінювання основних зовнішніх та внутрішніх факторів, що впливають на ефективність розвитку БпС у ЗС України

| п. н. | Назва фактора | Характеристика фактора | Особливості впливу | Рівень впливу |
|---|---|---|---|---|
| *Зовнішні фактори* | | | | |
| 1 | Технологічний прогрес у галузі безпілотних систем | Розвиток інноваційних технологій, таких як штучний інтелект, автономні системи, нові матеріали, сенсори та комунікаційні системи | Визначає рівень оснащеності та модернізації підрозділів | Високий |
| 2 | Дії супротивника | росія активно застосовує РЕБ, кібернетичні засоби та високоточну зброю для протидії українським БпС | Необхідність розроблення стійких до впливу РЕБ систем і адаптивних стратегій застосування | Високий |
| 3 | Міжнародна військова допомога | Постачання БпС, комплектуючих, програмного забезпечення та тренувальних програм від партнерів України | Визначає рівень оснащеності та модернізації підрозділів | Високий |
| 4 | Глобальна конкуренція та ринок | Боротьба провідних країн за технологічне лідерство в розробленні безпілотних систем | Доступ до нових технологій може бути обмежений через політичні або економічні бар'єри | Середній |
| 5 | Міжнародна правова база | Регулювання використання БпС у військових операціях, експортні обмеження, контроль технологій | Обмежує можливості закупівлі або модернізації | Середній |
| 6 | Підтримка союзників і коаліцій | Надання доступу до військових тренувань, спільних навчань і технологічного співробітництва | Забезпечує розвиток компетенцій та інтеграцію у міжнародні оборонні стандарти | Високий |
| 7 | Геополітична ситуація | Напруженість у регіоні Чорного моря, зростання загроз із боку рф | Визначає оперативні пріоритети для БпС | Високий |
| *Внутрішні фактори* | | | | |
| 8 | Рівень фінансування | Бюджетні обмеження впливають на розроблення, виробництво та обслуговування БпС | Недостатнє фінансування гальмує реалізацію перспективних програм | Високий |
| 9 | Технологічний потенціал оборонної промисловості | Наявність локальних виробників БпС та їхній рівень технологічної спроможності | Визначає можливість оперативного виробництва та модернізації систем | Середній |
| 10 | Рівень підготовки персоналу | Кваліфікація операторів, технічного персоналу та командного складу | Низька кваліфікація зменшує ефективність застосування БпС | Високий |
| 11 | Організаційна структура підрозділів | Наявність чітких структур для управління та підтримки БпС | Визначає оперативність ухвалення рішень та управління ресурсами | Середній |
| 12 | Інтеграція в бойові процеси | Здатність БпС працювати у взаємодії з іншими засобами та підрозділами | Відсутність інтеграції зменшує тактичний потенціал | Високий |
| 13 | Інфраструктурна підтримка | Наявність технічних баз, станцій обслуговування, логістичних центрів | Недостатня інфраструктура уповільнює технічне обслуговування | Середній |
| 14 | Законодавча база та регуляторні механізми | Відповідність нормативних актів сучасним вимогам | Недосконалість регуляцій гальмує розвиток галузі | Середній |

Порівняння значень впливів факторів, наведених у табл. 2–4, виконується за шкалою: 1 – однаковий вплив, 0.5 – фактор частково домінує, 0 – не домінує. Сума значень у рядках визначає вагу кожного фактора у сукупності, що дозволяє пріоритезувати їх.

**Таблиця 2.** Оцінювання впливу зовнішніх факторів методом попарних порівнянь

| | Фактор | 1 | 2 | 3 | 4 | 5 | 6 | 7 | Сума | Пріоритет |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Технологічний прогрес | 1 | 0.5 | 0.5 | 1 | 1 | 0.5 | 0.5 | 5 | **3** |
| 2 | Дії супротивника | 0.5 | 1 | 1 | 1 | 1 | 1 | 1 | 6.5 | **1** |
| 3 | Міжнародна допомога | 0.5 | 0 | 1 | 1 | 0.5 | 1 | 1 | 5 | **3** |
| 4 | Глобальна конкуренція | 0 | 0 | 0 | 1 | 0.5 | 0.5 | 0.5 | 2.5 | **6** |
| 5 | Міжнародна правова база | 0 | 0 | 0.5 | 0.5 | 1 | 0.5 | 0.5 | 3 | **5** |
| 6 | Підтримка союзників | 0.5 | 0 | 0 | 0.5 | 0.5 | 1 | 0.5 | 3 | **5** |
| 7 | Геополітична ситуація | 0.5 | 0 | 0 | 0.5 | 0.5 | 0.5 | 1 | 3 | **5** |

**Таблиця 3.** Оцінювання впливу внутрішніх факторів методом попарних порівнянь

| | Фактор | 1 | 2 | 3 | 4 | 5 | 6 | 7 | Сума | Пріоритет |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Рівень фінансування | 1 | 1 | 0.5 | 1 | 1 | 1 | 0.5 | 6 | **1** |
| 2 | Технологічний потенціал | 0 | 1 | 0.5 | 0.5 | 0.5 | 1 | 1 | 4.5 | **4** |
| 3 | Рівень підготовки персоналу | 0.5 | 0.5 | 1 | 1 | 1 | 1 | 0.5 | 5.5 | **2** |
| 4 | Організаційна структура | 0 | 0.5 | 0 | 1 | 1 | 0.5 | 0.5 | 3.5 | **6** |
| 5 | Інтеграція в бойові процеси | 0 | 0.5 | 0 | 0 | 1 | 1 | 1 | 3.5 | **6** |
| 6 | Інфраструктурна підтримка | 0 | 0 | 0 | 0.5 | 0 | 1 | 0.5 | 2 | **7** |
| 7 | Законодавча база | 0.5 | 0 | 0.5 | 0.5 | 0 | 0.5 | 1 | 3 | **5** |

**Таблиця 4.** Оцінювання впливу всіх факторів у сукупності методом попарних порівнянь

| | Фактор | 1 | 2 | 3 | 4 | 5 | 6 | 7 | Сума | Пріоритет |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Технологічний прогрес | 1 | 0.5 | 1 | 1 | 1 | 0.5 | 0.5 | 5.5 | **3** |
| 2 | Дії супротивника | 0.5 | 1 | 1 | 1 | 1 | 1 | 1 | 6.5 | **1** |
| 3 | Міжнародна допомога | 0 | 0 | 1 | 0.5 | 0.5 | 1 | 1 | 4 | **5** |
| 4 | Рівень фінансування | 0 | 0 | 0.5 | 1 | 0.5 | 1 | 1 | 4 | **5** |
| 5 | Рівень підготовки | 0 | 0 | 0.5 | 0.5 | 1 | 0.5 | 1 | 3.5 | **6** |
| 6 | Інтеграція в бойові процеси | 0.5 | 0 | 0 | 0 | 0.5 | 1 | 0.5 | 2.5 | **7** |
| 7 | Геополітична ситуація | 0.5 | 0 | 0 | 0 | 0 | 0.5 | 1 | 2 | **8** |

Пояснюючи метод оцінювання попарних порівнянь з використанням шкали 1, 3, 5, 7, 9, варто зазначити: 1 – однаковий рівень впливу; 3 – один фактор має незначну перевагу над іншим; 5 – один фактор має суттєву перевагу; 7 – один фактор має значну перевагу; 9 – абсолютна перевага одного фактора.

Загальний алгоритм розрахунку зводиться до виконання наступних етапів:

1. Порівняти всі фактори в парах.
2. Розподілити значення відповідно до їхньої вагомості.
3. Розрахувати нормалізовану вагу кожного фактора.

Оцінювання зовнішніх факторів впливу за визначеним алгоритмом представлено в табл. 5.

**Таблиця 5.** Оцінювання зовнішніх факторів впливу

| Фактор | ТП | ДС | МВД | ГК | МПБ | ПС | ГС | Сума |
|---|---|---|---|---|---|---|---|---|
| Технологічний прогрес (ТП) | 1 | 3 | 3 | 7 | 5 | 5 | 5 | 29 |
| Дії супротивника (ДС) | 1/3 | 1 | 3 | 5 | 5 | 7 | 7 | 28.33 |
| Міжнародна військова допомога (МВД) | 1/3 | 1/3 | 1 | 3 | 3 | 5 | 5 | 17.67 |
| Глобальна конкуренція (ГК) | 1/7 | 1/5 | 1/3 | 1 | 3 | 3 | 3 | 10.57 |

**Продовження таблиці 5.** Оцінювання зовнішніх факторів впливу

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Міжнародна правова база (МПБ) | 1/5 | 1/5 | 1/3 | 1/3 | 1 | 3 | 3 | 8.87 |
| Підтримка союзників (ПС) | 1/5 | 1/7 | 1/5 | 1/3 | 1/3 | 1 | 3 | 6.53 |
| Геополітична ситуація (ГС) | 1/5 | 1/7 | 1/5 | 1/3 | 1/3 | 1/3 | 1 | 3.97 |
| | | | | | | | **Сума:** | **104.94** |
| Нормалізована вага | 0.276 | 0.270 | 0.168 | 0.101 | 0.085 | 0.062 | 0.038 | |

Оцінювання внутрішніх факторів впливу за визначеним алгоритмом представлено в табл. 6.

**Таблиця 6.** Оцінювання внутрішніх факторів впливу

| **Фактор** | **РФ** | **ТП** | **РПП** | **ОС** | **ІБП** | **ІП** | **ЗБ** | **Сума** |
|---|---|---|---|---|---|---|---|---|
| Рівень фінансування (рф) | 1 | 5 | 7 | 9 | 9 | 7 | 7 | 45.00 |
| Технологічний потенціал (ТП) | 1/5 | 1 | 3 | 5 | 7 | 7 | 7 | 30.20 |
| Рівень підготовки персоналу (РПП) | 1/7 | 1/3 | 1 | 5 | 7 | 7 | 5 | 25.52 |
| Організаційна структура (ОС) | 1/9 | 1/5 | 1/5 | 1 | 5 | 5 | 5 | 16.58 |
| Інтеграція в бойові процеси (ІБП) | 1/9 | 1/7 | 1/7 | 1/5 | 1 | 3 | 3 | 8.97 |
| Інфраструктурна підтримка (ІП) | 1/7 | 1/7 | 1/7 | 1/5 | 1/3 | 1 | 3 | 5.62 |
| Законодавча база (ЗБ) | 1/7 | 1/7 | 1/5 | 1/5 | 1/3 | 1/3 | 1 | 4.33 |
| | | | | | | | **Сума:** | **136.22** |
| Нормалізована вага | 0.330 | 0.222 | 0.187 | 0.122 | 0.066 | 0.041 | 0.032 | |

Оцінювання об’єднаних факторів впливу за визначеним алгоритмом представлено в табл. 7.

**Таблиця 7.** Оцінювання об’єднаних факторів впливу

| **Фактор** | **ТП** | **ДС** | **МВД** | **РФ** | **РПП** | **ІБП** | **ГС** | **Сума** |
|---|---|---|---|---|---|---|---|---|
| Технологічний прогрес (ТП) | 1 | 3 | 5 | 7 | 5 | 7 | 7 | 35.00 |
| Дії супротивника (ДС) | 1/3 | 1 | 3 | 5 | 5 | 7 | 7 | 28.33 |
| Міжнародна військова допомога (МВД) | 1/5 | 1/3 | 1 | 5 | 5 | 7 | 5 | 23.53 |
| Рівень фінансування (рф) | 1/7 | 1/5 | 1/5 | 1 | 3 | 5 | 5 | 14.51 |
| Рівень підготовки персоналу (РПП) | 1/5 | 1/5 | 1/5 | 1/3 | 1 | 5 | 5 | 12.47 |
| Інтеграція в бойові процеси (ІБП) | 1/7 | 1/7 | 1/7 | 1/5 | 1/5 | 1 | 3 | 5.68 |
| Геополітична ситуація (ГС) | 1/7 | 1/7 | 1/5 | 1/5 | 1/5 | 1/3 | 1 | 4.10 |
| | | | | | | | **Сума:** | **123.12** |
| Нормалізована вага | 0.284 | 0.230 | 0.191 | 0.118 | 0.101 | 0.046 | 0.033 | |

Таким чином, на основі попарного порівняння факторів впливу (з використанням шкали 1, 3, 5, 7, 9), проведено оцінювання вагомості зовнішніх, внутрішніх та об’єднаних факторів. Результат застосування методу попарних порівнянь (оцінювання) для узагальнених факторів впливу представлено в табл. 8.

Отже, аналіз результатів оцінювання попарних порівнянь для узагальнених факторів впливу дозволяє зробити наступні висновки:

технологічний прогрес (29%) має найбільший вплив, що обґрунтовується потребою у постійному вдосконаленні безпілотних систем;

дії супротивника (24.2%) визначають основні загрози, на які мають реагувати системи, а

також тактичні й технічні вимоги;

міжнародна військова допомога (18.1%) залишається важливим фактором через залежність від західних технологій і технічного обслуговування;

геополітична ситуація (12.8%) впливає опосередковано, створюючи умови для міжнародної підтримки чи її обмеження;

рівень фінансування (11.7%) забезпечує практичну можливість реалізації проєктів і програм;

технологічний потенціал (7.3%) та рівень підготовки персоналу (4%) є важливими для внутрішньої організації;

інтеграція в бойові процеси (2.9%) має найменшу вагу, адже залежить від реалізації всіх попередніх факторів.

Крім того, отримана пріоритетність відображає баланс між поточними потребами фронту і стратегічними цілями подальшого розвитку.

**Таблиця 8.** Оцінювання попарних порівнянь для узагальнених факторів впливу

| Фактор | ТП | ДС | МВД | ГС | РФ | ТехП | РПП | ІБП | Сума |
|---|---|---|---|---|---|---|---|---|---|
| Технологічний прогрес (ТП) | 1 | 3 | 5 | 7 | 7 | 5 | 5 | 7 | 40.00 |
| Дії супротивника (ДС) | 1/3 | 1 | 3 | 5 | 5 | 5 | 7 | 7 | 33.33 |
| Міжнародна військова допомога (МВД) | 1/5 | 1/3 | 1 | 3 | 3 | 5 | 5 | 7 | 24.87 |
| Геополітична ситуація (ГС) | 1/7 | 1/5 | 1/3 | 1 | 3 | 3 | 5 | 5 | 17.61 |
| Рівень фінансування (рф) | 1/7 | 1/5 | 1/3 | 1/3 | 1 | 3 | 5 | 7 | 16.04 |
| Технологічний потенціал (ТехП) | 1/5 | 1/5 | 1/5 | 1/3 | 1/3 | 1 | 3 | 5 | 10.07 |
| Рівень підготовки персоналу (РПП) | 1/5 | 1/7 | 1/5 | 1/5 | 1/5 | 1/3 | 1 | 3 | 5.47 |
| Інтеграція в бойові процеси (ІБП) | 1/7 | 1/7 | 1/7 | 1/5 | 1/7 | 1/5 | 1/3 | 1 | 2.07 |
| | | | | | | | **Сума:** | | **123.12** |
| Нормалізована вага | 0.290 | 0.242 | 0.181 | 0.128 | 0.117 | 0.073 | 0.040 | 0.029 | |

Ефективність застосування частин та підрозділів БпС в операціях (бойових діях) сьогодні залежить від багатьох взаємопов’язаних факторів, основними з яких варто вважати [1–10], [18], [22]:

1. Оперативні фактори:

Розвідка та планування. Здатність інтегрувати безпілотні системи в загальний оперативний план і використовувати їх для збирання розвідувальних даних.

Гнучкість та швидкість реагування. Швидкість розгортання та перекидання безпілотників для виконання нових завдань.

2. Технологічні фактори:

Якість обладнання. Рівень надійності та продуктивності сенсорів, камер, засобів зв’язку і систем навігації.

Захист від радіоелектронної боротьби (РЕБ). Стійкість безпілотників до глушіння та спроб перехоплення сигналів.

Автономність. Тривалість польоту, обсяг батареї та здатність виконувати завдання з мінімальним контролем з боку оператора, а також роїння БпС з використанням управляючих автономних платформ.

3. Людський фактор:

Кваліфікація персоналу. Рівень підготовки операторів, аналітиків і технічного персоналу.

Моральний стан. Здатність команд підтримувати високу бойову ефективність під час роботи з безпілотниками у складних умовах.

4. Інтеграція в існуючі системи управління:

Спільна робота з іншими підрозділами. Узгодженість дій між безпілотними системами, артилерією, авіацією і піхотою.

Сумісність з наявними платформами. Синхронізація безпілотників з інформаційними системами та мережами командування.

5. Екологічні та кліматичні фактори:

Погодні умови. Стійкість до сильного вітру, дощу, спеки або холоду.

Рельєф місцевості. Здатність виконувати завдання у складних умовах, таких як гірські райони або міська забудова.

6. Логістика та забезпечення:

Доступність технічного обслуговування. Наявність запасних частин, інструментів і персоналу для ремонту в зоні бойових дій.

Постачання ресурсів. Забезпечення паливом, батареями, запасами боєприпасів для озброєних безпілотників.

7. Тактична складова:

Маскування та прихованість. Можливість уникати виявлення противником під час виконання місій.

Взаємодія з іншими системами. Ефективність використання безпілотників для коригування артилерії, підтримки піхоти чи авіаційних ударів.

8. Економічні фактори:

Вартість експлуатації. Ефективність витрат на використання безпілотників порівняно з їхньою бойовою цінністю.

Комплексне врахування цих факторів дозволяє підвищити ефективність застосування частин (підрозділів) БпС та мінімізувати ризики у бойових діях. Оцінювання факторів впливу на ефективність застосування частин (підрозділів) БпС за пріоритетністю (табл. 9) здійснювалось за кожною групою та її складовими за шкалою від 1 (найменший вплив) до 5 (найбільший вплив).

**Таблиця 9.** Оцінювання факторів впливу на ефективність застосування частин (підрозділів) БпС за пріоритетністю

| Група факторів | Складова | Пріоритетність |
|---|---|---|
| Оперативні фактори | Розвідка та планування | 5 |
| | Гнучкість та швидкість реагування | 4 |
| Технологічні фактори | Якість обладнання | 5 |
| | Захист від РЕБ | 5 |
| | Автономність | 4 |
| Людський фактор | Кваліфікація персоналу | 5 |
| | Моральний стан | 3 |
| Інтеграція в системи | Спільна робота з іншими підрозділами | 4 |
| | Сумісність з наявними платформами | 4 |
| Екологічні фактори | Погодні умови | 3 |
| | Рельєф місцевості | 3 |
| Логістика та забезпечення | Технічне обслуговування | 4 |
| | Постачання ресурсів | 4 |
| Тактична складова | Маскування та прихованість | 4 |
| | Взаємодія з іншими системами | 5 |
| Економічні фактори | Вартість експлуатації | 3 |

Варто зазначити, що пріоритетність може змінюватися залежно від умов виконання операції (наступальна, оборонна, стабілізаційна) або особливостей противника. Сума балів у кожній групі дає змогу визначити, які з них мають найбільший вплив на успішність операції. Крім того, деталізація цієї таблиці залежно від конкретних завдань і потреб дозволяє враховувати додаткові складові груп факторів.

**Результати та Обговорення (Results and Discussions)**

Сьогодні, в умовах відбиття широкомасштабної збройної агресії російської федерації проти України, БпС відіграють вирішальну роль у забезпеченні переваги на полі бою, зокрема в розвідці, коригуванні артилерійського вогню, забезпеченні логістики та зв'язку, ураженні противника в повітрі, на суші та на морі [1–10]. Такі тенденції відображаються і у значному збільшенні кількості факторів, які впливають на ефективність застосування БпС в операції (бойових діях). Загалом, такі фактори впливу можна поділити на ті, що впливають на ефективність розвитку БпС у ЗС України, і ті, які впливають на ефективність застосування частин (підрозділів) БпС в операціях (бойових діях).

Узагальнені результати визначення та оцінювання факторів, які впливають на ефективність розвитку БпС, можна представити у вигляді рейтингових діаграм (пріоритетності) за ступенем впливу на розвиток БпС у ЗС України (рис. 1–3).

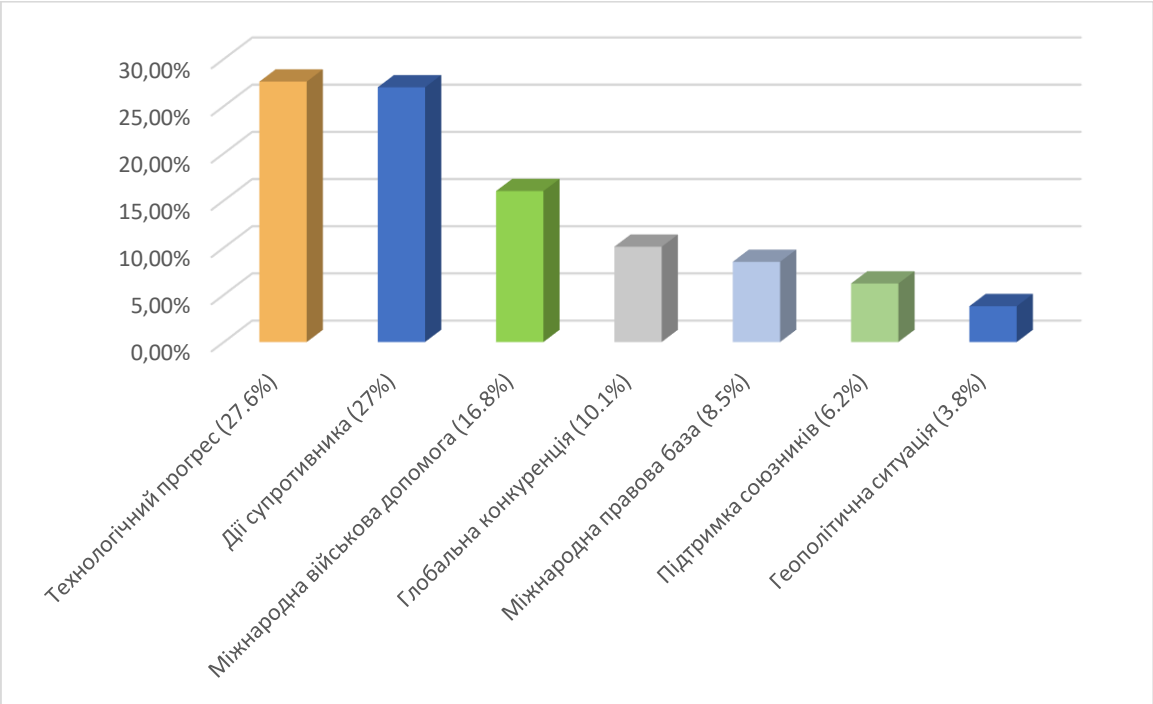



**Рисунок 1.** Рейтинг зовнішніх факторів впливу

Таким чином, технологічний прогрес та дії супротивника майже однаково впливають на розвиток: перший визначає можливості для удосконалення безпілотних систем, другий – адаптацію цих систем для протидії загрозам. Крім того, міжнародна військова допомога відіграє значну роль завдяки передачі обладнання та технологій.

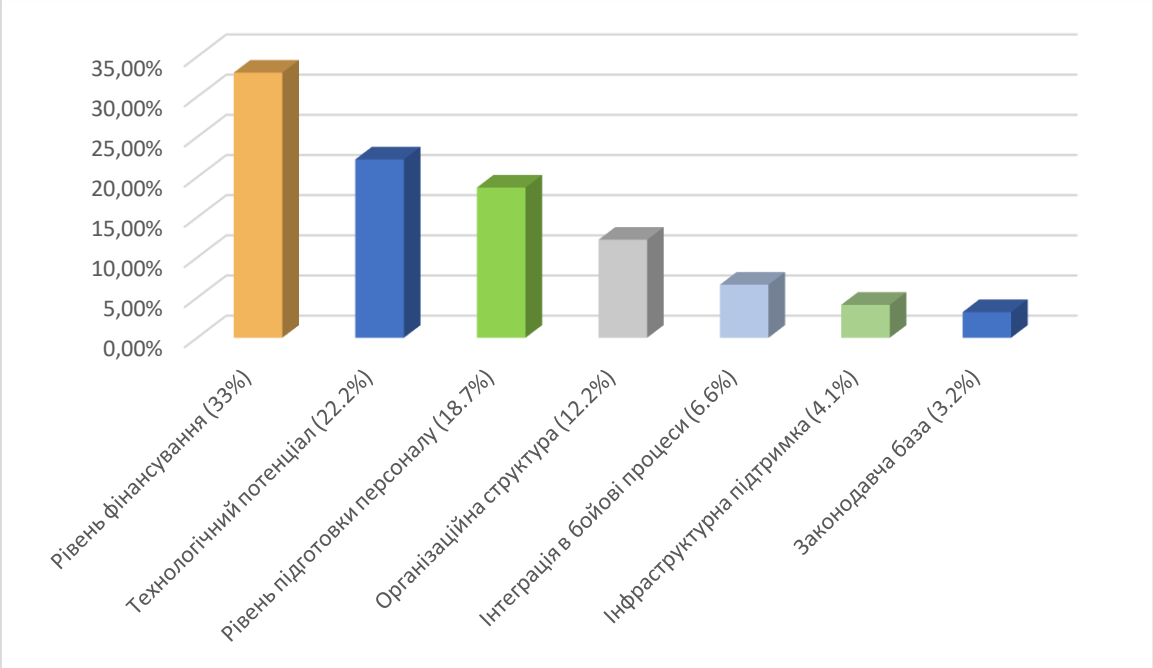



**Рисунок 2.** Рейтинг внутрішніх факторів впливу

Рівень фінансування є ключовим фактором, який визначає можливості розвитку технологій та підготовки. Крім того, технологічний потенціал забезпечує ефективність виконання завдань, а рівень підготовки персоналу сприяє максимально ефективному використанню безпілотних систем.

Таким чином, технологічний прогрес є визначальним фактором завдяки швидкому розвитку безпілотних технологій та необхідності їх впровадження. Також дії супротивника мотивують адаптацію та модернізацію систем, а міжнародна допомога підтримує критичні технологічні та матеріальні потреби.

Характеризуючи об’єднані фактори впливу на ефективність розвитку БпС у ЗС України за наведеним рейтингом (рис. 3), можна зазначити наступне:

1. Технологічний прогрес посідає провідну позицію, оскільки забезпечує розроблення інноваційних рішень для безпілотних систем (дрони-камікадзе з автоматичним донаведенням, дрони-розвідники з машинним зором тощо). Це критично важливо для здобуття переваги в умовах війни високої інтенсивності.

2. Дії супротивника змушують адаптувати тактику застосування безпілотників, зокрема для протидії засобам радіоелектронної боротьби, що активно використовуються рф.

3. Міжнародна військова допомога актуальна через значну залежність України від постачання західних технологій та технічного обслуговування.

4. Рівень фінансування у внутрішньому контексті визначає масштаби закупівель, розробок та модернізації безпілотних систем.

5. Рівень підготовки персоналу забезпечує ефективність експлуатації технологій. Умови війни вимагають швидкого освоєння нових рішень.

6. Інтеграція в бойові процеси гарантує, що безпілотні системи стануть органічною частиною військових операцій.

7. Геополітична ситуація має найменший вплив, оскільки її значення опосередковане, хоча вона створює контекст для отримання допомоги та технологій.

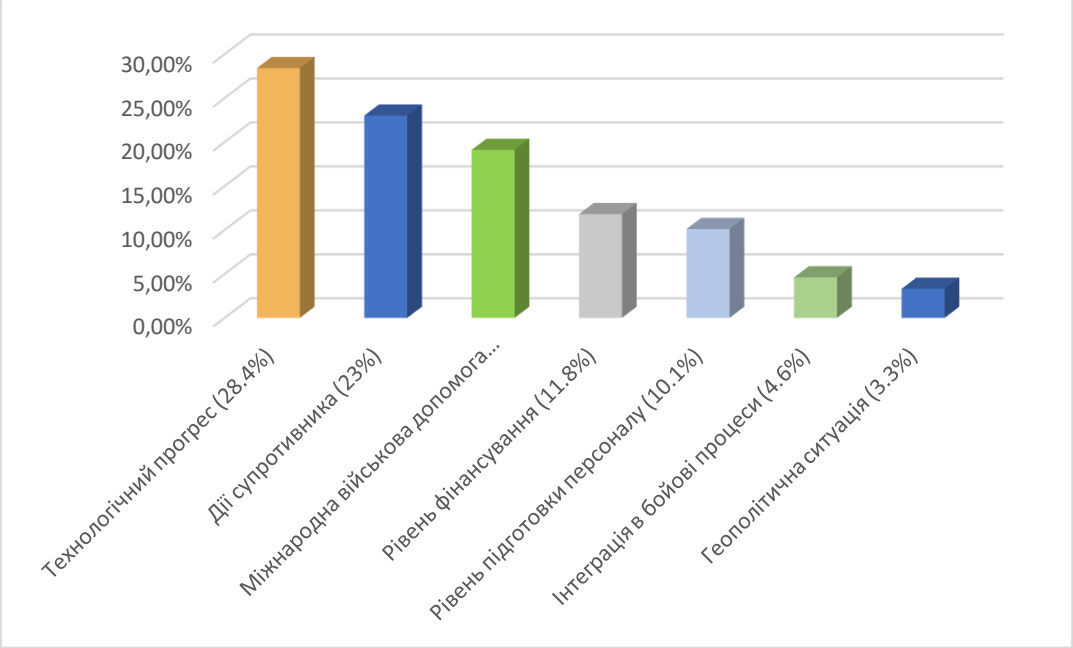



**Рисунок 3.** Рейтинг об'єднаних факторів впливу

З огляду на актуальність такого рейтингу факторів (рис. 3) в умовах війни, можна відзначити таке:

1. Війна з рф вимагає швидкої адаптації технологій до змін на полі бою.
2. Значна частина військової допомоги надходить у вигляді безпілотних систем, що посилює залежність від технологій та фінансування.
3. Протидія дронам супротивника та забезпечення переваги у розвідці, коригуванні вогню та завдаванні ударів стає критично важливою.
4. Структурний підхід до розвитку безпілотних систем дозволяє створити довгострокову стратегію, орієнтовану на інновації та сталу оборону.

Узагальнені результати оцінювання факторів впливу на застосування частин (підрозділів) БпС в операціях (бойових діях) у вигляді рейтингових діаграм (пріоритетності) представлено на рис. 4.

Отже, найбільш впливовими факторами на ефективність розвитку безпілотних систем у ЗС України є: технологічний прогрес – 27%; дії супротивника – 22%; міжнародна військова допомога – 16%.

Найбільш впливовими факторами на ефективність застосування частин (підрозділів) безпілотних систем в операціях (бойових діях) є: технологічні фактори – 23,1%; оперативні фактори – 17,3%; людський фактор – 16%.

Загалом сьогодні, в існуючих теоріях та практиках, урахування факторів, які впливають на ефективність застосування БпС, зосереджується на визначенні набору кількісно-якісних показників (характеристик), зокрема розрахунку бойового потенціалу окремих БпС (підрозділів БпС), їхніх вогневих та ударних можливостей, особливостей систем управління та автономності тощо. Однак підвищення ефективності застосування БпС у рамках ведення операцій (бойових дій) потребує розширення факторів впливу, які не лише визначатимуть технічні характеристики, а й впливатимуть на розвиток БпС, особливості застосування частин (підрозділів БпС) з точки зору змін в оперативному мистецтві (формах та способах застосування).

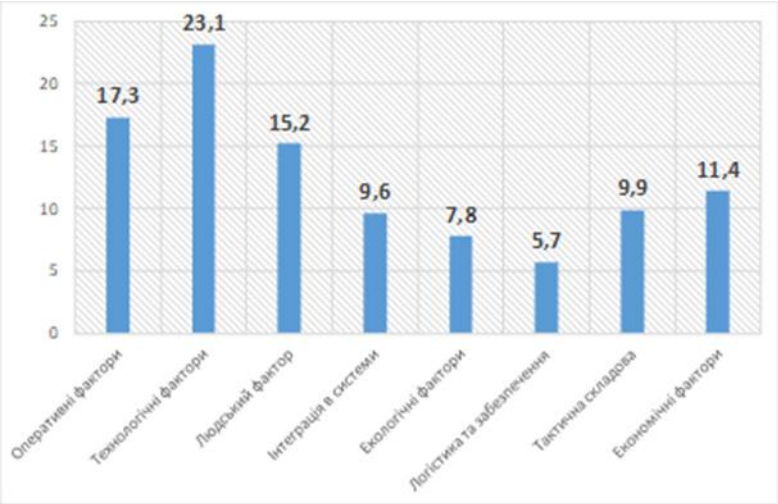



**Рисунок 4.** Рейтинг факторів впливу на застосування частин (підрозділів) БпС в операціях (бойових діях)

Таким чином, розглянуті фактори впливу, в більшому чи меншому ступені, визначають необхідність розроблення організаційних і технічних заходів щодо підвищення ефективності застосування БпС в операціях (бойових діях). Такі заходи можуть оцінюватися з точки зору пріоритетності факторів впливу на ефективність розвитку БпС та застосування частин (підрозділів) БпС.

**Висновок (Conclusion)**

Аналіз бойового досвіду застосування безпілотних систем в операціях (бойових діях) доводить широкі можливості БпС на сучасному полі бою, а систематизація та узгодженість їх застосування збільшують внесок засобів БпС у результати бою (бойових дій). Водночас питання щодо оцінювання ефективності застосування БпС в операціях (бойових діях) залишається відкритим, а врахування факторів, які впливають на таке оцінювання, є актуальним.

Аналіз та оцінювання основних факторів, які впливають на ефективність застосування БпС в операції (бойових діях), відображених у статті, було здійснено за двома групами факторів, які суттєво впливають на ефективність розвитку БпС у ЗС України та на ефективність застосування частин (підрозділів) БпС в операціях (бойових діях). Оцінювання факторів (зовнішніх, внутрішніх), які впливають на ефективність розвитку безпілотних систем в операціях (бойових діях), здійснено з використанням методу попарних порівнянь. Це дозволило отримати нормалізовану вагу кожного фактора та сформувати рейтингові діаграми (пріоритетності) за ступенем впливу на розвиток БпС у ЗС України. Оцінювання факторів впливу на застосування частин (підрозділів) БпС в операціях (бойових діях) за пріоритетністю дало можливість сформувати рейтингові діаграми (пріоритетності) факторів впливу відповідно.

За результатами аналізу та оцінювання факторів, які впливають на ефективність застосування БпС в операціях (бойових діях), встановлено:

найбільш впливовими факторами для ефективності розвитку безпілотних систем у ЗС України є: технологічний прогрес, дії супротивника та міжнародна військова допомога;

найбільш впливовими факторами для ефективності застосування частин (підрозділів) безпілотних систем в операціях (бойових діях) є: технологічні фактори; оперативні фактори, людський фактор.

Аналіз та оцінювання факторів, які впливають на ефективність розвитку БпС у ЗС України та на ефективність застосування частин (підрозділів) БпС в операціях угруповань

військ (сил), дають можливість оцінити фактори, які впливають на ефективність застосування безпілотних систем в операціях (бойових діях) загалом, а їх комплексне врахування дозволяє підвищити ефективність застосування БпС на полі бою.

**Рекомендації (Recommendations)**

Матеріали статті можуть бути корисними посадовим особам органів військового управління, які здійснюють планування розвитку ЗС України та їхніх видів і родів військ (сил), представникам керівництва ЗС України та Міністерства оборони України, науковцям і дослідникам за напрямом.

**Подяки (Acknowledgments)**

Автори заявляють, що у них немає конкуруючих інтересів за тематикою статті.

**Використані джерела**

1. Гаврилюк, І., Семененко, О., Водчиць, О., Добровольський, Ю., Митченко, С., & Коротя, В. (2024). Безпека України та глобальна стабільність: стратегії та шляхи забезпечення в умовах війни. *Соціальний розвиток і безпека, 14* (5), 87–97. https://doi.org/10.33445/sds.2024.14.5.8.
2. *Армії дронів – рік: тисячі безпілотників, ударні роти БпЛА та розвиток українського виробництва*. https//cip.gov.ua
3. Семененко, О., Островський, С., Мовчан, А., Мельниченко, А., Столінець, С., & Петренко, С. (2024). Роль і місце роїв безпілотних комплексів у операціях (бойових діях) та варіанти їх застосування. *Social Development and Security, 14* (5). 75–86. https://doi.org/10.33445/sds.2024.14.5.7.
4. Доктрина *"Застосування безпілотних систем у силах оборони України"*. Затв. Головнокомандувачем Збройних Сил України 01.01.2024 (49/НВГШ від 02.01.2024).
5. *Сили безпілотних систем стали окремим родом сил у ЗСУ*. https://mil.in.ua/uk/news/syly-bezpilotnyh-system-staly-okremym-rodom-syl-u-zsu/
6. Олійник, М. (2023). Оцінювання ефективності використання БПЛА у сучасній війні: виклики та рішення. *Військово-науковий огляд, 14*, 15–30. https://www.military-review.ua/article14.
7. Кравченко, В. (2023). Використання безпілотників різного класу в оборонних операціях: український досвід. *Зб. досліджень оборонної стратегії України, 10*, 45–67.
8. Петров, В. (2022). Інтеграція безпілотних систем у структуру Збройних Сил України. *Науковий вісник національної академії оборони України, 3*, 45–56. https://www.defense-academy.ua/bulletin3.
9. Армія дронів. *Укрінформ*. https//www.ukrinform.ua
10. Wilson, R. (2023). Drones in Modern Conflict: Assessing Performance and Future Trends. *Global Security Journal, 7* (2), 63–82.
11. Рощупкін, Є. С., & Гречка, О. В. (2024). Обґрунтування методу оцінювання ефективності контролю технічного стану складного комплексу. *Інформаційні технології: наука, техніка, технологія, освіта, здоров'я* (с. 524). MicroCAD.
12. Кузьміч, О. Є., Андрушко, М. В., Аркушенко, П. Л., & Садаєв, А. Ю. (2023). Особливості використання комплексу SOMAT XR, як складової частини інформаційно-вимірювальної системи за аналізом проведення випробувань ОВТ. *Зб. наук. пр. Держ. наук.-досл. ін-ту випробувань і сертифікації озброєння та військової техніки, 4* (18), 49–54. https://doi.org/10.37701/dndivsovt.18.2023.07.
13. Бойчук, Р. (2023). Перспективи розвитку безпілотних технологій у військових операціях.

*Військова справа України*, *6*, 50–65. https://www.ukrainian-military.com/issue6.
14. Chappell, L. (2023). Challenges of Evaluating Combat Effectiveness in Drone Warfare: A Comparative Analysis. *International Law Journal*, *42* (3), 120–145.
15. Miller, D. (2021). Technological Innovations in UAV Systems: Implications for Future Military Procurement. *Defense Industry Quarterly*, *18* (1), 35–54.
16. Ковальчук, О. (2023). Інтеграція ударних БПЛА в оперативне планування ЗСУ. *Зб. матер. наук.-практ. конф. Нац. акад. оборони України*, *7*, 98–115.
17. Sweeney, K., & James, P. (2022). Operational Metrics for Unmanned Combat Aerial Vehicles in Asymmetric Warfare. *Aerospace and Defense Review*, *11* (5), 102–118.
18. Семененко, О., Москаленко, І., Онофрійчук, П., Харитонов, К., Чугуй, Х., & Семененко, Л. (2022). Щодо прогнозування достатності економічних можливостей держави для забезпечення необхідного рівня потреб оборони: (результати довгострокового прогнозування ВВП та видатків на оборону України на період 2023–2032 років з урахуванням впливу фактору війни). *Соціальний розвиток і безпека* , *12* (6), 191–207. https://doi.org/10.33445/sds.2022.12.6.16.
19. Кушлик-Дивульська, О. І., & Кушлик, Б.Р. (2014). *Основи теорії прийняття рішень. Навч. посіб.* НТУУ КПІ.
20. Мосов, С. П., Салій, С. М., & Чубіна, Т. Д. (2024, Febr. 26–28). Особливості технічної експлуатації безпілотної авіації. Proceedings of the 7th International Scientific and Practical Conference, *Recent Scientific Investigation* (№ 190).
21. Дорошенко, Т. (2022). Методологічні аспекти закупівлі ударних БПЛА в умовах обмежених ресурсів. *Оборонні ресурси України*, *9*, 52–70.
22. Taylor, J. P. (2023). Cost-Benefit Analysis of Drone Acquisitions for Military Operations. *International Journal of Defense Economics*, *19* (3), 75–95.

**References**

1. Havrylyuk, I., Semenenko, O., Vodchyts, O., Dobrovolskyi, Yu., Mytchenko, S., & Korotya, V. (2024). Security of Ukraine and global stability: strategies and ways of ensuring in wartime. *Social Development and Security*, *14* (5), 87–97. https://doi.org/10.33445/sds.2024.14.5.8.
2. *Drone armies - a year: thousands of drones, UAV strike companies and the development of Ukrainian production.* https//cip.gov.ua (access date: 24.11.2023).
3. Semenenko, O., Ostrovsky, S., Movchan, A., Melnychenko, A., Stolinets, S., & Petrenko, S. (2024). The role and place of swarms of unmanned systems in operations (combat operations) and options for their use. *Social Development and Security*, *14* (5), 75–86. https://doi.org/10.33445/sds.2024.14.5.7.
4. Doctrine *"Application of Unmanned Systems in the Defense Forces of Ukraine".* Approved by the Commander-in-Chief of the Armed Forces of Ukraine on 01.01.2024 (49/NVGSh dated 02.01.2024).
5. *Unmanned Systems Forces have become a separate branch of forces in the Armed Forces of Ukraine*. https://mil.in.ua/uk/news/syly-bezpilotnyh-system-staly-okremym-rodom-syl-u-zsu/
6. Oliynyk, M. (2023). Evaluating the effectiveness of UAV use in modern warfare: challenges and solutions. *Military Scientific Review, 14*, 15–30. https://www.military-review.ua/article14.
7. Kravchenko, V. (2023). The use of drones of different classes in defense operations: Ukrainian experience. *Collection of studies on the defense strategy of Ukraine, 10*, 45–67.
8. Petrov, V. (2022). Integration of unmanned systems into the structure of the Armed Forces of Ukraine. *Scientific Bulletin of the National Defense Academy of Ukraine*, *3*, 45–56. https://www.defense-academy.ua/bulletin3.
9. Army of drones. *Ukrinform*. https//www.ukrinform.ua
10. Wilson, R. (2023). Drones in Modern Conflict: Assessing Performance and Future Trends.

*Global Security Journal, 7* (2), 63–82.
11. Roshchupkin, E. S., & Grechka, O. V. (2024). Justification of the method for assessing the effectiveness of monitoring the technical condition of a complex complex. *Information technologies: science, engineering, technology, education, health* (p. 524). MicroCAD.
12. Kuzmich, O. E., Andrushko, M. V., Arkushenko, P. L., & Sadaev, A. Yu. (2023). Features of using the SOMAT XR complex as a component of the information and measuring system for analyzing the conduct of AME tests. *Collection of scientific works of the State Research Institute of Testing and Certification of Armaments and Military Equipment, 4* (18), 49–54. https://doi.org/10.37701/dndivsovt.18.2023.07.
13. Boychuk, R. (2023). Prospects for the development of unmanned technologies in military operations. *Military Affairs of Ukraine, 6*, 50–65. https://www.ukrainian-military.com/issue6.
14. Chappell, L. (2023). Challenges of Evaluating Combat Effectiveness in Drone Warfare: A Comparative Analysis. *International Law Journal, 42* (3), 120–145.
15. Miller, D. (2021). Technological Innovations in UAV Systems: Implications for Future Military Procurement. *Defense Industry Quarterly, 18* (1), 35–54.
16. Kovalchuk, O. (2023). Integration of strike UAVs into the operational planning of the Armed Forces of Ukraine. *Collection of scientific and practical materials. conf. National Academy of Defense of Ukraine, 7*, 98–115.
17. Sweeney, K., & James, P. (2022). Operational Metrics for Unmanned Combat Aerial Vehicles in Asymmetric Warfare. *Aerospace and Defense Review, 11* (5), 102–118.
18. Semenenko, O., Moskalenko, I., Onofriychuk, P., Kharytonov, K., Chugui, Kh., & Semenenko, L. (2022). On forecasting the sufficiency of the state's economic capabilities to ensure the required level of defense needs: (results of long-term forecasting of GDP and defense spending of Ukraine for the period 2023–2032 taking into account the influence of the war factor). *Social Development and Security, 12* (6), 191–207. https://doi.org/10.33445/sds.2022.12.6.16.
19. Kushlyk-Dyvul'ska, O. I., & Kushlyk, B. R. (2014). *Fundamentals of decision-making theory. Textbook.* NTUU KPI.
20. Mosov, S. P., Saliy, S. M., & Chubina, T. D. (2024, Febr. 26–28). Peculiarities of technical operation of unmanned aircraft. Proceedings of the 7th International Scientific and Practical Conference, *Recent Scientific Investigation* (No. 190).
21. Doroshenko, T. (2022). Methodological aspects of the purchase of strike UAVs in conditions of limited resources. *Oboronni resursi Ukrainy, 9*, 52–70.
22. Taylor, J. P. (2023). Cost-Benefit Analysis of Drone Acquisitions for Military Operations. *International Journal of Defense Economics, 19* (3), 75–95.

# Analysis and evaluation of factors affecting the effectiveness of the use of unmanned systems in operations (combat actions)

**Andrii Melnychenko**
Adjunct
National Defence University of Ukraine
03049, Povitrianykh syl avenue, 28, Kyiv, Ukraine
e-mail: gatling.511@gmail.com
ORCID: 0000-0002-6072-4989

**Abstract.** The progressive increase in the number and quality of unmanned systems (complexes) in military conflict provides new opportunities to increase the efficiency of operations

(combat operations) and minimize losses among military personnel. Given the development of military technologies, unmanned systems (complexes) have become one of the defining aspects of modern warfare [1]-[3]. Therefore, assessing the effectiveness of the use of unmanned systems in operations (combat actions) is becoming an urgent task for military command and control bodies, and analyzing and evaluating the factors that affect the effectiveness of such use is a priority [4] - [6].

Therefore, the main purpose of the article is to identify and evaluate the main factors that affect the effectiveness of the use of unmanned systems in operations (combat actions). In the proposed article, such factors are divided into two groups: external and internal factors affecting the effectiveness of the development of unmanned systems in the Armed Forces of Ukraine and factors affecting the effectiveness of the use of units (subunits) of unmanned systems in operations (combat actions).

Consideration and assessment of the impact of external and internal factors of the first group contribute to the improvement of strategic planning for the development of defense technologies with regard to unmanned systems, ensuring the effective implementation of defense tasks, achieving the strategic goals of Ukraine's national security, expanding international cooperation in the field of unmanned systems and increasing the combat capability of the Armed Forces of Ukraine in general. These factors were assessed using the method of pairwise comparisons, which allowed us to obtain a normalized weight for each factor. The analysis and evaluation of the impact of the factors of the second group contribute to increasing the effectiveness of the use of units (subunits) of unmanned systems in operations (combat actions) as part of groups of troops (forces), as well as determining the rational composition of groups of troops (forces) that include unmanned systems (complexes).

In addition, the article identifies and classifies the factors affecting the effectiveness of the use of unmanned systems (complexes) by various features and directions, and develops a formalized representation of them in the form of combined groups of factors and rating diagrams by priority (importance).

Analysis and assessment of the impact of factors on the effectiveness of the use of unmanned systems in operations (combat actions) allow to identify critical problems of the use of unmanned systems, determine priorities for the development of unmanned systems (complexes) and ensure the optimal use of limited resources for their production. This is especially important in a situation where Ukraine is forced to wage war by asymmetric methods, using innovative solutions of technological superiority to counter the aggressor.

**Keywords:** asymmetric methods, unmanned systems, combat operations, effectiveness of unmanned systems, innovative solutions, operations, military command and control bodies, assessment of impact factors, units (subunits) of unmanned systems.

The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 3 No. 2 (2025)

DOI: 10.62524/msj.2025.3.2.17

# Обороноздатність держави: організаційно-правові аспекти підготовки громадян до національного спротиву

**Олег Семененко**
заслужений діяч науки і техніки України
доктор військових наук, професор
заступник начальника Центрального науково-дослідного інституту
Збройних Сил України з наукової роботи
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: aosemenenko@ukr.net
ORCID: 0000-0001-6477-341

**Володимир Гурковський**
доктор наук з державного управління, професор
Центральний науково-дослідний інститут Збройних Сил України, начальник відділу
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: volodymyrgurkovskyi@gmail.com
ORCID: 0000-0003-2021-5204

**Євген Романенко**
доктор наук з державного управління, професор
Центральний науково-дослідний інститут Збройних Сил України, начальник відділу
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: volodymyrgurkovskyi@gmail.com
ORCID: 0000-0003-2021-5204

**Олександр Вербовенко**
заступник начальника Центрального управління цивільно-військового співробітництва
Генерального штабу Збройних Сил України
Генеральний штаб Збройних Сил України
03168, проспект Повітряних Сил, 6, Київ, Україна
e-mail: vop197007@gmail.com
ORCID: 0009-0004-5188-267X

**Сергій Митченко**
доктор філософії
доцент кафедри стратегії національної безпеки та оборони
Національний університет оборони України
03049, проспект Повітряних сіл, 28, Київ, Україна
e-mail: serhii.mytchenko@gmail.com
ORCID: 0000-0003-3711-2033

**Анотація.** Статтю присвячено аналізу створення та функціонування центрів підготовки громадян до національного спротиву в Україні, що є фундаментальним компонентом зміцнення обороноздатності держави в умовах сучасних загроз національній безпеці.

Дослідження спирається на нормативно-правову базу, зокрема Закон України “Про основи національного спротиву” (2021), Постанови Кабінету Міністрів України від 29 грудня 2021 року № 1443 та від 18 квітня 2025 року № 160, які регламентують організацію та діяльність центрів. У статті розглядаються ключові аспекти: правові засади, організаційна структура, практична реалізація, а також суспільна значущість ініціативи.

Метою статті є дослідження правових та організаційних засад створення та функціонування центрів підготовки громадян до національного спротиву в Україні на основі нормативно-правової бази 2021–2025 років, розкриття їхніх завдань в мирний час та в умовах особливого періоду, оцінювання практичної реалізації та суспільної значущості, виявлення проблемних аспектів, пов’язаних із фінансовим та матеріально-технічним забезпеченням системи центрів підготовки громадян до національного спротиву.

Методологічну основу дослідження процесу створення та функціонування центрів підготовки громадян до національного спротиву в Україні становить інтеграція системного підходу з адаптованими до сучасних умов засадами картезіанського методу Рене Декарта. Така комбінація дозволяє глибоко проаналізувати досліджувану проблему, впорядкувати її складові елементи та сформулювати логічно обґрунтовані висновки щодо ефективності функціонування зазначених центрів.

Аналіз організаційно-правових аспектів функціонування центрів підготовки громадян до національного спротиву показує, що центри діють як комунальні установи під егідою обласних рад, координуються обласними військовими адміністраціями, а їхні навчальні програми відповідають стандартам НАТО. Особлива увага приділяється ролі ветеранів як інструкторів, що сприяє якості підготовки та їхній соціальній реінтеграції. Практична реалізація центрів підтверджується даними, зокрема про підготовку понад 400 осіб у Харківській області у 2025 році.

Публікація також висвітлює суспільний вимір ініціативи, підкреслюючи добровільність участі як фактор успіху, та історичний контекст, зокрема оборону Маріуполя у 2022 році, що демонструє важливість підготовки цивільного населення. Критичний огляд джерел свідчить про брак емпіричних даних про ефективність центрів у 2024–2025 роках, а також про виклики, пов’язані з фінансуванням і регіональною нерівністю.

У висновках наголошується, що центри підготовки є невід’ємним елементом системи національного спротиву, який сприяє формуванню підготовленого та згуртованого суспільства. Перспективи розвитку включають масштабування мережі центрів, інтеграцію з освітньою системою та залучення міжнародної підтримки. Стаття підкреслює необхідність подальших досліджень для оцінювання довгострокової ефективності ініціативи.

Практичне значення дослідження полягає не лише у вдосконаленні системи підготовки студентів, а й у переосмисленні державного підходу – замість обмеження базовою загальновійськовою підготовкою йдеться про підготовку всього населення України до участі в національному спротиві.

**Ключові слова:** національний спротив, центри підготовки, обороноздатність, територіальна оборона, ветерани, стандарти НАТО, Маріуполь.

## Вступ (Introduction)

У зв’язку з початком широкомасштабної збройної агресії російської федерації проти України згідно зі статтею 65 Конституції України та згідно із Законом України від 11 квітня 2024 року № 3633-IX “Про внесення змін до деяких законодавчих актів України щодо окремих питань проходження військової служби, мобілізації та військового обліку” законодавцем було запроваджено базову загальновійськову підготовку здобувачів вищої освіти чоловічої статі,

яка розпочинається з 1 вересня 2025 року, згідно зі статтею 101 Закону України “Про військовий обов’язок і військову службу”.

Відповідно до Постанови Кабінету Міністрів України від 21 червня 2024 р. № 734 “Про затвердження Порядку проведення базової загальновійськової підготовки громадян України, які здобувають вищу освіту, та поліцейських” базова загальновійськова підготовка починається з вивчення теоретичної компоненти у закладах вищої освіти та продовжується після її опанування з травня по жовтень 2026 року практичною місячною підготовкою студентів на полігонній базі вищих військових навчальних закладів, військових навчальних підрозділів закладів вищої освіти, у навчальних частинах (центрах) Збройних Сил України (ЗС України), інших утворених відповідно до законів України військових формувань, правоохоронних органів спеціального призначення, Державної спеціальної служби транспорту та тренінгових центрах органів поліції.

Одним із викликів у проведенні базової військової підготовки є обмежена спроможність полігонної бази збройних сил: проведення практичної підготовки близько 70 000 студентів потребує значних фінансових ресурсів та логістичних зусиль, а витрати понад 7,5 млрд гривень (за оцінками експертів) з державного бюджету є неспівмірними з рівнем отриманих знань, умінь і навичок. До того ж, тривалість такої підготовки не повною мірою відповідає вимогам стандарту базової загальновійськової підготовки військовослужбовців.

Проблемними для держави і громадян залишаються і такі наслідки запровадження базової загальновійськової підготовки: військовою підготовкою не охоплені студенти фахових коледжів, а також студентки закладів вищої, фахової передвищої освіти; суспільно проблематичними залишаються норми проходження військово-лікарської комісії, призову районними територіальними центрами комплектування та соціальної підтримки, складання Військової присяги невійськовозобов’язаними студентами університетів; проходження військової підготовки студентами, місцем проживання яких є тимчасово окуповані території.

Проблеми в реалізації базової загальновійськової підготовки здобувачів освіти стали критичним тригером для стрімкого розвитку та інституціоналізації системи національного спротиву й актуалізували потребу в масовій участі громадян у захисті держави. Тому постала об’єктивна необхідність у певній трансформації чинної моделі базової загальновійськової підготовки здобувачів освіти у напрямі її інтеграції в ширший контекст формування системи національного спротиву.

**Огляд літератури (Literature review)**

Аналіз сучасних публікацій щодо центрів підготовки громадян до національного спротиву в Україні дозволяє певною мірою оцінити їхню роль у системі національної безпеки. Огляд відкритих джерел за 2021–2025 роки охоплює правові, організаційні та суспільні аспекти цієї ініціативи.

У статті “Національний спротив: Закон, який чекали 7 років” (2022) на порталі АрміяInform розглядається Закон України “Про основи національного спротиву”. Автор, Євген Проворний, зазначає, що закон об’єднує територіальну оборону, рух опору та загальновійськову підготовку, створюючи правову основу для системної підготовки громадян через центри [11].

У спільному дослідженні І. І. Сурміло та О. А. Журавель “Національний супротив як основа обороноздатності України” аналізують роль національного спротиву в забезпеченні обороноздатності держави, зокрема в контексті територіальної оборони та руху опору. Ця праця була представлена на VIII Міжнародній науково-практичній конференції “Міжнародна та національна безпека: теоретичні і прикладні аспекти” у 2024 році [14].

У статті “Національний спротив в Україні: історія та виклики сьогодення” Р. О. Кудряшов та Л. М. Івашова досліджують історичні витоки національного спротиву та

його сучасні прояви, зокрема в умовах збройної агресії проти України. Робота була опублікована в матеріалах міжнародної науково-практичної конференції, присвяченої 25-річчю Національного університету "Одеська юридична академія" у 2022 році [15].

Питанням засекречування локацій вищих військових навчальних закладів та навчальних центрів ЗС України в умовах збройної агресії приділяли увагу дослідники Є. О. Романенко, В. І. Гурковський, В. Ю. Ромахін [17].

Стаття "Як пов'язані рух опору, ССО і територіальна оборона: пояснення законопроєкту "Про національний спротив" (2021) на "Радіо Свобода" пояснює взаємодію Сил територіальної оборони та Сил спеціальних операцій у підготовці громадян. Центри розглядаються як елемент ширшої системи національного спротиву, що включає ідеологічну та військову складові [12].

У суспільному вимірі заслуговує на увагу стаття "Національний спротив – це ми" (2021) на порталі "Твоє місто", у якій підкреслено важливість добровільної участі громадян у підготовці. Автор акцентує, що саме добровільність є ключовим фактором успіху таких центрів [13].

Також варто звернути увагу на ґрунтовну предметну статтю "Національна стійкість та національний спротив – наріжні камені незламності України: за досвідом російсько-української війни" авторитетних учених І. Гаврилюка, В. Черепа, В. Дідіченка, О. Коня [20]. Зазначені дослідники комплексно проаналізували феномен національної стійкості та національного спротиву України як основних чинників незламності в умовах російсько-української війни з 2014-го по 2025 рік. Національний спротив розглядається цими вченими як багаторівневий процес протидії, який включає як військову складову (діяльність ЗС України, територіальної оборони, партизанського руху), так і широкий спектр цивільних ініціатив (волонтерство, інформаційний спротив, культурний опір).

Водночас бракує емпіричних даних про їхню ефективність у 2024–2025 роках, що може пояснюватися новизною ініціативи. Питання щодо фінансування та матеріально-технічного забезпечення центрів в умовах регіональної нерівності залишаються відкритими й потребують висвітлення та подальшого дослідження.

**Методологічна основа (Methodological Framework)**

Методологічна основа дослідження створення та функціонування центрів підготовки громадян до національного спротиву в Україні базується на поєднанні системного аналізу та принципів картезіанського методу Рене Декарта, адаптованих до сучасних умов. Такий підхід забезпечує структуризацію складної проблеми, її всебічний розгляд і логічно обґрунтовані висновки.

1. Дослідження застосовує системний аналіз для вивчення центрів підготовки як комплексної системи, що включає правові, організаційні, практичні та суспільні компоненти. Центри розглядаються як частина ширшої системи національного спротиву, яка охоплює взаємодію Сил територіальної оборони (ТрО), місцевих адміністрацій і громадянського суспільства. Системний підхід дозволяє ідентифікувати взаємозв'язки між цими елементами, оцінити їхній вплив на обороноздатність держави та виявити потенційні виклики, такі як фінансування чи регіональна нерівність.

2. Для збирання та оброблення даних використано аналіз нормативно-правових актів, офіційних звітів державних установ і публікацій у медіа. Основними джерелами є Закон України "Про основи національного спротиву" (2021), Постанови Кабінету Міністрів України від 29 грудня 2021 року № 1443 і від 18 квітня 2025 року № 160, а також звіти Харківської та Івано-Франківської обласних державних адміністрацій. Аналітичні матеріали з медіа, таких як АрміяInform, "Радіо Свобода" та "Українська правда", доповнюють дані, надаючи контекст суспільної підтримки та історичних паралелей, зокрема оборони Маріуполя у 2022 році.

3. Для структуризації дослідження використано принципи картезіанського методу (методу Декарта). Зокрема, застосовано:

• декомпозицію: проблема створення центрів розкладена на ключові аспекти – правові засади, організаційна структура, практична реалізація, суспільний вимір та історичний контекст;

• послідовний аналіз: кожен аспект досліджено окремо, починаючи з нормативної бази (закони, постанови), переходячи до організаційних механізмів (роль Сил ТрО, Сил спеціальних операцій (ССО), ветеранів) і завершуючи оцінкою результатів;

• синтез: результати аналізу окремих компонентів об'єднано для формування цілісної оцінки ефективності центрів і їхнього внеску в забезпечення обороноздатності;

•перевірка повноти: виключення прогалин, зокрема врахування регіональних відмінностей для належного фінансового та матеріально-технічного забезпечення мережі центрів підготовки.

**Результати (Results)**

Правові засади створення центрів підготовки громадян до національного спротиву ґрунтуються на комплексі нормативно-правових актів. Правову основу для системної підготовки громадян до оборони, створення руху опору та розвитку Сил територіальної оборони заклав Закон України "Про основи національного спротиву" № 1702-IX, ухвалений 16 липня 2021 року та введений в дію 1 січня 2022 року, [6]. Документ було офіційно опубліковано в газеті "Голос України" 31 липня. Закон визначає правові та організаційні засади національного спротиву, основи його підготовки та ведення, завдання і повноваження сил безпеки та сил оборони та інших визначених цим Законом суб'єктів з питань підготовки і ведення національного спротиву.

Ключовим механізмом реалізації закону стала ініціатива Президента України щодо розгортання центрів підготовки цивільних громадян до національного спротиву, які в 2025 році почали активно функціонувати по всій Україні з метою підготовки суспільства до сучасних загроз, підвищення обороноздатності держави, формування патріотичної свідомості та забезпечення суспільної стійкості.

Попри наявність законодавчого підґрунтя, система центрів підготовки громадян до національного спротиву в Україні потребує певного вдосконалення: спостерігаються певні проблеми щодо фрагментарного правового регулювання, відсутності цілісної моделі реалізації, браку приміщень, належного ресурсного забезпечення та ін. Ці виклики зумовлюють необхідність оцінювання практичної реалізації цієї ініціативи та виявлення можливих шляхів подолання цих викликів.

Система підготовки громадян до національного спротиву базується на Законі України "Про основи національного спротиву" (2021) і регулюється Постановою Кабінету Міністрів України від 18 квітня 2025 року № 160, яка встановлює порядок створення та функціонування центрів підготовки цивільних громадян до національного спротиву. Вона деталізує організаційні аспекти, зокрема підпорядкування центрів обласним радам або Київській міській раді, а також визначає роль обласних військових адміністрацій (ОВА) у координації та моніторингу їхньої роботи [4]. Також постанова вносить зміни до Порядку організації та здійснення загальновійськової підготовки громадян України до національного спротиву, затвердженого постановою від 29 грудня 2021 року № 1443 [1]. Ці зміни уточнюють механізми залучення ветеранів війни до підготовки інструкторів, котрі мають бойовий досвід, для підвищення якості навчання. Також постановою передбачається активне залучення ветеранів до роботи центрів, що сприяє не лише підвищенню якості підготовки, а й соціальній реінтеграції ветеранів. Ці нормативні акти створюють міцну правову основу, яка забезпечує системність у реалізації ініціативи.

Порядок створення та функціонування центрів підготовки громадян до національного спротиву затверджено Постановою Кабінету Міністрів України від 18 квітня 2025 року № 478 “Про функціонування центрів підготовки громадян до національного спротиву” [7].

Відповідно до зазначеного Закону національний спротив – комплекс заходів, які організовуються та здійснюються з метою сприяння обороні України шляхом максимально широкого залучення громадян України до дій, спрямованих на забезпечення воєнної безпеки, суверенітету і територіальної цілісності держави, стримування і відсічі агресії та завдавання противнику неприйнятних втрат, з огляду на які він буде змушений припинити збройну агресію проти України Заходи з організації, планування і підготовки руху опору здійснюються в мирний час та особливий період. Ведення руху опору здійснюється з настанням особливого періоду на тимчасово окупованій території України, території України, яка захоплена агресором (противником) під час збройної агресії проти України.

Основою підготовки громадян України до національного спротиву є їхня загальновійськова підготовка, яка організовується за територіально-зональним принципом, ґрунтується на засадах високої мотиваційної привабливості та узгоджується з процесом трансформації системи комплектування за призовом відповідно до принципів та найкращих практик держав – членів НАТО. Загальновійськова підготовка громадян України полягає в опануванні базовими загальновійськовими знаннями, практичними вміннями і навичками та поділяється на початкову і базову підготовку.

Початкова підготовка організовується центральним органом виконавчої влади, який забезпечує формування й реалізує державну політику у сфері освіти і науки разом із Міністерством оборони, та проводиться в закладах загальної середньої освіти. У літній час проводиться військово-патріотична підготовка в ігровій формі у літніх таборах.

Базова підготовка організовується Міністерством оборони разом з іншими зацікавленими центральними органами виконавчої влади та проводиться з громадянами України, які досягли 18-річного віку та не проходять військову службу у ЗС України, інших утворених відповідно до законів України військових формуваннях, службу в правоохоронних органах, шляхом періодичних навчальних зборів, занять, курсів.

Постановою Кабінету Міністрів України від 18 квітня 2025 року № 478 “Про функціонування центрів підготовки громадян до національного спротиву” також затверджується Примірне положення про комунальну організацію (установу, заклад) обласної / Київської міської ради “Обласний Київський міський центр підготовки громадян до національного спротиву” [7].

Згідно з Примірним положенням метою діяльності Центру є реалізація комплексу заходів, спрямованих на забезпечення готовності громадян України до національного спротиву, сприяння обороноздатності держави та надання обороні України всеохоплюючого характеру.

Основними завданнями діяльності Центру в мирний час є:

- проведення базової підготовки громадян до національного спротиву, включаючи опанування загальновійськовими знаннями, практичними вміннями, правилами поводження зі зброєю, індивідуальними засобами захисту та засвоєння основ із тактичної медицини тощо;
- зміцнення у громадян української національної та громадянської ідентичності на основі суспільно-державних (національних) цінностей України, стійкої мотивації та психологічної готовності до виконання конституційного обов’язку щодо захисту України, її незалежності та територіальної цілісності;
- організація військово-патріотичного виховання, спрямованого на формування оборонної свідомості, готовності стати до лав ЗС України та інших формувань сектору безпеки та оборони України, готовності до національного спротиву, героїзація та вшанування подвигів захисників та захисниць України;

- навчання громадян основам поведінки в умовах бойових дій, захисту населення, територій і навколишнього природного середовища, а також реагування на надзвичайні ситуації, пов'язані з наслідками воєнних дій;

- сприяння культурному, духовному та фізичному розвитку громадян, зокрема через заходи, що сприяють їхній фізичній загартованості та громадянській стійкості;

- взаємодія з ветеранами війни та волонтерськими організаціями, іншими інститутами громадянського суспільства для забезпечення навчального процесу та підвищення ефективності підготовки громадян;

- розроблення та впровадження освітніх програм, тренінгів, семінарів для підвищення професійного рівня інструкторів, викладачів та керівників навчальних груп, а також використання новітніх технологій для вдосконалення навчального процесу;

- раціональне використання матеріально-технічної бази Центру, забезпечення її розвитку, включаючи модернізацію обладнання та впровадження сучасних технологій;

- участь у реалізації державних, регіональних та місцевих програм у сфері оборони, національного спротиву та утвердження української національної та громадянської ідентичності, зокрема за напрямом військово-патріотичного виховання;

- забезпечення дотримання законодавства з охорони праці, пожежної безпеки та збереження матеріальних цінностей;

- провадження іншої діяльності, дозволеної законом, що відповідає меті функціонування Центру. [7].

В умовах особливого періоду основним завданням Центру додатково є перехід на прискорені плани підготовки громадян України (у прифронтових областях).

У складі організаційної структури Центру в установленому законодавством порядку можуть утворюватись відокремлені підрозділи (філії) в окремих населених пунктах області, районах у містах. Відповідні сільські, селищні, міські, районні у містах (у разі їх утворення) ради сприяють виділенню приміщень, навчальних матеріально-технічних засобів, забезпечують розміщення Центрів. Вони мають відповідати санітарно-технічним, безпековим та іншим вимогам для проведення навчань, тренувань і зберігання обладнання та навчальної зброї.

Відповідно до постанови керівників центрів призначатимуть обласні ради за поданням ОВА. Крім того, на ОВА покладаються обов'язки щодо контролю, моніторингу й оцінювання їхньої діяльності зі щоквартальним звітуванням Міноборони. Сили територіальної оборони затверджуватимуть типову програму підготовки, а керівниками центрів та інструкторами призначатимуть передусім ветеранів. Інструктори з національного спротиву проходитимуть навчання та сертифікацію у військових закладах вищої освіти. [7].

Центри підготовки створюються як комунальні установи або підприємства, що підпорядковуються обласним радам. Керівників центрів призначають за поданням ОВА, що забезпечує регіональну координацію. Типові програми підготовки розробляються Силами ТрО ЗС України з урахуванням місцевих потреб, що дозволяє адаптувати навчання до специфіки регіонів. ОВА відповідають за контроль і моніторинг діяльності центрів, подаючи щоквартальні звіти до Міністерства оборони.

Також схвалено примірне положення про комунальну організацію (установу, заклад) обласної чи Київської міської ради "Обласний / Київський міський Центр підготовки громадян до національного спротиву" та Примірний статут комунального підприємства обласної / Київської міської ради "Обласний / Київський міський Центр підготовки громадян до національного спротиву". Місцева влада має сприяти діяльності філій обласних центрів в окремих районах і населених пунктах області [7].

Відповідно до п. 14 постанови від 29 грудня 2021 року № 1443 фінансування та матеріально-технічне забезпечення загальновійськової підготовки громадян здійснюється за

рахунок і в межах коштів державного бюджету, видатків місцевих бюджетів, а також з інших не заборонених законодавством джерел [4].

18 квітня 2025 р. на засіданні уряду міністр освіти та науки Оксен Лісовий повідомив, що базову військову підготовку (БЗВП) пройдуть 75–80 тисяч українських студентів. Це все здобувачі освіти чоловічої статі другого року навчання, дівчата доєднуються за бажанням. Теоретичне навчання розпочнеться з 1 вересня 2025 року. За словами міністра освіти, вже розроблено понад 170 програм та подано їх на затвердження Генеральному штабу.

Водночас, під час виступу Оксен Лісовий зазначив, що нині тривають консультації з Міністерством оборони щодо змісту і формату практичної частини. Чоловіків, які відмовляються проходити навчання без поважних причин, можуть відрахувати з університету. Фінансування програми нині відбувається з резерву МОН, проте Лісовий висловив сподівання, що під час перегляду бюджету вдасться отримати додаткові кошти зі спеціального фонду. Від проходження базової військової підготовки звільняються визнані непридатними до військової служби за станом здоров'я, особи, які проходили військову службу раніше, та ті, хто має сертифікат про її проходження. Студенти, які навчаються за заочною, дистанційною або іншими формами навчання, та іноземні громадяни не проходитимуть БЗВП. Інших підстав для звільнення від проходження програми законодавством не передбачено. Військова підготовка складатиметься з двох частин та триватиме 300 академічних годин. Теоретичний курс має 90 годин. Практичний курс складатиметься з 210 академічних годин й проводитиметься у навчальних частинах, центрах збройних сил та інших установах. [10].

Особливу увагу приділено кадровому складу центрів. Керівниками та інструкторами призначаються переважно ветерани війни, які мають бойовий досвід. Інструктори проходять обов'язкове навчання та сертифікацію у військових закладах вищої освіти, що забезпечує високий професійний рівень. За потреби до роботи залучаються діючі військовослужбовці Сил ТрО та ССО ЗС України, що сприяє інтеграції цивільної та військової підготовки [5].

Станом на 2025 рік центри підготовки успішно функціонують у щонайменше дев'яти областях України: Київській, Волинській, Дніпропетровській, Закарпатській, Львівській, Одеській, Сумській, Харківській і Хмельницькій. Зокрема, у Харківській області з початку 2025 року підготовку пройшли понад 400 осіб у 15 групах, що свідчить про активне залучення громадян. Ініціатива була започаткована за дорученням Президента України після консультацій із представниками громадянського суспільства, що підкреслює її суспільну значущість. [7].

Почин створення центрів підготовки має низку сильних сторін.

По-перше, системний підхід до організації, що включає залучення широкого кола стейкхолдерів, забезпечує комплексність і врахування регіональних особливостей.

По-друге, акцент на залученні ветеранів як інструкторів підвищує якість навчання та сприяє їхній соціальній реінтеграції.

По-третє, добровільність і безкоштовність підготовки сприяють залученню широких верств населення, що певною мірою посилює суспільну згуртованість. При цьому мета створення та функціонування центрів – не лише сприяти набуттю громадянами практичних навичок для захисту держави, а й зміцнити патріотичну свідомість, що є важливим для довгострокової стабільності суспільства.

Позитивними аспектами є залучення ветеранів як інструкторів, добровільність і доступність підготовки, а також багатосторонній підхід до розроблення програм. Центри підготовки мають значний потенціал для масштабування та інтеграції з іншими елементами системи національної безпеки. Вони можуть стати основою для військово-патріотичного виховання молоді, підготовки до базової загальновійськової підготовки, яка стане обов'язковою у вищих навчальних закладах з 1 вересня 2025 року, а також для синергії з системою територіальної оборони. Крім того, ініціатива сприяє реалізації Стратегії

утвердження української національної ідентичності до 2030 року [19], та Стратегії залучення, розвитку та утримання людського капіталу в силах оборони України в період до 2027 року [18], зміцнюючи патріотичну свідомість громадян.

**Висновок (Conclusion)**

Звичайно, попри очевидні переваги, ініціатива стикається з певними проблемними аспектами, зокрема щодо фінансування та матеріально-технічного забезпечення. Нерівномірний економічний розвиток регіонів може ускладнити створення центрів у менш забезпечених областях. Однак ці труднощі можуть бути подолані шляхом посилення співпраці із зарубіжними партнерами, залучення міжнародної допомоги.

Цілком очевидним є те, що, крім залучення міжнародної підтримки, перспективи розвитку системи підготовки громадян до національного спротиву включають масштабування мережі центрів з метою розширення баз обороноздатного населення, оскільки ефективність національного спротиву залежить від кількості та якості підготовлених осіб і посилення взаємодії між цивільними та військовими структурами. Безперечно, громадяни мають бути інтегровані у загальну архітектуру національної безпеки. До того ж, своєчасна підготовка населення дозволяє зменшити витрати у разі повторного вторгнення.

Без масштабування системи підготовки громадян держава ризикує втратити можливість оперативного залучення населення до спротиву, що є одним із ключових чинників національної стійкості у XXI столітті.

Отже, система підготовки до національного спротиву є важливим інструментом для забезпечення обороноздатності безпеки та суспільної єдності, яка закладає основу для готовності нації до сучасних безпекових загроз. Ініціатива щодо створення мережі центрів підготовки має глибокі історичні паралелі з подіями новітньої історії України, зокрема з героїчною обороною Маріуполя у 2022 році, коли військові та цивільні особи спільно чинили опір ворогу протягом 86 днів, демонструючи значення підготовленості та згуртованості для захисту держави та підкреслюючи необхідність підготовки для всіх громадян [9].

Слід підкреслити, що відповідно до статті 17 Конституції України захист суверенітету і територіальної цілісності України є справою всього українського народу, що робить систему національного спротиву не просто ініціативою для певних верств населення, таких як студенти, а загальнонаціональним обов'язком. Водночас стаття 65 Конституції України закріплює захист Вітчизни, її незалежності та територіальної цілісності України як обов'язок кожного громадянина, незалежно від віку, професії чи статусу.

**Використані джерела**

1. Кабінет Міністрів України. (2025, 23 квіт.) *Про внесення змін до Порядку організації та здійснення загальновійськової підготовки громадян України до національного спротиву*. Міністерство у справах ветеранів України. https://mva.gov.ua/ua/npa/proekt-postanovi-kabinetu-ministriv-ukraini-pro-vnesennia-zmin-do-poriadku-organizacii-ta-zdiisnennia-zagalnoviiskovoi-pidgotovki-gromadian-ukraini-do-nacionalnogo-sprotivu
2. *У кожному регіоні України запрацюють центри підготовки громадян до національного спротиву*. (2025, 18 квіт.). Рішення Уряду. https://www.president.gov.ua/news/u-kozhnomu-regioni-ukrayini-zapracyuyut-centri-pidgotovki-89897
3. *Кабінет Міністрів України затвердив порядок створення Центрів підготовки населення до національного спротиву*. (2025, 17 квіт.). Харківська обласна державна адміністрація. https://kharkivoda.gov.ua/news/126025
4. Кабінет Міністрів України. (2025, 14 лют.). *Про внесення змін до Порядку організації та здійснення загальновійськової підготовки громадян України до національного спротиву (160/2025)*. https://zakon.rada.gov.ua/laws/show/160-2025-%D0%BF

5. Українців готуватимуть до національного спротиву: Міноборони створить мережу центрів. (2025, 22 квіт.). *Українська правда*. https://www.pravda.com.ua/news/2025/04/22/7551234/
6. Закон України *"Про основи національного спротиву"* № 1702-IX (2021, 16 лип.). https://zakon.rada.gov.ua/laws/show/1702-20#Text
7. Кабінет Міністрів України. (2025, 18 квіт.). *Про функціонування центрів підготовки громадян до національного спротиву (478/2025).* https://www.kmu.gov.ua/npas/pro-funktsionuvannia-tsentriv-pidhotovky-hromadian-do-natsionalnoho-
8. По всій Україні запрацюють центри підготовки до нацспротиву: рішення уряду. (2025, 18 квіт.). *ТСН.* https://tsn.ua/ato/po-vsiy-ukrayini-zapracyuyut-centri-pidgotovki-do-nacsprotivu-rishennya-uryadu-2549879.html
9. Оборона Маріуполя: знищено бронетехніку і живу силу ворога. (2022, 13 бер.). *Українська правда*. https://www.pravda.com.ua/news/2022/03/13/7330937/
10. *Близько 80 тисяч студентів України пройдуть базову військову підготовку: що передбачає програма*. https://shkola.obozrevatel.com/ukr/news/blizko-80-tisyach-studentiv-ukraini-projdut-bazovu
11. Проворний, Є. (2022, 2 січ.). Національний спротив: Закон, який чекали 7 років. *АрміяInform.* https://armyinform.com.ua/2022/01/02/naczionalnyj-sprotyv-zakon-yakyj-chekaly-7-rokiv/
12. Як пов'язані рух опору, ССО і територіальна оборона: пояснення законопроєкту "Про національний спротив. (2021, 12 черв.). *Радіо Свобода*. https://www.radiosvoboda.org/a/nacionalnyj-sprotyv-zakonoproekt/31304739.html
13. Національний спротив – це ми. (2021, 10 груд.). *Твоє місто*. https://tvoemisto.tv/news/nacionalnyy_sprotyv__ce_my_126432.html
14. Сурміло, І. І., Журавель, О. А. (2024, 15 бер.). Національний супротив як основа обороноздатності України. У Матеріалах VIII Міжн. наук.-практ. конф., *Міжнародна та національна безпека: теоретичні і прикладні аспекти* (Ч. 1., с. 512–514). ДДУВС.
15. Кудряшов, Р. О., & Івашова, Л. М. (2022, 17 черв.). Національний спротив в Україні: історія та виклики сьогодення. У Матеріалах Міжнар. наук.-практ. конф., *Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття* (Т. 1., с. 195–198). Видавничий дім "Гельветика".
16. Романенко, Є. О., & Гурковський В. І. (2024, 7 жовт.). Створення єдиного державного реєстру військовослужбовців: нова ініціатива в Україні. У Матеріалах XLIX Міжн. наук.-практ. конф., *Сучасні аспекти модернізації науки: стан, проблеми, тенденції розвитку* (с. 20–23). (І. В. Жукова, Є. О. Романенко, Ред.). ВАДНД.
17. Романенко, Є. О., Гурковський, В. І., & Ромахін В. Ю. (2024). *Засекречування локацій стратегічних об'єктів України в умовах збройної агресії: правові підходи та безпекові наслідки.* Moderní aspekty vědy: XLVII. Díl mezinárodní kolektivní monografie Mezinárodní Ekonomický Institut s.r.o. (str. 5–69).
18. Міністерство оборони України. (2024, 29 груд.). *Про затвердження Стратегії залучення, розвитку та утримання людського капіталу в силах оборони України в період до 2027 року (862/нм/2024).* https://mod.gov.ua/diyalnist/normativno-pravova-baza/nakaz-ministerstva-oboroni-ukrayini-vid-29-12-2024-862-nm-pro zatverdzchennya-rozvitku-ta-utrimannya-lyudskogo-kapitalu-v-silah-oboroni-ukrayini-na-period-do-2027-roku/
19. Кабінет Міністрів України. (2023, 16 груд.). *Про схвалення Стратегії утвердження української національної та громадянської ідентичності на період до 2030 року та затвердження операційного плану заходів з її реалізації у 2023–2024 роках (1322/2023).* https://osvita.ua/legislation/other/90975/

20. Гаврилюк, І., Череп, В., Дідіченко, В., & Кінь, О. (2025). Національна стійкість та національний спротив – наріжні камені незламності України: за досвідом російсько-української війни *Military Science*, *3* (1), 73–86 . https://doi.org/10.62524/msj.2025.3.1.03
21. Декарт, Р. (2017). *Міркування про метод, щоб правильно вести свій розум і віднайти істину в науках*. (О. Й. Хоменко, Пер. з фр.). Дух і Літера.
22. Descartes, R. (1637). *Discourse on the Method of Rightly Conducting Ones Reason and of Seeking Truth in the Sciences.* https://www.gutenberg.org/files/59/59-h.html

**References**

1. Cabinet of Ministers of Ukraine. (2025, Apr. 23). *On Amendments to the Procedure for Organizing and Conducting General Military Training of Ukrainian Citizens for National Resistance*. Ministry for Veterans Affairs of Ukraine. https://mva.gov.ua/ua/npa/proekt-postanovi-kabinetu-ministriv-ukraini-pro-vnesennia-zmin-do-poriadku-organizacii-ta-zdiisnennia-zagalnoviiskovoi-pidgotovki-gromadian-ukraini-do-nacionalnogo-sprotivu
2. *Training Centers for Citizens' National Resistance to Begin Operation in Every Region of Ukraine*. (2025, Apr. 18). Government Decision. https://www.president.gov.ua/news/u-kozhnomu-regioni-ukrayini-zapracyuyut-centri-pidgotovki-89897
3. *Cabinet of Ministers of Ukraine Approved the Procedure for Establishing Population Training Centers for National Resistance*. (2025, Apr. 17). Kharkiv Regional State Administration. https://kharkivoda.gov.ua/news/126025
4. Cabinet of Ministers of Ukraine. (2025, Febr. 14). *On Amendments to the Procedure for Organizing and Conducting General Military Training of Ukrainian Citizens for National Resistance (160/2025)*. https://zakon.rada.gov.ua/laws/show/160-2025-%D0%BF
5. Ukrainians Will Be Trained for National Resistance: Ministry of Defense to Create a Network of Centers. (2025, Apr. 22). *Ukrainska Pravda*. https://www.pravda.com.ua/news/2025/04/22/7551234/
6. Law of Ukraine *"On the Foundations of National Resistance"* No. 1702-IX (2021, July 16). https://zakon.rada.gov.ua/laws/show/1702-20#Text
7. Cabinet of Ministers of Ukraine. (2025, April 18). *On the functioning of citizen training centers for National resistance (478/2025).* https://www.kmu.gov.ua/npas/pro-funktsionuvannia-tsentriv-pidhotovky-hromadian-do-natsionalnoho-
8. Nationwide Network of National Resistance Training Centers to Begin Operation: Government Decision. (2025, Apr. 18). *TSN.* https://tsn.ua/ato/po-vsiy-ukrayini-zapracyuyut-centri-pidgotovki-do-nacsprotivu-rishennya-uryadu-2549879.html
9. Defense of Mariupol: Enemy Armored Vehicles and Personnel Destroyed. (2022, March 13). *Ukrainska Pravda*. https://www.pravda.com.ua/news/2022/03/13/7330937/
10. *About 80,000 Ukrainian Students to Undergo Basic Military Training: What the Program Entails*. https://shkola.obozrevatel.com/ukr/news/blizko-80-tisyach-studentiv-ukraini-projdut-bazovu
11. Provorniy, Y. (2022, Jan. 2). National Resistance: The Law Awaited for 7 Years. *ArmyInform*. https://armyinform.com.ua/2022/01/02/naczionalnyj-sprotyv-zakon-yakyj-chekaly-7-rokiv/
12. How the Resistance Movement, Special Operations Forces, and Territorial Defense Are Connected: Explanation of the Draft Law 'On National Resistance. (2021, June 12). *Radio Svoboda*.
13. National Resistance — That's Us. (2021, Dec. 10). *Tvoe Misto.* https://tvoemisto.tv/news/nacionalnyy_sprotyv__ce_my_126432.html
14. Surmilo, I. I. & Zhuravel, O. A. (2024, March 15). National Resistance as the Basis of Ukraine's Defense Capability. International Scientific-Practical Conference, *International and National Security: Theoretical and Applied Aspects* (Part 1, pp. 512–514). DSUVS.

15. Kudryashov, R. O. & Ivashova, L. M. (2022, June 17). National Resistance in Ukraine: History and Contemporary Challenges. Proceedings of the International Scientific–Practical Conference, *Europe's Choice of Ukraine, the Development of Science and National Security in the Realities of Large-Scale Military Aggression and Global Challenges of the 21st Century* (Vol. 1, pp. 195–198). Helvetika Publishing House.
16. Romanenko, Ye. O. & Hurkovskyi, V. I. (2024, Oct. 7). *Creation of a Unified State Register of Servicemen: A New Initiative in Ukraine.* Proceedings of the 49th International Scientific-Practical Conference, *Modern Aspects of Science: Status, Problems, Development Trends* (pp. 20–23). (Ed. I. V. Zhukova & Ye. O. Romanenko). VADND.
17. Romanenko, Ye. O.; Hurkovskyi, V. I.; Romakhin, V. Yu. (2024). *Secrecy of Locations of Strategic Facilities in Ukraine under Armed Aggression: Legal Approaches and Security Consequences*. Moderní aspekty vědy: XLVII. Díl mezinárodní kolektivní monografie. International Economic Institute s.r.o. (pp. 58–69).
18. Ministry of Defense of Ukraine. (2024, Dec. 29). *On Approval of the Strategy for Attracting, Developing, and Retaining Human Capital in the Defense Forces of Ukraine through 2027 (862/нм/2024)* https://mod.gov.ua/diyalnist/normativno-pravova-baza/nakaz-ministerstva-oboroni-ukrayini-vid-29-12-2024-862-nm-pro zatverdzchennya-rozvitku-ta-utrimannya-lyudskogo-kapitalu-v-silah-oboroni-ukrayini-na-period-do-2027-roku/
19. Cabinet of Ministers of Ukraine. (2023, Dec. 16). *On Approval of the Strategy for Establishing Ukrainian National and Civic Identity through 2030 and Adoption of the Operational Plan of Measures for Its Implementation in 2023–2024 (1322/2023).* https://osvita.ua/legislation/other/90975/
20. Havryliuk, I., Cherep, V., Didichenko, V., & Kin, O. (2025). National Resilience and National Resistance – Cornerstones of Ukraine's Invincibility: Lessons from the Russo-Ukrainian War. *Military Science*, 3 (1), 73–86. https://doi.org/10.62524/msj.2025.3.1.03.
21. Descartes, R. (2017). *Meditations on the Method of Properly Guiding One's Reason and Seeking Truth in the Sciences*. (Transl. from French by O. Homenko). Dukh i Litera.
22. Descartes, R. (1637). *Discourse on the Method of Rightly Conducting One's Reason and of Seeking Truth in the Sciences*. https://www.gutenberg.org/files/59/59-h.html

## State Defense Capability: Organizational and Legal Aspects of Preparing Citizens for National Resistance

**Oleh Semenenko**
Honoured Science and Technology Figure of Ukraine
Doctor of Military Sciences, Professor
Deputy Commandant of the Central Research Institute of the
of the Armed Forces of Ukraine for scientific work
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl avenue, 28 B, Kyiv, Ukraine
e-mail: aosemenenko@ukr.net
ORCID: 0000-0001-6477-3414

**Volodymyr Hurkovskyi**
Doctor of Public Administration, Professor
Head of Department
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl avenue, 28 B, Kyiv, Ukraine
e-mail: volodymyrgurkovskyi@gmail.com
ORCID: 0000-0003-2021-5204

**Yevhen Romanenko**
Doctor of Public Administration, Professor
Head of Department
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl avenue, 28 B, Kyiv, Ukraine
e-mail: volodymyrgurkovskyi@gmail.com
ORCID: 0000-0003-2021-5204

**Oleksandr Verbovenko**
Deputy Chief of the Civil-Military Cooperation Central Directorate
General Staff of the Armed Forces of Ukraine
03168, Povitrianykh Syl avenue, 6, Kyiv, Ukraine
e-mail: vop197007@gmail.com
ORCID: 0009-0004-5188-267X

**Serhii Mytchenko**
Doctor of Philosophy
Associate Professor of the National Security and Defense Strategy Department
National Defence University of Ukraine
03049, Povitrianykh syl avenue, 28, Kyiv, Ukraine
e-mail: serhii.mytchenko@gmail.com
ORCID: 0000-0003-3711-2033

**Abstract.** This article is devoted to the analysis of the establishment and functioning of centers for training citizens in national resistance in Ukraine, which are a fundamental component of strengthening the state's defense capability amid modern threats to national security. The study is based on the legal framework, in particular the Law of Ukraine "On the Foundations of National Resistance" (2021), and Resolutions of the Cabinet of Ministers of Ukraine dated December 29, 2021 (No. 1443), and April 18, 2025, which regulate the organization and operation of these centers.

The article examines key aspects: legal foundations, organizational structure, practical implementation, and the social significance of the initiative. The purpose of the article is to explore the legal and organizational principles of establishing and operating citizen training centers for national resistance in Ukraine, based on the 2021–2025 regulatory framework, to reveal their roles in peacetime and special periods, evaluate their practical implementation and public relevance, and identify challenges related to the financial and material-technical support of the system.

The methodological basis of the study is the integration of a systems approach with the adapted principles of René Descartes' Cartesian method under modern conditions. This combination enables a thorough analysis of the issue, structuring its elements and formulating logically sound conclusions about the effectiveness of these centers.

The analysis of the organizational and legal aspects shows that the centers function as municipal institutions under the auspices of regional councils, coordinated by regional military administrations, with training programs aligned with NATO standards. Special attention is given to the involvement of veterans as instructors, enhancing the training quality and supporting their social reintegration. Practical implementation is evidenced by data, including the training of over 400 individuals in Kharkiv region in 2025.

The article also highlights the societal dimension of the initiative, emphasizing voluntary participation as a success factor, and places the issue in historical context, particularly the 2022 defense of Mariupol, demonstrating the importance of civilian readiness. A critical review of sources points to a lack of empirical data on the effectiveness of the centers in 2024–2025, as well as challenges related to funding and regional disparities.

In conclusion, the training centers are emphasized as an integral element of the national resistance system, contributing to the formation of a prepared and cohesive society. Future prospects include expanding the network, integrating with the educational system, and attracting international support. The article underscores the need for further research to assess the long-term effectiveness of this initiative.

The practical significance of the study lies not only in improving the student training system but also in rethinking the state's approach—from limiting training to basic military preparedness to training the entire population of Ukraine for participation in national resistance.

**Keywords:** national resistance, training centers, defense capability, territorial defense, veterans, NATO standards, Mariupol.

The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 3 No. 2 (2025)

DOI: 10.62524/msj.2025.3.2.18

# Аналіз теорії і практики розвитку когнітивних загроз у сфері воєнної безпеки: шляхи подолання

**Олександр Кінь**
кандидат технічних наук, доцент
старший науковий співробітник
Дипломатична академія України імені Геннадія Удовенка
при Міністерстві закордонних справ
01001, м. Київ, вул. Велика Житомирська, 2
email: cubalibre1972@ukr.net
ORCID: 0009-0001-2196-7515

**Анотація.** Державна політика безпеки, військова наука та практичне військове управління досі не мають системного підходу до вивчення й протидії когнітивним загрозам. Не вироблено єдиного понятійно-термінологічного апарату, методів діагностики, моніторингу й оцінювання рівня когнітивної безпеки. Відсутність доктринальної, нормативної та науково-методичної бази унеможливлює формування ефективної системи протидії. Отже, потреба у теоретико-прикладному аналізі процесів формування, розвитку та реалізації когнітивних загроз у сфері воєнної безпеки України є вкрай актуальною, оскільки безпосередньо пов'язана з потенціалом держави до стратегічного спротиву, стійкості системи національної безпеки, збереженням управлінської цілісності та морально-психологічної готовності до оборони. Основними результатами статті є те, що в ній: сформовано хронологічну послідовність розвитку когнітивних загроз у війнах і воєнних конфліктах (історичний аспект); розкрито порядок трансформації когнітивних загроз для України з 1991 року до сьогодення; удосконалено понятійно-термінологічний апарат методології стратегічного реагування на когнітивні загрози; сформовано станом на червень 2025 року сучасні когнітивні загрози воєнній безпеці України; розроблено матрицю пріоритезації когнітивних загроз; визначено ключові інтегральні показники, які дозволяють не лише виявляти небезпеки, а й оцінювати динаміку впливу, здатність до спротиву та потенціал до попередження негативних когнітивних ефектів; наведено результати експертного опитування щодо частоти появи та рівня впливу когнітивних загроз на рівень воєнної безпеки України, а також результати розрахунку індексу когнітивного тиску станом на червень 2025 року; сформовано систему рекомендацій щодо ефективної протидії актуальним когнітивним загрозам воєнній безпеці України станом на червень 2025 року; запропоновано модель (структура) реагування на когнітивні загрози воєнній безпеці України та визначено основні показники моніторингу когнітивних загроз і заходи реагування на них. Матеріали статті можуть бути корисними військовим, аналітикам, фахівцям з безпеки, науковцям і стратегам, які займаються захистом інформаційного простору та реагуванням на сучасні когнітивні загрози у сфері воєнної безпеки України.

**Ключові слова:** гібридна війна, воєнні дії, воєнна безпека, збройна боротьба, когнітивні загрози, когнітивний вплив, когнітивні виклики, воєнно-політична логіка, індекс когнітивного тиску, технології війни, тактика та стратегія воєнних дій, національна безпека, глобальна стабільність, методи ведення війни, трансформація збройних конфліктів, реагування на когнітивні загрози, моніторинг когнітивних загроз, форми воєнних дій.

**Вступ (Introduction)**

У сучасних умовах російсько-української війни, що триває, питання щодо забезпечення воєнної безпеки України набуло критичної важливості. Поряд із традиційними формами збройної агресії, дедалі більшого значення набуває використання когнітивних загроз – цілеспрямованого впливу на свідомість, поведінку та сприйняття суспільства, військовослужбовців, керівництва держави. Цей новий вимір війни – так звана когнітивна війна – охоплює інформаційно-психологічні операції, маніпуляції у медіа-просторі, використання штучного інтелекту (ШІ), соціальних мереж і цифрових платформ для формування викривленого уявлення про реальність, дезорієнтації, деморалізації або навіть провокування дій, вигідних агресору [1–6].

Сьогодні російська федерація системно застосовує когнітивні впливи як складову своєї стратегії гібридної війни. Це проявляється у спробах підірвати довіру до державних інституцій, розмиванні суспільної єдності, деморалізації військових, дискредитації міжнародної підтримки України, створенні ілюзії невідворотності поразки чи безсенсовності спротиву. Особливо небезпечними є складноідентифіковані або латентні загрози, які маскуються під “внутрішні” дискурси або позиціонуються як альтернативна правда. Водночас державна політика безпеки, військова наука та практичне військове управління досі не мають системного підходу до вивчення й протидії когнітивним загрозам. Не вироблено єдиного понятійно-категоріального апарату, методів діагностики, моніторингу й оцінювання рівня когнітивної безпеки. Через відсутність доктринальної, нормативної та науково-методичної бази неможливо сформувати ефективну систему протидії [1–22].

Отже, потреба у теоретико-прикладному аналізі процесів формування, розвитку та реалізації когнітивних загроз у сфері воєнної безпеки України є вкрай актуальною, оскільки безпосередньо пов’язана з потенціалом держави до стратегічного спротиву, стійкості системи національної безпеки, збереженням управлінської цілісності та морально-психологічної готовності до оборони.

Дослідження цієї тематики має не лише науково-пізнавальну, а й високу практичну значущість – для розроблення національної стратегії когнітивної безпеки, удосконалення доктринального апарату, підготовки військових кадрів нового покоління, здатних протистояти не лише фізичному, а й когнітивному впливу противника.

**Матеріали та методи (Materials and Methods)**

У контексті формування ефективної системи стратегічного реагування на когнітивні загрози у сфері воєнної безпеки особливої актуальності набуває всебічний аналіз наукових і прикладних джерел, що розкривають природу, механізми та наслідки таких загроз. Такий аналіз дозволяє: виявити існуючі підходи до трактування когнітивних загроз та їхнього впливу; визначити наукові та методологічні прогалини в сучасному дискурсі; зіставити вітчизняні й зарубіжні дослідницькі традиції; ідентифікувати потенційно релевантні практики, які можуть бути адаптовані до умов України. У табл. 1 представлено огляд джерел, який дає змогу сформувати наукове підґрунтя для подальшого розроблення теоретико-методичних засад протидії когнітивним загрозам у секторі безпеки і оборони.

Західна література більше зосереджена на системному аналізі, прогнозуванні, технологіях когнітивного впливу. Українські джерела концентруються на практиці протидії в умовах гібридної війни з росією. Спільна тенденція – визнання когнітивної сфери як одного з основних полів воєнного протиборства в XXI столітті [1–22].

На підставі аналізу літератури за тематикою розвитку когнітивних загроз сформуємо історичний алгоритм розвитку когнітивних загроз у війнах і воєнних конфліктах, представлений у вигляді хронологічної послідовності з виокремленням ключових періодів, особливостей когнітивного впливу, методів його реалізації та основоположників нових типів

загроз (табл. 2) [1–22].

**Таблиця 1.** Аналіз джерел за тематикою когнітивних загроз у воєнній безпеці

| Автор / Джерело | Назва або тип публікації | Короткий зміст / Основні положення |
|---|---|---|
| NATO Innovation Hub (2020) | *Cognitive Warfare – NATO's Sixth Domain of Operations* | Уперше вводиться концепт "когнітивної війни" як окремої домінанти. Описано використання дезінформації, соціальних медіа для впливу на мислення та ухвалення рішень. Когнітивна сфера визначена як поле сучасного конфлікту. |
| RAND Corporation (2019–2023) | Аналітичні доповіді: *Cognitive Security, Influence Operations, Disinformation Threats* | Поглиблено розглядається вплив інформаційних операцій на сприйняття, поведінку військових і цивільного населення. Увага на стратегіях рф і Китаю. Розглянуто методи оцінювання та протидії. |
| Hybrid CoE (Helsinki) | Аналітичні нотатки (2021–2024) | Вивчаються гібридні загрози, у т. ч. когнітивні. Особливу увагу приділено впливу на процеси ухвалення рішень, психологічній маніпуляції та створенню фальшивої реальності через цифрові платформи. |
| J. Q. Wilson, P. K. Davis | *Cognitive Domain Operations: Strategic Advantage in the Human Mind* (2021) | Підкреслено важливість когнітивного домену в концепції "multi-domain operations". Обґрунтовано важливість формування ментальної переваги для забезпечення стійкості збройних сил. |
| З. Манойла (НУОУ) | Монографія *Когнітивна безпека держави: теоретико-прикладні основи* (2021) | Розроблено класифікацію когнітивних впливів, визначено їхню роль у трансформації безпекового середовища. Запропоновано структуру когнітивного захисту держави. |
| І. Шевцов (Інститут стратегічних досліджень) | Аналітичні записки щодо інформаційної війни рф | Вказано, що когнітивні операції рф формуються на базі радянської школи маскування та сучасних інформаційно-психологічних технологій. Розглянуто приклади з війни проти України. |
| S. Bendett (CNA, США) | Аналітика про російські інформаційні та когнітивні підходи (2018–2023) | Детально аналізується підхід рф до когнітивних впливів як елемента "воєнно-інформаційної доктрини". Акцент на роботі з емоціями, страхом, фейками. |
| Збірник наукових праць "Воєнна безпека України" (НІСД, 2022–2024) | Збірка статей | Низка авторів аналізують когнітивний вплив у контексті війни з рф. Оцінюються ризики дезорієнтації населення, деморалізації військ, підриву довіри до влади. |
| Центр стратегічних комунікацій та інформаційної безпеки України (2021–2024) | Аналітика, доповіді | Системно досліджуються ворожі наративи, маніпулятивні кампанії в інформаційному середовищі. Створено базу прикладів когнітивних атак. |
| P. W. Singer, Emerson T. Brooking | *LikeWar: The Weaponization of Social Media* (2018) | Розкрито, як соціальні мережі перетворилися на інструмент ведення когнітивних бойових дій. Приклади з США, Близького Сходу, України. |

Історичний розвиток когнітивних загроз демонструє поступовий перехід від інстинктивно-психологічного впливу до високотехнологічної багаторівневої когнітивної війни, в якій мета – не фізичне знищення ворога, а перехоплення його мислення, нав'язування рішень і підрив системи ідентичності. Розуміння цієї історичної логіки – ключ до розроблення ефективних стратегій захисту в умовах сучасної війни.

**Таблиця 2.** Хронологічна послідовність розвитку когнітивних загроз у війнах і воєнних конфліктах (історичний аспект)

| Період | Особливості когнітивних загроз | Методи формування когнітивних загроз | Основоположники |
|---|---|---|---|
| Давньосхідний і Античний період (до V ст. н. е.) | Основу становили обман, дезінформація, психологічна маніпуляція через релігію, міфи, символіку, страх. Вплив здійснювався через ритуали, пророкування, демонстративні жорстокі дії. | Поширення чуток, чуттєвого залякування, використання "страху богів". Символічні дії (знищення священних артефактів, демонстрація трофеїв). | Сунь-Цзи, автор трактату *"Мистецтво війни"*, описав важливість обману і психологічної переваги. Артеміда і Александр Македонський – застосовували ритуальну демонстрацію сили й інформаційне нав'язування переваги. |
| Середньовіччя та Ранній Новий час (V–XVII ст.) | Інтеграція релігії та воєнної пропаганди. Когнітивний вплив через індоктринацію, фанатизм, створення образу "священного ворога". | Проповідницька війна (хрестові походи). Створення героїчних і демонічних образів через церковну пропаганду, літописи. Публічні страти, які мали когнітивний ефект покарання і страху. | Католицька церква, інквізиція – як інструменти когнітивного контролю. Мартін Лютер – започаткував реформаційні рухи, які мали потужний когнітивний вплив на світогляд народів. |
| Епоха Просвітництва і Національних війн (XVIII–XIX ст.) | Поява світської пропаганди, ідеологічного впливу через ідеї свободи, націоналізму, соціалізму. Когнітивна війна йде через інститути друку, школи, символіку влади. | Використання гасел ("Свобода, рівність, братерство"), памфлетів, театральних виступів. Створення культу особистості (Наполеон, Гарібальді). Нав'язування національної ідентичності через освіту. | Наполеон Бонапарт – активно використовував пропаганду як засіб контролю над масами. Французькі просвітники Вольтер, Руссо – створили інтелектуальне підґрунтя для нових когнітивних впливів. |
| Світові війни (1914–1945) | Широкомасштабна державна пропаганда як частина воєнної стратегії. Мілітаризація інформації та введення в оману як стратегічна зброя. | Мобілізаційна пропаганда через газети, плакати, кінематограф. Поширення фальшивих повідомлень (операції "London Black"). Використання радіо як інструменту масового впливу. | Йозеф Геббельс – творець нацистської інформаційної машини. Британський офіс воєнної інформації (MOI) – піонери психологічних операцій. |
| Холодна війна (1947–1991) | Формування концепції психологічної війни, стратегічної дезінформації, боротьби за уми та переконання. Війна ідеологій (капіталізм vs. комунізм). | Радіо-війни (Radio Free Europe, Голос Америки). Культурна експансія, контроль за інформаційними потоками, пропагандистські фільми. Спецоперації КДБ, ЦРУ для посилення внутрішніх конфліктів у державах супротивника. | КДБ СРСР – творці концепції активних заходів. ЦРУ США – розробники програм психологічного впливу і медійної дестабілізації. |
| Постмодерний етап (1991–2010) | Когнітивний вплив в умовах інформаційного перевантаження, маніпуляцій у глобальному медіа-просторі. Формування реальності через візуальні образи, масову культуру, соціальні наративи. | Використання CNN-ефекту, "інформаційного шуму", фабрикацій. Поява перших інформаційних операцій у кіберсередовищі. Цілеспрямована дестабілізація через медіа-сюжети (приклад – війна в Іраку 2003). | RAND Corporation – автори концепцій інформаційних операцій. Збігнєв Бжезинський – аналітик когнітивних і геополітичних взаємозв'язків. |

**Продовження таблиці 2.** Хронологічна послідовність розвитку когнітивних загроз у війнах і воєнних конфліктах (історичний аспект)

| | | | |
|---|---|---|---|
| Цифрова когнітивна війна – етап (2010–2014 ) | Масове застосування штучного інтелекту, ботів, deepfake, нейронних мереж для впливу на суспільну думку. Поняття когнітивного домену стає ключовим у концепціях нової війни (NATO Cognitive Warfare). | Мікротаргетинг через соціальні мережі (Facebook-Cambridge Analytica). Інфільтрація цифрових платформ, нав'язування "альтернативних реальностей". Глибока дезорієнтація та когнітивне виснаження суспільства. | Китайські концепції "brain-control warfare". NATO Innovation Hub – автори доктрини Cognitive Warfare. Російські структури (IRA, ФСБ) – практики інформаційної деструкції через Telegram, TikTok, YouTube. |
| Формативно-експериментальний етап когнітивної війни (2010–2014 рр.) | Формування передумов до масової гібридизації воєн;<br>Акцент на інформаційно-психологічному впливі у кіберсередовищі. Спроба маніпулювання протестними наративами. | Технології впливу через ЗМІ, тролі, "ботоферми". Викиди дезінформації; Таргетована реклама в соцмережах. | рф: концепція інформаційної війни Герасимова (2013). КНР, Іран – тестування цифрових впливів. |
| Етап гібридизації та інституціоналізації когнітивних загроз (2014–2022 рр.) | Інституціоналізація ІПСО як воєнного інструмента (після окупації Криму і вторгнення на Донбас). Введення в обіг терміна "когнітивна війна". Масова цифровізація впливу. | Операції впливу на Facebook, Twitter; Fake news. Конспірологічні наративи; Створення медіа-кілерів. | рф: "фабрика тролів", RT, Sputnik.<br>NATO StratCom дослідження когнітивних маніпуляцій. Cambridge Analytica. |
| Етап тотальної когнітивної війни та технологічної ескалації (2022–2025 рр.) | Системна когнітивна війна на тлі широкомасштабної війни в Україні. Інтеграція ШІ та Big Data в інформаційні атаки. Deepfake як масовий інструмент впливу. | Генерація фальшивих відео та заяв.<br>Інформаційне насичення / когнітивне перевантаження. Спроби деморалізації через Telegram, TikTok. | рф: ІПСО на фронті й у тилу (через Telegram, ботмережі). Китай – гібридні експерименти у Тайванському регіоні. Захід: розвиток контрнаративів, OSINT. |

До основних узагальнених трендів трансформації когнітивних загроз у період 2010–2025 років належать:

зміщення фокусу з фактів на емоції, від переконання до нав'язування альтернативної реальності, тобто тренд від інформаційної війни до когнітивної домінації;

активне використання ШІ, глибокого навчання, нейромереж, психометричних моделей для таргетованого впливу, тобто здійснюється ефект технологізації впливу;

активна глобалізація виконавців, тобто якщо раніше загрози реалізовували державні актори, то після 2014 року з'явилися квазідержавні структури, приватні фірми, IT-платформи, а після 2022 навіть автономні системи.

**Results (Результати)**

З моменту відновлення незалежності у 1991 році Україна послідовно стикалася з різними формами загроз, зокрема і когнітивного характеру. Спершу ці загрози мали переважно латентний, м'який характер і реалізовувалися через механізми культурного впливу, історичних наративів, медійного простору та освітніх програм, проте з плином часу вони набирали більш агресивної, організованої та системної форми, інтегруючись у загальну стратегію гібридної війни проти України.

Особливо інтенсивна трансформація когнітивних загроз спостерігається у трьох ключових періодах:

після 2014 року – із початком збройної агресії рф та активного використання інформаційної зброї;

після 2022 року – з розгортанням широкомасштабної війни та переходом рф до стратегій "ментального ураження";

станом на 2025 рік – з ускладненням загроз за рахунок штучного інтелекту, діпфейків, мікротаргетингу, багаторівневого впливу на командну єдність, національну рішучість і волю до спротиву.

У зв'язку із цим необхідність системного дослідження трансформації когнітивних загроз визначається кількома ключовими факторами:

по-перше, відсутністю єдиної хронологічної моделі еволюції таких загроз в українських умовах;

по-друге, зміною способів, інструментів і цільових аудиторій впливу з боку противника;

по-третє, зростаючим значенням когнітивної сфери як арени воєнної боротьби у XXI столітті.

Отже, у табл. 3 відображено аналітичну реконструкцію трансформації когнітивних загроз для України з 1991 року до сьогодення – з виокремленням характерних особливостей впливу, механізмів реалізації, джерел загроз і стратегічних наслідків для воєнної безпеки держави.

**Таблиця 3.** Трансформація когнітивних загроз для України з 1991 року до сьогодення

| Період | Характер когнітивних загроз | Першопричини змін | Наслідки для України |
|---|---|---|---|
| Період 1991–2003 рр. – пострадянська дезорієнтація та інфільтрація через "русскій мір" | Насадження постколоніального світогляду: ностальгія за срср, культурна меншовартість. Масована російська культурно-інформаційна експансія (ТБ, газети, фільми, література). Формування наративу "єдиного народу", "братніх націй", "неповноцінної української державності". | Відсутність повноцінної інформаційної політики України. Внутрішній розкол ідентичностей (Захід–Схід, україноцентризм – совєтоцентризм). Продовження функціонування радянських еліт в українській політиці та медіа. | Ослаблення української національної ідентичності. Вкорінення проросійських політичних сил. Системне гальмування процесу українізації армії, освіти, церковного простору. |
| Період 2004–2013 рр. – системна когнітивна боротьба за геополітичний вектор | Геополітичне розщеплення України на "Європейську" і "русскую" частини. Вплив через масові ЗМІ: дискредитація Заходу, просування образу "загниваючої Європи". Підживлення концепту "зовнішнього управління", "штучності Майдану". | Помаранчева революція 2004 року як виклик для рф. Активізація російських спецслужб та експансії медійних інструментів. Відсутність консолідованої державної інформаційної політики. | Поляризація суспільства. Ослаблення довіри до інституцій. Підготовка ґрунту для анексії та вторгнення (особливо в Криму та на Донбасі). |

**Продовження таблиці 3.** Трансформація когнітивних загроз для України з 1991 року до сьогодення

| | | | |
|---|---|---|---|
| Період 2014–2021 рр. – гібридна когнітивна війна у формі постправди та інформаційного терору | Масована пропаганда рф про "громадянську війну" в Україні.<br>Інформаційні атаки через соцмережі, тролі, боти, фейкові новини.<br>Деструктивний вплив на Захід: викривлення образу України за кордоном.<br>Інформаційне викривлення тем війни, втрат, героїв (атаки на УПА, ЗС України, волонтерів). | Анексія Криму та війна на Донбасі.<br>У відповідь на європейську інтеграцію – розгортання росією гібридної агресії.<br>Активна участь рф у глобальному інфопросторі (RT, Sputnik, YouTube, Telegram). | Часткова деморалізація суспільства, страх та апатія.<br>Розгубленість у міжнародному дискурсі: необхідність доводити свою правоту.<br>Водночас – зміцнення української ідентичності через спротив. |
| Період з 2022 р. – широкомасштабна когнітивна війна нового покоління (масштабована і цифрова) | Спроба росії зламати ментальну волю України до спротиву через інформаційне виснаження.<br>Кампанії: "Захід втомився", "влада вас зраджує", "не має сенсу воювати", "все вирішено за вас".<br>Масове застосування deepfake, ІІ-генерованого контенту, Telegram-операцій, психологічного терору.<br>Присутність когнітивних атак у військовому середовищі: вкиди про "оточення", "зраду", "катастрофу". | Зрив російського плану блискавичної перемоги та переходу до затяжної війни.<br>Український цифровий прорив: "Дія", OSINT, ІТ-спільнота – нова загроза для рф.<br>Відсутність ефекту від традиційної пропаганди змушує рф посилювати когнітивну війну. | Постійне психологічне напруження в суспільстві.<br>Посилення потреби у державній когнітивній обороні (аналітика, протидія дезінформації).<br>Водночас – підвищення рівня інформаційної стійкості громадян, розвиток критичного мислення, виникнення нової когнітивної суб'єктності української нації. |

З 1991 року до сьогодення когнітивні загрози для України трансформувалися від латентної культурно-лінгвістичної інфільтрації до високотехнологічної когнітивної війни нового покоління, де інформаційна атака вже дорівнює удару по системі оборони. Їхня еволюція була зумовлена як зовнішніми чинниками (російська агресія, геополітичні виклики), так і внутрішніми вадами (слабкість ідентичності, нерозвинена інформаційна політика). Відповіддю на ці виклики має стати формування національної системи когнітивної безпеки, інтегрованої у структуру воєнної стратегії.

Для ефективної протидії сучасним когнітивним загрозам, особливо в умовах гібридної та інформаційної війни, надзвичайно важливо мати чітко визначений і унормований понятійно-термінологічний апарат. Удосконалення термінології сприяє формуванню єдиного методологічного базису для аналізу, оцінювання та розроблення стратегічних заходів реагування.

Це дозволяє забезпечити уніфікованість підходів як у наукових дослідженнях, так і в практичній діяльності органів національної безпеки та оборони. Методологія стратегічного реагування на когнітивні загрози – це сукупність науково-обґрунтованих принципів, понять, процедур, механізмів і стратегій, спрямованих на ідентифікацію, передбачення, нейтралізацію та мінімізацію впливу когнітивних загроз на воєнну безпеку держави, з урахуванням інформаційного, психологічного, соціального і технологічного середовища.

У табл. 4 розкрито оновлені визначення ключових термінів, що відображають сучасні реалії розвитку когнітивних загроз і викликів, а також їхній вплив на воєнну безпеку держави. Такий системний підхід до кодифікації термінів є необхідною умовою для підвищення якості стратегічного реагування в умовах постійно зростаючої складності когнітивного простору. Деякі основні терміни методології стратегічного реагування на когнітивні загрози також розкрито у табл. 4. Усі терміни логічно інтегруються у понятійно-термінологічний апарат методології стратегічного реагування, зокрема як його науково-методичні інструменти.

**Таблиця 4.** Удосконалений понятійно-термінологічний апарат методології стратегічного реагування на когнітивні загрози

| Термін | Визначення | Джерело |
|---|---|---|
| Когнітивна загроза | Маніпуляції, спрямовані на сприйняття, ухвалення рішень і поведінку людини з метою дестабілізації національної безпеки, військових операцій чи суспільної згуртованості або впливу на них. | NATO Innovation Hub (2020) |
| | Психологічні та інформаційні дії, що спрямовані на підрив довіри, зміну переконань або провокування ірраціональних рішень. | RAND Corporation (2021) |
| | Ворожі дії, спрямовані на маніпуляцію когнітивною сферою: як люди мислять, сприймають, інтерпретують і діють. | Hybrid CoE (EU/NATO) |
| | Інформаційно-психологічні впливи на індивідуальну чи колективну свідомість, що призводять до спотвореного сприйняття реальності, порушення ухвалення рішень або дезорганізації управління. | Українські наукові джерела (ІСЗЗІ, НІСД, НУОУ) |
| | Цілеспрямований, переважно прихований вплив на ментальні процеси індивіда, групи чи суспільства, що спричиняє викривлення сприйняття, дезорієнтацію, підрив раціонального мислення чи здатності ухвалювати самостійні рішення з наслідками для безпеки держави. | Авторське |
| Когнітивний виклик | Ментальна, комунікаційна чи інформаційна ситуація, що ставить завдання збереження ідентичності, цінностей, критичного мислення й ухвалення обґрунтованих рішень в умовах інформаційного впливу; може перетворюватися на загрозу в разі ігнорування. | Авторське |
| Когнітивна загроза воєнній безпеці | Прихований вплив на когнітивний простір військово-політичного керівництва, командування, військових чи населення з метою підриву здатності адекватно оцінювати ситуацію, планувати оборону, мобілізувати ресурси і зберігати спротив. | Авторське |
| Вплив когнітивної загрози | Зміна ментальних моделей сприйняття, оцінювання ситуації або поведінки особи / групи / нації в результаті цілеспрямованого інформаційно-когнітивного втручання. | RAND, NATO StratCom CoE, авторське уточнення |
| Вплив когнітивної загрози на стан воєнної безпеки | Підрив спроможності командування, військ чи оборонної інфраструктури до адекватного ухвалення рішень, ведення бойових дій чи мобілізації ресурсів. | Авторське |
| Вплив когнітивної загрози на стан національної безпеки | Деструктивна трансформація стратегічних комунікацій, громадської свідомості, політичної єдності, що унеможливлює ефективне функціонування держави. | НІСД, Hybrid CoE, авторське доповнення |
| Когнітивне середовище (когнітивний домен) | Сукупність інтелектуальних, інформаційних, комунікативних і культурних процесів, у межах яких формується сприйняття реальності, ухвалення рішень і поведінкові реакції особистості, соціуму чи держави. | Авторське |

**Продовження таблиці 4.** Удосконалений понятійно-термінологічний апарат методології стратегічного реагування на когнітивні загрози

| | | |
|---|---|---|
| Когнітивна операція (операція у когнітивному домені) | Спланована діяльність, що має на меті змінити когнітивні моделі мислення противника, дезорієнтувати або нав'язати бажану картину реальності для досягнення стратегічної переваги без фізичного вторгнення. | Авторське |
| Когнітивна оборона | Комплекс заходів щодо виявлення, запобігання та нейтралізації когнітивних впливів через освіту, критичне мислення, кіберзахист і стратегічну комунікацію. | NATO StratCom CoE, авторське доповнення |
| Когнітивна вразливість | Наявність у свідомості або структурі держави слабких місць, через які можливе маніпулювання, нав'язування чужих наративів чи деморалізація. | Авторське (на основі терміну cognitive vulnerability в дослідженнях RAND) |
| Когнітивна стійкість | Здатність зберігати критичне мислення, психологічну рівновагу та спроможність до дій в умовах когнітивного тиску чи інформаційного терору. | NATO Resilience Concept, авторське уточнення |
| Когнітивне збройне втручання | Використання когнітивного впливу як інструменту досягнення політичних і воєнних цілей без прямого збройного насильства. | Авторське |
| Когнітивна розвідка | Системне вивчення джерел когнітивних загроз, їх поширення, впливу на свідомість та прогнозування сценаріїв їхньої еволюції. | Авторське |
| Реверсивна когнітивна операція | Контрвплив або нейтралізація джерела когнітивного впливу шляхом його демаскування, дискредитації або нав'язування зворотного образу. | Авторське |
| Методологія стратегічного реагування на когнітивні загрози | Сукупність науково-обґрунтованих принципів, понять, процедур (методів) і стратегій, спрямованих на виявлення, аналіз, запобігання та нейтралізацію когнітивних загроз у сфері безпеки. | Авторське (системне узагальнення |
| Метод пріоритезації когнітивних загроз в умовах невизначеності проблематики їхнього впливу | Система оцінювання та ранжування когнітивних загроз за критеріями потенційної небезпеки, ймовірності реалізації, масштабів впливу та здатності до поширення за умов неповноти інформації. | Авторське (на основі концептів decision science, risk management) |
| Метод ідентифікації, вибору та прогнозування впливу когнітивних загроз на стан воєнної й національної безпеки держави | Комплекс інструментів, моделей і процедур для виявлення джерел когнітивного впливу, класифікації загроз, оцінювання їхнього сценарного розвитку та прогнозування наслідків для національної стійкості. | Авторське (інтеграція підходів foresight, cognitive threat modeling, systems analysis) |
| Метод оцінювання ефективності заходів протидії когнітивним загрозам | Методологія вимірювання досягнутих результатів дій у відповідь на когнітивні загрози за показниками зниження їхнього впливу, підвищення обізнаності, зміцнення стійкості та недопущення повторних атак. | Авторське (на основі performance assessment, counter-influence operations) |
| Оцінювання ефективності протидії когнітивній загрозі | Аналіз рівня зниження когнітивного впливу, стабілізації суспільної думки, відновлення довіри та стійкості у цільовій аудиторії внаслідок захисних заходів. | Авторське |

**Закінчення таблиці 4.** Удосконалений понятійно-термінологічний апарат методології стратегічного реагування на когнітивні загрози

| | | |
|---|---|---|
| Проблематика когнітивних загроз | Сукупність актуальних теоретичних, прикладних та організаційних питань, пов'язаних з виникненням, розпізнаванням, масштабуванням і нейтралізацією впливу на свідомість. | Авторське |
| Ефективність когнітивної загрози | Ступінь досягнення поставлених цілей атакуючою стороною шляхом когнітивного впливу, включно з рівнем дезорієнтації, деморалізації та дестабілізації. | Авторське |
| Пріоритезація когнітивних загроз | Процес розподілу загроз за рівнем небезпеки, впливовості, масштабом потенційних наслідків і невідкладності реагування. | Авторське |
| Критерії потенційних небезпек від когнітивних загроз | Показники оцінювання рівня шкоди: масштаб цільової аудиторії, тривалість впливу, стійкість до розвінчання, здатність до реплікації. | Авторське визначення |
| Ймовірність реалізації когнітивної загрози | Ступінь імовірності того, що ворожий когнітивний вплив буде реалізовано в конкретному середовищі з досягненням цільового ефекту. | Теорія ризику, авторське уточнення |
| Критерій оцінювання ефективності реалізації когнітивної загрози | Визначений показник, за яким вимірюється ступінь досягнення мети когнітивного впливу (наприклад, зниження бойового духу, зростання протестної активності). | Авторське визначення |
| Невизначеність в системі когнітивізму | Наявність прогалин у знаннях про джерела, шляхи впливу, характер та наслідки когнітивних загроз, що ускладнює прогнозування й ухвалення рішень. | Теорія складних систем, авторське визначення |

**Примітка:** визначення адаптовані до реалій гібридної війни, цифрового інформаційного простору та стратегічних комунікацій. За потреби кожен термін може бути розгорнуто у підрозділ методології (наприклад, окремі моделі прогнозування, оцінювання, ідентифікації).

Станом на червень 2025 року воєнна безпека України залишається критично вразливою до багатокомпонентного когнітивного тиску з боку держави-агресора. Системність, інноваційність і багаторівневість сучасних когнітивних загроз, зокрема тих, що реалізуються через цифрові, інформаційні та психологічні канали, зумовлює необхідність їх чіткої ідентифікації, оцінювання та стратегічного прогнозування. Трансформація когнітивного впливу в умовах широкомасштабної війни призвела до появи нових типів загроз, яких раніше або не було, або їх не розглядали як фактори, здатні без фізичного ураження спричинити дезорганізацію військового управління, ерозію довіри, паніку в суспільстві або деморалізацію захисників.

У табл. 5 розкрито результати аналітичного узагальнення актуального стану когнітивного середовища воєнної безпеки України й надано сформований структурований опис, а саме: назву сучасної загрози; її змістовну характеристику (форма прояву, цільова аудиторія, спосіб впливу, стратегічна мета); оцінку ймовірності реалізації протягом найближчих шести місяців (на основі експертного оцінювання, з урахуванням наявних трендів і намірів противника). Необхідність такого аналізу зумовлена: потребою адекватного пріоритезування заходів реагування в умовах обмежених ресурсів; підготовкою системи стратегічного моніторингу загроз когнітивного типу; формуванням оперативного планування заходів інформаційної та психологічної безпеки в органах оборонного управління. Отже, табл. 5 виконує роль інструменту стратегічного аналізу та ухвалення рішень, спрямованих на попередження, пом'якшення або нейтралізацію найімовірніших когнітивних загроз у найближчому часовому горизонті.

**Таблиця 5.** Сучасні когнітивні загрози воєнній безпеці України (станом на червень 2025)

| № | Назва загрози | Характеристика | Імовірність реалізації (оцінка на 6 міс.) |
|---|---|---|---|
| 1 | Інформаційне виснаження населення та військових | Надмірне перенавантаження негативними повідомленнями, маніпулятивною "реальністю", змішаною з правдою, спрямоване на зниження бойового духу, віри у перемогу та довіри до влади. | Висока |
| 2 | Наратив про "втому Заходу" | Просування меседжів про нібито зниження підтримки України з боку США, ЄС, НАТО; формування уявлення про ізоляцію. | Висока |
| 3 | Розмиття довіри до військово-політичного керівництва | Створення образу "внутрішньої боротьби за владу", корупційних скандалів у тилу, нібито неефективного командування. | Висока |
| 4 | Делегітимація мобілізаційних заходів | Посилення протестних настроїв проти мобілізації шляхом поширення жахливих історій, фейків, маніпулятивних відео про нібито свавілля або жорстокість. | Середня ↗ висока |
| 5 | Підрив бойового духу ЗСУ через ІПСО | Масовані ІПСО, спрямовані на підрозділи ЗСУ, з використанням deepfake, месенджерів, Telegram-ботів з дезінформацією про "зрадженість", "оточення", "незворотні втрати". | Висока |
| 6 | Підміна стратегічних цілей війни | Просування думки, що "треба погодитись на мир за будь-яку ціну", "війна не має сенсу", "Крим не вартий жертв", – з метою зміни базових орієнтирів спротиву. | Середня |
| 7 | Емоційна десенсибілізація через постійні втрати | Зниження співчуття, згуртованості та сприйняття цінності людського життя внаслідок тривалого перебування у режимі "нормалізованої смерті". | Середня |
| 8 | Розколи всередині проукраїнських аудиторій | Маніпуляції темами волонтерства, цивільно-військових відносин, "зайвих" героїв, конфліктів між ветеранськими спільнотами. | Середня ↗ висока |
| 9 | Використання штучного інтелекту для генерації дезінформації | Автоматизоване створення зображень, текстів і відео для посилення недовіри, паніки, підриву репутації українських сил. | Середня ↗ висока |
| 10 | Інфільтрація через "нейтральні" платформи та блогерів | Поширення проросійських чи деморалізуючих тез через впливових блогерів, "експертів", журналістів, які формально не є проросійськими. | Висока |

Найбільш імовірні загрози: атаки на бойовий дух, стратегічну стійкість, довіру до влади та зовнішніх партнерів. Інструменти впливу: Telegram, YouTube, deepfake, псевдоаналітика, експлуатація травматичного досвіду. Джерело загроз: російські державні структури, проксі-медіа, а також інфільтровані платформи соцмереж.

У табл. 6 наведено матрицю пріоритезації когнітивних загроз воєнній безпеці України станом на червень 2025 року, побудовану за двома ключовими критеріями: імовірність реалізації (вертикальна вісь) – наскільки ймовірно, що загроза реалізується найближчим часом; рівень впливу (горизонтальна вісь) – наскільки суттєво загроза здатна вплинути на стан воєнної безпеки, бойову стійкість, управління та спротив.

У межах комплексної системи стратегічного моніторингу когнітивних загроз доцільно використовувати ключові інтегральні показники, які дають можливість не лише виявляти небезпеки, а й оцінювати динаміку впливу, здатність до спротиву та потенціал до попередження негативних когнітивних ефектів. Нижче наведено опис трьох основних таких показників:

*1. Індекс когнітивного тиску (ІКТ).*

Цей індикатор дозволяє кількісно оцінити сумарний рівень когнітивного навантаження на воєнну безпеку держави, який формується сукупністю активних когнітивних загроз. Розраховується цей показник за формулою:

*ІКТ = Σ (вага загрози × частота її появи × рівень впливу).*

Таким чином, індекс враховує: вагу (пріоритетність або стратегічну значущість конкретної загрози), частоту появи (інтенсивність повторення в інформаційному середовищі), рівень впливу (ступінь негативного когнітивного ефекту на об'єкт впливу – військо, населення, політичне керівництво тощо).

**Таблиця 6.** Матриця пріоритезації когнітивних загроз (оцінка за 5-бальною шкалою)

| № | Загроза | Імовірність реалізації (І) (1–5) | Рівень впливу (В) (1–5) | Пріоритетність (індекс = І×В) | Пріоритет |
|---|---|---|---|---|---|
| 1 | Інформаційне виснаження населення та військових | 5 | 5 | 25 | Критичний |
| 2 | Наратив про "втому Заходу" | 5 | 4 | 20 | Критичний |
| 3 | Підрив довіри до військово-політичного керівництва | 5 | 4 | 20 | Критичний |
| 4 | Делегітимація мобілізації | 4 | 4 | 16 | Високий |
| 5 | ІПСО проти ЗСУ ("оточення", "зрада") | 5 | 5 | 25 | Критичний |
| 6 | Підміна стратегічних цілей війни | 3 | 5 | 15 | Високий |
| 7 | Емоційна десенсибілізація | 3 | 3 | 9 | Помірний |
| 8 | Розколи всередині проукраїнських груп | 4 | 4 | 16 | Високий |
| 9 | Deepfake / ШІ-дезінформація | 4 | 3 | 12 | Помірний |
| 10 | Інфільтрація "нейтральних" медіа | 5 | 4 | 20 | Критичний |

**Примітка:** 20–25 – Критичний – Вимагає негайного реагування і постійного моніторингу; 15–19 – Високий – Потребує системної уваги в короткостроковій перспективі; 10–14 – Помірний – Слід враховувати у планах реагування; <10 – Низький – Допоміжна увага або відкладене реагування.

Призначення цього показника полягає у наданні можливості швидко оцінити критичність загального інформаційно-когнітивного навантаження та обґрунтувати необхідність заходів реагування.

*2. Індекс стійкості морального духу (ІСМД).*

Цей індикатор спрямований на визначення психологічної готовності та моральної витривалості населення, військових і лідерських структур до впливу когнітивних операцій.

Методика розрахунку цього показника полягає в узагальненні комбінованих даних з: опитувань громадської думки (рівень довіри до влади, готовність до спротиву тощо), аналітики соціальних мереж (настрої, поширення панічних чи деморалізуючих наративів), моніторингу ЗМІ (тональність, меседжі, антидержавна риторика).

Цей показник визначає потенційні зони деморалізації, втрати довіри або зниження бойового духу – критично важливі для раннього втручання.

*3. Когнітивний індекс раннього попередження (C-WARN).*

Цей показник функціонує як система сигналізації про зародження нових когнітивних загроз, які ще не виявлені або не мають сформованого профілю. Методика розрахунку формується на основі трендової аналітики інформаційного поля (виявлення аномальних змін у тематиках, емоційних коливаннях), а також із урахуванням особливостей машинного навчання для виявлення нових патернів (нові типи маніпуляцій, неочікувана лексика, повторювані поведінкові маркери).

Застосування показника забезпечує превентивне виявлення потенційно небезпечних тенденцій у когнітивному середовищі ще до початку їх активного впливу.

Загалом, система з трьох індексів (ІКТ, ІСМД, C-WARN) створює інтегровану аналітичну основу для виявлення, оцінювання та реагування на когнітивні загрози, формуючи базу для ухвалення стратегічних рішень у сфері воєнної безпеки.

У табл. 7 та на рис. 1, рис. 2 наведено кінцеві результати експертного опитування щодо частоти появи та рівня впливу загрози, а також розрахунку індексу когнітивного тиску. Інтегральне значення ІКТ на червень 2025 року становить: 0,6709 *(за шкалою від 0 до 1)*, що свідчить про високий рівень когнітивного навантаження на воєнну безпеку України сьогодні.

**Таблиця 7.** Компоненти ІКТ за загрозами

| № | Загроза | Вага (AHP) | Частота появи | Рівень впливу | Компонент ІКТ |
|---|---|---|---|---|---|
| 1 | Виснаження інформацією | 0,154 | 0,90 | 0,95 | 0,1318 |
| 2 | Недовіра до керівництва | 0,154 | 0,88 | 0,92 | 0,1248 |
| 3 | Наратив “втоми Заходу” | 0,154 | 0,85 | 0,90 | 0,1179 |
| 4 | ІПСО проти ЗСУ | 0,154 | 0,80 | 0.88 | 0,1085 |
| 5 | Інфільтрація нейтральних медіа | 0,154 | 0,70 | 0,75 | 0,0809 |
| 6 | Делегітимація мобілізації | 0,059 | 0,75 | 0,85 | 0,0375 |
| 7 | Підміна цілей війни | 0,059 | 0,70 | 0,70 | 0,0288 |
| 8 | Розколи проукраїнських груп | 0,059 | 0,60 | 0,60 | 0,0212 |
| 9 | Емоційна десенсибілізація | 0,027 | 0,65 | 0,60 | 0,0103 |
| 10 | ШІ-дезінформація (deepfake) | 0,027 | 0,50 | 0,70 | 0,0093 |

Топ-5 загроз дають понад 80% загального ІКТ, тому вони є ключовими цілями протидії: виснаження інформацією; недовіра до керівництва; наратив про “втому Заходу”; ІПСО проти ЗС України; інфільтрація нейтральних медіа; менш критичні, але зростаючі загрози (desensitization, deepfake) – потребують технологічного моніторингу та освітніх кампаній.

Найменш вагомими виявились загрози з глибокими наслідками, але меншою ймовірністю впливу у короткостроковій перспективі – десенсибілізація та deepfake / ШІ.

У сучасних умовах російсько-української війни, що триває, когнітивні загрози посідають ключове місце серед інструментів гібридного впливу, що використовуються противником для досягнення стратегічних цілей без прямого застосування сили. Вони націлені на підрив морально-психологічної стійкості, маніпуляцію громадською думкою, дезорієнтацію військово-політичного керівництва, а також на зниження боєздатності через руйнування довіри до державних інститутів.

З огляду на результати попереднього аналізу та розрахунок індексу когнітивного тиску, було здійснено систематизацію найбільш критичних загроз станом на червень 2025 року, які потребують пріоритетного реагування з урахуванням багаторівневого підходу до протидії.

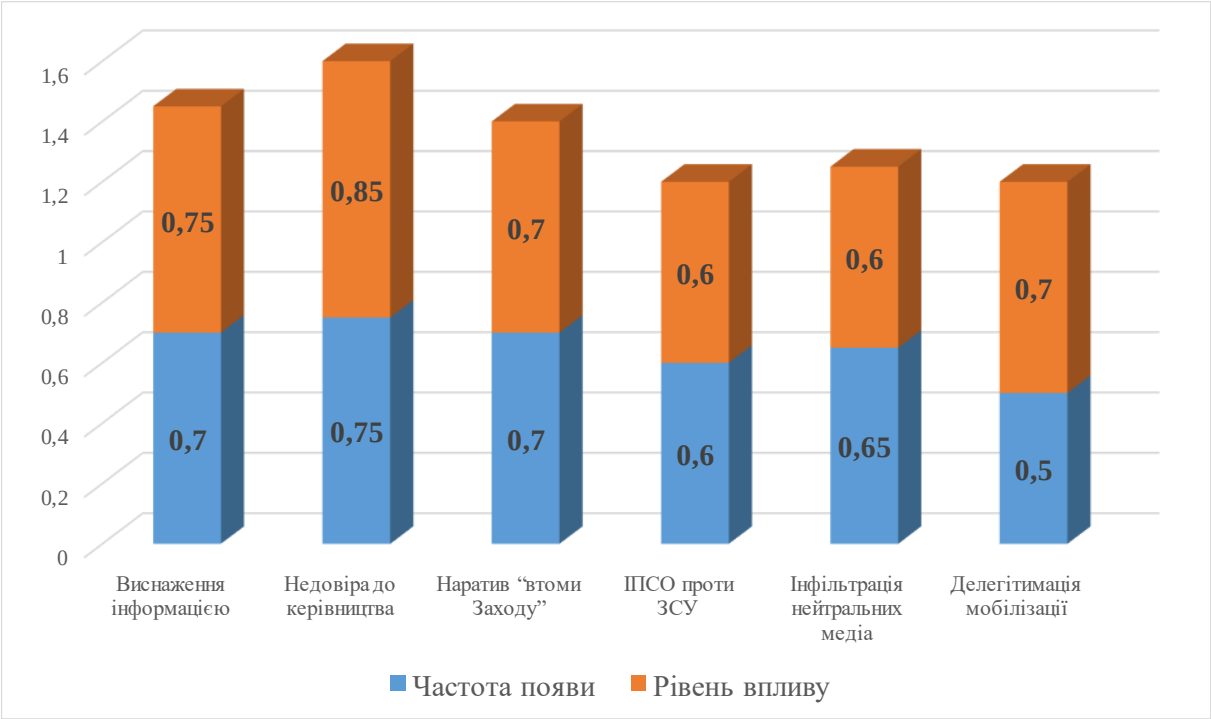



**Рисунок 1.** Результати експертного опитування щодо частоти появи та рівня впливу когнітивної загрози на стан воєнної безпеки України станом на червень 2025 року

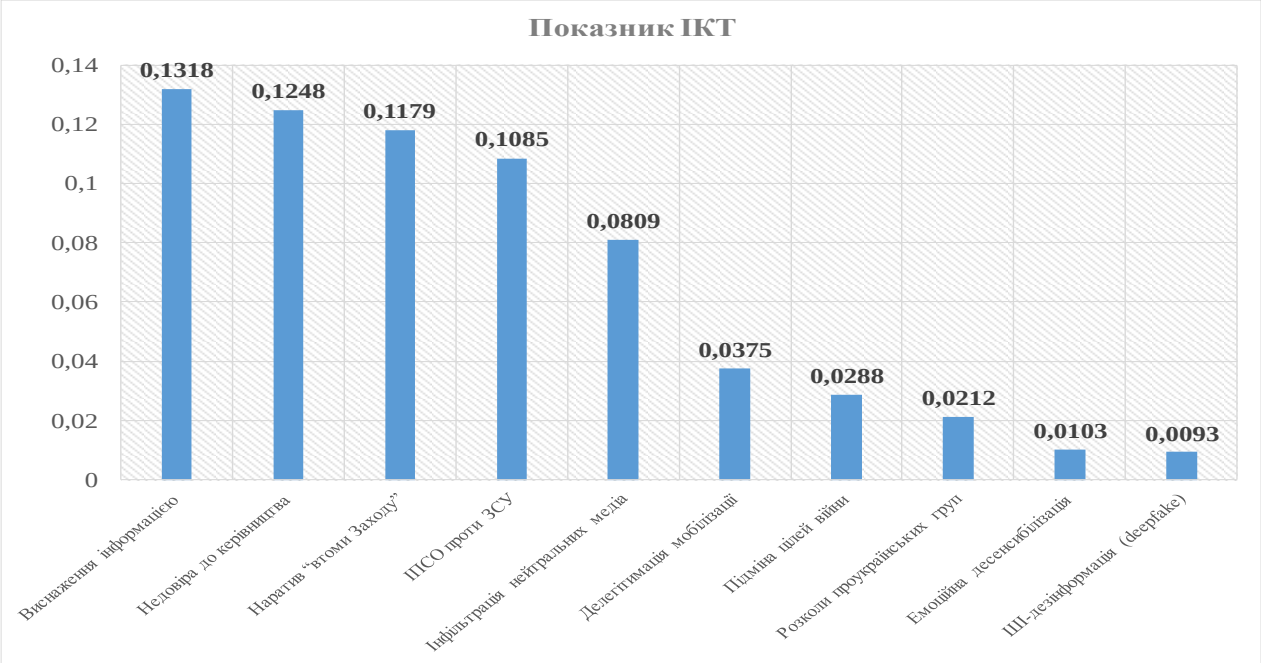



**Рисунок 2.** Кінцеві результати розрахунків індексу когнітивного тиску загроз на стан воєнної безпеки України станом на червень 2025 року

**Рекомендації (Recommendations)**

У табл. 8 розкрито систему рекомендацій щодо ефективної протидії актуальним когнітивним загрозам воєнній безпеці України станом на червень 2025 року, сформовану на

основі оцінок індексу когнітивного тиску та попереднього аналізу. Рекомендації сформовані за трьома рівнями впливу їх реалізації, а саме: стратегічний рівень – формування та адаптація державної політики у сфері національної безпеки; оперативно-тактичний рівень – інформаційно-психологічне забезпечення та захист оборонного сектору; психологічно-освітній рівень – посилення громадянської стійкості та критичного мислення. Очікувані результати реалізації рекомендацій та запропонованих дій відображені у форматі прогнозованого ефекту зниження рівня впливу загрози або її нейтралізації.

У табл. 8 здійснено також спробу переведення аналітичних знань в управлінські рішення, які є практичним орієнтиром для розробників безпекової політики, командирів, інформаційних стратегів, освітян і фахівців з психологічної оборони.

**Таблиця 8.** Система рекомендацій щодо ефективної протидії актуальним когнітивним загрозам воєнній безпеці України станом на червень 2025 року

| Загроза | Рекомендація | Очікуваний ефект |
|---|---|---|
| **1. Стратегічний рівень реагування (національна безпекова політика)** | | |
| “Виснаження інформацією” (0,1318) | Упровадження державної системи “гігієни інформації” (фільтрація, стандартизація, освітні кампанії). Обмеження деструктивного інфошуму в офіційних каналах. | Зниження перевантаження суспільства та збереження критичного мислення. |
| “Недовіра до керівництва” (0,1248) | Прозора та регулярна стратегічна комунікація уряду та ЗС України (звіти, відповіді, прямі трансляції). Публічне пояснення складних рішень (мобілізація, кадрові зміни, підтримка Заходу). | Підвищення легітимності рішень, стабілізація настроїв. |
| Наратив “втоми Заходу” (0,1179) | Випереджувальна дипломатія: активна медійна присутність України на Заході. Демонстрація результатів підтримки (вплив зброї, перемоги). | Зниження впливу деморалізаційних меседжів серед населення. |
| 2. Оперативно-тактичний рівень (інформаційна оборона ЗС України) | | |
| “ІПСО проти ЗС України” (0,1085) | Постійний моніторинг соцмереж (OSINT, SIGINT) та раннє виявлення фейків. Випереджувальні контрнаративи у військових пабліках. Посилення інформаційної присутності командирів. | Підтримання бойового духу, уникнення масового сумніву чи паніки. |
| “Інфільтрація нейтральних медіа” (0,0809) | Перевірка та сертифікація медіа, що співпрацюють з державою. Навчання редакцій медіаграмотності й протидії ШІ-фейкам. | Блокування каналів російських наративів під прикриттям. |
| **3. Психологічно-освітній рівень (громадянська стійкість)** | | |
| “Емоційна десенсибілізація” (0,0103) | Масова психологічна просвіта через серіали, подкасти, блоги. Позитивні історії, персоніфікація героїзму. | Відновлення емпатії та небайдужості до війни. |
| “ШІ-дезінформація (deepfake)” (0,0093) | Навчання виявленню deepfake у школах, на ТБ. Спільна боротьба з платформами: репортинг і бан фейкового контенту. | Утримання інформаційного простору в межах реальності. |

До найбільш пріоритетних рекомендації на короткий період (3–6 міс.) щодо протидії когнітивним загрозам воєнній безпеці України в умовах війни належать такі:

- запустити інформаційну доктрину протидії когнітивним загрозам;
- формалізувати реєстр інформаційних впливів, які кваліфікуються як загрози;

- упровадити регулярну звітність про інформаційні атаки на рівні РНБО / ГШ ЗС України;
- створити індекс медіастійкості аудиторії за регіонами

З метою комплексного розуміння та ефективного управління сучасними когнітивними загрозами, що набули системного характеру в умовах російсько-української війни, що триває, необхідно сформувати базову аналітичну модель стратегічного реагування та моніторингу когнітивних загроз воєнній безпеці України станом на 2025 рік. Цю модель (рис. 3) побудовано на основі попередньо проведеного експертного оцінювання, що дозволило ідентифікувати, класифікувати та пріоритезувати ключові когнітивні загрози з урахуванням їхньої імовірності реалізації та потенційного впливу на стан воєнної безпеки. Вона включає в себе логіку взаємозв'язку між джерелами загроз, механізмами впливу в когнітивному домені та рівнями реагування – стратегічним, оперативно-тактичним і психологічно-освітнім.

Для забезпечення ефективного моніторингу динаміки цих загроз та ухвалення своєчасних управлінських рішень у межах моделі було розроблено систему кількісних та якісних показників, що відображають інтенсивність когнітивного тиску, рівень морально-психологічної стійкості населення й військових, а також рівень раннього попередження щодо інформаційно-психологічних атак.

Показники моніторингу когнітивних загроз та відповідні заходи реагування на них систематизовано та розкрито у табл. 9, що є практичним інструментом для формування рішень на рівні національної безпеки.

Така систематизація даних є логічним продовженням аналітичної моделі (рис. 3) і відображає цілісну архітектуру: від виявлення загроз до рекомендованих дій, з урахуванням очікуваного ефекту впливу на безпекове середовище.




**Рисунок 3.** Модель (структура) реагування на когнітивні загрози воєнній безпеці України

Отже, наведена модель задає системну рамку аналізу, а система показників моніторингу деталізує інструменти впливу та контролю, що дозволяє здійснювати цілеспрямовану протидію когнітивним загрозам у реальному часі.

**Таблиця 9.** Показники моніторингу когнітивних загроз та заходи реагування на них

| Загроза | Показники моніторингу | Заходи реагування |
|---|---|---|
| 1. Виснаження інформацією | Обсяг новинного потоку<br>Частка негативних / тривожних повідомлень<br>Військові / цивільні скарги на "перевантаження" | Створення фільтрованих каналів інформування (штаби, медіацентри)<br>Інфо-гігієнічні кампанії |
| 2. Наратив "втоми Заходу" | Кількість згадок у медіа / соцмережах<br>Динаміка підтримки в західній пресі<br>Опитування про "марність спротиву" | Контрнаративи: приклади успіхів<br>Публічні кампанії в західному медіапросторі |
| 3. Недовіра до керівництва | Поширення критичних / дискредитуючих меседжів<br>Опитування щодо рівня довіри | Прозорі комунікації<br>Публічні звіти, діалог із суспільством |
| 4. Делегітимація мобілізації | Активність антипризовних груп<br>Кількість ухилянь / саботажів<br>Наративи про несправедливість | Стратегія моральної легітимізації<br>Пояснення мети, прозорість процедур |
| 5. ІПСО проти ЗС України | Сплески фейків про "оточення", "зраду"<br>Аномальна активність ботів / тролів | Rapid-response групи<br>Аналітика фейків, фактчекінг |
| 6. Підміна стратегічних цілей | Зміщення фокусу публічних дискусій<br>Вживання понять типу "мир будь-якою ціною" | Комунікація наративів стратегічної мети<br>Активізація державно-гуманітарного блоку |
| 7. Емоційна десенсибілізація | Зниження емпатії в соцмережах<br>Іронізація втрат / жахів війни<br>Втома від благодійності | Кампанії з "олюднення" фронту<br>Психоемоційна підтримка для суспільства |
| 8. Розколи серед союзників | Активність хейт-груп між волонтерськими / військовими спільнотами<br>Кампанії "свої проти своїх" | Посередництво, фасилітація порозуміння<br>Публічне визнання ролі всіх сторін |
| 9. Deepfake / ШІ-дезінформація | Виявлення підроблених відео / аудіо<br>Кількість фіксацій ШІ-деструктивного контенту | Технічний моніторинг<br>Освітні кампанії розпізнавання фейків |
| 10. Інфільтрація "нейтральних" медіа | Стиль і зміст нових статей у "нейтральних" медіа<br>Поява прихованої проросійської риторики | Моніторинг медіа<br>Виведення на світ внутрішніх лояльностей |

**Висновок (Conclusion)**

Під час дослідження встановлено, що когнітивні загрози стали ключовим компонентом сучасної гібридної війни, а їхнє значення у сфері воєнної безпеки України значно зросло в умовах російсько-української війни, що триває. Встановлено, що природа цих загроз зазнала еволюції від традиційної пропаганди до складних форм інформаційно-психологічного впливу з використанням штучного інтелекту, цифрових технологій, соціальних мереж і алгоритмів маніпуляції масовою свідомістю.

На основі аналітичного оцінювання та експертного ранжування сформовано пріоритети протидії актуальним когнітивним загрозам воєнній безпеці, визначено матрицю їх пріоритезації, а також розраховано інтегральний індекс когнітивного тиску, що дозволяє кількісно оцінювати динаміку інформаційної ситуації в країні. Запропонована система стратегічного реагування охоплює інституційний, технологічний, комунікаційний та освітній виміри протидії загрозам, що дає змогу не лише знижувати ймовірність їх реалізації, а й

підвищувати адаптивність державної політики до умов невизначеності та інформаційної турбулентності.

Наукова новизна матеріалу статті полягає у поєднанні кількісного та якісного підходів до оцінювання когнітивних загроз, формалізації понятійно-термінологічного апарату, а також розробленні інтегрованої моделі реагування на основі індексного аналізу.

До основних перспектив подальших досліджень за визначеним напрямом досліджень належать:

- необхідність розроблення математичної моделі прогнозування когнітивного тиску на регіональному рівні із залученням індикаторів соціальних мереж, медіа-активності, мобілізаційних настроїв та факторів довіри;
- розроблення системи індикаторів стратегічної стійкості держави до когнітивних впливів у межах воєнної доктрини України;
- моделювання адаптивної поведінки державних інституцій у відповідь на когнітивні виклики з урахуванням теорії ігор та сценарного аналізу;
- формування методології інтеграції когнітивного компоненту в плани оборонного планування, оперативного реагування та інформаційної безпеки ЗС України;
- створення єдиної міжвідомчої цифрової платформи моніторингу когнітивних загроз у режимі реального часу із використанням штучного інтелекту та машинного навчання.
-

**Подяки (Acknowledgments)**

Автори заявляють, що у них немає конкуруючих інтересів за тематикою статті.

**Використані джерела**

1. Thomas, T. (2022). *Russian Cognitive Warfare: Influence, Deception, and Perception Management in the Ukrainian Conflict*. Foreign Military Studies Office (FMSO).
2. Darczewska, J. (2014). *The Anatomy of Russian Information Warfare: The Crimean Operation, A Case Study.* Centre for Eastern Studies (OSW).
3. Pomerantsev, P. (2019). *This Is Not Propaganda: Adventures in the War Against Reality*. Faber & Faber.
4. Горбулін, В. П., & Литвиненко, О. В. (2020). *Гібридна війна: вижити і перемогти.* НІСД.
5. Minakov, M. (2023). *Russia's Cognitive Warfare in Ukraine: From Propaganda to Mental Occupation.* Wilson Center.
6. Kasekamp, A., Pabriks, A., Smith, J., & Veenendaal, W. (2022). *Strategic Narratives in the Russo-Ukrainian War: Competing for Minds and Morale.* NATO Strategic Communications Centre of Excellence.
7. Олійник, Д. А. (2024). Когнітивна війна у стратегічних комунікаціях: український вимір. *Військово-науковий вісник Національного університету оборони України, 2* (46),102–115.
8. *Cognitive Warfare. The Future of Conflict*. (2020). NATO Innovation Hub.
9. *Cognitive Security and Information Warfare Series*. *(2019–2023).* RAND Corporation. https://www.rand.org
10. *Cognitive Influence: Threat Landscape & Resilience*. (2022). Hybrid CoE (The European Centre of Excellence for Countering Hybrid Threats).
11. Singer, P. W., & Brooking, E. T. (2018). *LikeWar: The Weaponization of Social Media*. Houghton Mifflin Harcourt.
12. Bendett, S. (2020). *Russian Information Warfare: Cognitive and Psychological Dimensions*. CNA Corporation.
13. Wilson, J. Q., & Davis, P. K. (2021). *Cognitive Domain Operations: Strategic Advantage in the Human Mind*. RAND.

14. Манойла, З. А. (2021). *Когнітивна безпека держави: теоретико-прикладні основи*. НаУОУ.
15. *Аналітичні матеріали про дезінформацію та когнітивні операції РФ. (2021–2024).* Центр стратегічних комунікацій та інформаційної безпеки. https://spravdi.gov.ua
16. Шевцов, І. О. (2022). *Інформаційно-психологічні операції в гібридній війні: російська модель*. НІСД.
17. *Воєнна безпека України.* Збірник наукових праць. (2022–2024). НІСД.
18. Павлюк, С. В., & Притула, Ю. М. (Ред.). (2022). *Інформаційна війна і когнітивна безпека: український досвід спротиву*. НАН України.
19. Libicki, M. C. (2007). *Conquest in Cyberspace: National Security and Information Warfare*. Cambridge University Press.
20. McFate, S. (2019). *The New Rules of War: Victory in the Age of Durable Disorder*. William Morrow.
21. Thornton, R. (2018). Russian Hybrid Warfare: Resurgence and Politicisation. *Global Politics and Strategy, 60* (1).
22. Kaspersen, A. (2021). *The Weaponization of Information in the Age of AI*. World Economic Forum Report.

**References**

1. Thomas, T. (2022). *Russian Cognitive Warfare: Influence, Deception, and Perception Management in the Ukrainian Conflict*. Foreign Military Studies Office (FMSO).
2. Darczewska, J. (2014). *The Anatomy of Russian Information Warfare: The Crimean Operation, A Case Study.* Centre for Eastern Studies (OSW).
3. Pomerantsev, P. (2019). *This Is Not Propaganda: Adventures in the War Against Reality.* Faber & Faber.
4. Horbulin, V. P., & Lytvynenko, O. V. (2020). *Hybrid War: Survive and Win.* National Institute for Strategic Studies (NISS).
5. Minakov, M. (2023). *Russia's Cognitive Warfare in Ukraine: From Propaganda to Mental Occupation.* Wilson Center.
6. Kasekamp, A., Pabriks, A., Smith, J., & Veenendaal, W. (2022). *Strategic Narratives in the Russo-Ukrainian War: Competing for Minds and Morale.* NATO Strategic Communications Centre of Excellence.
7. Oliinyk, D. A. (2024). Cognitive Warfare in Strategic Communications: The Ukrainian Dimension. *Military-Scientific Bulletin of the National Defense University of Ukraine, 2* (46), 102–115.
8. *Cognitive Warfare. The Future of Conflict*. (2020). NATO Innovation Hub.
9. *Cognitive Security and Information Warfare Series. (2019–2023).* RAND Corporation. https://www.rand.org
10. *Cognitive Influence: Threat Landscape & Resilience*. (2022). Hybrid CoE (The European Centre of Excellence for Countering Hybrid Threats).
11. Singer, P. W., & Brooking, E. T. (2018). *LikeWar: The Weaponization of Social Media*. Houghton Mifflin Harcourt.
12. Bendett, S. (2020). *Russian Information Warfare: Cognitive and Psychological Dimensions*. CNA Corporation.
13. Wilson, J. Q., & Davis, P. K. (2021). *Cognitive Domain Operations: Strategic Advantage in the Human Mind.* RAND.
14. Manoyla, Z. A. (2021). *State Cognitive Security: Theoretical and Applied Foundations.* National Defense University of Ukraine.

15. *Analytical Materials on Disinformation and Russian Cognitive Operations. (2021–2024).* Centre for Strategic Communications and Information Security. https://spravdi.gov.ua.
16. Shevtsov, I. O. (2022). *Information and Psychological Operations in Hybrid Warfare: The Russian Model.* NISS.
17. *Military Security of Ukraine*. Collection of Scientific Works. (2022–2024). NISS.
18. Pavliuk, S. V., & Prytula, Yu. M. (Eds.). (2022). *Information War and Cognitive Security: Ukrainian Experience of Resistance.* National Academy of Sciences of Ukraine.
19. Libicki, M. C. (2007). *Conquest in Cyberspace: National Security and Information Warfare*. Cambridge University Press.
20. McFate, S. (2019). *The New Rules of War: Victory in the Age of Durable Disorder*. William Morrow.
21. Thornton, R. (2018). *Russian Hybrid Warfare: Resurgence and Politicisation*. *Global Politics and Strategy*, *60* (1).
22. Kaspersen, A. (2021). *The Weaponization of Information in the Age of AI*. World Economic Forum Report.

# Analysis of the Theory and Practice of the Development of Cognitive Threats in the Field of Military Security: Countermeasures

**Oleksandr Kin′**
Candidate of Technical Sciences, Associate Professor
Senior Research Fellow
Diplomatic Academy of Ukraine named after Hennadii Udovenko
under the Ministry of Foreign Affairs
01001, Velyka Zhytomyrska Street, 2, Kyiv, Ukraine
e-mail: cubalibre1972@ukr.net
ORCID: 0009- 0001-2196-7515

**Abstract.** National security policy, military science, and practical military leadership still lack a systematic approach to studying and countering cognitive threats. There is no unified conceptual and terminological framework, nor established methods for diagnosing, monitoring, and assessing the level of cognitive security. The absence of doctrinal, regulatory, and scientific-methodological foundations hinders the formation of an effective counteraction system.

Thus, a theoretical and applied analysis of the processes of formation, development, and realisation of cognitive threats in the domain of Ukraine's military security is highly relevant, as it is directly related to the state's potential for strategic resistance, the resilience of the national security system, preservation of managerial integrity, and moral and psychological readiness for defence.

This article outlines a chronological sequence of the development of cognitive threats in wars and military conflicts from a historical perspective and explains how cognitive threats to Ukraine have transformed since 1991. It improves the conceptual and terminological tools of the strategic response methodology, identifies current cognitive threats to Ukraine's military security as of June 2025, and develops a matrix for the prioritisation of such threats.

It also defines key integral indicators that not only detect threats but also assess the dynamics of their influence, resistance capacity, and the potential to prevent negative cognitive effects. The paper presents expert survey results on the frequency and impact level of cognitive threats on Ukraine's military security and includes a calculated index of cognitive pressure as of June 2025. Furthermore, it offers a system of recommendations for effectively countering present-day cognitive

threats to Ukraine's military security and proposes a structured model for responding to these threats, including main indicators for monitoring and response actions.

These findings may be valuable for military personnel, analysts, security experts, researchers, and strategists engaged in protecting the information space and addressing modern cognitive threats in the field of Ukraine's military security.

**Keywords:** hybrid warfare; military operations; military security; armed combat; cognitive threats; cognitive influence; cognitive challenges; military-political logic; cognitive pressure index; warfare technologies; tactics and strategy of military operations; national security; global stability; methods of warfare; transformation of armed conflicts; response to cognitive threats; monitoring of cognitive threats; forms of military action.

The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 3 No. 2 (2025)

DOI: 10.62524/msj.2025.3.2.19

# Обґрунтування змісту етапів і заходів та розроблення пропозицій щодо раціонального вибору системи захисту інформації під час створення інформаційно-комунікаційних систем

**Олександр Леоненко**
начальник науково-дослідного відділу
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: leonenkols@ukr.net
ORCID: 0009-0009-1994-438X

**Володимир Ремез**
доктор філософії
доцент кафедри управління військами
Національний університет оборони України
03049, проспект Повітряних Сил, 28, Київ, Україна
e-mail: remezv93145@gmail.com
ORCID: 0000-0002-2561-1081

**Алевтина Гетьман**
старший науковий співробітник
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут
Київ, Україна
e-mail: getman2017@gmail.com
ORCID: 0000-0002-6397-7412

**Юрій Мельничук**
старший викладач кафедри оперативного мистецтва
інституту державного військового управління
Національний університет оборони України
03049, проспект Повітряних Сил, 28, Київ, Україна
e-mail: um777@ukr.net
ORCID: 0000-0003-2043-1353

**Олексій Смілянський**
помічник заступника Головнокомандувача Збройних Сил України
Апарат Головнокомандувача Збройних Сил України
03168, проспект Повітряних Сил, 6, Київ, Україна
e-mail: lesha.smeliansky@gmail.com
ORCID: 0009-0006-8573-2068

**Юлія Пятова**
науковий співробітник – інженер випробувач науково-дослідної лабораторії
Державний науково-дослідний інститут
випробувань та сертифікації озброєння та військової техніки
Черкаси, Україна
e-mail: pyatova463@gmail.com
ORCID: 0009-0001-2713-8435

**Анотація.** З початком повномасштабної агресії російської федерації проти України значно зросло значення інформаційної безпеки в умовах гібридної війни. Інформаційний простір, який охоплює як військову, так і цивільну складову, трансформувався в критично важливу складову сучасного театру воєнних дій. Агресор активно використовує інструменти інформаційного впливу та кібероперацій, спрямованих на особовий склад, системи управління Збройних Сил України, а також на інформаційні платформи загального призначення. Оскільки функціонування ЗСУ все більше залежить від інформаційно-комунікаційних систем (ІКС), захист цих систем від зовнішніх і внутрішніх загроз набуває першочергового значення. Цифровізація процесів управління, з одного боку, підвищує ефективність та швидкість обміну інформацією, з іншого — створює нові вектори уразливості кіберпростору. У зв'язку з цим, формування ефективних систем захисту інформації є обов'язковою умовою під час проєктування та впровадження ІКС.

Метою цієї статті є обґрунтування структури етапів і заходів побудови систем захисту інформації, а також формування підходів до вибору раціональної моделі захисту залежно від функціональних і технічних характеристик ІКС, включаючи особливості інтеграції в загальну архітектуру системи.

У процесі дослідження використано метод системного аналізу, що дозволив структурувати етапи створення систем захисту, а також метод порівняльного аналізу, за допомогою якого здійснено оцінку ефективності різних підходів до побудови захисних механізмів в ІКС.

У статті запропоновано узагальнений підхід до вибору між комплексною системою захисту інформації (КСЗІ) та системою управління інформаційною безпекою (СУІБ) на основі законодавчих вимог і функціональних характеристик ІКС. Також систематизовано процедури створення захисних систем і наведено умови їх ефективної реалізації.

Матеріали статті можуть бути використані при розробці, проєктуванні та впровадженні ІКС у Збройних Силах України та інших структурах сектору безпеки й оборони. Запропонований підхід сприятиме підвищенню рівня захищеності інформаційної інфраструктури в умовах сучасної війни та цифрових трансформацій.

**Ключові слова:** інформаційно-комунікаційна система, система захисту інформації, комплексна система захисту інформації, система управління інформаційною безпекою, середовище функціонування інформаційно-комунікаційних систем.

## Вступ (Introduction)

Сучасні телекомунікаційні та інформаційні технології дозволяють створювати складні за архітектурою та функціональним наповненням інформаційно-комунікаційні системи (ІКС), які стають невід'ємними та актуально необхідними елементами системи управління, що підвищують ефективність керівництва життєдіяльністю, розвитком, підготовкою і застосуванням Збройних Сил України. Проведення заходів з організації створення, розвитку, інтеграції та підтримки ІКС відбувається відповідно до визначеного життєвого циклу ІКС. Обов'язковою умовою під час створення такої системи є захист інформації, який є сукупністю заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї. Будуючи систему захисту в ІКС, насамперед необхідно враховувати, яка інформація за порядком доступу буде циркулювати в цій системі – відкрита чи з обмеженим доступом, щоб оцінити ризики безпеки.

Інформаційна безпека в інформаційно-комунікаційних системах (ІКС) є важливою та невід'ємною складовою їх розробки та подальшої експлуатації. Забезпечення захисту має здійснюватися на кожному етапі життєвого циклу ІКС. Вітчизняна нормативно-правова база дозволяє паралельне проектування як самих ІКС, так і засобів захисту інформації в них. Проте на практиці нерідко спостерігається роздільне виконання цих робіт, що супроводжується відсутністю координації організаційно-технічних рішень. У результаті виникає необхідність

їх перегляду через труднощі із впровадженням вимог інформаційної безпеки. Під час створення ІКС необхідно враховувати низку чинників, що впливають на вибір відповідних організаційно-технічних підходів, зокрема: тип і рівень конфіденційності інформації, що обробляється, архітектурні особливості системи, методи керування доступом, місця зберігання даних та інші параметри.

Ще одним аспектом, який варто взяти до уваги, є те, що інформаційний обмін України з країнами Європейського Союзу (ЄС), включаючи вектор руху до повноправного членства в ЄС, передбачає необхідність синхронізації регулювання захисту інформації в України з європейським законодавством.

Потреба у глибокому розумінні загроз безпеки ґрунтується на реалістичному оцінюванні ризиків безпеки, що залежить від вразливості інформаційних систем і організаційної побудови в цілому та ґрунтується на їх реалізації, при порушенні конфіденційності та цілісності відбувається виникнення події імовірності негативних наслідків, а також порушення доступності та інших властивостей безпеки. З урахуванням стратегії управління ризиками мають бути сформульовані вимоги безпеки. При цьому пропонується звернути особливу увагу на практичну експлуатацією та ефективність впровадження заходів, пов'язаних із проєктуванням, що, у свою чергу, має передбачати особливості, витрати та порядок розроблення, придбання, розгортання.

Вибір заходів захисту інформації має ґрунтуватися на результатах аналізу ризиків, що супроводжують функціонування інформаційно-комунікаційних систем (ІКС). Визначення відповідного комплексу засобів безпеки починається з обрання профілю безпеки, який має відповідати специфічним потребам установи чи організації. Для того щоб забезпечити адаптивність до динамічних умов роботи ІКС і змін у зовнішньому середовищі, процес вибору заходів захисту повинен залишатися гнучким.

**Методологічна основа (Methodological Framework)**

Згідно із Законом України "Про захист інформації в інформаційно-комунікаційних системах", державні інформаційні ресурси або інформація з обмеженим доступом, захист якої передбачено законодавством, повинні оброблятися лише в ІКС із впровадженою та підтвердженою комплексною системою захисту інформації (КСЗІ). У випадку, коли система не оперує державною таємницею, службовою інформацією або даними з державних чи єдиних реєстрів, допускається функціонування без КСЗІ, за умови підтвердження відповідності системи управління інформаційною безпекою (СУІБ) чинним національним стандартам. Таким чином, для захисту відкритої або конфіденційної інформації можливе застосування одного з двох підходів: КСЗІ або СУІБ.

Для обґрунтування вибору оптимального варіанта системи захисту інформації у дослідженні подано їх порівняльну характеристику. Комплексна система захисту охоплює впровадження різноманітних технічних і організаційних рішень, спрямованих на запобігання витоку інформації через фізичні й технічні канали (зокрема акустоелектричні, електромагнітні, залишкові наведення тощо). Вона також забезпечує протидію спробам несанкціонованого доступу за допомогою використання чужих облікових даних, втручанню в програмне середовище, впровадженню шкідливого програмного забезпечення або технічних пристроїв. Крім того, до її функцій належить захист від навмисного знищення або викривлення інформації, у тому числі через генерацію штучних впливів або сигналів, здатних порушити роботу системи.

Концепція розробки комплексної системи захисту інформації (КСЗІ) передбачає створення відкритої архітектури безпеки, яка дозволяє незалежно проєктувати, впроваджувати, тестувати та експлуатувати кожен елемент системи окремо. Такий підхід сприяє уніфікації процесів, зниженню витрат на розробку та дає змогу здійснювати окрему оцінку кожного компонента КСЗІ під час будь-яких видів випробувань.

Побудова КСЗІ включає низку послідовних етапів, першим із яких є визначення

загальних вимог до системи в межах конкретної ІКС.

На цьому початковому етапі виконуються такі дії:

**1.1 Обґрунтування потреби у впровадженні КСЗІ.**

Під час аналізу приймається рішення щодо доцільності створення системи захисту на основі таких чинників:

- аналіз нормативно-правових актів (законів, указів, постанов, внутрішньовідомчих документів), які встановлюють обмеження на доступ до певної категорії інформації або вимагають обов'язкового її захисту;
- визначення необхідності гарантування цілісності, доступності або конфіденційності інформації, що підлягає обробці в автоматизованому режимі, згідно з чинними вимогами законодавства;
- у випадку впровадження КСЗІ на етапі експлуатації ІКС — проведення оцінювання можливих переваг такого рішення, серед яких можуть бути економічні, морально-психологічні, політичні, військові або соціальні вигоди.

**1.2 Проведення багаторівневого аналізу середовищ функціонування ІКС.**

Підготування основних засад та концептуальних даних у ході обстеження для формування вимог до КСЗІ з формуванням детального висвітлення кожного середовища функціонування ІКС з виділенням особливої уваги в ньому на об'єктах, що у будь-якій формі можуть передбачати вплив на безпеку інформації, визначення організації та порядку обміну інформацією між елементами та різних середовищах, проведення статистичного збору результатів обстеження, їх документування та архівування, що у подальшому має використовуватись при організації та проведенні наступних етапів робіт.

Обстеженню підлягають: обчислювальні системи ІКС, інформаційне середовище, технології оброблення інформації, фізичне середовище, середовище користувачів.

Формування Плану захисту інформації в ІКС відбувається за результатами обстеження середовищ функціонування ІКС, виявлення ризиків та визначення потенційних загроз для інформації, у складі якого затверджується перелік об'єктів захисту, окремими документами розробляються: модель загроз і модель порушника.

**1.3 Постановка завдання на розробку КСЗІ.**

На цьому етапі визначаються ключові завдання захисту інформації в ІКС, формулюється мета створення КСЗІ, обирається підхід до реалізації захисту та встановлюються основні напрями забезпечення інформаційної безпеки.
Також проводиться аналіз ризиків, у межах якого уточнюються моделі загроз і потенційних зловмисників, оцінюються можливі наслідки реалізації загроз і визначаються ймовірні втрати. На основі цього формується перелік критичних загроз. Окреслюється структура та складові КСЗІ, формулюються вимоги до технічних і організаційних заходів, засобів та методів захисту. Визначаються допустимі обмеження на їх застосування, середовище функціонування ІКС, допустимі витрати, умови створення, введення в експлуатацію та функціонування системи або її компонентів. Також встановлюються загальні принципи розподілу організаційних, інженерних, технічних, криптографічних та інших захисних заходів між підсистемами ІКС.

**2-й етап — формування політики інформаційної безпеки в ІКС.**
Цей етап включає:

**2.1 Аналіз об'єкта впровадження.**

Розробник вивчає характеристики об'єкта, де буде впроваджена КСЗІ, деталізує моделі загроз і порушників, перевіряє можливості ефективного управління ризиками.

**2.2 Вибір концептуальної моделі КСЗІ.** Аналізуються можливі варіанти побудови КСЗІ, оцінюються їх переваги та недоліки, після чого приймається рішення щодо найоптимальнішого варіанту.

**2.3 Розробка політики безпеки.** На цьому етапі визначаються основні підходи до захисту інформації, формуються загальні вимоги та правила використання безпечних

технологій, а також перелік конкретних захисних заходів, ролі користувачів і вимоги до документального оформлення політики безпеки.

**3-й етап — підготовка технічного завдання на створення КСЗІ.** Технічне завдання є базовим документом, який регламентує вимоги до захисту інформації в ІКС, порядок реалізації КСЗІ, проведення випробувань і введення її в експлуатацію в складі системи.

**4-й етап — проєктування КСЗІ.**

Проєкт КСЗІ формується згідно з технічним завданням і включає технічні рішення, що забезпечують сумісність компонентів і реалізацію вимог до безпеки.

Проєктування проходить у кілька стадій:

- **Ескізний проєкт.** На цьому етапі формуються попередні проєктні рішення, створюється проєктна документація, виконується погодження й затвердження.
- **Технічний проєкт.** Здійснюється деталізація проєктних рішень, зокрема: організаційно-технічна структура, опис середовища функціонування, програма випробувань, підготовка експлуатаційної документації.
- **Робочий проєкт.** Остаточна розробка та затвердження усієї документації, включно з робочими матеріалами та інструкціями для окремих підсистем КСЗІ (якщо потрібно).

**5-й етап — запуск КСЗІ та оцінювання рівня інформаційної безпеки в ІКС.** На цьому завершальному етапі здійснюється впровадження системи в реальне середовище, а також перевіряється ефективність реалізованих заходів із захисту даних.

На цьому етапі виконуються такі дії:

- **Розробка регламентуючої документації.** Створюються внутрішні нормативні документи, що визначають порядок забезпечення захисту інформації в ІКС. Паралельно формуються організаційні структури, готується сама КСЗІ до вводу в експлуатацію.
- **Підготовка персоналу.** Особи, відповідальні за адміністрування системи та всі категорії користувачів, проходять навчання з урахуванням участі технічного персоналу, що забезпечує обслуговування засобів захисту.
- **Комплектування КСЗІ.** Закуповуються технічні засоби захисту інформації, обладнання, необхідні матеріали та інші компоненти, відповідно до вимог комплектування системи.
- **Будівельно-монтажні роботи.** Здійснюються інженерні роботи, передбачені технічним завданням, з урахуванням архітектури системи.
- **Пусконалагоджувальні заходи.** Проводиться монтаж обладнання, випробування системи захисту інформації на відповідність вимогам ТЗІ, налаштування функціонування механізмів захисту від несанкціонованого доступу, тестування в автономному режимі та в умовах взаємодії з іншими компонентами. Атестація ТЗІ проводиться шляхом оцінки повноти робіт у захищених приміщеннях, за результатами оформлюється відповідний акт.
- **Попереднє тестування.** Виконується перевірка працездатності системи за встановленими критеріями, результати оформлюються протоколами, які передаються контролюючим структурам.
- **Дослідна експлуатація.** У процесі тимчасової експлуатації тестуються практичні аспекти: обробка інформації, взаємодія носіїв, розмежування прав доступу, дії користувачів, перевірка ефективності обраних засобів захисту. У разі потреби вносяться коригування до програмного забезпечення або документації.
- **Державна експертиза.** Окремою стадією є оцінка відповідності КСЗІ технічному завданню та нормативним документам. За необхідності допускається окрема експертиза кожного модуля КСЗІ. Нові модулі можуть додаватися без повторної повної перевірки, за умови оцінки їх сумісності з чинною системою.

**6-й етап — супровід КСЗІ.** На цьому етапі забезпечується постійна підтримка функціонування КСЗІ, зокрема обслуговування захисних засобів згідно з експлуатаційною

документацією, планами захисту та регламентами гарантійного й післягарантійного обслуговування.

**Система управління інформаційною безпекою (СУІБ)** є складовою загальної системи менеджменту, що реалізується на основі оцінки ризиків. Вона забезпечує побудову, впровадження, моніторинг і вдосконалення заходів інформаційного захисту. СУІБ гарантує збереження конфіденційності (захист від несанкціонованого доступу та поширення), цілісності (захист від несанкціонованих змін або знищення) та доступності (захист від блокування) інформації шляхом управління ризиками. Її основою є постійний моніторинг стану безпеки системи, аналіз змін в інформаційному середовищі, а також регулярна переоцінка ефективності обраних засобів захисту. Важливою перевагою СУІБ є її здатність до інтеграції національних і міжнародних стандартів інформаційної безпеки.

Процес створення СУІБ складається з таких етапів:

**1-ий етап** – проведення аналізу виникнення ризиків на різних рівнях (організаційному та системному). Реалізація методики управління ризиками безпекової сфери на організаційному рівні передбачає заходи підготовки що включає:

надання посадовим особам визначених ролей у сфері управління ризиками безпеки;

проведення робіт щодо створення Концепції інформаційної безпеки;

формулювання мети, обрання визначених цілей, формування часткових завдань, затвердження переліку функцій та складових процесів, які розглядаються до підтримування ІКС;

окреслення меж та визначення сторін та їх повноваження, які зацікавлені у функціонуванні ІКС;

роз’яснення категорії загроз та передбачувані потенційні збитки у разі реалізації впливу загроз на фізичних осіб та інформаційні системи;

здійснення постійного оцінювання ризиків на всіх рівнях інформаційного обміну;

ранжування переліку та його адаптація, узгодження та розстановку пріоритетів вимог безпеки;

побудову ІКС.

**2-ий етап** –визначення важливості рівнів та категорій безпеки. Визначення категорій всіх активів ІКС за результатами проведеного аналізу та ранжування відбувається на ґрунті оцінювання рівня критичності активів установи (організації) та ІКС в цілому. Визначення важливості рівнів та категорій безпеки здійснюється з урахуванням оцінювання рівня збитків та негативного впливу, що може відбутися при порушенні політики безпеки визначеної активів ІКС. Рівні критичності (низький, середній, високий) визначаються показниками оцінювання впливу за кожною політикою та властивістю ІКС. До цього етапу входять наступні заходи: детальний та повний опис суб’єктів та об’єктів системи, формування політик та категорій безпеки, затвердження порядку аналізу та ухвалення рішень щодо визначення політик та категорій безпеки в системі та інформації. Формування політик та категорій безпеки відбувається відповідно до положень [1].

**3-ій етап** – послідовність та порядок побудови вибору заходів захисту. Формування Програми безпеки інформації та обирання набору заходів захисту відбувається за результатами оцінювання збитків та ризиків безпеки та політик та категорій безпеки. З метою розширення повноважень та функціональних можливостей під час визначення заходів захисту враховуються вимоги міжнародних та міжвідомчих стандартів.

**4-й етап — реалізація заходів інформаційної безпеки.** Цей етап виконується відповідно до затвердженої Концепції безпеки інформації з використанням сучасних методів проєктування систем захисту. Він охоплює такі дії:

- налаштування початкового (базового) профілю безпеки;
- конкретизація та затвердження цільового профілю безпеки;
- інсталяція і конфігурація технічних засобів захисту інформації;
- проведення навчання персоналу, що користується системою.

**5-й етап — оцінювання рівня захищеності.** На цьому етапі перевіряється відповідність впроваджених заходів вимогам інформаційної безпеки. Він включає:

- підготовку до оцінювання впроваджених заходів;
- безпосереднє оцінювання ефективності засобів захисту в ІКС;
- оформлення та фіксацію результатів оцінювання у відповідній документації.

**6-й етап — сертифікація та авторизація засобів технічного захисту в ІКС.** Затвердження конфігурації та підтвердження функціональності системи управління інформаційною безпекою (СУІБ) оформлюється шляхом отримання сертифіката, що засвідчує законне право на експлуатацію системи. Інформація про авторизовану систему заноситься до відповідного державного реєстру. Всі рішення вважаються чинними після затвердження їх уповноваженим органом у сфері авторизації відповідно до положень нормативних документів з технічного захисту інформації (НД ТЗІ).

**7-й етап — безперервний моніторинг.**

Постійне спостереження за станом інформаційної безпеки є важливим для своєчасного виявлення змін як у самій ІКС, так і в організаційному середовищі. З цією метою формується стратегія постійного моніторингу, яка включає:

- відслідковування змін у безпековому середовищі;
- оновлення адаптованого профілю безпеки;
- підготовку звітів про поточний стан захищеності.

Результатом моніторингу є:

- актуалізований адаптований профіль безпеки;
- оновлені політики та плани захисту інформації;
- оновлений план дій у сфері безпеки;
- звіт про фактичний стан інформаційної безпеки в ІКС.

**Результати та дискусія (Results and discussions)**

Проведений аналіз свідчить про те, що створення КСЗІ відбувається за таким алгоритмом:

визначення й оцінювання загроз для інформації, формування вимог до захисту інформації на підставі аналізу середовищ функціонування ІКС;

вибір варіанта системи захисту інформації, в якому оптимально підібрані засоби і заходи з максимальної протидії всім суттєвим загрозам. Розроблення технічного завдання на створення КСЗІ;

виконання організаційних, інженерних та технічних заходів, спрямованих на створення та введення в дію КСЗІ;

супроводження КСЗІ.

Таким чином, набір способів, методів та механізмів КСЗІ реалізує гарантований захист інформації від: витоку технічними каналами; несанкціонованих дій та несанкціонованого доступу до інформації; спеціального впливу на інформацію. Такий алгоритм є чітким та лінійним, передбачає закриття всіх теоретично можливих шляхів витоку інформації, впливу на неї та ІКС в цілому, відповідає вимогам щодо захисту відкритої інформації та інформації з обмеженим доступом, але позбавлений гнучкості в реалізації захисту інформації, тому у разі виникнення будь-яких змін у середовищах функціонування ІКС або технології оброблення інформації потребує повторного проведення державної експертизи відповідності КСЗІ.

Створення СУІБ відбувається за схожим алгоритмом:

аналіз ризиків на організаційному та системному рівнях, формування вимог до захисту інформації;

вибір оптимального варіанта заходів захисту інформації (базового профілю безпеки);

виконання організаційних, інженерних та технічних заходів, спрямованих на створення та введення в дію (авторизацію) СУІБ;

постійний моніторинг системи (відстеження змін, формування адаптованого профілю

безпеки).

Отже, набір способів, методів та механізмів СУІБ спрямований на реалізацію заходів захисту в ІКС із забезпечення конфіденційності, цілісності та доступності інформації, відповідає вимогам щодо захисту відкритої (конфіденційної) інформації. Такий алгоритм є циклічним, що надає змогу визначення поточного стану ефективності заходів захисту, оперативного формування адаптивного профілю безпеки та необхідних змін в інформаційній системі й робочих середовищах, а також стану безпеки в цілому, при цьому повторна авторизація безпеки інформаційної системи не потрібна.

**Висновок (Conclusion)**

За результатами аналізу можна дійти висновку, що КСЗІ є надійним механізмом захисту інформації в ІКС, незалежно від ступеня обмеження доступу інформації, що в ній циркулює, за умови, що функціонування цієї ІКС не передбачає вихід за межі України. З огляду на той факт, що Україна має на меті стати повноправним членом ЄС, об'єми інформаційного обміну з країнами ЄС будуть надалі зростати, що зумовлює більшу інтеграцію в європейські інформаційні системи. Отже, все більш актуальним стає питання щодо необхідності синхронізації регулювання захисту інформації в України з європейським законодавством. Алгоритм побудови СУІБ формується відповідно до вимог міжнародних стандартів, що надає можливість власнику ІКС, за потреби, отримати відповідний міжнародний сертифікат. Тому вибір СУІБ під час створення ІКС, де циркулює відкрита інформація, які навіть потенційно можуть інтегруватись в міжнародні інформаційні системи, є актуальним та необхідним. Матеріали цієї статті можуть бути корисними власникам інформаційно-комунікаційних систем у виборі системи захисту інформації під час їх побудови.

**Використані джерела**

1. *НД ТЗІ 3.7-003-2023 Порядок проведення робіт зі створення комплексної системи захисту інформації в інформаційно-комунікаційній системі*.
2. *НД ТЗІ 3.6-004-21 Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці.*
3. Закон України *"Про захист інформації в інформаційно-комунікаційних системах"* № 1089-IX (2020, 16 груд.).
4. Процюк, Ю. О., Паламарчук, Н. А., Паламарчук, С. А., & Штонда, Р. М. (2019). Пропозиції з вибору організаційно-технічних рішень для автоматизованих систем з врахуванням вимог до їх захисту. *Зб. наук. пр. ВІТІ, 3*, 77–83.
5. Тарасенко, Ю. С., Клим, В. Ю., Гарагатая, С. В., & Солянников, В. Г. (2021, 13–15 груд.). Аспекти безпеки та захищеності критичної інфраструктури. У Зб. матер. міжн. наук.-практ. інтернет- конференції, *Інноваційні технології, моделі управління кібербезпекою – ІТМК – 2021*. Ч. 2. Дніпро.
6. Скіцько, Олексій, & Ширшов, Роман. (2023). Система управління інформаційної безпеки як інструмент підвищення захищеності та ефективності об'єктів критичної інфраструктури. *International Science Journal of Engineering & Agriculture, 2*, (6), 12–22. https://doi.org/10.46299/j.isjea.20230206.02.

**References**

1. *ND TZI 3.7-003-2023 Procedure for carrying out work on creating a comprehensive information protection system in the information and communication system.*
2. *ND TZI 3.6-004-21 Procedure for implementing an information security system in state bodies, enterprises, organizations whose information and communication systems process information, the protection requirement for which is established by law and does not constitute a state secret.*

3. Law of Ukraine "On Information Protection in Information and Communication Systems" No. 1089-IX (2020, Dec. 16).
4. Protsyuk, Yu. O., Palamarchuk, N. A., Palamarchuk, S. A., & Shtonda, R. M. (2019). Proposals for the selection of organizational and technical solutions for automated systems taking into account the requirements for their protection, *Coll. of Scientific Proceedings of VITI, 3,* 77–83.
5. Tarasenko, Yu. S., Klym, V. Yu., Garagataya, S. V., & Solyannikov, V. G. (2021, December 13–15). Aspects of security and security of critical infrastructure. In Collection of materials of the international scientific-practical internet conference, *Innovative technologies, models of cybersecurity management – ITMK* – 2021. Part 2. Dnipro.
6. Skitsko, Oleksiy, & Shirshov, Roman. (2023). Information Security Management System as a Tool for Improving the Security and Efficiency of Critical Infrastructure Facilities. *International Science Journal of Engineering & Agriculture, 2,* (6), 12–22. https://doi.org/10.46299/j.isjea.20230206.02.

## Substantiation of the content of stages and measures and development of proposals for a rational choice of information protection system when creating information and communication systems

**Oleksandr Leonenko**
head of the research department
The Central research institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl avenue, 28 B, Kyiv, Ukraine
e-mail: leonenkols@ukr.net
ORCID: 0009-0009-1994-438X

**Volodymyr Remez**
Doctor of Philosophy
Associate Professor of the Military Command and Control Chair
National Defence University of Ukraine
03049, Povitrianykh Syl avenue, 28, Kyiv, Ukraine
e-mail: remezv93145@gmail.com
ORCID: 0000-0002-2561-1081

**Alevtyna Hetman**
Senior Researcher
Military Institute of Telecommunications and Informatization named after Heroes of Kruty
Kyiv, Ukraine
e-mail: getman2017@gmail.com
ORCID: 0000-0002-6397-7412

**Yurii Melnychuk**
Senior Lecturer of the Operational Art Department
at the Institute of State Military Management
National Defence University of Ukraine
03049, Povitrianykh Syl avenue, 28, Kyiv, Ukraine
e-mail: um777@ukr.net
ORCID: 0000-0003-2043-1353

**Oleksii Smilianskyi**
Assistant to the Deputy Commander-in-Chief of the Armed Forces of Ukraine
Office of the Commander-in-Chief of the Armed Forces of Ukraine
03168, Povitrianykh syl avenue, 6, Kyiv, Ukraine
e-mail: lesha.smeliansky@gmail.com
ORCID: 0009-0006-8573-2068

**Yuliia Piatova**
Researcher – Test Engineer of the Scientific Research Laboratory
State Scientific Research Institute
of Armament and Military Equipment Testing and Certification
Cherkasy, Ukraine
e-mail: pyatova463@gmail.com
ORCID: 0009-0001-2713-8435

**Annotation.** With the onset of the full-scale aggression by the Russian Federation against Ukraine, the importance of information security has significantly increased in the context of hybrid warfare. The information space, encompassing both military and civilian sectors, has transformed into a critically important domain of modern warfare. The aggressor actively employs tools of informational influence and cyber operations targeting personnel, the command and control systems of the Armed Forces of Ukraine, and general-use information platforms. As the functioning of the Ukrainian Armed Forces increasingly relies on information and communication systems (ICS), protecting these systems from both external and internal threats has become a top priority. On the one hand, the digitalization of command processes improves efficiency and speed of information exchange; on the other hand, it introduces new vulnerabilities into cyberspace. Consequently, establishing effective information protection systems is a necessary condition in the design and deployment of ICS.

The purpose of this article is to substantiate the structure of stages and measures in building information protection systems, as well as to develop approaches for selecting a rational protection model based on the functional and technical characteristics of ICS, including integration features within the overall system architecture.

This study employs the method of systems analysis to structure the stages of protection system development, along with comparative analysis to evaluate the effectiveness of different approaches to designing protective mechanisms within ICS.

The article proposes a generalized approach for choosing between a Comprehensive Information Protection System (CIPS) and an Information Security Management System (ISMS), based on legal requirements and the operational specifics of ICS. Additionally, the paper systematizes the procedures for developing protection systems and outlines the conditions necessary for their effective implementation.

The article's findings can be applied during the development, design, and implementation of ICS in the Armed Forces of Ukraine and other entities within the national security and defense sector. The proposed approach will help enhance the resilience of the information infrastructure under conditions of modern warfare and digital transformation.

**Keywords:** information and communication system, information protection system, comprehensive information protection system, information security management system, information and communication systems operating environment.

The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 3 No. 2 (2025)

DOI: 10.62524/msj.2025.3.2.20

# Аналіз та оцінювання впливу факторів на вимоги до системи управління оперативного угруповання військ в операціях (бойових діях): досвід російсько-української війни

**Роман Войцеховський**
ад'юнкт кафедри управління військами інституту
державного військового управління
Національний університет оборони України
03049, проспект Повітряних Сил, 28, Київ, Україна
e-mail: voytsehovskiy31@gmail.com
ORCID: 0009-0000-6408-9620

**Анотація.** Досвід Збройних Сил України з 2022 року засвідчив, що саме здатність системи управління залишатися функціональною в умовах втрат, ізоляції командних пунктів, змін тактичної обстановки та перевантаження інформаційними потоками є ключовою передумовою збереження боєздатності угруповань військ. Успішні приклади децентралізації ухвалення рішень, інтеграції цифрових платформ, використання безпілотних і автономних систем, а також модульної побудови командних структур дозволяють сформулювати нові підходи до формування вимог до системи управління оперативного угруповання військ з урахуванням критерію стійкості. Отже, головною метою статті є проведення аналізу та оцінювання впливу факторів на вимоги системи управління оперативного угруповання військ в операціях (бойових діях) на основі досвіду російсько-української війни.

Основними результатами статті є те, що в ній: визначено основні зовнішні та внутрішні фактори, які впливають на вимоги до системи управління оперативного угруповання військ в операціях (бойових діях), а також проведено оцінювання їхнього впливу методом попарних порівнянь; сформовано рекомендації щодо підвищення стійкості системи управління оперативного угруповання військ; визначено основні показники вимог до живучості пунктів управління. Основними методами досліджень є: аналіз та синтез, а також експертного опитування на основі процедури попарних порівнянь для оцінювання рівня впливу факторів на стійкість системи управління оперативного угруповання військ в операціях (бойових діях). Матеріали статті можуть бути корисними військовим теоретикам та практикам, які займаються розробленням стратегій сучасного ведення війни; аналітикам у сфері безпеки та оборони, які досліджують трансформацію збройних конфліктів; дослідникам у галузі формування філософії війни, військової історії та міжнародних відносин; політикам і військовим керівникам, які формують оборонну політику та військові доктрини.

**Ключові слова:** автоматизація пунктів управління, бойові дії, вимоги до системи управління військами, воєнні дії, кіберзброя, живучість пунктів управління, операція оперативного угруповання військ, оперативне угруповання військ, оперативність управління, російсько-українська війна, пункти управління, система управління військами (силами), стійкість системи управління військами.

## Вступ (Introduction)

Сучасні воєнні конфлікти, зокрема російсько-українська війна, що триває, продемонстрували зростання складності бойового середовища, що зумовлює принципову трансформацію вимог до системи управління оперативного угруповання військ (ОВУ).

В умовах високої динаміки бойових дій, масованого застосування високоточного озброєння, безпілотних систем, РЕБ, кібератак, засобів розвідки і впливу в усіх доменах класичні моделі централізованого управління втрачають ефективність. Це зумовлює необхідність переосмислити підходи до формування вимог до системи управління ОВУ.

Основним критерієм таких вимог стає стійкість системи управління, тобто здатність зберігати ефективність ухвалення рішень, організації командної взаємодії, обміну інформацією та контролю над підрозділами в умовах активного впливу противника та ураження критичних елементів. Фактори, що впливають на цю стійкість, можуть бути як зовнішніми (ворожі дії, електронне подавлення, фізичне ураження), так і внутрішніми (організаційна структура, цифрова зрілість, рівень автоматизації, людський фактор, резервування та адаптивність управління).

Досвід Збройних Сил України (ЗС України) з 2022 року засвідчив, що саме здатність системи управління залишатися функціональною в умовах втрат, ізоляції командних пунктів, змін тактичної обстановки та перевантаження інформаційними потоками є ключовою передумовою збереження боєздатності угруповань військ. Успішні приклади децентралізації ухвалення рішень, інтеграції цифрових платформ, використання безпілотних і автономних систем, а також модульної побудови командних структур дозволяють сформулювати нові підходи до формування вимог до системи управління ОВУ з урахуванням критерію стійкості [1]–[5].

Отже, дослідження взаємозв’язку між впливовими факторами та вимогами до системи управління ОВУ, з урахуванням досвіду сучасної війни, є надзвичайно актуальним як для теоретичного осмислення трансформацій у сфері військового управління, так і для практичного удосконалення командно-штабної діяльності, нормативного регулювання та розвитку автоматизованих систем управління в силах оборони України.

**Матеріали та методи (Materials and Methods)**

російсько-українська війна засвідчила зміну характеру сучасних операцій, де одним із ключових викликів стало збереження керованості військами в умовах вогневого і інформаційного впливу противника, порушення зв’язку, втрати вузлів управління, знищення командирів або зламу каналів управління. Це потребує переосмислення підходів до організації, побудови і функціонування системи управління на рівні оперативних угруповань, а також ідентифікації факторів, які впливають на її стійкість – як негативних (дестабілізуючих), так і тих, що здатні забезпечити адаптивність, живучість і безперервність управління [3–7].

Урахування бойового досвіду ЗС України, які на практиці реалізували низку інноваційних підходів до управління, децентралізації рішень, резервного зв’язку, розосередження органів управління, а також використання цифрових технологій та безпілотних систем, робить це дослідження вкрай актуальним. Його результати дозволять удосконалити теорію та практику оперативного управління, підвищити боєздатність угруповань військ та стійкість командних структур у майбутніх конфліктах. Отже, дослідження спрямоване на вирішення нагального завдання національної безпеки та оборони України, а також формування нових підходів до побудови стійких систем управління в умовах гібридної, мережецентричної та широкомасштабної війни.

Аналіз публікацій за тематикою статті показує, що сьогодні, у контексті війни нового покоління, а також мережецентричних і гібридних підходів до ведення бойових дій, проблема стійкості систем управління набуває особливої ваги. У сучасній науковій та військово-аналітичній літературі, як вітчизняній, так і закордонній, розглядаються різноманітні аспекти забезпечення цієї стійкості під впливом зовнішніх (ворожих) і внутрішніх (організаційних,

технологічних) факторів. У табл. 1 розкрито результати аналізу деяких джерел за тематикою статті.

**Таблиця 1.** Результати аналізу досліджень та публікацій за тематикою аналізу та оцінювання впливу факторів на стійкість системи управління військами (силами) оперативного угруповання в операціях (бойових діях)

| Джерело та автори | Особливості тематики | Підходи та направленість |
|---|---|---|
| Біліченко, С. І., Воронін, О. Г., & Кулик, В. Ю. (2021). Стійкість системи управління військами в умовах збройної боротьби. *Збірник наукових праць ЦНДІ ЗС України.* | Розглядається модель системи управління як цілісної структури із зворотним зв'язком, оцінюються фактори живучості, резервування, адаптивності. | Упровадження багаторівневої адаптації та принципів мережецентричного управління. Обґрунтовано доцільність застосування систем резервного управління. Наголос на необхідності гнучкості структури управління як відповіді на втрати командних пунктів. |
| *Аналітичні матеріали Національного інституту стратегічних досліджень (2022–2024).* | Фокус на змінах у системі управління ЗС України внаслідок широкомасштабного вторгнення рф. | Акцент на цифровій трансформації, автоматизації управління, децентралізації ухвалення рішень. Висвітлено застосування вітчизняних цифрових платформ типу "Дельта" в підвищенні оперативності реагування. |
| *NATO STO (Science and Technology Organization) "C2 Agility in the Age of Hybrid Threats".* (2020). | Аналізується концепція "agility" (гнучкість) у командно-контрольних структурах НАТО у відповідь на гібридні виклики. | Упровадження багаторівневої моделі реагування в умовах багатовекторного впливу (кібератаки, ІПСО, дезінформація). Пропонується адаптивне управління на базі мультидоменних (MDO) структур. |
| *Command and Control in U.S. Military Operations: A Systematic Review.* RAND Corporation. (2021). | Оцінювання ефективності системи С2 США у збройних конфліктах останніх років. | Підкреслено роль штучного інтелекту, автономних систем, а також важливість горизонтальної взаємодії замість вертикального управління. Розглянуто вплив ворожих електронних атак і інформаційних впливів на ухвалення рішень. |
| Martin van Creveld. (перевид., 2020). *Command in War.* | Класичне дослідження, переосмислене крізь призму сучасних конфліктів. | Акцент на людському чиннику в управлінні та психологічному вимірі втрати керованості. Підкреслюється, що технологічна перевага не гарантує стійкості без належної організації процесів управління. |

Аналіз сучасних вітчизняних і зарубіжних публікацій демонструє, що наукове середовище дедалі більше фокусується на дослідженні динамічної стійкості систем управління в умовах складного і нестійкого бойового середовища. Українські джерела акцентують на практичному досвіді стійкості в умовах постійного впливу з боку противника, натомість західні концентруються на системній адаптації командно-контрольних структур до нових форм загроз, включаючи кібер-, РЕБ, інформаційні атаки. У російських дослідженнях наголошується на створенні технократичних, централізованих систем із високим ступенем захищеності та резервування [9–10].

У результаті аналізу літератури виявлено, що загальною тенденцією розвитку системи управління є трансформація від централізованих, вертикальних до гнучких, децентралізованих, цифрових, адаптивних, зі включенням автономних елементів, що забезпечують стійкість у реальному часі. Особливої ваги набуває здатність системи не лише зберігати функціональність під тиском, а й швидко відновлюватися після ураження [11–18]. Актуальність тематики такого дослідження беззаперечна нині, оскільки саме стійкість системи

управління (СУ) визначає ефективність військового реагування, збереження боєздатності оперативних угруповань та загальну спроможність держави до ведення війни в умовах багатофакторної загрози. російсько-українська війна продемонструвала, що боротьба за керованість – це ключовий фронт сучасного збройного протистояння.

**Results (Результати)**

У сучасних умовах ведення бойових дій ефективність системи управління оперативного угруповання військ визначається не лише її структурними й технічними характеристиками, а передусім її здатністю відповідати змінним і багатовекторним викликам. Формування вимог до такої системи потребує глибокого аналізу зовнішніх та внутрішніх факторів, які безпосередньо впливають на її функціонування, адаптивність і головне – стійкість.

Зовнішні фактори – це ті умови та дії, що виникають поза межами самої системи управління, але суттєво змінюють її контекст функціонування. До них належать дії противника (вогневе ураження, РЕБ, кібератаки), особливості тактичної та оперативної обстановки, характер театру воєнних дій, інтенсивність і темп операцій, рівень інформаційного протиборства. Ці фактори визначають, наскільки система управління має бути живучою, гнучкою, мобільною, прихованою та здатною до швидкого відновлення.

Внутрішні фактори стосуються організації, структури, технічного забезпечення, кадрового складу, рівня автоматизації, функціональної побудови та принципів взаємодії всередині самої системи управління. Саме внутрішні фактори формують базову спроможність системи забезпечувати ефективне планування, ухвалення рішень, доведення команд, обмін інформацією та зворотний контроль у будь-яких умовах. Недосконаліть внутрішніх механізмів або невідповідність сучасним умовам знижує загальну стійкість системи навіть за помірного зовнішнього впливу.

Беручи до уваги досвід російсько-української війни, дослідження цих двох груп факторів дозволяє цілісно визначити реальні, а не лише нормативні вимоги до системи управління ОВУ, з урахуванням характеру сучасного бою. Саме виявлення залежностей між конкретними зовнішніми загрозами й внутрішніми можливостями системи дає підґрунтя для формулювання обґрунтованих вимог, головним критерієм яких є стійкість як здатність забезпечувати безперервність управління навіть в умовах часткової деструкції.

російсько-українська війна, що триває, показує, що до основних зовнішніх факторів, які впливають на вимоги до СУ ОУВ, належать:

- масштаб і характер вогневого впливу з боку противника;
- роль і місце з’єднань (частин) в оперативній побудові військ;
- можливості високоточної зброї щодо ураження елементів СУ;
- можливості засобів радіоелектронної боротьби противника щодо придушення СУ;
- воєнно-економічні можливості країни;
- фізико-географічні та кліматичні умови.

Бойові дії в сучасних умовах характеризуються: зростаючими можливостями технічних засобів розвідки різних видів; різким підвищенням ефективності вогневих засобів ураження противника, включаючи ракетні, артилерійські системи і комплекси, безпілотні комплекси (системи), авіацію, аеромобільні підрозділи; зростанням ролі повітряних ударів і високоточної зброї противника у ході бойових дій, їх динамічністю та напруженістю.

Порівнюючи віддаленість пунктів управління (ПУ), об’єктів ОУВ від переднього краю оборони й можливості сучасних систем розвідки і засобів ураження та радіоелектронного подавлення (РЕП) [11–18], можна сказати, що ураження елементів СУ ОУВ можливе на всю глибину оперативної побудови ОУВ. При цьому особливе значення приділяється розвідувально-ударним комплексам (РУК) та іншим системам високоточної зброї як найбільш

ефективним засобам ураження; для ураження менш захищених елементів ПУ активно використовуються безпілотні комплекси середнього та дальнього радіуса дії.

Радіоелектронне подавлення передбачає вплив на радіоелектронні засоби системи управління військами. На сучасному етапі російсько-української війни характер цього впливу істотно посилився, оскільки суттєво зросла дальність дії засобів розвідки та ураження елементів системи управління (табл. 2).

Аналіз спроможностей провідних країн світу у сферах ведення розвідки, вогневого та радіоелектронного впливу, а також їх порівняння з наявним станом і можливостями пунктів управління ЗС України дає підстави стверджувати [1–18], що:

по-перше, досяжність засобів розвідки зазначених країн дозволяє їм здійснювати комплексну розвідку території України на глибину до 600 км;

по-друге, можливості сучасних засобів вогневого ураження забезпечують здатність завдавати ударів по пунктах управління ЗС України на всій глибині оперативної побудови угруповань військ (сил) — орієнтовно до 600 км;

по-третє, потужність та точність застосування високоточної зброї (ВТЗ) дають змогу ефективно виводити з ладу ключові елементи та компоненти пунктів управління у разі їх виявлення;

по-четверте, час реакції противника від моменту виявлення ПУ до їх вогневого ураження скоротився до 10–30 хвилин;

по-п’яте, інтеграція розвідувально-ударних контурів у провідних арміях світу забезпечує майже безперервний цикл “виявлення–рішення–ураження”, що унеможливлює тривале функціонування виявлених ПУ без ризику їх ураження;

по-шосте, засоби радіоелектронної боротьби противника здатні ефективно подавляти або дезорганізовувати роботу каналів зв’язку та автоматизованих систем управління, що суттєво знижує спроможності ПУ навіть без фізичного знищення;

по-сьоме, активне застосування безпілотних авіаційних та наземних систем у розвідувально-ударних операціях дозволяє противнику здійснювати постійний моніторинг місця розташування пунктів управління та оперативно коригувати вогонь;

по-восьме, автономні або напівавтономні дрони-камікадзе застосовуються не лише проти цілей першої лінії, а й проти командних пунктів тактичного й навіть оперативного рівнів, що вимагає нових підходів до маскування, мобільності та живучості ПУ.

Отже, у сучасних умовах немає суттєвої проблеми ураження пунктів управління та інших елементів системи управління ОУВ; основною проблемою залишається лише швидке і точне виявлення місця їх розташування. Урахування безпілотних систем як одного з ключових засобів розвідки, спостереження та ураження дає змогу об’єктивно оцінити динаміку змін у характері загроз для системи управління військами. У сучасній війні безпілотні платформи перетворюються на один із головних чинників, що визначають вимоги до побудови, мобільності, децентралізації й захищеності ПУ.

Аналіз досліджень за тематикою статті показує, що у разі застосування противником розвідувально-ударних комплексів, масованих нальотів авіації та засобів РЕП повітряного, наземного та морського базування можна очікувати, що вже в перші дні агресії може бути уражено до 30–40 % елементів СУ ОУВ і до 50 % радіоелектронних засобів ПУ подавлено перешкодами. За деякими оцінками, у разі заглушення противником понад 50–60% каналів вузла зв’язку ПУ тривалість циклу управління військами (силами) може зрости більш ніж утричі [9–18]. Стан захищеності рухомих ПУ від вогневого впливу може бути визначено імовірністю їх виживання (Рж), залежно від тривалості роботи на одному місці (рис. 1) [13].

**Таблиця 2.** Можливості засобів розвідки, ураження і РЕП

| Найменування груп засобів | Досяжність (км) |
|---|---|
| Розвідки | |
| Розвідувальні групи (такт. рівень) | до 150 |
| Розвідувальні групи (операт. рівень) | до 450 |
| Розвідувально-ударні комплекси | до 600 |
| Розвідувальна авіація | 1000 та більше |
| Повітряна розвідка УКВ-діапазону | до 100 |
| Наземна розвідка УКВ-діапазону | до 30 |
| Наземні пости фото-, інфрачервоної та радіолокаційної розвідки | до 30 |
| Ураження | |
| Диверсійно-розвідувальні групи | до 150 |
| Диверсійно-розвідувальні групи рейнджерів | до 450 |
| Реактивні системи залпового вогню | до 40 |
| Польова артилерія | до 30 |
| Розвідувально-ударні комплекси | до 500 |
| Оперативно-тактичні ракети | до 120 |
| Ударні безпілотні літальні апарати | до 170 |
| Тактична авіація | 300 та більше |
| Радіоелектронного подавлення | |
| УКВ-діапазону повітряні | до 150 |
| УКВ-діапазону наземні | до 30 |
| КВ-діапазону повітряні | до 300 |
| КВ-діапазону наземні | до 100 |

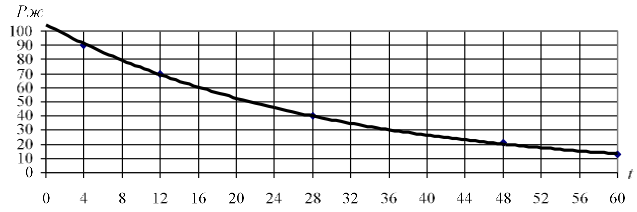



**Рисунок 1.** Залежність живучості рухомого ПУ від терміну його роботи на одному місці

На графіку видно, що рівень живучості рухомого ПУ, розміщеного в операційній зоні, залишається достатньо високим тільки впродовж перших 8–12 годин роботи. Крім того, можливості щодо живучості ПУ обмежені великими втратами часу на їх згортання та розгортання, необхідністю ешелонованого переміщення тощо.

Однією з вимог підвищення живучості системи ПУ ЗС України є проведення комплексу організаційних та технічних заходів, спрямованих на підвищення їхньої розвідзахищеності (маскування, створення макетів, нанесення радіо- й теплопоглинального покриття, встановлення масок із покриттями, що розсіюють радіохвилі, і тепловідбивальних екранів) (табл. 3).

Аналіз факторів впливу на живучість системи ПУ свідчить про те, що прихованість функціонування системи ПУ залежить від імовірності виявлення противником елементів ПУ і ступеня захищеності циркулюючої по каналах зв'язку інформації. Зниження прихованості функціонування ПУ в сучасних умовах пов'язане, з одного боку, з їх великим насиченням технічними засобами, розміщення і роботу яких необхідно приховати, а з іншого боку – зі зростаючими можливостями засобів розвідки ймовірного противника щодо здійснення розвідки (радіо, радіотехнічної, радіолокаційної, телевізійної, оптико-електронної, гідроакустичної тощо). Наслідками радіоелектронного впливу на лінії, вузли зв'язку ПУ є суттєве скорочення часу проходження інформації між органами управління, а також викривлення або втрата інформації. З огляду на це наразі набув розвитку такий вид інформаційних операцій, як боротьба із системами управління збройних сил. Він передбачає

фізичне знищення систем управління або комунікацій, які з'єднують ПУ з підлеглими військами (силами), з метою порушення безперервності управління.

**Таблиця 3.** Вимоги до живучості пунктів управління ОУВ

| № з/п | Показники живучості ПУ | Значення показників живучості ПУ за типом | | | | | |
|---|---|---|---|---|---|---|---|
| | | Рухомий ПУ (блок, модуль) | Допоміжні ПУ | | Повітряні ПУ | | ПУ в ППД (приміщення) |
| | | | ШМ, СМ на автомоб. | КШМ, СМ на бронебаз | на літаку | на вертольо | |
| 1 | Імовірність збереження за умов впливу уражаючих чинників звичайної зброї і ЗМУ у ході оборонних, контрнаступальних операцій, не менше ніж | 0,75 | 0,78 | 0,81 | 0,85 | 0,67 | 0,55 |
| 2 | Імовірність розкриття засобами розвідки у ході оборонних, контрнаступальних операцій, менше ніж | 0,37 | 0,46 | 0,43 | 0,57 | 0,59 | 0,83 |
| 3 | Імовірність ураження у ході оборонних, контрнаступальних операцій, не більше ніж | 0,53 | 0,58 | 0,47 | 0,73 | 0,79 | 0,62 |
| 4 | Клас захисту від уражаючих чинників від звичайної зброї і ЗМУ | IV | IV | II | – | – | IV |
| 5 | Захист від куль і осколків | – | – | + | – | – | + |
| 6 | Повітряна ударна хвиля (ПУХ):<br>– надлишковий тиск у фронті повітряної ударної хвилі не менше, кг/см$^2$;<br>– тиск проникаючої повітряної ударної хвилі у робочих відсіках не більше, кг/см$^2$;<br>– час спрацювання системи захисту від ПУХ, с | <br>0,3<br>0,1<br>0,1 | <br>0,3<br>0,1<br>0,1 | <br>1<br>0,1<br>0,1 | <br>–<br>–<br>– | <br>–<br>–<br>– | <br>0,3<br>0,1<br>0,1 |
| 7 | Проникаюча радіація від вибуху нейтронного боєприпасу – кратність послаблення сумарної дози проникаючої радіації на робочих місцях бойової обслуги, одиниць, не менше ніж | 2 | 2 | 4 | – | – | 2 |
| 8 | Випромінювання радіоактивної ураженої місцевості – кратність послаблення дози гамма-випромінювання на робочих місцях, одиниць, не менше ніж | 3 | 3 | 6 | – | – | 3 |
| 9 | Світлове випромінювання ядерного вибуху:<br>– імпульс опромінювання за захисними пристроями має бути, кал/см$^2$, не більше;<br>– час спрацювання захисних пристроїв, с, не більше ніж;<br>– час максимуму опромінення, с, не більше ніж | <br>4<br>2·10-4<br>0,56 | <br>4<br>2·10-4<br>0,56 | <br>4<br>2·10-4<br>0,2 | <br>–<br>–<br>– | <br>–<br>–<br>– | <br>4<br>2·10-4<br>0,56 |
| 10 | Електромагнітний імпульс наземного ядерного вибуху та його нормативних параметрів:<br>– вертикальна складова напруги електричного поля, кВ·м-1, не менше ніж;<br>– горизонтальна складова електричного поля, кВ·м-1, не менше ніж;<br>– напруга магнітного поля, А·м-1 | <br>40<br>0,5<br>30 | <br>40<br>0,5<br>30 | <br>60<br>2,6<br>270 | <br>–<br>–<br>– | <br>–<br>–<br>– | <br>40<br>0,5<br>30 |
| 11 | Отруйні речовини, бактеріальні аерозолі, радіоактивний пил – надлишковий тиск повітря в населених відсіках за номінальної продуктивності загальнообмінно-колекторних або загальнообмінних ФВУ, мм. вод. ст., не менше | 25 | 25 | 50 | – | – | 25 |

Кібератаки, спрямовані проти державних та військових інформаційно-телекомунікаційних систем і мереж разом з управлінням викраденими даними роблять цей вид протиборства надзвичайно ефективним.

Для захисту від радіоелектронного впливу ПУ поряд із традиційними організаційними заходами (зміни робочих частот, каналів зв'язку та місць розгортання) необхідно

використовувати ефективні технологічні способи паролювання інформації; імітозахищені коди, що виявляють і виправляють помилки, а також протистоять нав'язуванню обманної й застарілої інформації; апаратуру підвищення імітостійкості й вірогідності інформації; апаратуру засекречування інформації гарантійної стійкості; одночасне передавання того самого повідомлення по різних каналах зв'язку або в незалежних напрямках; спеціальні заходи для нейтралізації акустичних, віброакустичних, гідроакустичних та електроакустичних каналів просочення інформації; оптико-волоконні лінії зв'язку в межах ПУ.

Природно-географічний фактор – комплекс природних умов, характерних для конкретного театру воєнних дій, країн, стратегічних та операційних напрямків, які впливають на підготовку та проведення воєнних дій. Особливістю його є незалежність впливу на СУ від діяльності та волі людини. Його елементами є: географічне положення, рельєф, гідрографія, ґрунти, рослинність, клімат тощо.

У сучасних умовах економічний фактор відіграє ключову роль у створенні обороноздатності держави. Саме він визначає відповідність економічних можливостей держави поставленим військовим цілям.

Зовнішні фактори, що впливають на СУ ОУВ, пред'являють певні вимоги до мобільності, які можна забезпечити шляхом створення рухомих ПУ на автомобільній та бронетанковій базі. Оснащеність ПУ має відповідати вимогам щодо мобільності, автономності, захищеності. Розміщуючи ПУ ОУВ, необхідно враховувати вплив розглянутих факторів.

Проаналізуємо вплив внутрішніх факторів на вимоги до системи управління оперативного угруповання військ. До основних внутрішніх факторів, які впливають на вимоги до СУ ОУВ, належать:

- склад і можливості своїх військ;
- укомплектованість і рівень підготовленості органів управління (ОУ) до виконання завдань, які покладаються на СУ;
- організація управління, форми і методи роботи ОУ;
- ступінь прихованості й маневреність ПУ;
- ступінь забезпеченості засобів зв'язку і автоматизації (ЗЗіА).

Для обґрунтування пріоритетності різних факторів, що впливають на вимоги до системи управління ОВУ, було застосовано метод аналізу ієрархій Сааті. Цей підхід дозволяє шляхом попарного порівняння кількісно оцінити відносну важливість як зовнішніх, так і внутрішніх факторів, які визначають ефективність функціонування системи управління.

Результати попарного оцінювання подано у вигляді рейтингів, що відображають вагомість кожного фактора у відповідній групі. Рейтинги зовнішніх та внутрішніх факторів наведено у табл. 4 та на рис. 2.

Найвпливовішим зовнішнім фактором є масштаб і характер вогневого впливу, що безпосередньо впливає на необхідність підвищення живучості, мобільності та резервування СУ. Серед внутрішніх факторів домінує склад і можливості своїх військ, оскільки саме бойовий потенціал визначає обсяг, складність і швидкість управлінських рішень.

Зовнішні фактори загалом мають більший вплив (60%) на формування вимог до системи управління, особливо в умовах війни високої інтенсивності, як у випадку з російсько-українською війною.

Під час розроблення, модернізації чи трансформації системи управління ОВУ першочергову увагу слід приділяти адаптації до зовнішніх загроз, з урахуванням обмежень і потенціалу внутрішніх ресурсів.

**Таблиця 4.** Рейтинги зовнішніх факторів впливу на вимоги до системи управління ОВУ

| Зовнішні фактори | | Внутрішні фактори | |
|---|---|---|---|
| **Фактор** | **Рейтинг (вага)** | **Фактор** | **Рейтинг (вага)** |
| **Масштаб і характер вогневого впливу з боку противника** | **0.4481** | **Склад і можливості своїх військ** | **0.4185** |
| **Роль і місце з'єднань (частин) в оперативній побудові військ** | **0.2205** | **Укомплектованість і рівень підготовленості органів управління (ОУ)** | **0.2625** |
| **Можливості засобів РЕБ противника щодо придушення СУ** | **0.1427** | **Організація управління, форми і методи роботи ОУ** | **0.1599** |
| **Можливості високоточної зброї щодо ураження елементів СУ** | **0.0909** | **Ступінь прихованості й маневреність пунктів управління** | **0.0973** |
| **Фізико-географічні, кліматичні умови** | **0.0584** | **Ступінь забезпеченості засобами зв'язку і автоматизації** | **0.0618** |
| **Воєнно-економічні можливості країни** | **0.0394** | | |

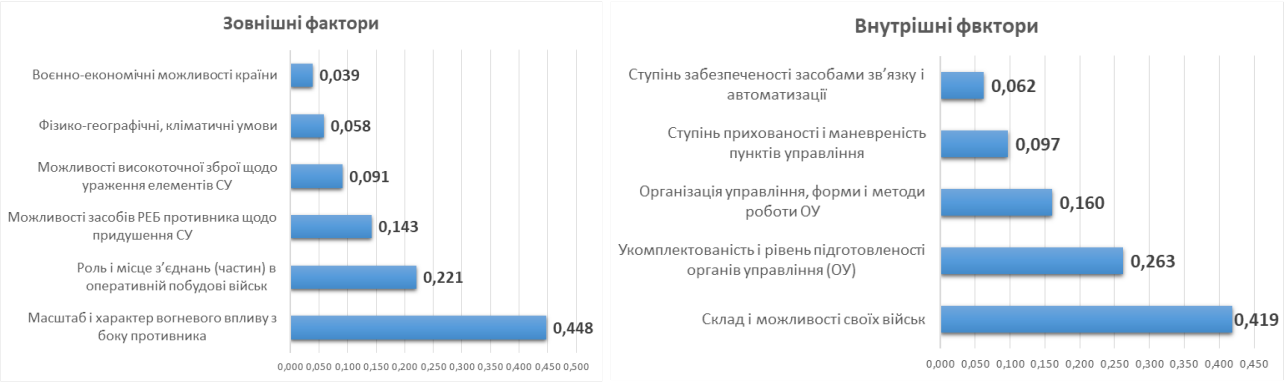



**Рисунок 2.** Ілюстрація результатів оцінювання зовнішніх та внутрішніх факторів, що впливають на вимоги до системи управління оперативного угруповання військ

**Рекомендації (Recommendations)**

Для розміщення оперативного складу та забезпечення його ефективної роботи з управління військами у ході підготовки та ведення операцій (бойових дій) створюється система ПУ, яка є сукупністю ПУ всіх ланок управління, розгорнутих за єдиним замислом, що структурно, функціонально, технічно й інформаційно взаємопов'язані між собою для забезпечення ефективної роботи постійно діючих та тимчасово створених органів управління. Кожний ПУ є сукупністю робочих місць, розташованих у захищених спорудах, будівлях або на рухомих засобах, та призначений для роботи оперативного складу ОУ. На функціонування СУ ОУВ безпосередньо впливає стан, у якому можуть знаходитися елементи СУ: ОУ, ПУ, ЗЗіА ОУВ. Вплив внутрішніх факторів призводить до змін стану елементів та СУ в цілому. При цьому під станом мають на увазі певні числові характеристики процесу їхнього функціонування в заданих умовах, такі, наприклад, як кількість працездатних або непрацездатних ПУ, можливості засобів зв'язку та автоматизації щодо вирішення покладених на них завдань (збирання, оброблення, аналізування необхідної інформації тощо в певний момент часу).

Під час планування та здійснення управління ОУ ОУВ виконують покладені на них завдання в операції ОУВ. Важливим фактором під час виконання цих завдань є рівень укомплектованості та підготовленості ОУ до виконання завдань, які покладаються на СУ ОУВ. Досягнення відповідного рівня підготовки є результатом сукупності індивідуальних

знань, умінь, навичок – з одного боку, та сукупністю навичок колективних дій – з іншого. Цю сукупність можна відобразити кількістю дій, прийомів та типових завдань у процесі підготовки. Підготовленість технічного складу ПУ необхідно враховувати шляхом оцінювання його злагодженості та натренованості у виконанні заходів розгортання та згортання елементів рухомих ПУ, зокрема робочих місць (апаратних) керівного та оперативного складу, проведення заходів маскування, інженерного обладнання районів розгортання ПУ, розгортання вузлів зв'язку та прокладання ліній зв'язку, інформаційної синхронізації баз даних для розв'язання задач на робочих місцях оперативним складом з використанням комплексів засобів автоматизації, організації захисту, охорони та оборони ПУ, створення хибних ПУ, вузлів зв'язку та імітації їхньої життєдіяльності.

Керівними документами встановлено, що орган управління вважається готовим до виконання завдань, коли він укомплектований особовим складом за посадовим призначенням не менше як на 70%. Це дає можливість встановити, що рівень укомплектованості ОВУ на початок ведення операцій (бойових дій) має бути понад 70%.

Злагодженість функціонування, єдність форм і методів роботи структурних підрозділів та посадових осіб ОВУ залежать від рівня їхньої особистої професійної підготовки, раціонального розподілу завдань та оперативного складу між центрами (групами) ПУ, відпрацьованості типових (формалізованих) алгоритмів їхнього функціонування за шатними ситуаціями, інструкцій з організації роботи центрів (груп) ПУ, технологічної можливості сумісної роботи технічних засобів зв'язку та інформаційно-аналітичного забезпечення роботи ОВУ.

Форма роботи ОВУ – обраний порядок взаємовідносин, інформаційного забезпечення ОВУ та їхніх структурних підрозділів, розподілу робіт між виконавцями. Залежно від рівня підготовки ОВУ, умов обстановки, отриманих завдань, їхнього обсягу, послідовності та часу виконання формами роботи ОВУ можуть бути: індивідуальна; у складі функціональних груп; дистанційна (у тому числі у формі відеоконференцій); комбінована (змішана).

Метод роботи ОВУ є сукупністю правил, прийомів та способів виконання поставлених завдань під час підготовки і в процесі ведення операцій (бойових дій). Залежно від рівня підготовки ОВУ, умов обстановки, отриманих завдань, їхнього обсягу, послідовності та часу виконання методами роботи ОВУ можуть бути: послідовний, паралельний, комбінований.

Відповідно до вимог щодо забезпечення ергономічних умов [17] для роботи посадових осіб ОВУ, як показує досвід ведення бойових дій, а також результати досліджень на заходах оперативної підготовки, оперативна місткість основного командного пункту (ОКП) має забезпечувати розміщення близько 220 осіб основного та постійного оперативного складу. Оперативна місткість стаціонарних ПУ визначається насамперед можливостями споруд, що мають спеціальний фортифікаційний захист для забезпечення необхідного рівня живучості.

Для своєчасного та якісного виконання завдань управління робота оперативного складу на ПУ організовується зазвичай у три зміни – основна зміна, зміна підсилення та зміна, яка відпочиває (кожна по 30%). З урахуванням цього, оперативна місткість ОКП має передбачати необхідну кількість автоматизованих робочих місць (АРМ) для основної чергової зміни, яка працює разом з командувачем, місць у складі структурних підрозділів ОКП для зміни підсилення, яка надає їй практичну допомогу в оперативній роботі, та місць для відпочинку третьої зміни. При цьому необхідно дотримуватися ергономічних вимог, що регламентують організацію робочих місць, взаємне розташування засобів відображення інформації, органів управління і засобів зв'язку в межах робочого місця.

Приміщення ОКП, де розгортаються автоматичні робочі місця (АРМ) та місця відпочинку, мають бути обладнані системами електроживлення, вентиляції та опалення для підтримання необхідного температурного режиму й відносної вологості повітря. Крім того, на ОКП слід передбачити місця для розміщення засобів індивідуальної спеціальної обробки, засобів пожежогасіння, засобів надання першої медичної допомоги, індивідуального дозиметричного контролю випромінювання.

Якщо не врахувати вплив фактора ергономічних умов на ПУ, це може призвести до неможливості забезпечення ефективного функціонування системи ОВУ.

На діяльність ОВУ має суттєвий вплив фактор готовності (повнота відпрацювання) документів щодо управління військами. Зазначені документи можуть мати текстову або графічну форму. Нині форми директивних документів (наказів, розпоряджень) недостатньо формалізовані та часто дублюються за змістом. Це призводить до зниження якості та оперативності виконання завдань управління військами (силами). У зв'язку із цим, обґрунтований перелік документів та їхня форма для організації спільної роботи різних суб'єктів сектору безпеки і оборони України набувають особливого значення.

Важливе значення має оснащеність ПУ сучасними системами зв'язку, автоматизації, у тому числі інформаційно-аналітичним забезпеченням.

Засоби зв'язку та автоматизації мають забезпечувати оперативному складу ПУ умови для своєчасного збирання й аналізування інформації для ухвалення відповідних рішень, доведення їх до виконавців і отримання результатів. Водночас, досвід [4], [8] свідчить про таке:

– у системі зв'язку здебільшого використовується застаріла аналогова елементна база, несумісна з телекомунікаційними мережами України та сучасними засобами автоматизації управління (75% засобів зв'язку ІВФ переведені на цифрову елементну базу). Якість зв'язку (особливо в польових мережах), пропускна здатність каналів, захищеність ліній та їхня стійкість щодо впливу засобів радіоелектронної боротьби є недостатніми;

– сертифікованих засобів захисту інформації, у тому числі й криптографічних, немає;

– терміни готовності частин, у яких знаходиться польова (рухома) база ПУ оперативних командувань, не забезпечують в особливий період ефективне функціонування системи управління;

– в ОВУ немає дієвих важелів впливу на підготовку засобів зв'язку, автоматизації управління та обслуги вузла зв'язку ТПУ;

– технічні засоби засекреченого зв'язку ЗС України несумісні з аналогічними технічними засобами ІВФ.

На цей час, за результатами аналізу досвіду розвитку систем управління військами (силами) провідних країн світу, основні тенденції в цій галузі спрямовуються на автоматизацію діяльності посадових осіб ОВУ – як ключовий напрям підвищення оперативності та обґрунтованості ухвалення рішення командувачем щодо обстановки, що склалася.

Серед основних факторів впливу на автоматизацію діяльності посадових осіб ОВУ та процеси управління військами (силами) доцільно визначити три:

– рівень технічного забезпечення посадових осіб ОВУ;

– рівень інформаційного забезпечення посадових осіб ОВУ;

– рівень аналітичного (спеціального математичного та програмного) забезпечення посадових осіб ОВУ.

Водночас, необхідно зазначити, що другий та третій фактор впливу безпосередньо взаємопов'язані та окремо не можуть використовуватися, однак з метою більшої деталізації аналізу розглянемо їх окремо.

Зокрема, під технічним забезпеченням посадових осіб ОВУ мають на увазі сукупність технічних засобів (комплексів засобів), які функціонально призначені для забезпечення збирання, оброблення, зберігання, відображення, обміну інформацією між посадовими особами ОВУ.

Оснащення ними робочих місць посадових осіб безпосередньо впливає на оперативність управління військами (силами) за рахунок скорочення часу виконання управлінських завдань.

Під інформаційним забезпеченням посадових осіб ОВУ мають на увазі наявність необхідного систематизованого, класифікованого, кодифікованого достовірного та повного інформаційного ресурсу, з яким працюють посадові особи ОВУ і на підставі якого оперативно

обґрунтовується рішення командувача. Важливу роль в процесі обміну інформаційним ресурсом та його актуалізації відіграє досконала система уніфікованих документів, яка безпосередньо впливає на оперативність відпрацювання документів з планування операцій (бойових дій).

У зазначеному контексті варто відзначити, що повноцінне інформаційне забезпечення ОВУ можна вважати створеним лише після систематизації інформаційних ресурсів ЗС України та держави, їхньої класифікації, кодування, створення відповідних баз (банків) даних для їх зберігання, чого наразі немає.

Під аналітичним (спеціальним математичним та програмним) забезпеченням посадових осіб ОВУ мають на увазі сукупність інформаційних, інформаційно-розрахункових задач, їхніх комплексів та моделей операцій (бойових дій). За своїм функціональним призначенням аналітичне забезпечення безпосередньо впливає як на оперативність планування операцій (бойових дій), так і на ступінь обґрунтованості рішення командувачем за обстановкою, що склалася.

Перелік інформаційних, інформаційно-розрахункових задач, їхніх комплексів та моделей операцій (бойових дій) для всіх ОВУ не може бути сталим. Він має містити певну сукупність задач та моделей, які притаманні будь-якому ОВУ, а решта – має відповідати його конкретному функціональному призначенню. Крім того, оснащеність ОВУ сучасними системами автоматизації, в тому числі інформаційно-аналітичним забезпеченням, впливає на чисельність його структурних підрозділів.

**Висновок (Conclusion)**

Сучасна війна, зокрема російсько-українська, підтвердила принципову зміну характеру загроз для системи управління військами: вона дедалі більше стає об’єктом високоточного, багатоаспектного і багатоджерельного впливу – від кінетичних засобів ураження до радіоелектронних і кіберзасобів. Найбільш критичним зовнішнім фактором є масштаб і характер вогневого впливу противника, який безпосередньо визначає потребу у високій мобільності, маневреності та захищеності пунктів управління. Це саме стосується і впровадження нових принципів просторової організації командних структур. Зростання досяжності засобів розвідки, розширення можливостей високоточної зброї та скорочення циклу “виявлення–ураження” призвели до фактичного зникнення “глибини безпеки” навіть для командних пунктів оперативного рівня.

Активне застосування безпілотних систем як для виявлення, так і для ураження ПУ робить традиційні підходи до побудови системи управління застарілими. Це вимагає впровадження децентралізованих, мережецентричних, багаторівневих рішень із резервуванням управління.

Проблема ураження пунктів управління сьогодні не технічна, а розвідувальна: у разі виявлення об’єкта — його знищення є майже гарантованим. Тому вимоги до системи управління мають ґрунтуватися на принципах скритності, постійної зміни місцеположення, швидкого згортання / розгортання та використання цифрових автономних засобів.

Провідні країни світу вже реалізують інтеграцію розвідувально-ударних контурів, у тому числі з використанням БпЛА, що дозволяє їм вести безперервне полювання на командні центри супротивника. Україні необхідно враховувати цей досвід для випереджального розвитку власних систем СУ.

Результати попарного оцінювання методом Сааті засвідчили перевагу зовнішніх факторів у формуванні вимог до СУ ОУВ, при цьому внутрішні фактори також залишаються критично важливими для реалізації необхідних змін.

Отже, стійкість системи управління ОУВ у сучасній війні має розглядатися як головна вимога до її побудови, і саме від здатності до адаптації, самовідновлення, децентралізації та цифрової трансформації залежатиме боєздатність угруповань ЗС України в умовах високотехнологічного протистояння.

**Подяки (Acknowledgments)**
Автори заявляють, що у них немає конкуруючих інтересів за тематикою статті.

**Використані джерела**

1. Біліченко, С. І., Воронін, О. Г., & Кулик, В. Ю. (2021). Стійкість системи управління військами в умовах збройної боротьби. *Збірник наукових праць Центрального науково-дослідного інституту Збройних Сил України, 3* (84), 34–42.
2. *Трансформація системи управління Збройними Силами України в умовах повномасштабної війни: аналітична записка*. (2023). Національний інститут стратегічних досліджень. https://niss.gov.ua
3. Застосування цифрових рішень у системі управління силами оборони: виклики війни та перспективи розвитку. Інститут проблем національної безпеки. (2023). *Науковий вісник ІПНБ, 2*, 45–53.
4. Пархоменко, М. С., & Чорний, П. П. (2023). Удосконалення структури управління угрупованнями військ в умовах інтенсивного вогневого впливу противника. *Воєнна думка, 7*, 22–30.
5. Кузьменко, С. М. (2023). Децентралізація управління як фактор підвищення стійкості системи управління військами в умовах гібридної війни. *Збірник наукових праць Харківського національного університету Повітряних Сил*, *4* (74), 85–92.
6. NATO Science and Technology Organization. (2020). *Command and control agility in the age of hybrid threats* (STO-TR-HFM-260). NATO.
7. Peltz, J. L., Paul, L., & Johnson, B. (Ред.). (2021). *Command and control in U.S. military operations: A systematic review*. RAND Corporation. https://doi.org/10.7249/RRA394-1
8. Van Creveld, M. (2020). *Command in war*. Harvard University Press.
9. Управление войсками в условиях современных операций: от автоматизации до цифрового суверенитета. (2022). *Военная мысль*, *9*, 11–18.
10. Уроки Сирії та України: трансформація систем управління військами. (2023). Центр воєнно-стратегічних досліджень ГШ ЗС РФ. *Вестник Академии военных наук*, *1* (74), 26–35.
11. *Платформа “Дельта” як інструмент ситуативної обізнаності* [Презентаційні матеріали]. (2023). ГУР МО України. https://gur.gov.ua
12. Олійник, А. О., & Козаченко, О. М. (2023). Особливості забезпечення стійкості системи управління військами в умовах повномасштабної війни. *Сучасні інформаційні технології у сфері безпеки та оборони*, *2* (45), 17–26. https://doi.org/10.33099/2618-1614/2023-45-2-17–26.
13. Якименко, О. О. (2023). Фактори впливу на систему управління в умовах інформаційного та кібервпливу противника: український досвід. *Воєнна безпека і стратегія*, *1*, 41–48.
14. *Уроки російсько-української війни: як зберігати керованість військами в умовах сучасного бою: аналітичний звіт.* (2023). Центр оборонних стратегій. https://defence.org.ua
15. Sabbagh, D. (2023, 10 вер.). How Ukraine’s battlefield coordination is reshaping modern command and control. *The Guardian*. https://www.theguardian.com/world/2023/sep/10/ukraine-command-and-control
16. Ігнатов, С. В., & Остапчук, В. М. (2023). Інноваційні підходи до побудови стійкої системи управління в умовах війни нового типу. *Схід*, *4* (184), 55–62. https://doi.org/10.21847/1728-9343.2023.4(184).285534
17. *Defence Command Paper Refresh 2023: Mobilising for Secure Britain* (розділ про C2 resilience). (2023). UK Ministry of Defence. https://www.gov.uk/government/publications/defence-command-paper-2023

18. Коваль, О. В., & Дубовик, М. М. (2023). Удосконалення системи оперативного управління в Збройних Силах України з урахуванням досвіду війни 2022–2023 років. *Збірник наукових праць НАОУ*, *2* (79), 73–80.

**References**

1. Bilichenko, S. I., Voronin, O. H., & Kulyk, V. Yu. (2021). Resilience of the military command system under armed conflict conditions. *Scientific Journal of the Central Research Institute of the Armed Forces of Ukraine*, *3* (84), 34–42.
2. *Transformation of the Command System of the Armed Forces of Ukraine during the Full-Scale War: Analytical Note*. (2023). National Institute for Strategic Studies. https://niss.gov.ua.
3. Application of digital solutions in the defense command system: wartime challenges and development prospects. (2023). Institute for National Security Issues. *Scientific Bulletin of the INSI*, *2*, 45–53.
4. Parkhomenko, M. S., & Chornyi, P. P. (2023). Improving the command structure of military groups under intensive enemy fire. *Military Thought*, *7*, 22–30.
5. Kuzmenko, S. M. (2023). Decentralization of command as a factor for increasing resilience of the military command system under hybrid war conditions. *Scientific Journal of the Kharkiv National Air Force University*, *4* (74), 85–92.
6. NATO Science and Technology Organization. (2020). *Command and Control Agility in the Age of Hybrid Threats* (STO-TR-HFM-260). NATO.
7. Peltz, J. L., Paul, L., & Johnson, B. (Eds.). (2021). *Command and Control in U.S. Military Operations: A Systematic Review*. RAND Corporation. https://doi.org/10.7249/RRA394-1
8. Van Creveld, M. (2020). *Command in War*. Harvard University Press.
9. Commanding troops in modern operations: From automation to digital sovereignty. (2022). *Military Thought (Russian Journal)*, *9*, 11–18.
10. Lessons from Syria and Ukraine: Transformation of troop command systems. (2023). Center for Military-Strategic Research of the General Staff of the RF Armed Forces. *Bulletin of the Academy of Military Sciences*, *1* (74), 26–35.
11. *Delta Platform as a Tool for Situational Awareness* [Presentation materials]. (2023). Defence Intelligence of Ukraine. https://gur.gov.ua
12. Oliinyk, A. O., & Kozachenko, O. M. (2023). Features of ensuring resilience of the military command system under full-scale war conditions. *Modern Information Technologies in the Security and Defense Sector*, *2* (45), 17–26. https://doi.org/10.33099/2618-1614/2023-45-2-17-26.
13. Yakymenko, O. O. (2023). Factors influencing the command system under enemy informational and cyber attacks: Ukrainian experience. *Military Security and Strategy*, *1*, 41–48.
14. *Lessons from the Russo-Ukrainian War: How to Maintain Command and Control in Modern Combat: Analytical Report*. (2023). Center for Defense Strategies. https://defence.org.ua
15. Sabbagh, D. (2023, Sept. 10). How Ukraine's battlefield coordination is reshaping modern command and control. *The Guardian*. https://www.theguardian.com/world/2023/sep/10/ukraine-command-and-control
16. Ihnatov, S. V., & Ostapchuk, V. M. (2023). Innovative approaches to building a resilient command system under new types of warfare. *Skhid*, *4* (184), 55–62. https://doi.org/10.21847/1728-9343.2023.4(184).285534
17. *Defence Command Paper Refresh 2023: Mobilising for Secure Britain* (Section on C2 Resilience). (2023). UK Ministry of Defence. https://www.gov.uk/government/publications/defence-command-paper-2023
18. Koval, O. V., & Dubovyk, M. M. (2023). Improving the operational command system of the Armed Forces of Ukraine based on the experience of the 2022–2023 war. *Scientific Journal of the National Defence University of Ukraine*, *2* (79), 73–80.

The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 3 No. 2 (2025)

# Analysis and Assessment of the Influence of Factors on the Requirements for the Command and Control System of an Operational Military Grouping in Operations (Combat Actions): The Experience of the Russo-Ukrainian War

**Roman Voitsechovskyi**
Adjunct Lecturer at the Department of Troop Command and Control,
Institute of State Military Management
National Defence University of Ukraine
03049, Povitrianykh Syl Avenue, 28, Kyiv, Ukraine
e-mail: voytsehovskiy31@gmail.com
ORCID: 0009-0000-6408-9620

**Abstract.** The experience of the Armed Forces of Ukraine since 2022 has demonstrated that the ability of the command and control system to remain functional under conditions of losses, isolation of command posts, changes in the tactical situation, and information overload is a key prerequisite for maintaining the combat effectiveness of military groupings. Successful examples of decentralised decision-making, integration of digital platforms, use of unmanned and autonomous systems, and modular command structures allow for the development of new approaches to formulating requirements for the command and control system of operational military groupings based on the criterion of resilience.

The main purpose of this article is to analyse and assess the influence of various factors on the requirements for the command and control system of operational military groupings in operations (combat actions), drawing on the experience of the Russo-Ukrainian war.

This article identifies the main external and internal factors influencing the requirements for the command and control system and evaluates their impact using the method of pairwise comparisons. It offers recommendations for enhancing the resilience of the command and control system and defines key indicators for the survivability of command posts. The research methodology combines analysis and synthesis with expert surveys, utilising the pairwise comparison procedure to assess the level of influence of each factor on the system's resilience in operational contexts.

The findings of this article may be of use to military theorists and practitioners developing modern warfare strategies; security and defence analysts studying the transformation of armed conflicts; researchers in the philosophy of war, military history, and international relations; as well as policymakers and military leaders shaping defence policies and doctrines.

**Keywords:** automation of command posts, combat actions, requirements for command and control systems, military operations, cyber weapons, survivability of command posts, operational military grouping operations, operational military grouping, command responsiveness, Russo-Ukrainian war, command posts, command and control systems, resilience of command and control systems

*Наукове видання*

**Центральний науково-дослідний інститут**
**Збройних Сил України**

Міжнародний науковий журнал
“Military Science”

Редактор Васянович М.
Коректор Котляр Т.
Комп’ютерне верстання Возняк І.

Підп. до друку 25.06.2025. Формат 70x100/16
Папір офсетний. Друк цифровий.
Ум. друк. арк. 23,34. Зам. №. 2507-25/3.
Наклад 50 прим.

Видавець і виготовлювач ТОВ «7БЦ»
03067, м. Київ, вул. Олекси Тихого, 84
e-mail: 7bc@ukr.net, тел: (044) 592-00-80
Свідоцтво суб’єкта видавничої справи ДК №5329 від 11.04.2017