The Central Research Institute
of the Armed Forces of Ukraine

Military Science

JOURNAL

Vol. 4 No. 1

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

themilitaryscience.com

The Central Research Institute
of the Armed Forces of Ukraine

Military Science
JOURNAL

Vol. 4 No. 1

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

themilitaryscience.com

УДК 355/359:623.09/98 (08)
DOI: 10.62524/msj.2026.4.1
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 із 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 № 3 від 08.04. 2026 року)

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

Телефон:
+38 (044) 520-19-44

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

Інформаційний сайт:
themilitaryscience.com

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

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

© ЦНДІ ЗС України, 2026

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

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.
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.
Машкін О.	д-р техн. наук, ст. наук. співроб.
Мірненко В.	заслужений працівник освіти України, д-р техн. наук, проф.
Потетюєва М.	д-р екон. наук, доц.
Потьомкін М.	д-р техн. наук, проф.
Сілі Р.	PhD, Research Associate (Сполучене Королівство Великої Британії та Північної Ірландії)
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.
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.

Технічні редактори: Возняк І., канд. пед. наук, доц.;
Шнукало А.

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Contents

Syrskyi O., Semenenko O., Kin O., Nashchubskyi V.
Consciousness as a battlefield – the evolution of cognitive warfare in the global security system (cognitive operations – a tool of geopolitical dominance): prospects for organising a cognitive combat system in Ukraine 6

Muzhenko V., Bohdanovych V., Huliak O., Vysidalko A.
A Methodical Approach to Forming the Outline and Database of the Military and Strategic Analysis of Destructive Geopolitical and Conflict-Generating Factors Influencing the Defence and Industrial Complex of Ukraine 27

Комаров В., Сокоринський Ю., Твердохліб Є., Поливода М.
Трансформація напрямів розвитку засобів збройної боротьби російської федерації на поточному етапі російсько-української війни: основні тенденції 39

Zinchenko A., Lunov I., Kozlov V., Tarasov O.
The State Policy Life Cycle in the Defence Domain 51

Solomatin D., Sedliar A., Pasichnyk V., Lutseviat O., Sliusarenko M., Popkov S.
The Analysis of Global Trends in the Development of Operational (Operational-Strategic) Reconnaissance-Strike Complexes Based on Unmanned Aerial Vehicles 62

Царинник В., Баранов С., Ремез В., Васянович А.
Визначення пріоритетних факторів впливу на ефективність функціонування системи кадрового менеджменту Збройних Сил України на основі методу інтерпретаційного структурного моделювання 76

Zvarych S., Trokhymenko O., Vorobyov A., Poberezhets T., Kotiukh Yu.
Methodological Approach to Creating a Cyber Defence Terminology System 91

Гнатов А., Лебеденко А., Семененко А., Ярмольчик М.
Турецький досвід багаторівневої системи фізичних, інженерних та технічних засобів контролю і стримування "Стіна безпеки": аналіз, результати та перспективи адаптації для Збройних Сил України 99

Толок П.
Метод оцінювання стану воєнно-економічної безпеки держави на основі нечітких оцінок ресурсних можливостей 114

Hurkovskyi V., Ovanesian R., Kalashnikov D., Tsybizov A., Nedbalek K.
The Foresight of the russian federation's Mobilisation Potential: Structure, Mechanisms and Development Scenarios for 2025–2026 years 127

Темний О.
Методика пріоритезації та оцінювання впливу когнітивних загроз на ефективність системи стратегічних комунікацій Збройних Сил України 145

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Ткаченко В., Тимків О., Закусило П., Харченко В., Ткаченко Н.
Методика планування порядку оновлення озброєння, військової та спеціальної техніки військових формувань 157

Гризо А, Костиря О., Трофимов І., Нелінь Д., Лук'янчиков А.
Аналіз підходів НАТО до системи моделювання та імітації, перспективи їх адаптації й упровадження в Україні 174

Добровольський Ю.
Переваги, виклики та застереження застосування роботизованих систем у військовій сфері: комплексний аналіз та рекомендації 197

Клименко В.
Модель підвищення гнучкості циклу управління оперативно-тактичним угрупованням в умовах множинних невизначеностей обстановки 206

Чернишова І., Марко І., Бусель В., Марко Є., Рахімов В.
Воєнно-економічне прогнозування в системі національної безпеки України: роль, місце та вплив на забезпечення обороноздатності держави 216

Соломицький О., Ігнатьєв А., Кудрицький М., Коваль В., Молчанов Д.
Рекомендації щодо забезпечення інтероперабельності ситуаційних центрів України 227

Колесник О.
Понятійна невизначеність штурмових дій та методичні наслідки для оцінювання ефективності їх ведення 239

Дідіченко В., Горгуленко В., Янковий Я., Рибак Д., Череп Д.
Проблемні питання оборонного менеджменту: організаційно-правовий аспект 251

Карпусь А., Кенгерлі А.
Аналіз впливу хімічної та радіаційної дифузії на організм людини 265

AL-Rawi M.
Literature Survey on Warfighter Information Network-Tactical 279

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Received: *December 2, 2025* | **Revisions Requested:** - | **Revision Received:** -
Accepted: *January 28, 2026* | **Published Online:** *April 10, 2026*

Licensed (C) by Creative Commons Attribution International License 4.0 (CC BY-NC-SA)

DOI: 10.62524/msj.2026.4.1.1

Consciousness as a battlefield – the evolution of cognitive warfare in the global security system (cognitive operations – a tool of geopolitical dominance): prospects for organising a cognitive combat system in Ukraine

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

Oleh Semenenko
Honoured Figure of Science and Technology of Ukraine
Doctor of Military Sciences, Professor
Deputy Commandant 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

Oleksandr Kin
PhD in Technical Sciences, Associate Professor
Hennadii Udovenko Diplomatic Academy of Ukraine
under the Ministry of Foreign Affairs
01001, Velyka Zhytomyrska Street, Kyiv, Ukraine
e-mail: cubalibre1972@ukr.net
ORCID: 0009-0001-2196-7515

Vitalii Nashchubskyi
Commander of the 92nd separate assault brigade
named after the Kosh Ataman Ivan Sirko
63505, Horishnogo St., 142, Chuguev, Kharkiv region, Ukraine
e-mail: xcii.mgm@gmail.com
ORCID: 0009-0006-1362-6549

“Le buone leggi nascono dalle buone armi.” –
“Good laws are born from good weapons.”
Niccolò Machiavelli

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

"The highest art of war is not to fight and win in all battles, but to undermine the enemy's resistance without fighting."
Sun Tzu "The Art of War"

"World order exists to the extent that people believe in it."
"Deterrence works through imagination, not through the use of force."
Henry Kissinger

Abstract. The current stage of development of international security is characterised by a profound transformation of the forms and methods of confrontation, within which intangible factors of influence are becoming increasingly important. Under these conditions, the consciousness of a person and society as a whole becomes a key object of targeted military-political actions, and the struggle for control over thinking, ideas and values goes beyond traditional ideas about war. This necessitates an urgent need for a scientific understanding of the evolution of cognitive warfare and its place in the global security system, taking into account modern challenges and realities of the military-political situation. Therefore, the main goal of the article is a comprehensive understanding of the evolution of cognitive warfare as an independent dimension of the modern confrontation in the global security system, revealing the role of cognitive operations as an instrument of geopolitical dominance, as well as substantiating the need to form a holistic strategic vision of organising cognitive warfare at the state level, taking into account the experience of the russian-Ukrainian war and growing global threats. The main results of the article are that it: analyses scientific, military-theoretical and political sources of awareness of the decisive role of consciousness in war; the main terms and concepts in the modern understanding of cognitive warfare are formulated; an approach to the formation of a general indicator of the effectiveness of cognitive influence (integral indicator of consciousness possession) is proposed and a scale for its evaluation is determined; views on the creation of special Cognitive Influence Forces (CIF) within the Armed Forces of Ukraine are determined. The materials of the article may be useful to state authorities and the security and defense sector, military and political leadership, scientists and analytical centers working in the fields of military science, philosophy of war, international relations, security studies, education, for the training of specialists in the field of strategic communications, information security and public administration, civil society and the media.

Keywords: struggle for consciousness, military-political situation, military conflicts, globalism, hybrid war, information war, information security, cognitive operations, cognitive influence, international politics, international coalitions, defence capability, russian-Ukrainian war, national security, criteria of defence adequacy, technological advantages, consciousness, consciousness of the nation, stability of the state.

Introduction

The relevance of studying cognitive influence on individuals and nations is driven by the rapid evolution of the forms and methods of armed confrontation in the modern world, within which human consciousness, as well as national consciousness as a whole, is increasingly transforming into an independent battlespace that directly affects the resilience of states, the behaviour of societies and the outcomes of military political confrontations [1]–[35].

A comprehensive understanding of the phenomenon of cognitive warfare at the global level emerged following the illegal occupation of the Autonomous Republic of Crimea and the outbreak of war in eastern Ukraine in 2014, when information psychological and cognitive influence became a key instrument in the preparation and conduct of military aggression. At the same time, the peak awareness of the decisive role of cognitive confrontation occurred at the onset of the full scale

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

invasion of Ukraine by the russian federation in 2022, which clearly demonstrated the capacity of cognitive operations to shape not only the course of combat operations but also the resilience of states, societies and international coalitions [1]–[19].

Today, amid the expansion of the geographical scope of military conflicts and crises, the struggle for the consciousness of individuals and nations has acquired global characteristics. It is no longer confined to individual regional wars or bilateral confrontations but increasingly encompasses global consciousness as a whole. In effect, a global cognitive environment has emerged in which all key actors of international politics operate, as current conditions have effectively removed constraints on the use of cognitive influence tools by leading states, in the absence of clear limitations and effective deterrence mechanisms. A distinctive feature of cognitive warfare is that influencing even 30 to 40 percent of a target audience, along with shaping 20 to 30 percent of individuals who remain undecided or wavering, may already be considered a strategic victory over the consciousness of a nation. Under such conditions, it is not only influence over the adversary's audience that is decisive but also the assurance of cognitive resilience within one's own society, as this constitutes the foundation of effective cognitive confrontation. Vulnerability of internal consciousness automatically reduces a state's defence capability regardless of its military or economic strength.

It is therefore no coincidence that leading global actors such as the United States, russia and China view human consciousness as a strategic resource and systematically invest significant portions of their national potential, estimated at 5 to 10 percent of GDP, into shaping, maintaining and transforming both their own national consciousness and that of other nations. In this context, the absence of a well formed national consciousness effectively precludes the existence of a state, as statehood is fundamentally grounded in the conscious willingness of a nation to possess, sustain and defend its own country.

At the same time, cognitive influence, while not new in its essence, has today evolved into one of the most effective and essential forms of strategic weaponry. A state's lag in both internal and external domains of cognitive warfare significantly complicates armed confrontation in the event of its escalation, since achieving dominance over the adversary's consciousness or gaining control over the consciousness of its key audience often creates the conditions for attaining strategic objectives without complete military defeat or total occupation of territory [20]–[21], [28], [34]. Strategic miscalculations in cognitive warfare pose a particular danger, as their consequences may be irreversible. Ill considered or situational actions in the domain of cognitive influence can trigger cascading global processes, erode international norms and rules, and effectively legitimise similar actions by other states [28], [32]. A telling example in this regard is the russian federation, which, while concentrating its main efforts on the Ukrainian direction, simultaneously lost the capacity for effective cognitive response to other regional and global developments, including Syria, the Middle East and Latin America, thereby demonstrating the limitations of even major powers in the event of strategic miscalculations. In this context, the study of the evolution of cognitive warfare within the system of global security is of critical importance, as it enables an understanding of consciousness as a key battlespace of present and future confrontation and supports the development of scientifically grounded approaches to the strategic planning of cognitive influence under conditions of increasing instability in the world order.

At the present stage of the development of the military and security environment, Ukraine recognises the critical importance of the struggle for consciousness as one of the key domains of confrontation in a new generation of warfare. The practical experience of countering russian aggression since 2014, and especially under conditions of the full scale invasion since 2022, has demonstrated the decisive influence of cognitive operations on societal resilience, the level of national mobilisation and international support for the state. At the same time, this awareness has not yet been transformed into a coherent strategic vision for the organisation and conduct of cognitive warfare.

At present, Ukraine lacks systematic and conceptually formalised approaches to the

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

development of cognitive confrontation, both with the russian federation and with other potential sources of threat. This applies to both the external dimension, aimed at influencing international audiences and the adversary's human resources, and the internal dimension, which must ensure the cognitive resilience of the nation and protection against destructive influence. The fragmentation of approaches, the absence of a unified planning centre and the lack of long term forecasting significantly reduce the effectiveness of state efforts in this domain. The current situation creates objective preconditions for immediate response and proactive strategic anticipation of cognitive influence activities targeting both national consciousness and the perceptions and behavioural patterns of the adversary's personnel. The implementation of such an approach requires not only regulatory and methodological support but also the establishment of specialised military formations and civil military institutions capable of professionally planning, coordinating and conducting cognitive warfare.

The presence of such structures would enable the systematic organisation of cognitive confrontation, timely identification of threats and their mitigation or substantial reduction in the short and medium term, thereby creating a strategic advantage without the use of excessive military force. Under these conditions, the struggle for consciousness emerges not as a supporting element but as an independent instrument for ensuring national security and state resilience.

Thus, the primary objective of this article is to provide a comprehensive understanding of the evolution of cognitive warfare as an independent dimension of modern confrontation within the global security system, to reveal the role of cognitive operations as an instrument of geopolitical dominance and to substantiate the necessity of forming an integrated strategic vision for organising cognitive warfare at the state level, taking into account the experience of the russian Ukrainian war and the growing global threats.

Materials and Methods

According to the analysis of scientific, military theoretical and political sources, the recognition of the decisive role of consciousness in warfare emerged long before the appearance of modern terms such as "cognitive operations" or "information warfare" [1]–[35]. In different historical periods, this idea was expressed through concepts of morale, fighting spirit, political will, legitimacy, identity and control over mass perceptions.

Early historical sources emphasised that consciousness is a prerequisite for victory. The earliest works focusing on the targeting of the adversary's consciousness are represented by the writings of Sun Tzu. In The Art of War (5th century BC), the principle was first clearly articulated that "the supreme art is to subdue the enemy without fighting". This provision effectively constitutes the first systematic concept of struggle for consciousness, where deception, demoralisation, undermining trust in leadership and the imposition of false perceptions are regarded as primary instruments of warfare.

The further development of this idea can be observed in the works of Carl von Clausewitz, who in On War defines war as the continuation of policy by other means. In his approach, the consciousness of the nation and political will form the foundation of a state's capacity to wage war. Clausewitz explicitly notes that defeat begins not with the destruction of the army but with the loss of the will to resist.

The twentieth century shaped the understanding that mass consciousness is an object of systematic influence. Sources from the first half of the twentieth century demonstrate the transition from an intuitive understanding of the importance of consciousness to its institutionalised application. The works of Harold Lasswell, particularly his studies of propaganda during the First World War, laid the scientific foundations for analysing influence on mass consciousness as a tool for mobilisation, demobilisation and the justification of violence.

In parallel, Edward Bernays, drawing on Freud's psychoanalytic theory, viewed the manipulation of consciousness as a normal element of both democratic and wartime processes. His

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

work clearly introduced the idea that control over public perceptions enables the management of behaviour without direct coercion.

The Second World War and the Cold War, as reflected in the works of Western and Soviet authors, ultimately consolidated the perception of consciousness as a strategic resource. Concepts such as psychological operations, political warfare and ideological confrontation became integral components of national security doctrines [28]–[33].

By the late twentieth and early twenty first centuries, the terms national identity narratives and soft power became firmly established. In the works of Joseph Nye, the concept of soft power shifted the focus from direct coercion to the attractiveness of values culture and models of the future. In this context, the consciousness of a nation is viewed not only as an object of protection but also as an instrument of influence on others [22].

Philosophical approaches of Michel Foucault and representatives of post structuralism complemented military political analysis by interpreting power as the ability to shape discourses norms and “truth”. This became the theoretical foundation for the modern understanding of the struggle for consciousness as a struggle for the right to define reality.

russia has not remained aside from this domain, as its intellectual tradition considers consciousness a field for domination over both its own population and others. A distinct group of sources is formed by russian military theoretical works, particularly those associated with the so called Gerasimov doctrine [28]–[29]. In these works, the consciousness of the adversary is directly defined as the primary target of influence, while the boundary between war and peace is effectively erased. These authors view cognitive and informational operations as a means of paralysing a nation without formally declaring war. These sources make it clear that the russian Ukrainian war is not an anomaly but the implementation of a long term strategy aimed at destroying Ukrainian identity and replacing historical memory.

Ukrainian academic sources clearly define how painful the experience of identity loss has been for Ukraine and emphasise the necessity of restoring national consciousness. Ukrainian research, particularly after 2014, has focused on national resilience information security and cognitive threats. In the works of Ukrainian military scholars philosophers and sociologists, national consciousness is regarded as an integral factor of state defence capability. These studies emphasise that historical defeats of Ukraine were largely linked not to a lack of resources but to the degradation of national consciousness prolonged existence within чужий semantic frameworks and the absence of a systematic policy for protecting identity [1]–[10], [30].

Analysis of theoretical research allows for the formation of a historical description of key terms such as consciousness national consciousness and struggle for consciousness. In classical understanding within philosophy and psychology, consciousness was defined as the ability of an individual to perceive reality and oneself within it, as seen in the works of Descartes and Kant. In military political sources of the twentieth and twenty first centuries, consciousness is interpreted more broadly as a set of perceptions beliefs emotions and readiness to act that can be subject to deliberate influence, as reflected in the works of Lasswell and Foucault. In turn, the concept of national consciousness is formed at the intersection of sociology political theory and security studies. In modern sources, it denotes collective identity historical memory a system of values and visions of the future that determine societal behaviour under crisis conditions.

In early sources, the concept of struggle for consciousness was not formally defined but existed implicitly in the works of Sun Tzu and Carl von Clausewitz [21], [20]. In contemporary research, it is defined as a purposeful activity by states or non state actors aimed at changing undermining or protecting the system of perceptions and decisions of another nation. Unlike earlier interpretations, today the struggle for consciousness is recognised not as a supporting element but as an independent domain of confrontation.

The results of the literature review indicate that the struggle for consciousness has historically

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

evolved from an intuitive instrument of warfare into a central element of national and global security. The war of russia against Ukraine has become a concentrated example of this evolution, where the outcome of confrontation is determined not only on the battlefield but within the cognitive domain.

For Ukraine, this analysis confirms that the future security of the state depends not only on the ability to defend its own consciousness but also on the capacity to act proactively in shaping narratives identity and meaning both domestically and globally.

Results and Discussions

As the transformation of the nature of armed conflicts and the growing role of non material security factors become a central object of confrontation, the consciousness of individuals and nations is increasingly emerging as the ultimate outcome of conflict. This situation necessitates a clear terminological distinction between concepts describing processes of cognitive influence, cognitive confrontation and their place within the global security system. In this regard, Table 1 presents the key terms and concepts reflecting the contemporary understanding of cognitive warfare, taking into account the current military political environment and the experience of recent armed conflicts.

Classically, the idea is interpreted in such a way that undermining the cognitive unity plans or will of the adversary may at times be more valuable than the direct application of force.

The conditions of the full scale war of russia against Ukraine demonstrate that modern armed confrontation extends far beyond the traditional physical battlefield. Alongside the use of military force, increasing importance is attached to systematic and targeted influence on the consciousness of individuals society and the nation as a whole, which necessitates a scientific rethinking of the relevant conceptual and categorical framework. In the twenty first century, consciousness itself is becoming both a key object and a resource of war, while the struggle for its formation is emerging as one of the decisive factors of a state’s strategic resilience.

The terms and concepts presented in Table 1 reflect the modern understanding of cognitive warfare as a systemic phenomenon that integrates informational psychological cultural value based and meaning centred dimensions of confrontation.

Some of these are refined interpretations of already established categories such as consciousness informational influence and psychological operations, yet under contemporary conditions they require expanded interpretation in light of the globalisation of the information space the development of digital technologies social media and artificial intelligence. Other terms are relatively new to the national academic and security discourse but in practice describe processes that are already actively employed by the adversary within the framework of hybrid and cognitive aggression against Ukraine.

The relevance of the proposed terminological framework is driven by the fact that russia is waging not only a war for territory against Ukraine but also a war for meaning identity and historical memory, seeking to dismantle national consciousness demoralise society undermine trust in state institutions and deprive Ukrainians of confidence in their future. Under such conditions, the absence of a clear scientifically grounded understanding of such phenomena as the cognitive front cognitive resilience cognitive sovereignty and cognitive dominance significantly limits the state’s ability to build an effective system of counteraction.

The growing importance of understanding human and national consciousness as a strategic resource and the last line of state security cannot be overstated. Even under conditions of military losses and economic exhaustion, the preservation of societal cognitive resilience determines a state’s ability to sustain resistance, conduct mobilisation, maintain international coalitions, and ultimately achieve long term victory. For this reason, such concepts as cognitive mobilisation, cognitive demoralisation, and the war for societal thinking possess not only theoretical but also direct practical significance for the national security and defence system of Ukraine.

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Table 1. Key Terms and Concepts in the Contemporary Understanding of Cognitive Warfare

Term / Concept	Contemporary Interpretation
Consciousness	The ability of an individual to perceive oneself and the surrounding world, form representations of reality, evaluate events, make decisions and bear responsibility for them. In the twenty first century, consciousness is shaped not only by rational thinking but also by a system of values, emotional responses, historical memory and the influence of the information environment, media and targeted cognitive operations.
National Consciousness	The collective perception of a community about itself, its origin, values, history, enemies and allies, acceptable limits of compromise and the image of a desired future. It includes national identity, language, culture, historical memory and the willingness to defend the state. A nation without a сформована consciousness is vulnerable to cognitive subjugation.
Struggle for National Consciousness	A systemic confrontation for the right to shape, transform or preserve a nation's perceptions about itself and the world. It is implemented through informational and media influence, historical narratives, education, culture and manipulation of fear, hatred or guilt. In modern wars, this struggle often determines a society's readiness to resist or capitulate.
Cognitive Warfare	A form of strategic confrontation aimed at altering thinking, perception, values and behaviour of individuals, groups and nations in order to achieve political, military or geopolitical objectives without necessarily applying direct military force.
Cognitive Warfare in the Global Security System	A globalised dimension of confrontation in which cognitive operations are used as a tool to influence international stability, alliances, state institutions and global public opinion, extending beyond individual regional conflicts.
Cognitive Operations	Purposeful, planned actions carried out by state or non state actors aimed at shaping, distorting or destroying the perceptions, beliefs and behavioural models of a target audience. They may be conducted in both peacetime and wartime.
Cognitive Influence	The process of influencing the thinking, emotions and behaviour of an individual or community through information, symbols, images, narratives, language and social practices in order to achieve a predetermined outcome.
Human Consciousness as a Strategic Resource	The aggregate intellectual, value based and motivational potential of a population that determines a state's capacity for resistance, mobilisation and recovery. In contemporary conditions, it is considered alongside economic, military and technological resources.
Consciousness as a Battlefield	A concept according to which human thinking, perceptions and values become objects of targeted military political influence, and the outcome of confrontation is determined not only in the physical domain but also in the mental domain.
Cognitive Dominance	A state in which one side is able to impose its own interpretation of reality, norms of behaviour and frameworks of thinking on another side, limiting its ability to make independent decisions and resist.
Cognitive Front	The totality of directions, channels and instruments of conducting cognitive warfare through which influence is exerted on the consciousness of the population, elites, military personnel and the international community.
Global Cognitive Front of Confrontation	The global level of cognitive competition in which leading states compete for control over global narratives, values and models of human development.
Cognitive Superiority	The ability of a state or coalition to more effectively shape its own and the adversary's consciousness, maintain resilience to external influence and employ cognitive tools to achieve strategic objectives.
Cognitive Transformation of Modern Warfare	The process of changing the nature of warfare in which not only armed actions but also the struggle for thinking, beliefs and the moral resilience of societies become decisive.
Cognitive Confrontation	The set of offensive and defensive actions in the domain of consciousness aimed at protecting one's own cognitive sphere and disrupting that of the adversary.
War for Societal Thinking	A form of warfare in which the object is the collective perceptions, values and decisions of social groups and nations, and the outcome is determined by the ability to control meanings and interpretations of events.
Consciousness as the Last Line of State Security	A conceptual proposition according to which the preservation of national consciousness and cognitive resilience of society is a decisive condition for the survival of the state in hybrid and cognitive wars.
Cognitive Resilience	The ability of a society to resist manipulation and maintain value coherence and integrity.
Cognitive Security	The state of protection of the consciousness of individuals, society and the state from destructive influence.
Cognitive Mobilisation	The process of forming a society's readiness for prolonged confrontation.
Cognitive Demoralisation	The deliberate undermining of belief in victory, the state or the meaning of resistance.
Cognitive Sovereignty	The ability of a state to independently shape its own informational and semantic space.

Equally important is the global dimension of cognitive warfare. Today, Ukraine is positioned at the centre of the global cognitive front, where competition unfolds over international support, interpretation of the causes and consequences of war, the construction of images of the aggressor and the victim, and the future architecture of global security. In this context, the development of a national scientific approach to cognitive warfare is essential not only for protecting national interests but also

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

for achieving cognitive superiority in a broader geopolitical dimension.

Thus, the systematisation, clarification, and introduction into scientific discourse of the terms presented in Table 1 constitute an objective necessity shaped by the nature of modern warfare, Ukraine's experience in countering hybrid aggression, and the need to establish a coherent theoretical and methodological foundation for state policy in the field of cognitive security. At present, Ukraine must not only respond to cognitive threats but also proactively develop its own school of thought in this domain, transforming wartime experience into a source of strategic advantage.

In modern warfare, the struggle for consciousness becomes decisive, as it determines whether societies are willing to continue or abandon war, support or resist political decisions, mobilise or become demoralised. Unlike classical military metrics, cognitive outcomes are probabilistic and mass in nature; therefore, they are assessed through the proportion of audiences exhibiting specific attitudes.

1. Adversary Audience:

25–30% anti war sentiment represents a critical threshold at which internal narrative conflict emerges, the legitimacy of war is undermined, and pressure on political leadership increases. This group may remain passive but contributes to the spread of doubt, demoralisation of the majority, and erosion of support for war.

20–40% neutral attitude toward war. In cognitive warfare, neutrality signifies a latent defeat for the aggressor, as it reduces mobilisation potential, lowers willingness to endure losses, and weakens support for coercive measures.

Combined effect (45–70%) indicates a loss of cognitive dominance by the adversary, even in the absence of mass protests.

2. Ukrainian Audience:

Over 40% resilient consciousness constitutes the core of national resilience. This segment resists demoralisation, maintains trust in statehood, and accepts prolonged hardship as necessary. It represents the minimum threshold required for sustained resistance and effective governance.

20–30% active support for the war of liberation forms the mobilisation core. This group generates military, volunteer, and informational capacity, shapes the moral climate, and produces meaning and examples for society. Without it, resilience risks degrading into passive survival.

Key Supporting Cognitive Indicators:

Over 40% informational losses of the adversary indicate declining propaganda effectiveness, loss of trust in official narratives, and fragmentation of informational cohesion;

Over 80% transparency of decision making (own side) is a critical condition for preventing internal cognitive disruption, countering disinformation, and maintaining public trust even under crisis conditions.

The overall effectiveness of cognitive influence during cognitive operations is measured as an integral indicator of control over audience consciousness.

This indicator consists of two interconnected subsystems:

Consciousness of one's own nation (resilience + mobilisation);

Consciousness of the adversary nation (demoralisation + neutralisation).

The overall indicator of cognitive influence effectiveness (i.e., the formation of consciousness) can be represented as an additive convolution with weighting coefficients of its main components:

$$E(t) = f(W_1, W_2) = \alpha \cdot W_1 + \beta \cdot W_2, \quad (1)$$

where α_1, α_2 – weighting coefficients of the effectiveness indicators of cognitive influence (formation of consciousness) for the own nation (W_1) and the adversary nation (W_2), $\alpha + \beta = 1$ (recommended values $\alpha = 0,6$, $\beta = 0,4$).

The formation of the indicator of the consciousness of one's own nation can be expressed as:

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

$$W_1 = \lambda_1 \cdot S + \lambda_2 \cdot M + \lambda_3 \cdot T\,, \quad (2)$$

where $\lambda_1, \lambda_2, \lambda_3$ – weighting coefficients of the respective indicators: S – cognitive resilience (the proportion of the population that does not succumb to panic, preserves values and trust in the state); M – cognitive mobilisation (the proportion of citizens ready for active participation in the struggle); T – trust and transparency (the level of trust in governmental decisions and their perception as legitimate and necessary); recommended weights $\lambda_1 = 0,4,\ \lambda_2 = 35,\ \lambda_3 = 0,25$.

The formation of the indicator of the adversary's national consciousness can be expressed as:

$$W_1 = \mu_1 \cdot S + \mu_2 \cdot M + \mu_3 \cdot T\,, \quad (3)$$

where μ_1, μ_2, μ_3 – weighting coefficients: D – cognitive demoralisation (the proportion of the adversary population that has lost belief in the purpose of the war); N – neutralisation of war support (the proportion of the population holding neutral or passive positions); I – informational losses (the level of loss of trust in official propaganda and information sources); recommended weights: $\mu_1 = 0,25,\ \mu_2 = 40,\ \mu_3 = 0,35$.

The general evaluation scale for the integral indicator of cognitive influence effectiveness is presented in Table 2.

Table 2. Evaluation Scale of the Integral Indicator of Cognitive Influence Effectiveness (Control over Consciousness)

Value of the Integral Indicator	Value of the Integral Indicator
< 0,4	Cognitive vulnerability of the state
0,4 – 0,6	Parity in cognitive confrontation
0,6 – 0,8	Cognitive superiority
>0,8	Cognitive dominance

The proposed system of indicators enables a quantitative assessment of the struggle for consciousness, facilitates the integration of the cognitive dimension into the system of military strategic analysis, and allows a transition from an intuitive understanding of cognitive warfare to a manageable and measurable process.

In the context of the ongoing transformation of military and political confrontations, the cognitive dimension is increasingly emerging as an independent domain of geopolitical competition. Cognitive operations are no longer merely auxiliary tools of informational influence; they have evolved into a system forming mechanism for achieving strategic advantage, as they target not only the information environment but also the deliberate transformation of consciousness, thinking patterns, and behavioural models of individuals, social groups, and entire nations. By influencing perceptions of reality, value systems, identity, and decision-making logic, cognitive operations enable states to shape favourable environments for the pursuit of geopolitical interests, impose advantageous interpretations of events, and undermine the adversary's capacity for organised resistance even before or without large scale military engagement.

Therefore, cognitive operations should be regarded as an instrument of geopolitical dominance, capable of controlling the dynamics, duration, intensity, and outcomes of conflicts. By shaping collective perceptions regarding legitimacy, justice, fear, losses, and future prospects, the actor conducting cognitive influence gains the ability to indirectly control political and military decision making of the opponent through altering their internal logic of threat perception and opportunity assessment. In this sense, the struggle for control over consciousness becomes no less important than the struggle for territory or resources.

The war of the russian federation against Ukraine represents a demonstrative case of the evolution of cognitive confrontation within a large scale geopolitical conflict. The application of

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

cognitive operations by the aggressor has been systemic and long term, encompassing efforts to delegitimise Ukrainian statehood, erode national identity, impose distorted historical narratives, construct the image of the "artificiality" of the Ukrainian nation, and promote the inevitability of external control. Following the onset of open armed aggression, cognitive pressure intensified further, manifesting in attempts to demoralise the population and armed forces, discredit political leadership, manipulate narratives of losses, war fatigue, and the perceived futility of resistance, as well as influence international perceptions of the conflict in order to reduce support for Ukraine.

At the same time, Ukraine's experience demonstrates that effective counteraction in the cognitive domain can serve as a source of asymmetric advantage even under conditions of limited resources. The consolidation of national identity, clear articulation of value orientations, strategic communications, symbolic actions, and leadership discourse have contributed to the formation of a high level of societal resilience and the preservation of the will to resist during a prolonged war. This confirms that cognitive resilience of society is a critical element of military and national security, and its erosion or strengthening directly affects the course and outcomes of armed confrontation.

Against the backdrop of increasing global hybrid threats, the proliferation of digital technologies, and the use of artificial intelligence to manipulate informational and cognitive processes, the formation of a comprehensive strategic vision for organising cognitive warfare at the state level becomes particularly relevant. Fragmented measures in the field of information policy or psychological protection are no longer sufficient to ensure an adequate level of state resilience. What is required is an integrated system, in which the cognitive dimension is organically embedded into the overall architecture of national security and defence, with clearly defined functions, authorities, and responsibilities among state institutions, the security and defence sector, as well as educational, cultural, and informational domains.

The development of such a strategic vision presupposes a combination of defensive and offensive approaches in cognitive confrontation, reliance on scientifically grounded methodology, interdisciplinary research, and systematic forecasting. Without this, the state remains vulnerable to long term cognitive attacks capable of gradually eroding national identity, critical thinking, and societal cohesion even in the absence of active hostilities.

Within this framework, cognitive operations should be considered as a complex of interconnected types of influence. One of the fundamental categories includes operations aimed at changing or destroying identity, targeting perceptions of belonging, historical memory, and value orientations. These are achieved through the substitution of narratives, discrediting of symbols and national heroes, and the imposition of alternative models of self identification. Closely related are operations aimed at shaping perceptions of reality, the purpose of which is to construct a worldview favourable to the influencing actor by manipulating causal relationships, normalising aggression, or distorting the assessment of risks and threats.

A significant role is played by operations designed to undermine the will to resist, targeting the demoralisation of the population, military personnel, and political leadership through the cultivation of fear, fatigue, hopelessness, and the perception of the inevitability of defeat. In parallel, operations are conducted to influence decision making processes, targeting the cognitive mechanisms of strategic and operational thinking of elites, implemented through information overload, the imposition of false dilemmas, or inducement toward erroneous or untimely decisions. A separate category consists of long-term cognitive erosion operations, designed for strategic and intergenerational impact. These are implemented through educational, cultural, and media channels and gradually transform value orientations and the level of critical thinking within society.

In summary, in the context of modern warfare and global confrontation, cognitive operations are becoming a key factor in achieving geopolitical advantage. The war of the russian federation against Ukraine convincingly demonstrates that the outcome of confrontation is determined not only by material resources or military power, but also by the state of societal consciousness, the level of

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

resilience, and the ability to withstand external cognitive pressure. Accordingly, the formation of a comprehensive, systematic, and institutionally embedded state policy in the field of cognitive warfare is not optional, but an objective necessity for ensuring national security, strategic resilience, and long-term competitiveness of the state.

Therefore, it is necessary to outline перспективи (prospects) for Ukraine in creating an effective system of cognitive confrontation under the conditions of the ongoing war.

Modern wars are increasingly conducted within the information and cognitive domain, encompassing the shaping of public decision making, undermining the adversary's morale, demoralisation, disruption of logistics through deception, and the construction of strategic narratives. All these effects produce tangible operational and strategic outcomes. Given that the adversary (the russian federation) actively employs informational tools in combination with cyber and electronic warfare, Ukraine requires a centralised, highly professional, and ethically grounded institutional mechanism capable of both strategic response and proactive influence.

Therefore, under current conditions, it is necessary to consider the establishment within the Armed Forces of Ukraine of a specialised branch or force, for example, the Cognitive Influence Forces (CIF). However, such a structure must be developed in a deliberate and balanced manner: not as "another headquarters," but as an interagency, operationally capable, and long-term oriented force component with a clearly defined mandate, legal constraints, and accountability mechanisms.

Reference: Cognitive influence refers to targeted actions (communication, informational, technological, and organisational) aimed at shaping perceptions, representations, evaluations, decision-making, and behaviour of specific audiences through воздействие on cognitive processes (attention, memory, judgment, and risk assessment). The key distinction lies in the focus not merely on "messages," but on the modification of decision-making mechanisms: (Perception → Interpretation → Action). This concept encompasses: traditional psychological operations; information manipulation; algorithmic pressure (social media, recommendation systems); bot networks and automated amplification; deepfake technologies and AI-driven manipulation; attacks on decision-making processes at individual and institutional levels.

Information-psychological influence and information-psychological operations (IPO and PSYOP) traditionally focus on the delivery of specific messages, the formation of narratives, and the influence on emotions and morale (i.e. "what to say" and "to whom"). Such an approach is widely described in russian and Soviet doctrines as "information-psychological pressure (influence)".

Cognitive influence and cognitive warfare are considered more broadly, namely how information, technologies (algorithms, bots, deepfakes), infrastructure, and organisational actions alter the very process of perception and decision-making within target systems, specifically individuals, groups, and institutions. This includes, but is not limited to, information-psychological measures.

Cognitive influence is broader and more conceptual, whereas information-psychological influence represents a practical subset of instruments used to achieve cognitive effects.

Let us consider examples of foreign experience in establishing and organising processes of cognitive influence on internal and external audiences within the framework of cognitive operations as instruments of geopolitical dominance across various territorial scales (from a specific region to the global level as a whole).

The United States has long developed psychological operations (PSYOP), information operations (IO), and Civil Affairs forces capable of planning and executing tactical, operational, and strategic influence campaigns (for example, USACAPOC and Information Operations units – the United States Army Civil Affairs and Psychological Operations Command). Their primary tasks include conducting cognitive and information influence in conflict zones, supporting combatant command through the provision of analysis and influence tools, organising civil-military cooperation, and assisting in stabilisation operations following combat activities. In essence, USACAPOC represents an American analogue of structures that could, within the Armed Forces of Ukraine, be responsible for integrating cognitive influence and CIMIC functions.

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

The United Kingdom has established the UK Strategic Command and the concept of "information advantage", which integrates specialised capabilities to achieve informational superiority (a strategic command that unifies covert and integrated capabilities).

In 2015–2016, the PLA Strategic Support Force was established by China as an integrated structure encompassing space, cyber, electronic warfare, and psychological/information operations, designed to generate synergy across capabilities.

In 2017, russia created "information operations forces" and cyber forces within the Ministry of Defence, forming a system that incorporates the MoD, GRU, FSB, private networks, troll farms, media outlets, and other instruments. This represents more of a "hybrid ecosystem" than a single unit.

Leading states integrate cyber capabilities, electronic warfare, psychology, and strategic communications into unified organisational structures or ensure their close coordination at the strategic level.

The "Cognitive Influence Forces of the Armed Forces of Ukraine" as a distinct branch of service should possess a clear hierarchy, budget, personnel, and doctrine; however, this requires extensive legislative development and resources.

Such a structure should function as a joint component within the General Staff of the Armed Forces of Ukraine or Ministry of Defence of Ukraine (Joint Cognitive Operations Command) in order to ensure coordination among Land, Air, Cyber, Special Operations Forces, Air Assault Forces, and civilian agencies.

It is advisable to begin as a separate interagency joint force, with the prospect of evolving into a distinct branch of service as tasks and authorities expand. This approach would provide flexibility, rapid integration, and a sound legal foundation.

Figure 1 presents a proposed prospective structure of the Cognitive Influence Forces Command of the Armed Forces of Ukraine, while the tasks and, in part, the functions of the main components of this system within the General Staff of the Armed Forces of Ukraine are outlined below.

1) Command and Planning (HQ Cognitive Operations).

strategic planning over decades (meta-narratives, timelines, points of influence);

coordination with the General Staff of the Armed Forces of Ukraine, the Ministry of Defence of Ukraine, the Security Service of Ukraine, the Ministry of Foreign Affairs, and civilian institutions (public security centres, the National Council on Television and Media).

2) Operational Units (Execution).

psychological operations units (PSYOP/IO teams) – production of messages and targeted delivery (media, social networks, field campaigns);

cognitive-analytical groups – social and behavioural research, linguistic localisation, audience targeting;

cyber and electronic warfare (EW) integration – technical support of operations in cooperation with cyber units;

SIGINT (Signals Intelligence) – intelligence based on signal interception (radio, telephone, internet, satellite channels, adversary tactical communications systems); GEOINT (Geospatial Intelligence) – intelligence based on geospatial information (satellite and aerial imagery, maps, data from drones, sensors, GPS); HUMINT liaison (Human Intelligence) – human-source intelligence, i.e. acquisition of information from individuals: witnesses, informants, agents in the adversary's rear;

field influence teams – operations within the theatre (psychological pressure along the adversary's rear areas, engagement with the local population).

3) Research and Development Centre (Behavioral & Influence Lab).

experts in psychology, linguistics, sociology, and AI/ML for retargeting (application of machine learning algorithms and artificial intelligence for automated and personalised delivery of messages or content to audiences that have previously interacted with specific services or materials), narrative analysis, message testing, and ethical assessment;

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

data provenance and audit trail (records of actions, evidentiary base) to ensure legal and international protection of operations.

4) Strategic Communications and PR Coordination.

liaison with official channels (MoD press centre, government institutions), ensuring compliance with national legislation and principles of non-interference and avoidance of unintended influence on civilian populations.

5) Legal and Ethical Department.

comprehensive legal assessment of each campaign (domestic and international law), mechanisms for transparency and accountability.

6) Training, Education and Doctrine.

centre for training and certification of specialists (psychologists, data specialists, IO operators), development of doctrinal documents.

7) Coordination with Civil Institutions and Allies.

безперервна інтеграція з МВС, СБУ, МЗС, НБУ, медіарегуляторами та міжнародними партнерами (NATO StratCom, UK, US liaison).

The core personnel should be formed from specialists in the following fields: psychologists (social/clinical), linguists, anthropologists, sociologists; data scientists, AI engineers, user experience researchers (UX/UX researchers); information support officers, PSYOP operators; journalists, speechwriters, crisis communicators; cyber engineers, electronics specialists; legal experts and ethical auditors.

The initial phase of establishing the Cognitive Influence Forces Command (rapid deployment) creation within the General Staff of the Armed Forces of Ukraine of a separate “Cognitive Operations Centre” with interagency authority. This enables operational coordination without a lengthy legislative process.

Subsequently, within 0.5–1 year, it should be transformed into a “Cognitive Influence Forces Command” with several regional groups.

Further, within 1–2 years, it should be formalised as a distinct branch of service with dedicated state funding, personnel, and standards.

The Cognitive Influence Forces Command must be closely subordinated to and coordinated with the General Staff of the Armed Forces of Ukraine.

The Security Service of Ukraine and the Ministry of Information Policy, as well as the Centre for Countering Disinformation, should maintain coordination capabilities within the civilian domain, alongside a clear division of responsibilities (the Ministry of Defence should focus on military missions, while civilian agencies should be responsible for organising the national information environment for the population).

The Cognitive Influence Forces of the Armed Forces of Ukraine are designed to achieve informational and psychological advantage over the adversary through systematic influence on their consciousness, motivation, and behaviour, as well as to enhance the resilience of Ukrainian society under conditions of war.

The main areas of activity of the Cognitive Influence Forces in the Armed Forces of Ukraine can be defined as follows:

Influence on the adversary: shaping a critical attitude toward aggression and reducing support for military actions among enemy military personnel and civilians; weakening the moral and psychological potential of the enemy and disrupting decision-making processes; countering hostile propaganda, disinformation, and cognitive manipulations.

Protection and support of the Ukrainian audience: increasing the population’s resilience to informational attacks and psychological pressure; ensuring transparency of decisions and communications regarding defence and state actions; preventing loss of informational advantage and supporting the moral and psychological condition of the Armed Forces of Ukraine and the civilian

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

population.

Analytical and research activities: utilisation of modern technologies (artificial intelligence, analytics, modelling) to forecast adversary reactions; supporting the Armed Forces of Ukraine command in decision-making based on integrated intelligence and analytical data; developing innovative cognitive influence methods in accordance with international law and NATO standards.

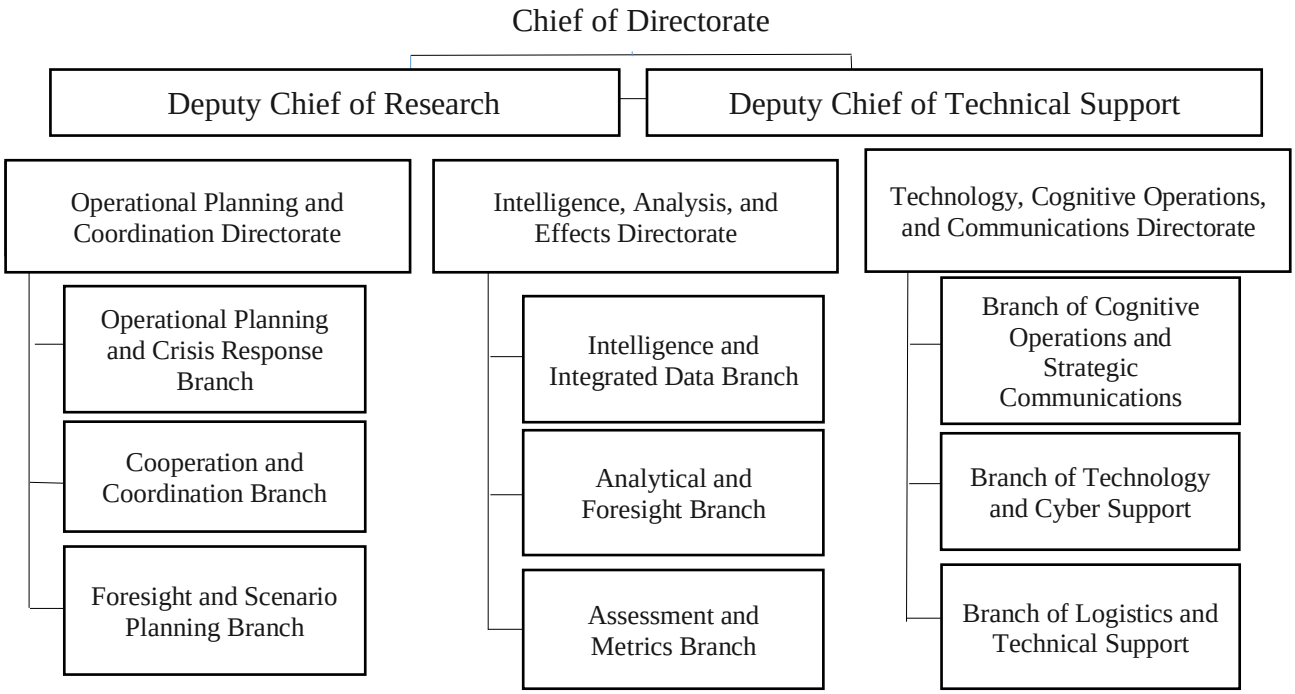


Figure 1. Draft Prospective Structure of the Cognitive Influence Forces Command of the Armed Forces of Ukraine

The key effect is the creation of systemic and controlled influence on the consciousness and behaviour of both the adversary and the population, enhancing the effectiveness of national defence and contributing to the accelerated conclusion of hostilities under conditions favourable to Ukraine.

The primary goal of establishing the Cognitive Influence Forces is to ensure that the Armed Forces of Ukraine are capable of planning, coordinating, and executing informational-cognitive operations to increase operational and strategic advantage, protect national interests, and reduce the combat effectiveness of the adversary through legitimate, ethical, and lawful influence measures.

The main task of the Cognitive Influence Forces is the formation and execution of targeted, ethically vetted, and evidence-based cognitive campaigns to achieve operational and strategic outcomes in support of Ukraine's combat and national objectives, and to ensure the informational resilience of own forces and the civilian population.

Key tasks and functions of the Cognitive Influence Forces (practical cases):

Strategic development of narratives integrated into the overall military strategy, i.e., formation of long-term strategic messages aligned with military and political objectives;

Psychological operations (PSYOP), planning and conducting campaigns to demoralise the adversary, influence enemy command decisions, and undermine local support for opponents;

Operational informational support for troops through deployment of local influence teams, text, voice, and multimedia messaging for units at the front and in the rear;

Synchronisation with cyber and electronic warfare (EW) actions and coordination of technical means (cyber intrusions, DDOS, data leaks, EW) to enhance informational effects (i.e., integration of

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Information Operations (IO) + Cyber-Electromagnetic Activities (CEMA));

Control and protection of own informational environment through securing communication channels, discrediting adversary channels, and internal information oversight;

Analytics and targeting using SIGINT / GEOINT, OSINT, and behavioural data for precise audience selection and delivery channels.

Structure of the Cognitive Influence Forces Command with Task and Function Distribution

1. Operational Planning and Coordination Directorate – centralised planning and coordination of all cognitive operations, interaction with the General Staff of the Armed Forces of Ukraine and interagency structures.

1.1 Operational Planning Branch – development of campaigns, preparation of plans and scenarios.

1.2 Cooperation and Coordination Branch – interaction with other branches of the Armed Forces of Ukraine, interagency structures, and partners.

1.3 Crisis Response Branch – operational management during unforeseen events and rapid adjustment of plans.

2. Intelligence, Analysis, and Effects Directorate – collection and analysis of data, creation of intelligence products for cognitive influence, assessment of campaign effectiveness.

2.1 Intelligence and Integrated Data Branch – HUMINT, SIGINT, GEOINT, OSINT, and analysis of acquired sources.

2.2 Analytical and Foresight Branch – development of models, forecasts, and recommendations for effect planning.

2.3 Assessment and Metrics Branch – analysis of campaign outcomes, KPIs, and evaluation of side effects.

3. Technology, Cognitive Operations, and Communications Directorate – operational execution, technical support, strategic communications, cyber and algorithmic influence.

3.1 Branch of Cognitive Operations and Strategic Communications – planning and execution of campaigns, creation of narratives and counter-narratives.

3.2 Branch of Technology and Cyber Support – operation of AI/analytical platforms, cyber defence, and electronic warfare.

3.3 Branch of Logistics and Technical Support – deployment of infrastructure, technical support for field operations, ensuring platform functionality.

Risks, Ethical, and Legal Considerations in Establishing the Cognitive Influence Forces Command

Internal constraints are dictated by the fact that Ukrainian legislation and international law do not permit operations that would violate the rights of domestic or foreign citizens or cause harm to civilians.

Reputational risks arise from the possibility that operations may enter the public domain without proper justification, potentially undermining trust in the state. Mechanisms for audit and provenance (action logs, evidentiary base) are required.

Adversary countermeasures demonstrate the need to prepare scenarios for indirect responses and informational “backfires.”

Technical risks stem from reliance on private platforms and tools, necessitating separate agreements and policies.

Key elements include planning (strategic doctrine over decades), operational PSYOP/IO units, R&D (behavioural sciences + AI), cyber / EW integration, legal support, and coordination with civilian institutions.

russia’s war against Ukraine is characterised not only by physical combat on the battlefield but also by active use of informational, psychological, and cognitive influence tools. Experience from the war and analysis of contemporary international operations indicate that an advantage in the cognitive

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

domain often determines success or failure in military campaigns.

The establishment of a Cognitive Influence Forces Command within the Armed Forces of Ukraine will allow for systematic planning and implementation of influence on the consciousness and behaviour of the adversary to reduce their moral and organisational resilience, enhance the resilience of the Ukrainian population and own military personnel against informational and psychological pressure, and utilise modern analytical and technological tools, including artificial intelligence and integrated information systems, for rapid and evidence-based decision-making. It will also ensure that the actions of the Armed Forces of Ukraine are compliant with international standards and NATO practices in the field of cognitive and informational influence.

Thus, the creation of the Cognitive Influence Forces Command represents a strategically necessary step to enhance Ukraine's defensive potential, ensure informational advantage, effectively counter aggression, and facilitate the integration of the Armed Forces of Ukraine into a modern combat operations paradigm, where success depends not only on physical but also on cognitive superiority over the adversary.

Conclusion

As a result of the conducted research, it has been established that in the 21st century, consciousness has become an independent domain of warfare, and the struggle for it is a key factor in shaping the national resilience of a state. Contemporary armed conflicts are increasingly less resolved exclusively by military force and are increasingly dependent on the parties' ability to influence the perceptions, values, and behaviour of societies. Historical analysis has shown that influence over the consciousness of nations has been used in wars and political confrontations for centuries; however, it is precisely in the 20th–21st centuries that it has acquired a systemic, institutionalised character. Totalitarian regimes demonstrated the possibility of transforming mass consciousness into an instrument of mobilisation, legitimisation of violence, and prolonged retention of power. russia's war against Ukraine is a demonstrative example of modern cognitive confrontation, in which the targeting of consciousness is considered by the aggressor as an equivalent or even priority alternative to conventional military action. In this context, the struggle for consciousness has become a central element of the strategy to undermine Ukrainian statehood. At the same time, it has been established that Ukraine has achieved significant progress in strengthening the consciousness of its own nation, which has become one of the key factors in its resilience, capacity for prolonged resistance, and international support. The formation of a clear national identity, the reassessment of historical memory, and the consolidation of society around the values of freedom and dignity have significantly reduced the effectiveness of adversarial cognitive influence.

It has been proven that the cessation of active hostilities will not signify the end of the war; on the contrary, it will open a new phase of the struggle for consciousness both within Ukraine and in the international and adversary informational-cognitive domain. The outcome of this phase will have long-term consequences for national and global security.

Today, modern warfare has entered a phase in which the decisive factor is not the destruction of enemy forces, but the disruption of their will, motivation, and ability to make rational decisions, while simultaneously maintaining the resilience of one's own society. The cognitive war against Ukraine is being conducted systematically and without restraint by the Russian Federation. At the same time, the Armed Forces of Ukraine lack a single body that would plan, synchronise, and assess cognitive influence in combination with combat, cyber, and electromagnetic operations. росія's war against Ukraine has taken on a systemic character, in which the decisive role is played not only by the physical neutralisation of enemy forces and assets but also by targeted influence on their consciousness, motivation, decision-making capacity, and societal support for the war. The adversary consistently employs informational, psychological, cyber, and organisational tools within a unified cognitive framework, allowing them to achieve indirect strategic effects without large-scale use of military force.

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Currently, the Armed Forces of Ukraine possess separate capabilities in informational-psychological influence, strategic communications, and cyber- and electromagnetic warfare. However, there is no single body responsible for centralised planning, synchronisation, and assessment of cognitive effects in combination with combat operations and inter-agency measures. This reduces the overall effectiveness of existing resources and creates a strategic asymmetry in favour of the adversary.

International experience (USA, United Kingdom, PRC, russia) demonstrates that leading states integrate cognitive, informational, cyber, and electromagnetic influence within specialised commands or combined strategic-level structures. In these conditions, initiating a similar process within the Armed Forces of Ukraine is advisable, taking into account national legislation, international law, and NATO standards.

Therefore, the existing strategic gap in this domain can be initially closed by a decision of the Commander-in-Chief through the phased establishment of the Cognitive Influence Forces of the Armed Forces of Ukraine. The foundational decision (starting mechanism) for addressing the identified issues is the creation, within the General Staff of the Armed Forces of Ukraine, of a: Cognitive Operations Centre of the Armed Forces of Ukraine (COC AFU) (a temporary, joint-service, inter-agency structure with potential for transformation). This military management body is intended not as a new headquarters but as an operational-analytical centre, subordinated to the Commander-in-Chief of the Armed Forces of Ukraine via the Chief of the General Staff of the Armed Forces of Ukraine.

russia’s war against Ukraine has a complex character and is conducted simultaneously across physical, informational, cyber, and cognitive dimensions. Combat practice demonstrates that the adversary deliberately influences not only Ukrainian forces and population but also its own audience, shaping a distorted perception of reality, support for aggression, and readiness for prolonged war. Therefore, the struggle for consciousness and decision-making processes become among the key factors of strategic state resilience.

The Armed Forces of Ukraine possess certain elements of informational-psychological influence, strategic communications, cyber- and electromagnetic warfare, as well as scientific capabilities within the military science system. However, a unified system is absent, one that would combine practical planning and execution of cognitive operations with targeted scientific support, effect-assessment methodology, and forecasting of cognitive influence outcomes at various levels of command.

International experience demonstrates that leading states combine operational structures for cognitive and informational influence with robust research centres, which provide evidence-based, long-term, and adaptive support for such operations. In these conditions, it is essential to simultaneously launch both operational and scientific components in establishing the cognitive influence system within the Armed Forces of Ukraine.

The objective is to create a controlled, scientifically substantiated, and manageable cognitive influence system within the Armed Forces of Ukraine, capable of:

systematically influencing the consciousness, motivation, and behaviour of enemy military personnel and civilian populations;

enhancing the cognitive resilience of the personnel of the Armed Forces of Ukraine and the Ukrainian society;

providing the Ukrainian Armed Forces command with evidence-based recommendations for managing behaviour, morale, and decision-making processes;

laying the foundation for rapid scaling of this domain to the level of the Ministry of Defence of Ukraine and the state as a whole.

To achieve this objective, it is necessary to implement two interrelated directions:

Operational – through the establishment of the Cognitive Operations Centre within the General Staff of the Armed Forces of Ukraine;

Research – through the formation of a specialised research unit within the Central Research Institute of the Armed Forces of Ukraine.

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

The implementation of these measures constitutes a direct instrument of strategic influence, aimed at enhancing combat effectiveness without additional losses, as well as controlling the informational-cognitive domain in compliance with NATO practices concerning the establishment of strategic-level legacy.

The simultaneous creation of operational (Cognitive Operations Centre of the Armed Forces of Ukraine) and scientific-research (specialised department within the Central Research Institute of the Armed Forces of Ukraine) components will establish a systemic, scientifically substantiated foundation for the formation of the Cognitive Influence Forces. This approach will ensure effective use of cognitive tools in combat conditions, reduce risks, provide long-term resilience of the system, and create conditions for rapid scaling to the Ministry of Defence and national level.

Initiating the formation of the cognitive influence system in the Armed Forces of Ukraine through the creation of the Cognitive Operations Centre is justified, timely, and necessary. Implementation of this proposal will increase the effectiveness of the Ukrainian Armed Forces, strengthen indirect influence on the adversary, maintain the resilience of own forces and society, and create the groundwork for the further development of modern forms of armed struggle.

Promising directions for further scientific research in this area include:

development of a national model for the protection of consciousness as an integral part of Ukraine's national security system;

study of cognitive operations in the post-conflict period and their impact on the stability of peace agreements;

analysis of the role of education, culture, and historical policy in shaping a resilient national consciousness;

examination of mechanisms for influencing the consciousness of societies in authoritarian and totalitarian states under conditions of informational isolation;

creation of methodologies for assessing societal cognitive resilience and detecting early signs of its compromise;

comparative analysis of the struggle for consciousness in contemporary conflicts involving aggressor states and democratic societies.

The practical significance of the article's materials lies in the fact that the main research results may be necessary or useful for:

state authorities and the security and defence sector in formulating strategies for national, informational, and cognitive security;

military and political leadership to understand the modern nature of warfare and post-conflict threats;

scholars and analytical centres in the fields of military science, the philosophy of war, international relations, and security studies;

educational institutions for preparing specialists in strategic communications, information security, and public administration;

civil society and media as an analytical basis for countering disinformation and manipulation.

Overall, the article can serve as a scientific-analytical foundation for developing long-term policies to strengthen the national consciousness of Ukraine as one of the key factors of its security, resilience, and future development in the context of the transforming global order.

Conflict of Interest

One of the article authors is the Head of editorial team. For avoiding the conflict of interests the editorial process was made by the Deputy of the Head of editorial team Oleksandr Deinega.

References

1. Maksymenko, S., & Derkach, L. (2024). Modern cognitive-information warfare: The role of manipulation of Ukrainians' consciousness in personality transformation. *Problems of Modern Psychology, 64*, 157–181. https://doi.org/10.32626/2227-6246.2024-64.157-18.
1. Taranenko, A. (2024). Cognitive security as a dimension of the russian-Ukrainian war. *Political*

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Bulletin, 92, 371–382. https://doi.org/10.17721/2415-881x.2024.92.371-382.
2. Vorobets, N. (2024). Russia's information war against Ukraine: Dynamics of influence on public consciousness and challenges for national formation. *Bulletin of Precarpathian University. Series: Political Science*. https://doi.org/10.32782/2312-1815/2024-1-3.
3. Kobets, T. (2024). Cognitive security in the conditions of hybrid warfare. *Bulletin of Precarpathian University. Series: Political Science, 17* (9). https://doi.org/10.32782/2312-1815/2024-17-9.
4. Strelbytskyi, M., & Hryn, M. (2023). *russia's cognitive war against Ukraine*. Scientific Works of MAUP. Legal Sciences. https://doi.org/10.32689/2522-4603.2023.1.7.
5. Horbulin, V. P. (2022). *How to defeat russia in the war of the future.* Bright Books.
6. Portnikov, V. (2022). *Psychological warfare: russia, Ukraine, and the war in consciousness.* Krytyka.
7. *Information wars and national security of Ukraine.* (2021). Ukrainian Association of Strategic Communications. https://www.ukrstrategic.info/.
8. *White Paper. Strategic communications and information security*. (2021). Ministry of Defence of Ukraine. https://www.mil.gov.ua/.
9. *russia's information war: Strategies and tactics*. (2017). russian Institute for Strategic Studies.
10. Giles, K. (2023). *russian Cyber and Information Warfare in Practice: Lessons from the War on Ukraine.* Chatham House.
11. Slusher, M. (2025). *Lessons from the Ukraine Conflict: Modern Warfare in the Age of Autonomy, Information, and Resilience.* CSIS Report.
12. *Decoding manipulative narratives in cognitive warfare: a case study of the russia-Ukraine conflict. (*2025). Frontiers in Artificial Intelligence. https://doi.org/10.3389/frai.2025.1566022.
13. Gerard, P., Volkova, S., Penafiel, L., Lerman, K., & Weninger, T. (2024). *Modeling Information Narrative Detection and Evolution on Telegram during the russia-Ukraine War.*
14. Gouliev, Z. (2025). *Propaganda and Information Dissemination in the russian-Ukrainian War: Natural Language Processing of Twitter Narratives.*
15. Khan, S. A., Furuly, J. G., & Vold, H. B., et al. (2023). *Online Multimedia Verification with Computational Tools and OSINT: russia-Ukraine Conflict Case Studies*.
16. Lasswell, H. D. (1927). *Propaganda Technique in the World War*. A. A. Knopf.
17. Bernays, E. L. (1928). *Propaganda*. Horace Liveright.
18. Bernays, E. L. (1923). *Crystallizing Public Opinion*. Boni & Liveright.
19. Clausewitz, C. von. (1976). *On War.* Princeton University Press.
20. Sun Tzu. (2008). *The Art of War.* Oxford University Press.
21. Nye, J. S. (2004). *Soft Power: The Means to Success in World Politics.* Public Affairs.
22. Rid, T. (2020). *Active Measures: The Secret History of Disinformation and Political Warfare.* Farrar, Straus & Giroux.
23. Castells, M. (2009). *Communication Power.* Oxford University Press.
24. Ellul, J. (1973). *Propaganda: The Formation of Men's Attitudes.* Vintage Books.
25. Huntington, S. P. (1996). *The Clash of Civilizations.* Simon & Schuster.
26. Freedman, L. (2017). *The Future of War: A History.* PublicAffairs.
27. Surkov, V. (2020). *Technologies of consciousness manipulation in politics: The role of information wars in hybrid conflicts.* moscow University.
28. Gerasimov, V. V. (2013). The value of science in prediction. *Military-Industrial Courier, 8* (476).
29. Syrskyi, O. S., Semenenko, O. M., Lebedenko, A. V., & Tristan, A. V. (2025). The struggle for consciousness as a primary factor of national resilience in the global security system: Historical analysis and assessment of the current state during war. *Collection of Scientific Works of the Central Research Institute of the Armed Forces of Ukraine, 3* (114), 6–20.
30. Ellul, J. (1965). *Propaganda: The Formation of Men's Attitudes*. Vintage Books.
31. Kershaw, I. (2000). *The Nazi Dictatorship: Problems and Perspectives of Interpretation*. Arnold.

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

32. Fitzpatrick, S. (1999). *Everyday Stalinism: Ordinary Life in Extraordinary Times: Soviet Russia in the 1930s.* Oxford University Press.
33. Chang, J., & Halliday, J. (2005). *Mao: The Unknown Story*. Jonathan Cape.
34. Foucault, M. (1980). *Power/Knowledge: Selected Interviews and Other Writings 1972–1977.* Pantheon Books.

Свідомість як поле бою – еволюція когнітивної війни у системі глобальної безпеки (когнітивні операції – інструмент геополітичного домінування): перспективи організації системи когнітивної боротьби в Україні

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

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

Олександр Кінь
кандидат технічних наук, доцент
Дипломатична академія України імені Геннадія Удовенка
при Міністерстві закордонних справ
01001, вул. Велика Житомирська, 2, Київ, Україна
e-mail: cubalibre1972@ukr.net
ORCID: 0009-0001-2196-7515

Віталій Нащубський
командир 92 окремої штурмової бригади
імені кошового отамана Івана Сірка
63505, вул. Горішного, 142, Чугуїв, Харківська обл., Україна
e-mail: xcii.mgm@gmail.com
ORCID: 0009-0006-1362-6549

“Le buone leggi nascono dalle buone armi.” –
“Добрі закони народжуються з доброї зброї.”
Нікколо ді Бернардо де’ Макіавеллі (Niccolò Machiavelli)

“Найвище мистецтво війни – не в битві й перемозі в усіх сутичках, а в тому, щоб підірвати опір ворога без бою.”
Сунь Дзи “Мистецтво війни”

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

“Світовий порядок існує настільки, наскільки люди в нього вірять.”
“Стримування працює через уявлення, а не через застосування сили.”
Генрі Кіссінджер

Анотація. Сучасний етап розвитку міжнародної безпеки характеризується глибокою трансформацією форм і способів протиборства, у межах яких дедалі більшого значення набувають нематеріальні чинники впливу. За цих умов свідомість людини та суспільства загалом стає ключовим об’єктом цілеспрямованих воєнно-політичних дій, а боротьба за контроль над мисленням, уявленнями та цінностями виходить за межі традиційних уявлень про війну. Це зумовлює нагальну потребу наукового осмислення еволюції когнітивної війни та її місця у системі глобальної безпеки з урахуванням сучасних викликів і реалій воєнно-політичної обстановки. Отже, головною метою статті є комплексне осмислення еволюції когнітивної війни як самостійного виміру сучасного протиборства у системі глобальної безпеки, розкриття ролі когнітивних операцій як інструменту геополітичного домінування, а також обґрунтування необхідності формування цілісного стратегічного бачення організації когнітивної боротьби на державному рівні з урахуванням досвіду російсько-української війни та зростаючих глобальних загроз. Основними результатами статті є те, що в ній: проведено аналіз наукових, військово-теоретичних і політичних джерел усвідомлення вирішальної ролі свідомості у війні; сформовані основні терміни та поняття у сучасному розумінні когнітивної війни; запропоновано підхід до формування загального показника ефективності когнітивного впливу (інтегральний показник володіння свідомістю) та визначено шкалу його оцінювання; визначено погляди щодо створення у складі Збройних Сил України спеціальних Сил когнітивного впливу (Cognitive Influence Forces). Матеріали статті можуть бути корисними органам державної влади та сектору безпеки і оборони, військовому та політичному керівництву, науковцям і аналітичним центрам, що працюють у галузях воєнної науки, філософії війни, міжнародних відносин, безпекових студій, освіти, для підготовки фахівців у сфері стратегічних комунікацій, інформаційної безпеки та державного управління, громадянського суспільства та медіа.

Ключові слова: боротьба за свідомість, воєнно-політична обстановка, воєнні конфлікти, глобалізм, гібридна війна, інформаційна війна, інформаційна безпека, когнітивні операції, когнітивний вплив, міжнародна політика, міжнародні коаліції, обороноздатність, російсько-українська війна, національна безпека, критерії оборонної достатності, технологічні переваги, свідомість, свідомість нації, стійкість держави.

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Received: *December 6, 2025* | **Revisions Requested:** - | **Revision Received:** -
Accepted: *January 25, 2026* | **Published Online:** *April 10, 2026*

Licensed (C) by Creative Commons Attribution International License 4.0 (CC BY-NC-SA)

DOI: 10.62524/msj.2026.4.1.2

A Methodical Approach to Forming the Outline and Database of the Military and Strategic Analysis of Destructive Geopolitical and Conflict-Generating Factors Influencing the Defence and Industrial Complex of Ukraine

Viktor Muzhenko
Doctor of Military Sciences
Leading Research Fellow
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl Avenue, 28 B, Kyiv, Ukraine
e-mail: vic.muzh@gmail.com
ORCID: 0000-0002-5023-6463

Volodymyr Bohdanovych
Doctor of Technical 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: bogdnr11@gmail.com
ORCID: 0000-0003-0481-9454

Oleh Huliak
Candidate of Legal Sciences
Associate Professor of the Department of Humanities and Socio-Economic Sciences
Military Academy (Odesa)
65009, Fontanska Doroha St., 10, Odesa, Odesa Oblast, Ukraine
e-mail: oleggulyak24@gmail.com
ORCID: 0000-0002-4588-5979

Andrii Vysidalko
Analyst
National University of Ukraine on Physical Education and Sport
e-mail: andrewval220376@gmail.com
ORCID: 0009-0008-2469-1834

Abstract. The relevance of this article consists in the fact that it develops a methodological approach to constructing the outline and database of military-strategic analysis of the main destructive geopolitical and conflict-generating factors and processes that decisively influence the development of the defence-industrial complex of Ukraine. The article addresses the general problem of developing a methodological framework and information technologies for substantiating strategic tasks for national security and defence sector entities during strategic analysis of the geopolitical and military-political situation through automation of information-analytical processes, in particular the formation

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

of an analytical outline and development of a database for organising and managing the expert modelling function within an automated decision-support system. An important element of the methodological approach is the application of the Saaty comparative scale, which makes it possible to convert complex qualitative expert judgements into a formalised quantitative form, ensuring objectivity, consistency and the possibility of updating assessments in a dynamic environment (database). The use of the specialised computer technology M7 is proposed for conducting expert-analytical procedures and accumulating knowledge in the emerging strategic monitoring database. This approach makes it possible both to conduct comparative analysis of threats from unfriendly states and to develop well-grounded strategic recommendations for adjusting foreign and defence policy, in particular optimisation of partnerships and conclusion of strategic agreements. Thus, the presented approach provides an integral, adaptive and hierarchical assessment of external threats, which makes it an effective instrument for long-term military-strategic analysis and strategic planning of the state defence-industrial complex.

Keywords: security environment; military security; state military potential; geopolitical factors; conflict-generating factors; threats of a military nature; methodological approach; national security; strategic analysis.

Introduction

The National Security Strategy of Ukraine stipulates [1] that the automation of procedures for assessing the levels of internal and external threats and dangers, forecasting the geopolitical and military and political situation (MPS), the state of the security and defence sector of Ukraine (SDSU), the state's capabilities to introduce mechanisms for safeguarding national interests (NI), assessing risks arising from the implementation of defined "neutralisation" measures, and selecting from a set of possible response scenarios (behavioural options) of national security and defence sector entities the most rational one – confirmed by expert judgement in quantitative terms – constitute key tasks facing the national security provision system (NSPS), which may be addressed more effectively through the introduction of an automated system of expert-analytical modelling. In view of the above, a methodological approach to constructing the analytical outline and the database for military-strategic analysis of the principal destructive geopolitical and conflict-generating factors and processes that decisively influence the development of the defence and industrial complex (DIC) of Ukraine is proposed for consideration, based on the modelling of expert-analytical scenarios for neutralising threats posed by unfriendly states.

The article is devoted to the general problem of developing a methodological framework and information technologies for substantiating strategic tasks for national security provision system entities in the course of strategic analysis of the geopolitical and military-political situation through the automation of information-analytical processes, in particular the formation of an analytical outline and the development of a database for organising and managing the expert modelling function within an automated decision-support system (ADSS)

Traditional approaches to the analysis of threats of a military nature increasingly reveal their limitations, as they are unable to encompass the full range of non-linear, stochastic and rapidly evolving factors shaping the contemporary security environment [2, 3]. Geopolitical factors determine the place of a state within the global and regional security architecture, conditioning the spectrum of risks associated with its spatial location, resource base, military and political alliances, or configuration of international relations. At the same time, in the twenty-first century these structural parameters are becoming ever more closely intertwined with conflict-generating phenomena – processes of degradation of the security environment, regional and global crises, a growing level of aggressiveness among state and non-state actors, as well as unstable socio-political processes – which determines the relevance of this study.

The information-analytical report [4] of the non-profit analytical organisation "Foreign Affairs

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Institute" is devoted to the analysis of the geopolitics of the russian invasion of Ukraine. The report examines the interests and strategic objectives of russia, the geopolitical impact of the war, and also provides a detailed analysis of the military and politico-strategic lessons of the conflict. The document considers the russian invasion of 2022 as a geopolitical phenomenon that goes beyond the limits of a local conflict and shapes new trends in the global security environment, the change in the strategic balance of power and the role of key international actors, which makes the report relevant for research in the field of strategic analysis of external threats to the military security of the state. However, in the report the priorities of analysis are given to experts.

The monograph [5] analyses theoretical and practical approaches to the creation of a new format of strategic leadership of the security and defence sector of Ukraine and military command and control of the defence forces under contemporary conditions. The directions for determining rational models of functioning are considered, and a vision regarding the introduction of a more effective strategy for countering the aggressor under the conditions of hybrid warfare is presented. The key problems of strategic leadership and military command and control are highlighted, as well as issues of defence forces capability development for joint actions in the processes of reintegration of the temporarily occupied territories of Ukraine. A number of draft legislative and subordinate regulatory legal acts are presented. However, the monograph does not consider the expert-analytical toolkit for conducting strategic analysis of the geopolitical and military power of individual countries, which limits the practical significance of the theoretical part of the research.

The article [6] reveals contemporary forms of escalation of threats of a military nature in the context of growing global instability. It is shown that instability of the international environment increases the probability of regional conflicts. The study emphasises the necessity of adapting the strategic methods of security assessment to the new military-political reality, but the presented methodological apparatus requires increased timeliness and accuracy of calculations.

Such a state of affairs somewhat reduces the possibility of substantiating the strategic tasks for the national security provision system entities during the strategic analysis of the geopolitical and military-political situation that would meet the requirements of the present day.

Methodological Framework

As a possible solution to the identified problem, the development of a methodological approach to constructing the analytical outline and the database for the military-strategic analysis of the main destructive geopolitical and conflict-generating factors and processes that decisively influence the development of the defence-industrial complex of Ukraine is proposed.

The strategic documents of Ukraine on issues of national (military) security and the development of the defence-industrial complex define the key tasks [7, 8]:

the automation of the procedures for assessing the internal and external threats;

the forecasting of the military-political situation, the state of the security and defence sector of Ukraine, the capabilities of the state to introduce the mechanisms for safeguarding the national interests, and the risks arising from the implementation of the defined "neutralisation" measure;

the selection, from various possible response scenarios (behavioural options) of the national security provision system entities, of the most rational one – confirmed by expert judgement in quantitative terms;

the implementation of the automated system of expert-analytical modelling [9, 10].

In view of the above, it is proposed to consider a methodical approach to forming the analytical outline of the automated expert and analytical system intended for modelling the expert and analytical scenarios for limiting the levels and neutralising the threats to the national (military) security of the state.

Results and Discussions

At present, the methodological apparatus for the formation of the analytical outline of the automated decision-making support system (ADMSS) in Ukraine is based only on the experience and

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

knowledge of the developers. In other words, the methodological apparatus for the formation of the analytical outline of the ADMSS lies in the creative domain, reflecting both the system functions and the structure, as well as the principles and algorithms of functioning, and represents the result of the synthesis of the decision-making algorithms against the background of the capabilities of the information-processing means [10]. Therefore, from the standpoint of the decision-making theory, the approach to the formation of the analytical outline of the ADMSS should be considered as the possibility of selecting such an option under which the maximum efficiency of the functioning of the automated system would be achieved [11].

Taking into account the research direction initiated in [9] and relying, from the system perspective, on the functional-structural approach, it is proposed to classify the functions of the ADMSS for the use within the national security provision system (NSPS). Thus, in order to accomplish the main tasks facing the decision-maker (DM) in the NSPS, the ADMSS should ensure:

modelling the information-analytical processes. Modelling, within the proposed coordinate system "state" – "capability" – "risk" [9, 10], or within other existing or new decision-making models, of the real information processes for the reproduction of events in the NSPS, the creation of the forecast models of the course of the information-analytical processes and the subsystems for the *synthesis of the optimal decisions* based on the results of the functioning of the information-monitoring system of national security (IMS NS) [12] – on the previous purposeful observations;

modelling the criteria. The development of the description of the models and the determination of the rules for the automated integration of their attributes not only within the framework of one multi-level hierarchical model, but also in different scenarios. The implementation, for the integration of the attributes, of a set of specialised operations that would characterise different decision options and remove the cognitive constraints for the decision-maker;

management of the information (predominantly descriptive), information-analytical (specially prepared for analysis) and analytical (the models and the results of their functioning) flows for the storage, use and additional processing of the data in the course of working with the ADMSS.

Within the framework of the proposed coordinate system "state" – "capability" – "risk" [10], the task of the automated substantiation of the strategic tasks for the NSPS entities was addressed by distinguishing it as a separate functional block, as a subsystem of the decision-support system, which determined the formation of a classified set of the special functions of the ADMSS presented for consideration in Table 1.

For implementating the modelling function within the information-analytical processes and the criteria, it is also proposed to define the general scheme for organising the above-mentioned function and to present it in a formalised form in the ADMSS.

In order to transfer the formal aspect of the scheme for implementing the modelling function into the practical domain, it is proposed to present it in the form of a general hierarchical scheme for implementing the modelling function of the ADMSS. The hierarchical tree of representing the organisation of the modelling function on the basis of the expert decision (ED), the expert scenario (ES) and the micro-scenario (MS) is shown in Fig. 1.

In order to transfer the formal aspect of the scheme for implementing the modelling function into the practical domain, it is proposed to present it in the form of a general hierarchical scheme for implementing the modelling function of the ADMSS. The hierarchical tree representing the organisation of the modelling function on the basis of the expert decision (ED), the expert scenario (ES) and the micro-scenario (MS) is shown in Fig. 1.

Thus, structurally, the expert decision will consist of a set of the target expert scenarios which, in turn, will reflect different variants of the models – the expert micro-scenarios of modelling, where the total number of the EDs – K, the total number of the ESs – N, and the total number of the MSs – P will fully depend on the creative potential of the expert analyst.

That is, if, from the standpoint of the expert analyst, a single micro-scenario is sufficient for forming a scientifically substantiated decision, the assessment or forecasting of the relevant information processes / criteria is suspended; otherwise, the modelling may continue both within the

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

framework of the same ES – through the creation of a new micro-scenario, and within the limits of a single ED – through the creation of a new ES and, accordingly, through the opening / creation of a new ED. At the same time, it is assumed that the expert should constantly be provided with a hierarchical representation of those EDs, ESs and MSs that constitute an *intellectual expert value*. Thus, in the author's conception, the micro-scenarios of both the information-analytical processes and the modelling of the criteria should, in this way, provide the expert analyst with the possibility of a scientifically substantiated search precisely for a set of satisfactory decisions in order to adopt the most correct (rational) one [9–10].

Table 1. Classified set of the special functions of the ADMSS

Classifier	List of the ADMSS functions
Automated	1. The function of creating the databases and storing the NSPS indicators: the spheres, the threats to the implementation of the national interests, the "neutralisation" measures, the strategic tasks of the national security entities, the expected "negative" consequences. 2. The function of the hierarchical representation of the information-analytical data of the relevant database for the use (assessment / forecasting) and additional processing in the course of working with the ADMSS. 3. The function of determining the unified scale for the assessment and forecasting. 4. The function of calculating the integral threat level, the coefficient of the escalation of the threat level, the integral level of the state capabilities, the coefficient of the de-escalation of the threat level, the integral risk level, and the integral risk coefficient. 5. The function of displaying the modelling results. 6. The function of notifying the expert about the course of the ADMSS functioning – the compliance of the expert manipulations and the absence of errors in the calculations.
Semi-automated	1. The function of forming the information-analytical data subject to storage in the relevant database: the spheres, the threats to the implementation of the national interests, the "neutralisation" measures, the strategic tasks of the national security entities, and the expected "negative" consequences. 2. The function of synthesising the hierarchy of the information-analytical data – the expert selection of the data from the database and their input into the scenario for further assessment / forecasting. 3. The function of distributing the information-analytical data by priorities – the expert manipulation of the data in relation to their assessment or forecasting. 4. The function of manipulating the scenarios and the selective inter-scenario input (output) data: creating, copying, deleting, editing, blocking / unblocking (access in the viewing / editing mode).

Taking into account the proposed sequence of modelling (Fig. 1), there arises a need to organise and manage both the expert decision, expert scenarios, and microscenarios. To address this issue, it is proposed to use the relational data model as the most developed mathematical apparatus to date for the structured storage and processing of data in the ADMSS. The application of the relational data model [13] should formalise the processes of generating optimal algorithms, from a technological point of view, not only for the automated substantiation of strategic tasks, but in general for the ADMSS. At the same time, the data stored in software-accessible variables in the course of modelling may be tracked during report generation and stored in special databases of current information resources, for example: the expert decision database (EDDB), the expert scenario database (ESDB), and the microscenario database (MSDB), which should be used to the maximum extent, that is repeatedly, in order to ensure the multifunctionality of the ADMSS when modelling processes/criteria. In order to ensure the organisation and management of expert modelling processes defined above, a general data structure for organising and managing the expert modelling function of the ADMSS is proposed for consideration (Fig. 2).

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

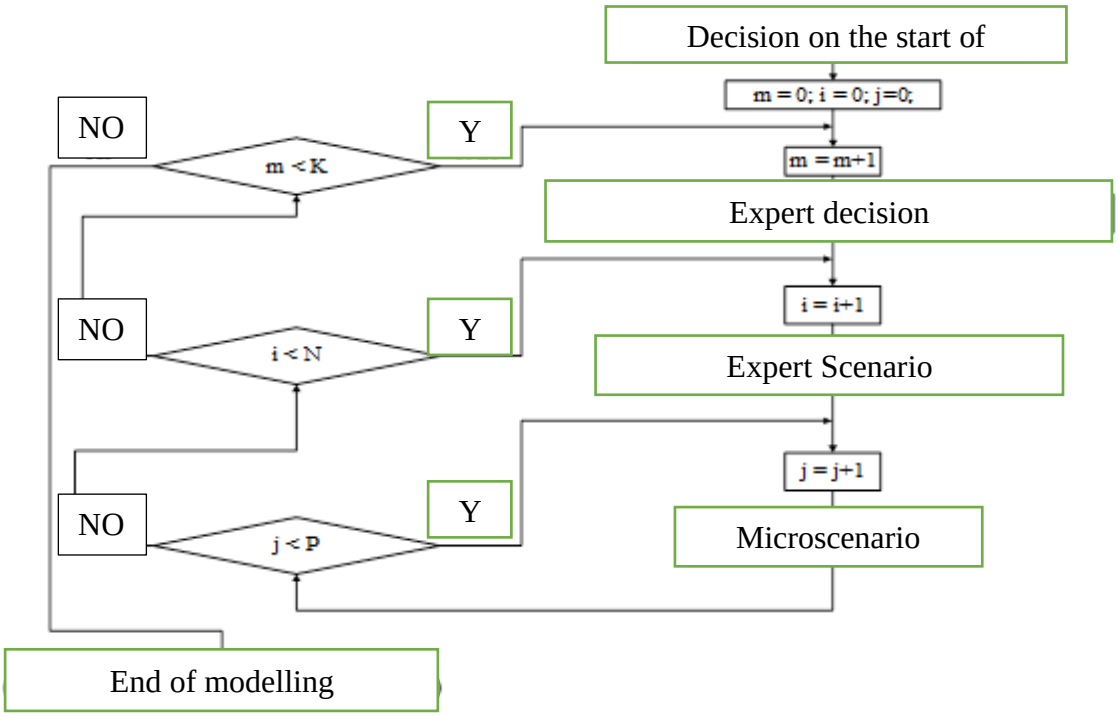


Figure 1. General scheme for organising the modelling function of the ADMSS

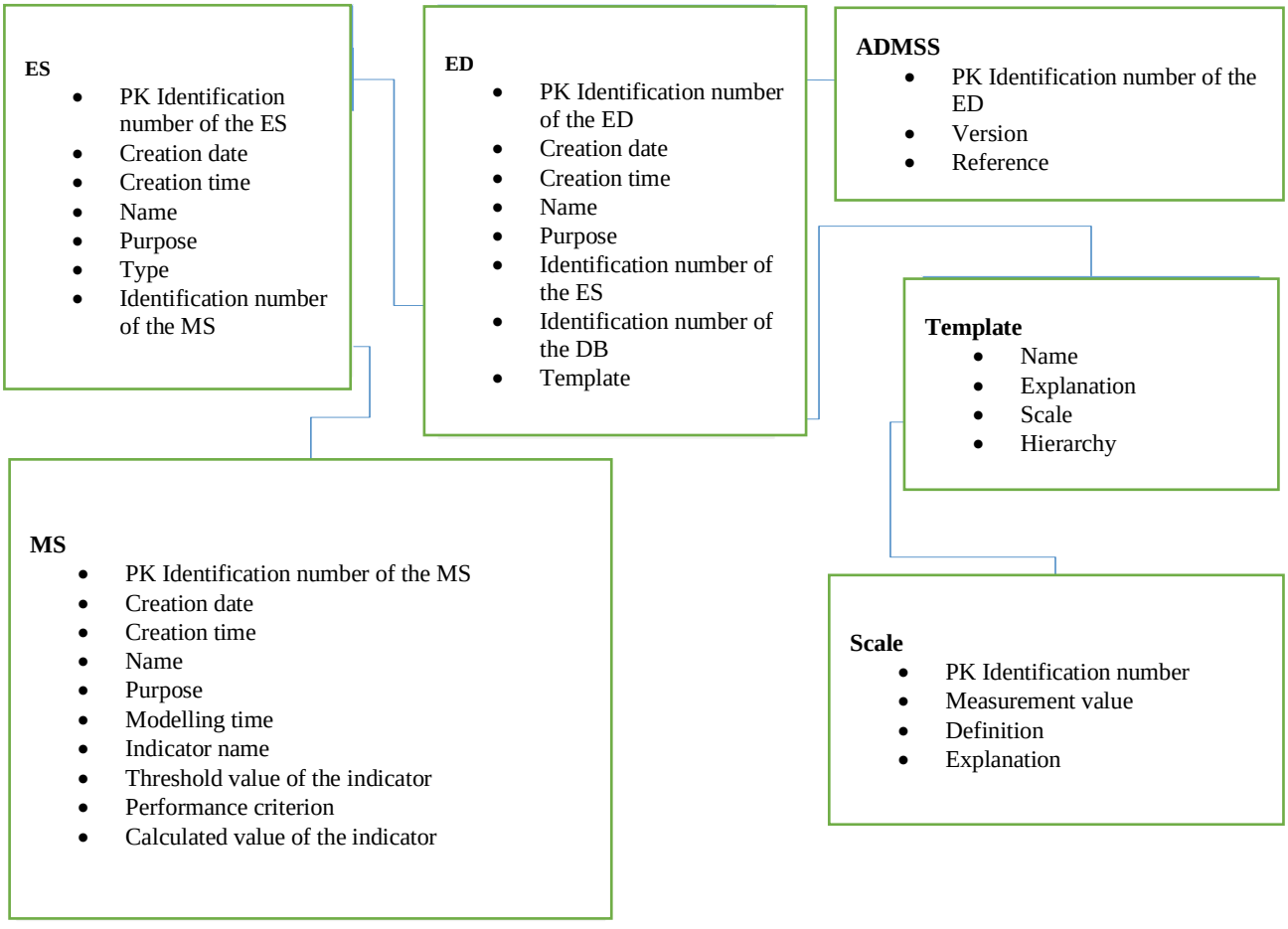


Figure 2. General data structure for organising and managing the expert modelling function of the ADMSS

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

It should be noted that the data objects “ADMSS”, “Template”, and “Scale” contain purely static data – data that remain unchanged during the modelling process and that should be defined at the stage of developing the software tools of the automated expert-analytical system. At the same time, the data objects “ED”, “ES”, and “MS” are presented as dynamic, hierarchically dependent data objects intended to ensure the organisation of the modelling function of processes/criteria and a classified set of special functions of the ADMSS presented in Table 1.

The data object “Hierarchy” (Fig. 3), which is part of the data object “Template”, by its structure is intended to provide and display an architecturally invariant three-level hierarchical scheme for input, storage, manipulation, and representation of the input information-analytical data array of the ADMSS.

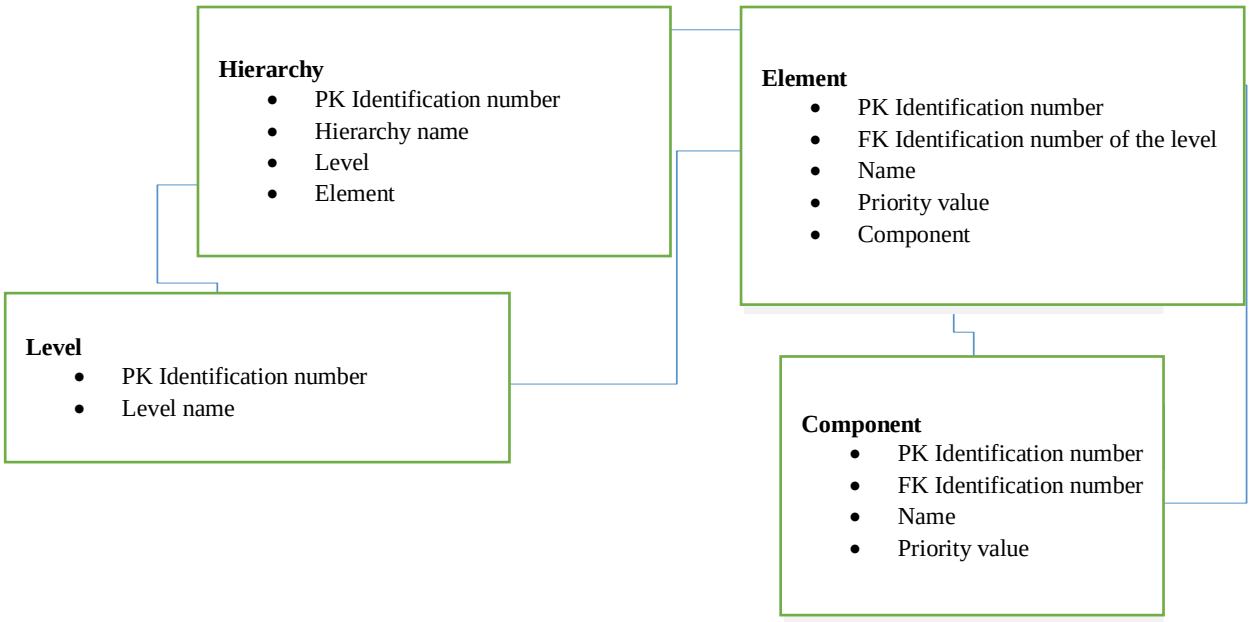


Figure 3. Structure of the hierarchy data description

A three-level hierarchical scheme based on spheres and indicators, for example, is presented in Fig. 4.

It should be noted that with such an approach to organising and managing the expert modelling function of the automated system, the expert-analyst is given the opportunity to work not only with spheres and indicators, but also with any other classification features of the scenario – objects, determinants, indicators, factors, etc.

The methodological apparatus for forming the outline of the ADMSS, as noted above, lies in the creative domain and reflects, as a rule, system functions, structure, principles, and functioning algorithms, and represents the result of the synthesis of decision-making algorithms against the background of the capabilities of information processing means [13].

Therefore, from the standpoint of decision-making theory [2], the approach to forming the outline of the ADMSS should be considered as the possibility of selecting such an option under which the maximum efficiency of the functioning of the automated system would be achieved. In this case, according to the methodology of automated solving of decision-making tasks in the NSPS [3], it is advisable to create the ADMSS on the basis of optimisation algorithms that make it possible to calculate optimal trajectories for the implementation of a certain management process while ensuring security support for the implementation of NI. In this regard, a general structural scheme for the representation of the expert-analytical system for the automated substantiation of strategic tasks for the subjects of the NSPS is proposed for consideration (Fig. 5).

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

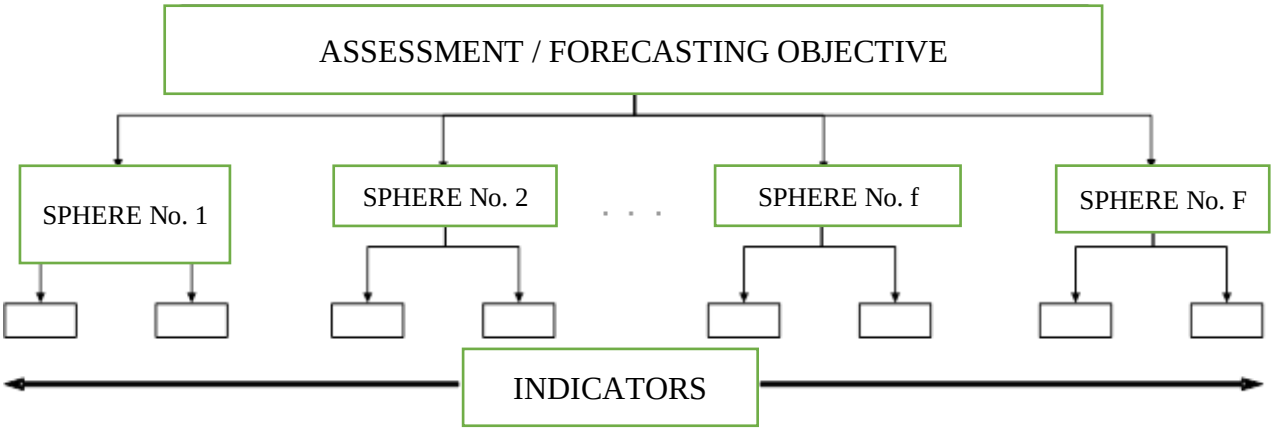


Figure 4. Three-level hierarchical scheme for the representation of spheres and indicators

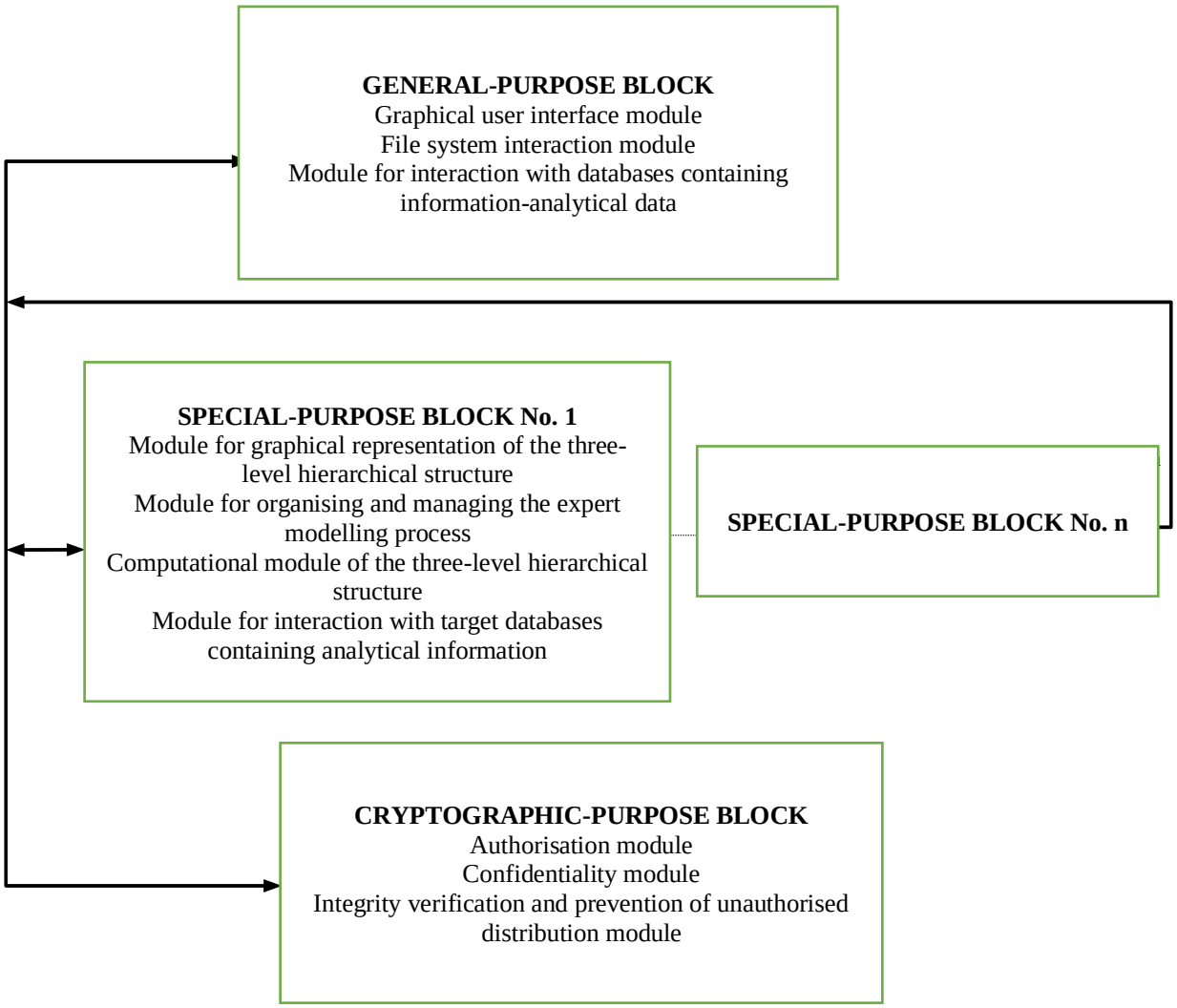


Figure 5. General structural scheme for the representation of the expert-analytical system for the automated substantiation of strategic tasks for the subjects of the NSPS

The structural scheme of the analytical tool for decision support in the NSPS conventionally consists of three main parts and provides for a modular-block structure:

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

the general-purpose block – the expert-analyst subsystem intended to ensure communication between the users of the ADMSS and the internal elements of the system. It provides access to models and data;

the special-purpose blocks. In our case, this is an algorithmically oriented functional block capable of ensuring the implementation of the algorithm for the automated substantiation of strategic tasks for the subjects of the NSPS. It provides access to the functions for implementing optimisation algorithms, information input and output of results, and solving decision-making tasks in accordance with the developed methodology [3]. It makes it possible to carry out efficient unified data exchange between all elements of the system;

the cryptographic-purpose block – the subsystem for organising the protection of the ADMSS, models, and data;

indicators and assessment criteria are also very important, but the issue of data storage and protection must be addressed as one of the first.

The target database (TDB), access to which is provided by the analytical tool, may contain a very large amount of analytical data that may reflect the activities of the NSPS.

The issues of assessing the quality and efficiency of the functioning of similar ADMSSs are sufficiently substantiated and considered in [11]. The most critical aspect of implementing the analytical tool, as well as of any ADMSS, is the organisation of data protection.

Conclusion

Proceeding from the above, a general overview of the concepts on the basis of which it is possible to create a practical tool to ensure the protection of the ADMSS, models, and data is proposed:

1. Authentication – a procedure for establishing the identity of a person who ensures interaction with the ADMSS and the software service of the TDB archive. In order to carry out this procedure, in the opinion of researchers, a user name and password are sufficient. The authentication procedure should ensure mutual confirmation of the parties. That is, the expert-analyst must be confident that his practical developments – modelling scenarios and analytical data – cannot be used without his knowledge.

2. Authorisation. After establishing the authenticity of the requesting party, it is necessary to determine whether it is permitted to perform the action requested. Authorisation is carried out on the basis of an internal role distribution system (the user's right to perform a certain procedure), that is, the expert-analyst, in order to work with the TDB, must have certain rights, for example, to modernise it.

3. Confidentiality. Confidentiality is understood as a mechanism that prevents third parties from reading the information exchanged by the expert-analyst with the TDB.

4. Integrity and protection against copying. This is required in order to guarantee that the ADMSS has not been altered during operation and that the licence conditions are fully complied with.

Confidentiality and data integrity can be ensured by using certificate mechanisms for encryption and signing of the TDB.

Another aspect of ADMSS security is the availability of audit tools. This includes the possibility of creating logs and audit reports on actions related to the security of services. When the audit and logging service is launched, both successful and unsuccessful authentication attempts, as well as information about the expert-analyst and the time of his work, should be recorded in the service log.

Recommendations

The main and special functions proposed in the paper, the sequence of organising expert modelling, and the data structures for organising and managing the expert modelling function fully

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

satisfy the defined structure of the analytical tool, which as a whole includes a sufficient list of functionally distributed modules capable of ensuring the implementation of automated modelling of the processes of forming and distributing strategic tasks among the subjects of the NSPS.

In subsequent publications, it is planned to present an analytical-measurement scheme, the idea of which is revealed in the "linguistic-logical" coordinates "state" – "capability" – "risk" within the planes of "assessment" and "forecasting". Within the framework of this scheme, a conceptual model for automated decision-making on the substantiation of strategic tasks for the subjects of the NSPS will be developed.

Conflict of Interest

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

References

1. Prezydent Ukrainy. (2020). *Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 veresnia 2020 roku "Pro Stratehiiu natsionalnoi bezpeky Ukrainy" (392/2020).* http://www.president.gov.ua
2. Dzharatano Dzhosef, & Raili Hari. (2007). *Ekspertnye sistemy: printsipy razrabotki i programmirovaniia* (4-e izd.). (Per. s angl. K. A. Ptitsyna). OOO "I.D. Vil'iams".
3. Klir Dzh. (1990). *Sistemologiia. Avtomatizatsiia resheniia sistemnykh zadach*. Radio i sviaz.
4. Kotoulas, I. E., & Pusztai, W. (2022). *Geopolitics of the War in Ukraine. [Геополітика війни в Україні] Report № 4.* Foreing Affair Institute (FAINS). Athens. 76. https//euagenda.eu/upload/publications/geopolitics-of-the-war-in-ukraine-final.pdf
5. Sahaniiuk, F. V., Frolov, V. S., & Pavlenko, V. I. ta in. (2018). *Sektor bezpeky i oborony Ukrainy: stratehichne kerivnytstvo ta viiskove upravlinnia: monohr*. (Za red. d.viisk.n., prof. I. S. Rusnaka). TsZ MO ta HSh ZS Ukrainy.
6. Loza, V., Myronenko, V., & Myronenko, P., et al. (2024). The escalation of military threats as a reality of modern geopolitics. *Multidisciplinary Science Journal, 6*. https://doi.org/10.31893/multiscience.2024ss0223
7. Prezydent Ukrainy. (2016). *Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 bereznia 2016 roku "Stratehiia rozvytku oboronno-promyslovoho kompleksu Ukrainy na period do 2028 roku" (92/2016).* http://www.president.gov.ua
8. Prezydent Ukrainy. (2021). *Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 25 bereznia 2021 roku "Pro Stratehiiu voiennoi bezpeky Ukrainy" (121/2021).* http://www.president.gov.ua
9. Bohdanovych, V. Yu., & Vysidal'ko, A. L. (2014). Metodolohichnyi pidkhid do avtomatyzatsii informatsiino-analitychnykh protsesiv bezpekovoho suprovodu realizatsii natsionalnykh interesiv. *Suchasnyi zakhyst informatsii, 3*, 4–10.
10. 10. Bohdanovych, V. Yu., & Vysidal'ko, A. L. (2015). Metodychnyi pidkhid do formuvannia obrysu ta rozbudovy baz danykh avtomatyzovanoi systemy bezpekovoho suprovodu realizatsii natsionalnykh interesiv. NUU: *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony, 1* (22), 14–23.
11. Mesarovich, M., Mako, D., & Takakhara, I. (1973). *Teoriia iierarkhichnykh bahatorivnevykh system.* Vydavnytstvo "Myr".
12. Bohdanovych, V. Yu., & Vysidal'ko, A. L. (2014). Kontseptualna model informatsiino-monitorynhovoi systemy natsionalnoi bezpeky. NAU: *Zakhyst informatsii, 16* (1), 81–88.
13. Sauter, Vicki Lynn. (2010). *Decision support systems for business intelligence*. (2nd edition). (Vicki L. Sauter. John Wiley & Sons).

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Методичний підхід до формування обрису та бази даних воєнно-стратегічного аналізу деструктивних геополітичних і конфліктогенних факторів впливу на оборонно-промисловий комплекс України

Віктор Муженко
доктор військових наук
головний науковий співробітник
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28-Б, Київ, Україна
e-mail: vic.muzh@gmail.com
ORCID: 0000-0002-5023-6463

Володимир Богданович
доктор технічних наук, професор
головний науковий співробітник
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28-Б, Київ, Україна
e-mail: bogdnr11@gmail.com
ORCID: 0000-0003-0481-9454

Олег Гуляк
кандидат юридичних наук
доцент кафедри гуманітарних і соціально-економічних наук
Військова академія (Одеса)
65009, вул.Фонтанська дорога, 10, Одеса, Україна
e-mail: oleggulyak24@gmail.com
ORCID: 0000-0002-4588-5979

Андрій Висідалко
Аналітик
НУФВСУ
e-mail: andrewval220376@gmail.com
ORCID: 0009-0008-2469-1834

Анотація. Актуальність даної статті полягає у тому, що в ней розроблено методичний підхід до побудови обрису та бази даних воєнно-стратегічного аналізу основних деструктивних геополітичних і конфліктогенних факторів і процесів, які визначально впливають на розвиток оборонно-промислового комплексу України. Стаття присвячена загальній проблемі розроблення методологічного апарату та інформаційних технологій обґрунтування стратегічних завдань суб'єктам СЗНБ при проведенні стратегічного аналізу геополітичної та воєнно-політичної обстановки шляхом автоматизації інформаційно-аналітичних процесів, зокрема формування обрису та розбудови бази даних з організації і управління функцією експертного моделювання автоматизованої системи підтримки прийняття рішень. Важливим елементом методичного підходу є застосування порівняльної шкали Сааті, що дозволяє переводити складні якісні судження експертів у формалізовану кількісну форму, забезпечуючи об'єктивність, узгодженість та можливість оновлення оцінок у динамічному середовищі (базі даних). Запропоновано використання Спеціалізованої

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

комп'ютерної технології М7 для проведення експертно-аналітичних процедур та накопичення знань у формованій базі стратегічного моніторингу. Даний підхід дає змогу здійснювати як порівняльний аналіз загроз із боку недружніх держав, так і формувати обґрунтовані стратегічні рекомендації щодо коригування зовнішньої та оборонної політики, зокрема оптимізації партнерства і укладення стратегічних угод. Отже, представлений підхід забезпечує інтегральну, адаптивну та ієрархічну оцінку зовнішніх загроз, що робить його ефективним інструментом довгострокового військово-стратегічного аналізу та стратегічного планування оборонно-промислового комплексу держави.

Ключові слова: безпекове середовище; воєнна безпека; воєнний потенціал держави; геополітичні фактори; конфліктогенні фактори; загрози воєнного характеру; методичний підхід; національна безпека; стратегічний аналіз.

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Received: *October 20, 2025* | **Revisions Requested:** - | **Revision Received:** -
Accepted: *December 25, 2025* | **Published Online:** *April 10, 2026*

Licensed (C) by Creative Commons Attribution International License 4.0 (CC BY-NC-SA)

DOI: 10.62524/msj.2026.4.1.3

Трансформація напрямів розвитку засобів збройної боротьби російської федерації на поточному етапі російсько-української війни: основні тенденції

Володимир Комаров
лауреат Національної премії імені Бориса Патона
доктор військових наук, професор
головний науковий співробітник управління
Науково-дослідний інститут воєнної розвідки
04050, вул. Юрія Іллєнка, 81, Київ, Україна
e-mail: komarvlad@ukr.net
ORCID: 0000-0003-2873-8261

Юрій Сокоринський
доктор юридичних наук, доцент
співробітник Служби безпеки України
Служба безпеки України
01601, вулиця Володимирська, 33, Київ, Україна
e-mail: usokorinskiy@ukr.net
ORCID: 0000-0002-8907-9880

Євген Твердохліб
викладач кафедри військової підготовки
Державного університету "Київський авіаційний університет"
03048, вулиця Медова, 1, Київ, Україна
e-mail: xleb33@ukr.net
ORCID: 0009-0002-6958-1280

Максим Поливода
старший викладач кафедри військової підготовки
Державного університету "Київський авіаційний університет"
03048, вулиця Медова, 1, Київ, Україна
e-mail: maksym.polivoda@npp.kai.edu.ua
ORCID: 0000-0002-4673-008X

Анотація. російська федерація продовжує здійснювати послідовні кроки з адаптації власної економіки та оборонно-промислового комплексу до війни на виснаження, проведення мобілізації економіки росії та її переходу на військові рейки з нарощуванням обсягів військового виробництва для поповнення втрат у бойових діях. Актуальність статті обумовлена потребою аналізу основних напрямів розвитку озброєння та військової техніки збройних сил російської федерації та можливостей оборонно-промислового комплексу росії

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

щодо його розроблення, модернізації та виробництва на поточному етапі російсько-української війни та на найближчу перспективу. Метою статті та її спрямованістю є аналіз напрямів створення озброєння та військової техніки збройних сил російської федерації та визначення основних тенденцій його розвитку на нинішньому етапі війни. Основним результатом статті є аналіз напрямів розвитку засобів збройної боротьби збройних сил росії на поточному етапі російсько-української війни та визначення їхніх основних тенденцій. Практична значущість результатів статті полягає у можливості використання основних тенденцій розвитку засобів збройної боротьби російської федерації на поточному етапі програмно-цільового планування для своєчасного обґрунтування основних напрямів подальшого розвитку озброєння та військової техніки сил оборони України.

Ключові слова: засоби збройної боротьби, оборонно-промисловий комплекс російської федерації, напрями розвитку озброєння, військової та спеціальної техніки, російсько-українська війна, тенденції розвитку.

Вступ (Introduction)

Намагання російської федерації (рф) реалізувати свої воєнно-політичні цілі на п’ятому році широкомасштабної збройної агресії проти України свідчать лише про те, що вона трансформувалася у війну на виснаження [1]. У цих умовах вивчення кількісно-якісного складу номенклатури озброєння та військової техніки (ОВТ), яке застосовується агресором, аналіз напрямів функціонування підприємств його оборонно-промислового комплексу (ОПК) та визначення пріоритетів розвитку на найближчу перспективу дадуть змогу сформувати основні тенденції розвитку засобів збройної боротьби рф на поточному етапі російсько-української війни. Їх урахування забезпечить силам оборони України збереження паритету військової могутності з противником для ефективної протидії йому.

З огляду на зазначене актуальність статті обумовлена потребою в аналізі основних напрямів розвитку ОВТ збройних сил (зс) рф та можливостей ОПК рф щодо його розроблення, модернізації та виробництва на поточному етапі російсько-української війни та на найближчу перспективу.

Огляд літератури (Literature review)

Аналіз досвіду російсько-української війни та його узагальнення свідчить про те, що рф намагається підвищити ефективність застосування власних зс різними шляхами, а саме: збільшуючи їхню чисельність, оснащеність ОВТ, змінюючи керівництво, тактику та методи застосування військ (сил) [2]. Трансформацію напрямів розвитку російського ОПК ретельно досліджують провідні міжнародні та українські аналітичні центри, зокрема RAND Corporation, Стокгольмський інститут дослідження проблем миру (SIPRI), Парламентська асамблея НАТО, Міжнародний інститут стратегічних досліджень (IISS), Національний інститут стратегічних досліджень України (NISS), Фонд Карнегі, Королівський об’єднаний інститут оборонних досліджень (RUSI) та ін. Дослідження зосереджено на трьох основних напрямах: оцінювання структури та корпоративного розвитку російського ОПК, аналіз впливу санкцій та залежності від імпорту, а також дослідження військово-логістичних обмежень, втрат ОВТ та особового складу. Але наведені дані не містять інформації, як саме рф здійснює адаптаційні заходи щодо набуття спроможностей для розроблення нового, виробництва та модернізації існуючого озброєння, військової та спеціальної техніки (ОВСТ) [3–12].

Викладене вище спонукає до вирішення нагального завдання – аналізу напрямів створення ОВТ зс рф та визначення основних тенденцій його розвитку на поточному етапі російсько-української війни.

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Методологічна основа (Methodological Framework)

Методологічну основу статті становить комплексний системний підхід до аналізу трансформаційних процесів у воєнно-технічній сфері агресора, що базується на поєднанні методів воєнно-стратегічного прогнозування та порівняльного аналізу. У ході дослідження використано метод контент-аналізу відкритих звітів міжнародних (RAND, SIPRI, IISS, RUSI) та вітчизняних аналітичних центрів, моніторинг поточної діяльності підприємств ОПК рф, а також емпіричні дані щодо бойового застосування нових та модернізованих зразків ОВТ у ході російсько-української війни. Для верифікації тенденцій застосовано логіко-аналітичне моделювання напрямів розвитку систем озброєння з урахуванням циклів НДДКР, впливу міжнародних санкцій та переходу економіки рф на «військові рейки», що дозволило обґрунтувати пріоритетні вектори розвитку засобів збройної боротьби противника на середньострокову перспективу.

Результати та обговорення (Results and Discussions)

Науково-дослідні організації зс рф системно аналізують досвід російсько-української війни, застосування новітнього та сучасного ОВТ, наданого силам оборони України партнерами, вивчають зразки ОВСТ, захоплених як трофеїв, та виявлені недоліки власного, яке перебуває на озброєнні зс рф. Результати проведеного аналізу використовуються під час трансформації російського ОПК під сучасні потреби, обґрунтування розроблення (копіювання) нового або модернізації існуючого ОВТ та/або закупівлі у інших країнах в обхід накладених санкцій готових зразків чи елементної бази для їх виробництва на підприємствах рф. Незважаючи на санкційні обмеження, в ході розроблення, виготовлення та ремонту ОВТ у рф триває використання електронної елементної бази західного виробництва, отриманої через треті країни.

Для відновлення втрат та забезпечення ведення бойових дій національна економіка рф переведена на воєнний стан, що дало змогу: здійснити посилення спроможностей ОПК для виробництва озброєнь та впровадження нових технологій; проаналізувати та впровадити здобутий у бойових діях досвід застосування власного ОВТ; здійснити жорстку централізацію виробництва через створення промислових кластерів з чітко визначеними спеціалізаціями тощо.

Ознаками трансформації ОПК рф є застосування агресором нових (модернізованих) зразків ОВСТ широкої номенклатури, боєприпасів (засобів повітряного нападу), безпілотних бойових платформ наземного, повітряного та морського базування, що свідчить про розвиток системи озброєнь під потреби, які обумовлені змінами характеру, форм та способів ведення бойових дій [2].

Для підтримання боєздатності та збереження переваги над силами оборони України основні зусилля ОПК рф спрямовані на: організацію нових виробництв для збільшених обсягів виготовлення ракетної зброї, артилерійських боєприпасів, засобів повітряного нападу і засобів РЕБ, бронетехніки тощо; спрощення конструкції ОВСТ для зменшення їхньої вартості; переоснащення російських оборонних підприємств сучасним обладнанням іноземного виробництва; заміну імпортних комплектувальних та сировини на вітчизняні аналоги; імпорт критичних електронних компонентів та матеріалів через треті країни в обхід санкційних обмежень; розроблення в рамках дослідно-конструкторських робіт нових та перспективних систем (комплексів, зразків) засобів збройної боротьби, які забезпечать домінування та технологічну перевагу.

На поточному етапі війни сили оборони України використовують нову модель ведення бойових дій – “активну оборону” – з акцентом на масове застосування безпілотних (роботизованих) платформ наземного, повітряного та морського базування, високоточних боєприпасів у складі розвідувально-вогневих контурів на основі єдиного розвідувально-

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

інформаційного простору, побудованого на відповідних програмно-апаратних системах (комплексах). Така модель забезпечує перевагу в гнучкості ведення бойових дій, точності ураження, зменшенні часу планування і здійснення ударів по об'єктах противника на випередження (у тому числі в глибині території рф) та зниженні втрат серед особового складу тощо.

Зазначене вище обумовлює нагальну необхідність створення для зс рф адекватних інструментів протидії шляхом розроблення нових та модернізації існуючих зразків ОВТ на власному ОПК та (або) закупівлі у країнах "осі зла" готових зразків чи комплектувальних для крупновузлового складання на власних підприємствах.

У всіх сегментах ОПК рф здійснюються заходи з нарощення спроможностей для виробництва сучасних систем (комплексів, зразків) ОВСТ [13].

У космічному сегменті основні зусилля спрямовані на формування сучасної інформаційної космічної системи; створення багатофункціональної низькоорбітальної системи супутникового зв'язку та забезпечення безперешкодного зв'язку по лінії "супутник–цільовий об'єкт–наземна станція" з використанням спеціальних модулів підсилення; нарощення орбітального угруповання існуючих космічних апаратів зв'язку, створення космічного комплексу радіолокаційного всепогодного зондування (S-діапазону); триває удосконалення радіооптичних комплексів пошуку та ідентифікації низькоорбітальних космічних об'єктів тощо. При цьому гальмується подальший розвиток космічного сегмента системи попередження про ракетний напад через відсутність потрібної номенклатури електронної компонентної бази західного виробництва.

Для підтримання стратегічних сил стримування триває виробництво міжконтинентальних балістичних ракет "Ярс", здійснюється модернізація ракетного комплексу стратегічного призначення "Сармат", виробництво мобільного ґрунтового ракетного комплексу "Орешник". Тривають заходи з удосконалення елементів системи управління (командних пунктів) і зв'язку стратегічних ядерних сил.

За напрямом розвитку озброєння та техніки протиповітряної оборони (у тому числі військ ППО СВ та зенітно-ракетних військ повітряно-космічних сил (ЗРВ ПКС) зс рф) країною-агресором здійснюється низка перспективних науково-дослідних та дослідно-конструкторських робіт (НДДКР), спрямованих на розроблення нового, модернізацію та удосконалення існуючого ОВТ ЗРВ ПКС рф, підвищення його живучості та автономності пунктів бойового управління, розроблення нових автоматизованих систем управління тощо. Триває модернізація всієї існуючої номенклатури ЗРС (С-350, С-400, С-500 тощо); розроблення нового мобільного ракетного комплексу; розроблення на основі ЗГРК "Панцирь" протидронового ЗРК ближньої дії "Панцирь-СМД-Э" з новою ("малою") ракетою; створюються модернізовані зразки ЗРГК "Панцирь" за рахунок підвищення можливостей станції наведення; розробляються нові зенітні керовані ракети для ЗРК з новими типами бойових частин; створюється малогабаритна автоматизована установка ППО для виявлення та знищення БпЛА на малій висоті у складі РЛС та 2–4 пускових контейнерів ракет; розробляються сучасні гарматні бойові модулі ППО (типу "Цитадель") тощо.

Для врахування досвіду високотехнологічної російсько-української війни з активним та ефективним застосуванням БпЛА рф продовжує реалізацію концептуальних змін у підходах до побудови ешелонованої ППО всіх рівнів, приділяючи основну увагу протидії маловисотним засобам повітряного нападу. Намагається створити прийнятну систему загально-об'єктового ППО, здійснюючи пошук найбільш ефективних компонентів для протидії існуючим загрозам.

Основні зусилля ОПК рф стосовно подальшого розвитку повітряно-космічних сил спрямовані на розроблення та виробництво нових авіаційних комплексів з низькою ефективною площею розсіювання, сучасним цифровим бортовим обладнанням з елементами

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

штучного інтелекту та перспективними авіаційними засобами ураження великої дальності й потужності. На цей час у різному стані готовності перебувають проєкти створення перспективних авіаційних комплексів військово-транспортної авіації, дальньої авіації (“Изделие 80”), дальнього радіолокаційного виявлення та управління (А-100), перспективний авіаційний комплекс дальнього перехоплення (МіГ-41), проєкт малопомітного багатофункціонального винищувача п’ятого покоління “Chekmate” (Су-75) тощо. У період до 2034 року на заміну літакам воєнно-транспортної авіації Ан-22 та Ан-124 заплановано розроблення та виробництво перспективного авіаційного комплексу Іл-100 “Слон”.

Для нарощування спроможностей з виробництва сучасних і новітніх літаків оперативно-тактичної авіації противник концентрує зусилля на таких напрямах: створення новітнього уніфікованого двигуна бойових літаків; модернізація бортового електронного обладнання та програмного забезпечення; глибока модернізація літаків Су-25 через нестачу сучасних штурмовиків; підвищення бойової ефективності літаків шляхом застосування сучасного озброєння тощо. Головний пріоритет надається винищувачам-бомбардувальникам Су-34М, що є основними носіями авіаційних бомб, оснащених УМПК. Водночас противник нарощує виробництво Су-35С, глибоко модернізованого надманевреного багатофункціонального винищувача покоління 4++. Також ОПК рф нарощує темпи виробництва багатоцільових винищувачів 5 (4+++) покоління Су-57, реалізує заходи з модернізації обладнання, розширення функціоналу застосування авіаційних засобів ураження, підвищення надійності й працездатності систем, розроблення засобів для контролю та обслуговування. Належної уваги заслуговують дослідно-конструкторські роботи з розроблення функціонального програмного забезпечення для створення уніфікованої системи, яка поєднує завдання ситуаційної обізнаності авіаційного з’єднання; керування координованою атакою повітряної цілі (цілей) одночасно групою літаків із різними інформаційними системами (типу Су-57, Су-35, Су-34, Су-30); керування комплексом озброєння літака для ураження кількох цілей одночасно.

Тривають роботи з розроблення нових та модернізації існуючих авіаційних двигунів для всіх родів авіації.

Вживаються активні заходи з підвищення ефективності застосування ударних вертольотів Мі-28НМ та Ка-52М.

Зменшення втрат агресора в бойовій броньованій техніці може свідчити про загальне технічне виснаження російської армії. Виробництво (компенсація втрат) бойової броньованої техніки здійснюється шляхом використання існуючих військових запасів з баз зберігання та ремонтних підприємств. Приблизно 80% танків та інших бойових броньованих машин не є новими, а відремонтованими і модернізованими. Обсяги запасів, що зберігаються на складах, дозволяють підтримувати рівень поповнення втрат до кінця 2026 року. Промислові потужності можуть бути спрямовані на виробництво нових бойових платформ, але це неминуче означатиме зменшення кількості техніки, що постачатиметься зс рф у найближчій перспективі.

Підприємства ОПК рф посилюють спроможності у кластері бойової броньованої техніки шляхом: нарощення виробництва нових, сучасних танків; зменшення обсягів капітального ремонту з модернізацією та відновленням; скорочення номенклатури бойових танків. Слід звернути увагу на те, що у 2025 році зс рф почали використовувати нову модифікацію ТОС-1А “Солнцепек” – ТОС-3 “Дракон”. Модифікована версія отримала збільшену дальність стрільби та посилений захист, що підвищує її живучість в ході контрбатарейного вогню та ударів БпЛА сил оборони України (оновлена пускова установка з 15 направляючими замість 24). Проведений аналіз свідчить про те, що у зс рф є нагальна потреба у БМД-4М, БТР-МДМ, бронеавтомобілях “Атлет”, “Сармат”, “Тайфун” тощо, що стимулює прискорені темпи їх виробництва.

З метою задоволення потреб ведення бойових дій рф нарощує обсяги виробництва

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

основних номенклатур боєприпасів та засобів ураження. Крім інтенсифікації темпів виробництва існуючої номенклатури боєприпасів та закупівлі у країн "осі зла", агресор здійснює розроблення нових зразків.

Тривають заходи щодо удосконалення системи зв'язку на всіх рівнях, а також системи управління військами (силами). Створені: нова система вузькосмугового цифрового рухомого радіозв'язку; новий комплекс тактичного зв'язку; система безпроводового широкосмугового передавання даних у різних умовах ("точка-точка", "точка-многоточка", mesh-мережа); системи зв'язку для FPV-дронів "Пеппа", "Гермес" та "Кузнечик"; новітній супутниковий комплекс зв'язку; триває розроблення автоматизованої системи тактичної розвідки й аналізу інформації ("АСТРА"); триває створення технічних засобів інтегрованої системи розвідувально-інформаційного забезпечення та бойового управління для побудови на її основі єдиного інформаційного простору поля бою; створюються системи та комплекси інтеграції звичайної та високоточної зброї різних видів базування у розвідувально-вогневі контури тощо.

Простежується системний підхід до нарощування потенціалу інтегрованих засобів радіоелектронної розвідки (РЕР) та радіоелектронної боротьби (РЕБ), насамперед на тактичному рівні. рф активізувала розроблення високотехнологічних засобів РЕР+РЕБ, орієнтованих на виявлення, супровід та цілевказання по джерелах випромінювання малої потужності.

Для ефективної протидії вогневому впливу сил оборони України розробляються засоби контрбатарейної боротьби. Створюються комплекси (системи), які є складовими розвідувально-вогневого (ударного) контуру, і в автоматичному режимі визначають координати вогневих позицій засобів вогневого ураження із подальшою передачею цілевказівок екіпажам ударних БпЛА та іншим засобам ураження (розвідувально-вогневих комплексів / розвідувально-ударних контурів).

За напрямом розвитку озброєння та техніки ракетних військ і артилерії створюються новітні високоточні засоби ураження великої дальності із сучасними завадозахищеними системами наведення й управління, розроблені малогабаритні переносні апаратно-програмні комплекси передачі даних та управління вогнем артилерії для скорочення циклу бойового управління та забезпечення автоматизації процесу розрахунку вихідних даних для завдавання вогневого ураження за принципом "виявив–уразив" тощо. Триває модернізація існуючої номенклатури озброєння та техніки, у тому числі глибока модернізація радянського оперативно-тактичного комплексу "Эльбрус" з аеробалістичною ракетою наземного базування в звичайному та спеціальному спорядженні, а також крилатою ракетою. Тривають випробування в бойових умовах роботизованої самохідної гармати "Клевер", яка являє собою безпілотну 122-мм артилерійську установку Д-30 на гусеничному шасі, інтегровану з дистанційно керованою платформою.

Підприємствами ОПК рф інтенсифіковані заходи за напрямом розроблення безпілотних (безекіпажних) комплексів наземного, повітряного та морського базування. Розроблення роботизованих наземних комплексів (РНК) військового призначення є одним із пріоритетних напрямів розвитку ОВТ зс рф. На цей час створені спеціальні гусеничні шасі модульного типу, конструкція яких дає змогу створювати РНК із заданими функціональними можливостями – від розвідувально-ударних до логістичних, але залежність від електронної компонентної бази західного виробництва в умовах санкцій не дає можливості здійснювати їх серійне виробництво. Нині тривають дослідно-конструкторські роботи зі створення РНК на принципах багатофункціональності, модульності, стандартизації архітектури і програмного забезпечення; групового (ройового) застосування; підвищення стійкості функціонування комплексів в умовах застосування засобів РЕБ; підвищення надійності та пропускної здатності каналів радіообміну (технологія MANET); збільшення радіусу дистанційного керування; підвищення рівня автономності тощо.

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Противник продовжує розвивати складову безпілотної авіації та нарощує виробництво та застосування ударних безпілотних літальних апаратів (БпЛА) великої дальності дії. Збільшується номенклатура ударних БпЛА (“Тювик”, “Герань-3”, “Герань-4”, “Герань-5”, “Шахед-107” тощо), створюються нові та удосконалюються існуючі баражуючі боєприпаси повітряного та наземного старту (“Клин”, “Молнія-250”, “Молнія-500”, “Бандероль”, “Посылка”, “Открытка”, “Ланцет-Р”, “Довод-МД”, “Филин” тощо), УМПК, УМПБ тощо.

На початок 2026 року збройними силами рф використовувалося біля 60 основних видів FPV-дронів коптерного типу, більше 25 літакового типу, майже 10 найменувань БпЛА-перехоплювачів, більше 25 варіантів ударного навантаження FPV, більше 40 найменувань комплексів придушення каналів зв’язку, управління та навігації БпЛА різних типів. Особливої уваги заслуговує розроблення та виготовлення комплексів, у яких інтегровані засоби РЕР та РЕБ з БпЛА-перехоплювачами. Створюються нові універсальні безпілотні платформи на основі БпЛА “Крокодил”, “Скворец”, “Ударник”, “Сибирь”, “Лунь” та інші.

Почали застосовувати технологію виробництва моноплатних FPV-дронів.

Розроблена та впроваджується технологія автономного управління безпілотними авіаційними системами на основі елементів штучного інтелекту, яка передбачає реалізацію можливостей реконфігурації системи управління та ухвалення самостійного рішення на основі програмно реалізованих механізмів під час зміни типових умов застосування.

Під час розроблення нових БпЛА рф використовує технології передачі сигналу, які менш вразливі до перешкод, активно впроваджує нові способи управління та наведення, а саме: управління FPV-дронами по оптоволокну, багатодіапазонні канали управління, штучний інтелект, систему самозахоплення цілі з машинним зором, Mesh, нові завадозахищені системи зв’язку тощо.

На тлі збільшення застосування силами оборони України ударних БпЛА зростає інтенсивність застосування противником комплексів протидії БпЛА і, як наслідок, відбувається нарощування обсягів виробництва стаціонарних, мобільних та “окопних” засобів РЕБ, а також кінетичних засобів ураження (інноваційні боєприпаси, активні засоби ураження БпЛА індивідуального використання на основі самонавідного реактивного боєприпасу з радіолокаційною ГСН у вигляді компактної ракети; зенітні артилерійські комплекси калібром 30 мм тощо).

Керівництво росії, враховуючи досвід війни з Україною та високу ефективність застосування морських роботизованих комплексів Силами безпеки й оборони України, вживає все більше заходів з метою створення новітніх, перспективних зразків для потреб вмф рф. НДДКР за цим напрямом реалізуються в рамках “Програми розвитку морських робототехнічних комплексів та спеціального морського підводного озброєння на період до 2035 року”, затвердженої у червні 2024 року. На початок 2026 року завершена розробка низки багатофункціональних морських безпілотних платформ, здійснюються випробування та бойове застосування ударних швидкісних безекіпажних катерів (БЕК). Одночасно в рф здійснюється розроблення надводних і підводних, активних і пасивних засобів протидії БЕК сил оборони України.

На підприємствах ОПК рф триває низка НДДКР, спрямованих на розроблення інноваційного і модернізацію існуючого авіаційного озброєння та систем управління ним. Здійснюються дослідження зі створення трансформної модульної зброї другого покоління, уніфікованої на міжвидовому рівні. Їхньою метою є розроблення обґрунтування створення уніфікованої лінійки авіаційних засобів ураження, адаптації та уніфікації наземних засобів підготовки, а також пускових пристроїв, стандартів інформаційного обміну та електроживлення бортових систем зразків авіаційного озброєння (ракети, авіабомби, некеровані реактивні снаряди тощо). Результати досліджень мають вирішити комплекс завдань, пов’язаних із розширенням номенклатури носіїв та підвищенням їхніх бойових

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

характеристик, збільшенням їхньої бойової потужності та радіусу застосування, забезпеченням високої мобільності, розміщенням усередині фюзеляжного простору для зниження радіолокаційної помітності.

Підприємства ОПК рф нарощують обсяги виробництва високоточної ракетної зброї – балістичних, крилатих, гіперзвукових аеробалістичних та протикорабельних ракет наземного, повітряного та морського базування. На постійній основі здійснюється модернізація ракетного озброєння для більш ефективного його застосування для ураження об'єктів в глибині території нашої держави. Основними напрямами модернізації ракетного озброєння є підвищення точності ураження, збільшення потужності бойової частини, підвищення завадозахищеності та зниження залежності від іноземної елементної бази.

Таким чином, проведений аналіз основних напрямів розвитку російського ОПК, кількісно-якісного складу нового та модернізованого ОВТ, що застосовуються на поточному етапі російсько-української війни, а також перспективних НДДКР, спрямованих на їхній подальший розвиток, дає змогу визначити вісім основних тенденцій розвитку засобів збройної боротьби рф:

визначальна роль повітряно-космічних систем у вирішенні завдань розвідки, навігації, управління військами (зв'язок та АСУ) через розроблення систем, комплексів, засобів для забезпечення оперативного доведення інтегрованої інформації розвідки та сигналів бойового управління до всіх рівнів управління військами; створення нових та удосконалення існуючих засобів повітряно-космічної оборони у складі підсистем управління, розвідки та попередження про повітряно-космічний напад, ураження та придушення засобів повітряно-космічного нападу; створення всіх сегментів єдиного інформаційного контуру управління зс рф;

підвищення ефективності озброєння, військової та спеціальної техніки різних типів базування через удосконалення оперативно-тактичних вимог та якісне підвищення тактико-технічних характеристик на основі досвіду російсько-української війни;

підвищення потужності, швидкості, завадозахищеності, точності та дальності засобів вогневого ураження через розроблення перспективних та удосконалення існуючих комплексів гіперзвукової зброї; високоточного ракетного озброєння; розроблення нових боєприпасів для ракетно-артилерійського озброєння; розширення номенклатури носіїв авіаційних засобів ураження; розроблення та удосконалення баражуючих боєприпасів повітряного та наземного старту; збільшення потужності та точнісних характеристик керованих авіаційних бомб всіх калібрів та типів тощо;

"інтелектуалізація" засобів збройної боротьби шляхом створення дистанційно керованих, роботизованих та автономних комплексів військового призначення повітряного, наземного та морського базування з використанням технологій штучного інтелекту реалізується через інтенсифікацію впровадження цивільних технологій та технологій подвійного призначення для потреб ведення збройної боротьби. Досвід російсько-української війни свідчить, що інверсія цивільних технологій для потреб війни може здійснюватися ефективно не тільки державними і великими корпоративними акторами, а й недержавними та волонтерськими спільнотами і групами;

удосконалення та розвиток засобів розвідки, зв'язку, систем автоматизованого управління військами (силами) та їх комплексування через застосування інформаційних технологій автоматизації управління військами та оперативного обміну даними, відхід від традиційних систем управління, побудованих на ієрархічній структурі та централізованих каналах зв'язку, впровадження мережецентричних підходів, які забезпечують вищу швидкість ухвалення рішень, гнучкість та ефективність взаємодії;

створення і масштабування нових високоефективних, малогабаритних та порівняно дешевих зразків ОВТ (засобів ураження) реалізує асиметричне завдавання противнику суттєвого збитку, непорівняльного з вартістю засобу ураження, який був використаний;

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

підвищення захищеності та живучості ОВСТ, особового складу та об'єктів інфраструктури через підвищення мобільності систем, комплексів, зразків ОВТ; зниження помітності систем, комплексів, зразків ОВТ та військових об'єктів у всіх діапазонах довжин хвиль; оснащення броньованої техніки пристроями постановки перешкод у каналах управління БпЛА, встановлення додаткових елементів захисту, зниження помітності від оптичних, тепловізійних та радіолокаційних засобів розвідки, комплектування сучасними радіостанціями та приладами нічного бачення, системами кругового огляду; проведення НДДКР зі створення нових типів броньового захисту для підвищення спроможностей поглинати та розсіювати кінетичну енергію боєприпасів та вибухостійкості тощо;

підвищення вимог щодо стандартизації, уніфікації, спрощення експлуатації та надійності функціонування систем, комплексів, зразків ОВСТ через скорочення типажу і номенклатури системи озброєння та зосередження зусиль на розвитку уніфікованих бойових платформ, засобів високоточної зброї, пускових установок та систем розвідувально-інформаційного забезпечення; розроблення системи стандартів зберігання та обміну даними, єдиної для зс рф; побудову складних систем, комплексів зі вбудованою діагностикою на основі неремонтованих та необслуговуваних технічних елементів (складових) ОВСТ тощо.

Висновок (Conclusion)

Підбиваючи підсумки, можна констатувати таке.

1. Проведений аналіз основних напрямів розвитку російського ОПК, кількісно-якісного складу нового та модернізованого ОВТ, що застосовуються на поточному етапі російсько-української війни, а також перспективних НДДКР, спрямованих на їхній подальший розвиток, дав змогу визначити вісім основних тенденцій розвитку засобів збройної боротьби рф.

2. Основні напрями розвитку ОВТ зс рф корелюють із глобальними технологічними трендами у сфері оборони та безпеки, визначеними провідними країнами світу, а саме: космічні платформи військового та подвійного призначення; військова авіація; бронетанкова техніка; високоточна зброя та боєприпаси; ракетні війська і артилерія; безпілотні бойові платформи; засоби розвідки, протиповітряної оборони, радіолокації, радіоелектронної боротьби та зв'язку тощо. За цими напрямами на підприємствах ОПК рф збільшуються обсяги виробництва, модернізації та капітального ремонту, а також розпочато низку НДДКР, у рамках яких здійснюється розроблення перспективних систем (комплексів) ОВСТ.

3. Визначені основні тенденції розвитку засобів збройної боротьби рф взаємопов'язані між собою та стимулюють подальший взаємний розвиток.

4. російська федерація намагається збільшити технологічну перевагу за окремими напрямами формування спроможностей, проте не в змозі забезпечити власну самодостатність за всім спектром критичних оборонних технологій.

Рекомендації (Recommendations)

Визначені тенденції розвитку засобів збройної боротьби зс рф можуть бути використані на поточному етапі програмно-цільового планування для своєчасного та ефективного обґрунтування основних напрямів подальшого розвитку озброєння, військової та спеціальної техніки сил оборони України.

Конфлікт інтересів (Conflict of Interest)

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

Використані джерела

1. Komarov, V. S., Oleksiiuk, V. V., & Shcherban, K. A. (2024). Key elements of russian federation's strategic adaptation for sustaining a prolonged war of attrition against Ukraine.

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Наука і оборона, *4*, 3–10.
2. *Зміни у формах і способах ведення операцій (бойових дій) збройних сил російської федерації у ході збройної агресії проти України (січень-грудень 2025 року): Інформаційний бюлетень, книга ІІІ*. (2025). НДІ ВР.
3. Vasylyk, D. (2025). The Russian military-industrial complex in the context of preparation and implementation of military aggression against Ukraine: Functioning, vulnerabilities and international countermeasures. *Political and Legal Studies*, *4* (2), 28–42.
4. Center for Strategic and International Studies (CSIS). (2026). *War and the modern battlefield insights from Ukraine and the Middle East*. https://features.csis.org/war-modern-battlefield
5. Center for Strategic and International Studies (CSIS). (2025). *Defense industrial base lessons from Russia-Ukraine conflict focus*. https://www.csis.org/analysis/defense-industrial-base-lessons-russia-ukraine-conflict-focus
6. Institute for the Study of War (ISW). (2025, June 27). *Russian force generation and technological adaptations update June 27, 2025*. https://understandingwar.org/research/future-of-war/russian-force-generation-and-technological-adaptations-update-june-27-2025/
7. European Security & Defence (ESD). (2025, Sept.). *Mapping the expansion of Russia's defence industry*. https://euro-sd.com/2025/09/articles/exclusive/46685/mapping-the-expansion-of-russias-defence-industry
8. Center for Strategic and International Studies (CSIS). (2024). *Back in stock? The state of Russia's defense industry after two years of the war*. https://www.csis.org/analysis/back-stock-state-russias-defense-industry-after-two-years-war
9. Royal United Services Institute (RUSI). (2024). *Russian military objectives and capacity in Ukraine through 2024*. https://www.rusi.org/explore-our-research/publications/commentary/russian-military-objectives-and-capacity-ukraine-through-2024
10. Royal United Services Institute (RUSI). (2024). *Disrupting Russian air defence production: Reclaiming the sky*. https://www.rusi.org/explore-our-research/publications/research-papers/disrupting-russian-air-defence-production-reclaiming-sky
11. Royal United Services Institute (RUSI). (2024). *Struggling, not crumbling: Russian defence AI in a time of war*. https://www.rusi.org/explore-our-research/publications/commentary/struggling-not-crumbling-russian-defence-ai-time-war
12. Global Espreso. (2025). *Russia's arms industry now employs 4.5 million, says RUSI report*. https://global.espreso.tv/russia-ukraine-war-russias-arms-industry-now-employs-45-million-says-rusi-report
13. *Тенденції розвитку засобів збройної боротьби російської федерації в ході російсько-української війни: Інформаційний бюлетень, книга V*. (2025). НДІ ВР.

References

1. Komarov, V. S., Oleksiiuk, V. V., & Shcherban, K. A. (2024). Key elements of russian federation's strategic adaptation for sustaining a prolonged war of attrition against Ukraine. *Science and Defense*, *4*, 3–10.
2. *Changes in forms and methods of conducting operations (combat actions) of the armed forces of the russian federation during the armed aggression against Ukraine (January-December 2025): Information Bulletin, Book III*. (2025). Scientific Research Institute of the Armed Forces (NDI VR).
3. Vasylyk, D. (2025). The Russian military-industrial complex in the context of preparation and implementation of military aggression against Ukraine: Functioning, vulnerabilities and international countermeasures. *Political and Legal Studies*, *4* (2), 28–42.
4. Center for Strategic and International Studies (CSIS). (2026). *War and the modern battlefield*

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

insights from Ukraine and the Middle East. https://features.csis.org/war-modern-battlefield
5. Center for Strategic and International Studies (CSIS). (2025). *Defense industrial base lessons from Russia-Ukraine conflict focus*. https://www.csis.org/analysis/defense-industrial-base-lessons-russia-ukraine-conflict-focus
6. Institute for the Study of War (ISW). (2025, June 27). *Russian force generation and technological adaptations update June 27, 2025*. https://understandingwar.org/research/future-of-war/russian-force-generation-and-technological-adaptations-update-june-27-2025/
7. European Security & Defence (ESD). (2025, Sept.). *Mapping the expansion of Russia's defence industry*. https://euro-sd.com/2025/09/articles/exclusive/46685/mapping-the-expansion-of-russias-defence-industry
8. Center for Strategic and International Studies (CSIS). (2024). *Back in stock? The state of Russia's defense industry after two years of the war*. https://www.csis.org/analysis/back-stock-state-russias-defense-industry-after-two-years-war
9. Royal United Services Institute (RUSI). (2024). *Russian military objectives and capacity in Ukraine through 2024*. https://www.rusi.org/explore-our-research/publications/commentary/russian-military-objectives-and-capacity-ukraine-through-2024
10. Royal United Services Institute (RUSI). (2024). *Disrupting Russian air defence production: Reclaiming the sky*. https://www.rusi.org/explore-our-research/publications/research-papers/disrupting-russian-air-defence-production-reclaiming-sky
11. Royal United Services Institute (RUSI). (2024). *Struggling, not crumbling: Russian defence AI in a time of war*. https://www.rusi.org/explore-our-research/publications/commentary/struggling-not-crumbling-russian-defence-ai-time-war
12. Global Espreso. (2025). *Russia's arms industry now employs 4.5 million, says RUSI report*. https://global.espreso.tv/russia-ukraine-war-russias-arms-industry-now-employs-45-million-says-rusi-report
13. *Trends in the development of weapons and military equipment of the russian federation during the russian-ukrainian war: Information Bulletin, Book V*. (2025). Scientific Research Institute of the Armed Forces (NDI VR).

Transformation of the development of russian means of warfare at the current stage of the russia-ukraine war: key trends

Volodymyr Komarov
Laureate of the Borys Paton National Prize
Doctor of Military Sciences, Professor
Chief Researcher of department
Defence Intelligence Research Institute
04050, Yurii Illienko Str., 81, Kyiv, Ukraine
e-mail: komarvlad@ukr.net
ORCID: 0000-0003-2873-8261

Yurii Sokorynskyi
Doctor of Juridical Sciences, Associate Professor
Security Service of Ukraine officer
Security Service of Ukraine
01601, Volodymyrska Street, 33, Kyiv, Ukraine
e-mail: usokorinskiy@ukr.net
ORCID: 0000-0002-8907-9880

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Yevhen Tverdokhlib
Lecturer Department of Military Training
State University “Kyiv Aviation University
03048, Medova Street, 1, Kyiv, Ukraine
e-mail: xleb33@ukr.net
ORCID: 0009-0002-6958-1280

Maxim Polivoda
Senior Lecturer
Department of Military Training
State University “Kyiv Aviation University”
03048, Medova Street, 1, Kyiv, Ukraine
e-mail: maksym.polivoda@npp.kai.edu.ua
ORCID: 0000-0002-4673-008X

Abstract. The Russian Federation continues to take consistent steps to adapt its economy and defense industrial complex to a war of attrition. This includes the mobilization of the national economy and its transition to a war footing, accompanied by a significant increase in military production to compensate for losses incurred during combat operations. The relevance of this article is обусловлена (driven by) the need to analyze the main directions of development of weapons and military equipment (WME) of the Armed Forces of the Russian Federation, as well as the capabilities of its defense industrial complex in terms of their development, modernization, and production at the current stage of the Russia–Ukraine war and in the near-term perspective. The aim of the article is to analyze the directions of development of weapons and military equipment of the Armed Forces of the Russian Federation and to identify the key trends in their evolution at the current stage of the Russia–Ukraine war. The main result of the study is an analysis of the development directions of means of armed warfare of the Armed Forces of the Russian Federation at the present stage of the war, as well as the identification of their principal trends. The practical significance of the results lies in the application of the identified trends in the development of Russian means of warfare within program-based defense planning, in order to substantiate timely decisions regarding the priority directions for further development of weapons and military equipment of the Defense Forces of Ukraine.

Keywords: means of armed warfare, defense industrial complex of the Russian Federation, directions of weapons development, military and special equipment, Russia–Ukraine war, development trends.

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Received: *January 7, 2026* | **Revisions Requested:** - | **Revision Received:** -
Accepted: *March 27, 2026* | **Published Online:** *April 10, 2026*

Licensed (C) by Creative Commons Attribution International License 4.0 (CC BY-NC-SA)

DOI: 10.62524/msj.2026.4.1.4

The State Policy Life Cycle in the Defence Domain

Andrii Zinchenko
Doctor of Technical Sciences, Professor
Chief Inspector
The Main Inspectorate of the Ministry of Defence of Ukraine
03168, Povitrianykh Syl Avenue, 8, Kyiv, Ukraine
e-mail: zinchenko.andrei@ukr.net
ORCID: 0000-0002-4734-3401

Ihor Lunov
First Deputy General Inspector
of the Ministry of Defence of Ukraine
The Main Inspectorate of the Ministry of Defence of Ukraine
03168, Povitrianykh Syl Avenue, 8, Kyiv, Ukraine
e-mail: igr.lunov@gmail.com
ORCID: 0009-0005-3028-1581

Viktor Kozlov
Senior Research Fellow
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl Avenue, 28 B, Kyiv, Ukraine
e-mail: vvkadet1@ukr.net
ORCID: 0000-0002-6737-212X

Oleh Tarasov
Candidate of Military Sciences, Associate Professor
Associate Professor of the Military Training Department
State University “Kyiv Aviation University”
03048, Medova Street, 1, Kyiv, Ukraine
e-mail: tarasovo@ukr.net
ORCID: 0000-0002-6763-8653

Abstract. The relevance of the research is determined by the growing role of state policies in the field of defence under the conditions of martial law, a dynamic security environment and limited resources, which necessitates improving the quality of managerial decision-making and ensuring its adaptability. Under such conditions, state policy should be considered not as a set of fragmented decisions or regulatory legal acts, but as an integral and continuous managerial process with a clearly defined logic of development and feedback mechanisms. The aim of the article is to substantiate a universal model of the life cycle of state policy in the field of defence and to determine its main stages, taking into account the specific features of the formulation and implementation of policies falling within the competence of the Ministry of Defence of Ukraine. The article employs system and

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

process approaches, structural-functional analysis, methods of analysis and synthesis, induction and deduction, as well as elements of comparative and risk-oriented analysis, which made it possible to consider state policy in the field of defence as a multi-stage life cycle. The main results of the research consist in substantiating a universal model of the life cycle of state policy in the field of defence, distinguishing its principal stages – from goal-setting and policy initiation to monitoring and evaluation of outcomes – and demonstrating the decisive role of feedback in ensuring the effectiveness and sustainability of defence policies. It is shown that the effectiveness of the policies of the Ministry of Defence of Ukraine largely depends on the coherence of all stages of the life cycle and on the ability of the management system to engage in institutional learning and timely adjustment of managerial decisions. The results of the research may be of interest to officials of public administration bodies in the field of national security and defence, specialists of the Ministry of Defence of Ukraine and the General Staff of the Armed Forces of Ukraine, researchers and academic staff in the field of public administration and military security, as well as analysts and experts involved in the formulation, implementation and evaluation of defence policies.

Keywords: state policy, policy life cycle, defence policy, public administration, Ministry of Defence of Ukraine, monitoring and evaluation, feedback.

Introduction

Under the contemporary conditions of transformation of the national security and defence system of Ukraine, particular importance is attached to improving the quality of public administration in the field of defence. The full-scale armed aggression of the russian federation, the prolonged regime of martial law, as well as the need simultaneously to conduct combat operations and implement profound institutional reforms, determine increasing requirements for the soundness, coherence and adaptability of state policies in the security and defence sector. Under such conditions, state policy cannot be regarded solely as a set of regulatory legal acts or one-off managerial decisions, but requires consideration as an integral and continuous managerial process.

In the public administration theory, the process approach is becoming increasingly widespread, according to which state policy is interpreted through the prism of its life cycle – from the emergence of a problem and the formulation of a goal to implementation, monitoring, evaluation of outcomes and subsequent adjustment. Such an approach makes it possible to analyse systematically the logic of policy development, to identify internal linkages between its stages, and also to assess the effectiveness of managerial decisions not in isolation but in the context of their impact on the achievement of strategic objectives.

For the defence domain, the state policy life cycle is of fundamental importance, since defence policies are implemented under conditions of high uncertainty, limited resources, a dynamic security environment and constant influence of external threats. In addition, Ministry of Defence of Ukraine (MoD of Ukraine) policies are, as a rule, interagency in nature, rely on a complex system of strategic documents and require coordination between military, political, economic and legal components. In the absence of a clearly structured life cycle with feedback mechanisms, such policies lose manageability, which leads to the accumulation of systemic errors and reduced effectiveness.

In this context, the scientific task of conceptualising the state policy life cycle in the defence domain as an integral managerial loop becomes particularly relevant. Such a loop covers all key stages – from goal-setting to monitoring and evaluation of outcomes – and ensures feedback at each phase. Formalisation of this approach creates methodological prerequisites for improving public administration quality in the defence domain, as well as for introducing institutional learning and adaptation principles into the MoD of Ukraine activities.

The aim of this article is to substantiate a universal model of the state policy life cycle in the defence domain and to determine its key stages, taking into account specific features of policy

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

formulation and implementation entrusted to Ministry of Defence of Ukraine. Achieving this aim involves systematic analysis of policy cycle logic, managerial decision role at each stage and feedback mechanism significance for ensuring defence policy effectiveness and sustainability.

Literature Review

State policy life cycle issues constitute one of the key topics in contemporary public administration theory, since they make it possible to consider policy not as a one-off act of decision-making but as a continuous managerial process that covers problem formulation, decision development, implementation, monitoring and outcome evaluation followed by subsequent adjustment [1, 2]. Such an approach creates a methodological basis for analysing state policy effectiveness in complex and dynamic domains, in particular in the defence domain.

In classical works on state policy analysis, the life cycle is described as a sequence of functionally interconnected stages, each characterised by its own instruments, actors and managerial decision quality criteria [1, 3]. At the same time, contemporary research emphasises that linear interpretation of policy cycle is methodologically limited, since it does not take into account feedback presence, process iterativity and policy capacity for adaptation under changing external environment conditions [2, 4]

For the defence domain, such iterativity is of critical importance. Defence policies are formulated and implemented under conditions of high uncertainty, constant transformation of the security environment and significant resource constraints, which requires regular revision of goals, instruments and implementation mechanisms [5, 6]. Defence management literature stresses that the absence of a formalised cycle with clearly defined stages and feedback mechanisms leads to policy fragmentation, a gap between strategic goals and practical outcomes, as well as reduced resource use efficiency [6, 7].

A significant proportion of defence management research is focused on analysing capability planning and development processes which, by their logic, are also cyclical in nature. In particular, within defence planning processes of NATO member states, the policy life cycle is integrated with multi-year cycles of requirement definition, target allocation, implementation and outcome review [8]. The NATO Defence Planning Process is considered an example of an institutionalised cycle in which political decisions, resource constraints and outcome evaluation are combined within a single managerial loop [8, 9].

A separate body of scholarly works is devoted to state policy implementation issues, where it is emphasised that this particular life cycle phase is most vulnerable to managerial disruptions [3, 10]. In the defence domain, this is manifested in the complexity of coordination between numerous actors, institutional inertia, limited capacity for rapid adaptation and the high cost of managerial errors [6, 10]. In this regard, researchers underline the need to integrate mechanisms of ongoing control and action adjustment directly into policy implementation process [5, 7.

A significant place in contemporary literature is occupied by issues of state policy monitoring and evaluation as instruments for ensuring accountability, effectiveness and institutional learning [11]. OECD recommendations define policy evaluation as systematic and objective analysis of its design, implementation and outcomes with the aim of improving managerial decision quality and adjusting policies on an evidence-based basis [11, 12]. For defence policies, this has particular importance, since it makes it possible to distinguish between achievement of planned outcomes and efficiency of limited resource use [9, 12].

In Ukrainian scholarly and regulatory discourse, state policy life cycle issues are considered mainly in a fragmented manner – through separate planning, implementation or evaluation elements. At the same time, in methodological documents and policy preparation practices for public authorities, in particular in the security and defence domain, process approach use with structured “policy description”, goal system and indicator framework is gradually becoming established [5, 12].

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

This creates prerequisites for scientific formalisation of a universal state policy life cycle model in the defence domain, adapted to specific features of the MoD of Ukraine activities.

Thus, the analysis of scholarly and applied sources indicates the existence of a sufficient theoretical basis for considering state policy as a cyclical managerial process. At the same time, defence domain specificity highlights the need to generalise and systematise existing approaches in order to build an integral state policy life cycle model in the defence domain, which determines the direction of further research.

Methodological Framework

The methodological basis of the research consists of a set of general scientific and specialised methods that ensure the analysis of the state policy life cycle in the defence domain as an integral, multi-stage managerial process. The method selection is determined by defence domain complexity, multi-level management system structure and the need to combine theoretical generalisation with analysis of the MoD of Ukraine practice.

At the stage of goal-setting and state policy initiation, a system approach and a scientific abstraction method were applied, which made it possible to consider policy as an element of a broader national security and defence system, as well as to identify key problems requiring political intervention.

For the state policy formulation stage, process and structural-functional approaches are fundamental. They made it possible to formalise policy internal logic, determine managerial action sequence and define role and functions of main actors at different management levels. A synthesis method was used to develop a generalised policy life cycle model suitable for application to various defence activity domains.

At the political decision-making and policy implementation stage, managerial process analysis methods and results-oriented approach were applied, which made it possible to assess policy goal coherence with available resources and institutional capacities. Elements of the risk-oriented approach were used to take into account uncertainty influence and external threat impact on policy implementation course.

For the monitoring and evaluation stage, comparative analysis and generalisation methods were applied, which ensured assessment of policy effectiveness, resource use efficiency and feedback generation for managerial decision adjustment. This made it possible to consider monitoring and evaluation not as policy completion but as a mechanism for transition to a new development cycle.

An applied methodological toolkit ensures comprehensive research of the state policy life cycle in the defence domain and creates scientific prerequisites for practical use of the proposed model in activities within the MoD of Ukraine.

Results and Discussions

Within a contemporary public administration theory, the state policy is increasingly considered not as a set of fragmented managerial decisions or regulatory legal acts but as an integral process characterised by its own development logic, internal structure and feedback mechanisms [13]. Such an approach is of particular relevance in the defence domain, where policies are implemented under conditions of high uncertainty, limited resources and constant influence of external threats.

The state policy life cycle in the defence domain should be interpreted as an institutionalised managerial loop that combines state strategic objectives, mechanisms for their transformation into practical decisions and an evaluation system for achieved outcomes. Such a loop is not fixed once and for all but operates in a mode of continuous clarification and adaptation, which is of fundamental importance for the MoD of Ukraine policies under martial law conditions and long-term transformation of the security and defence sector.

The state policy life cycle universality consists in the fact that, regardless of substantive domain

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

(personnel, resource, technological, organisational or regulatory), policy passes through the same basic stages. Differences between policies lie not in cycle logic itself but in the content, instruments and managerial mechanisms that fill each stage.

The methodological recommendations by the MoD of Ukraine, in particular regarding "policy description" development [14], in fact establish precisely such a cyclical understanding of policy, although it is not always formalised as a single conceptual model. In this context, scientific task consists in systematising existing approaches and presenting the state policy life cycle as a universal analytical framework suitable for application to all policies whose formulation and implementation are entrusted to the MoD of Ukraine.

A key characteristic of such a framework is feedback presence at each cycle stage, which distinguishes contemporary policy management approaches from traditional linear models in which policy implementation was regarded as final stage. In the defence domain, absence or formal character of feedback inevitably leads to accumulation of systemic errors, inconsistency between objectives and resources and reduced trust in managerial decisions.

The general outline of the state policy life cycle for policies whose formulation and implementation are entrusted to MoD of Ukraine is presented in Figure 1.

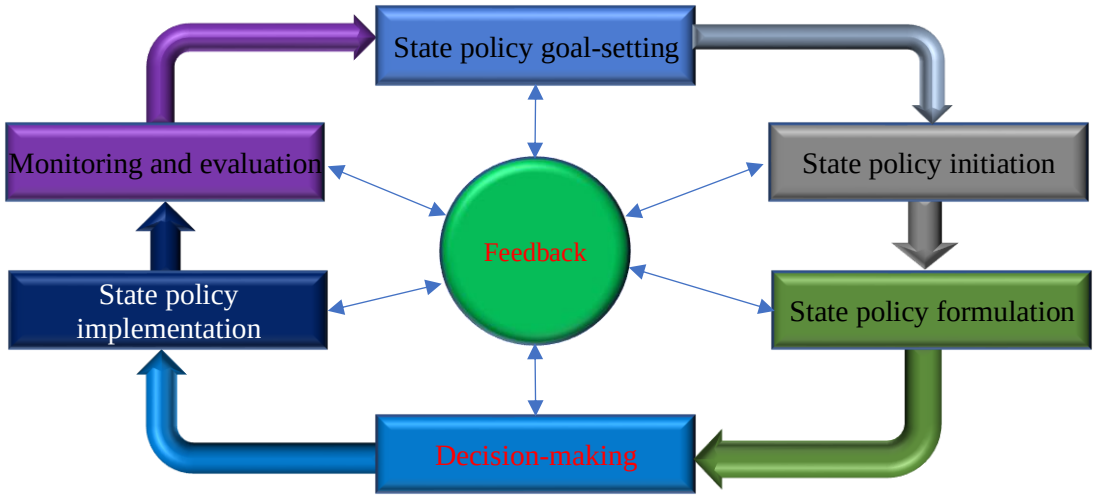


Figure 1. State policy life cycle,
formulation and implementation of which are entrusted to the MoD of Ukraine

Stage 1. State policy goal-setting. The state policy goal-setting stage is not only a starting point of the life cycle but also a key element that determines quality of all subsequent managerial decisions. In the defence domain, a policy goal cannot be formulated in isolation from overall state strategic planning architecture, since any MoD of Ukraine policy derives from national security and defence strategic objectives.

At this stage, a conceptual understanding of the problem requiring political intervention takes place. This involves not only identifying an existing deficit or shortcomings in a particular domain but also achieving a systemic understanding of their causes, interconnections with other policies and possible consequences of inaction. It is precisely here that the boundary is drawn between policies of strategic character and operational response measures that do not form a full-fledged life cycle.

The state policy goal in the defence domain must meet a number of fundamental requirements, namely:

be aligned with higher-level strategic documents, which ensures its legitimacy and political support;

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

be sufficiently specific to allow further decomposition into objectives, tasks and performance indicators;

take into account real institutional and resource constraints, which is particularly important under wartime condition.

Feedback at the goal-setting stage is implemented through analysis of previous policy implementation experience, assessment of achieved and unachieved outcomes, as well as through systematic updating of security environment assessments. In international defence planning practice, this stage is often accompanied by scenario analysis use, threat development modelling and assessment of alternative goal formulation options, which makes it possible to reduce the risk of erroneous strategic choice.

Stage 2. State policy initiation. State policy initiation is the stage at which an abstractly formulated goal acquires an organisational and managerial dimension. It is at this point that the transition takes place from strategic intent to a formalised policy development process, which includes identification of responsible actors, procedures, time frames and resource constraints.

For the MoD of Ukraine, policy initiation is, as a rule, associated with decisions of the state leadership, results of strategic or defence reviews, as well as with identified capability gaps following comprehensive analysis. It is important to emphasise that policy initiation presupposes conscious recognition of a problem as one that cannot be resolved within existing mechanisms.

At this stage, initial institutional policy model is formed: range of internal and external stakeholders is determined, their roles and authorities are outlined, and coordination and decision-making principles are established. Errors made at the initiation stage tend to be reproduced at all subsequent life cycle stages, which makes this stage critically important from managerial quality perspective.

Feedback during the initiation process is manifested through clarification of the problem field, revision of initial assumptions and adjustment of process participant composition. If the absence of the necessary institutional capacity or a sufficient resource base is identified, the initiation of the policy may be suspended or returned to the stage of the objective revision.

Stage 3. State policy formulation. A state policy formulation stage is the central and methodologically most substantive phase of the life cycle, since it is at this stage that a strategically defined goal is transformed into a structured set of objectives, tasks, instruments and implementation mechanisms. For the MoD of Ukraine policies, this stage is particularly complex due to the defence domain multidimensional nature, interagency decision character and high requirements for coherence with national and international state commitments.

Policy formulation should not be equated with preparation of a single document. It is a process of analytical, organisational and managerial design of policy as an integral system. At this stage, problem specification takes place, alternative decision options are developed, their consequences are assessed and the most optimal policy configuration is selected.

An important methodological prerequisite for policy formulation in the defence domain is an application of system approach. The policy is considered not in isolation but as an element of a broader defence management system that includes doctrinal, organisational, personnel, resource, infrastructure and regulatory components.

This stage involves the implementation of several sub-stages (Figure 2).

Policy formulation begins with an in-depth analysis aimed at substantiating the need for political intervention and determining optimal ways of achieving the defined goal. An analytical component includes assessment of current state, identification of gaps and imbalances, analysis of their causes and forecasting consequences of maintaining existing conditions.

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

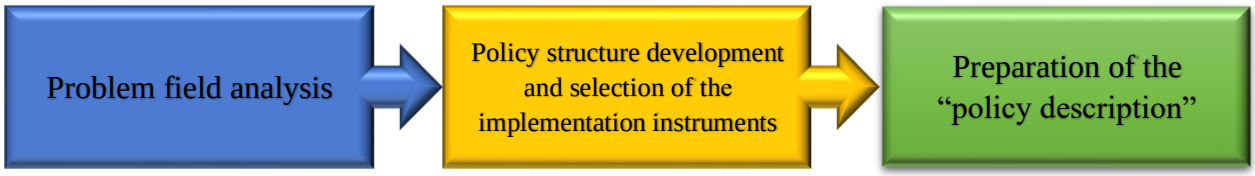


Figure 2. Components of state policy formulation stage

The next step in policy formulation is constructing its internal structure. At this stage, the overall policy goal is decomposed into strategic objectives, specific tasks and expected outcomes. Such decomposition should ensure a logical linkage between the level of strategic intent and the level of practical implementation.

The final result of the formulation stage is preparing the "policy description" – a basic document that records policy content, logic and implementation mechanisms. Policy description performs the role of a reference framework against which all subsequent managerial actions, decisions and effectiveness assessments are aligned.

Feedback in the process of the policy structure formation is manifested through testing logical coherence between objectives, tasks and instruments. If imbalances or internal contradictions are identified, policy is subject to adjustment even before transition to decision-making stage.

Stage 4. Political decision-making. This stage represents a transition from an analytically formulated policy to its official approval and the acquisition of a binding character. For the MoD of Ukraine, this stage has not only managerial but also politico-legal significance, since it is at this point that the policy becomes integrated into the public administration system.

Decision-making presupposes the consideration of the policy by authorised bodies and the assessment of its compliance with current legislation, strategic documents, and budgetary capacities. In this process, an important role is played by the balance between the expert substantiation of the policy and the political expediency of its approval.

The institutional complexity of this stage consists in the multi-level nature of decision-making within the defence domain. Depending on the subject of the policy, decisions may be taken at the level of the Ministry of Defence, the Cabinet of Ministers, the National Security and Defence Council of Ukraine, or by the higher political leadership of the state. This necessitates the thorough preparation of materials, sound argumentation, and the coordination of positions between different actors.

Feedback at the decision-making stage is implemented through the mechanisms of policy refinement and adjustment following the results of consideration. If critical remarks or inconsistencies are identified, the policy may be returned to the formulation stage for revision, which confirms the non-linear character of the life cycle.

Stage 5. State policy implementation. A state policy implementation stage in the defence domain is the longest, most resource-intensive and managerially complex element of the life cycle. It is at this phase that viability of political decisions developed and approved at previous stages is tested, as well as their capacity to be transformed into practical outcomes under real defence system functioning conditions. Unlike previous stages, policy implementation cannot be regarded as a set of formally defined measures, since it always takes place in a dynamic environment, under conditions of limited resources and influence of external and internal factors.

In the context of the MoD of Ukraine, policy implementation means management of a complex adaptive system that includes numerous governance bodies, military formations, institutions, defence-industrial complex enterprises, as well as external partners and stakeholders. Each of these elements has its own interests, constraints and level of institutional capacity, which significantly affects policy implementation course.

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

State policy implementation is not mechanical execution of plans or roadmaps. It presupposes continuous managerial balancing between planned objectives, actual conditions for their achievement and the need for timely response to changes in the security environment. In this sense, policy implementation acquires characteristics of a process of permanent managerial decision-making that adjusts initial policy logic without losing its strategic orientation.

Feedback at the policy implementation stage is of fundamental importance. It is ensured through regular analysis of measure execution, assessment of interim outcomes, as well as through information collection from implementers and final policy beneficiaries. It is precisely at this stage that implicit assumptions not taken into account during policy formulation, as well as systemic constraints preventing achievement of planned objectives without adjustment of approaches, are identified.

Stage 6. Monitoring and evaluation. Monitoring and evaluation of state policy implementation outcomes constitute the final stage, which at the same time ensures transition to a new management cycle. This stage should be regarded not as a formal procedure of summarising results but as a key mechanism for management system learning and improvement of future policy decision quality.

Monitoring in the defence policy domain consists in systematic collection and analysis of information on policy implementation progress, adherence to timelines, resource use and achievement of interim outcomes. Its main function is timely identification of deviations from planned parameters and ensuring managerial response to such deviations. Monitoring should be continuous and integrated into policy management system rather than reduced to episodic reporting.

Evaluation, unlike monitoring, is aimed at deeper analysis of policy effectiveness and its impact on defence system condition. In this context, evaluation acts as an instrument of strategic reflection that makes it possible to assess adequacy of policy logic itself.

For the MoD of Ukraine, it is particularly important to distinguish between the evaluation of policy effectiveness in terms of results and evaluation of policy efficiency. The former focuses on achievement of defined indicators, whereas the latter concerns the relationship between obtained outcomes and expended resources. The presence of positive outcomes in the absence of efficient resource use cannot be regarded as a fully successful policy.

Feedback generated on the basis of monitoring and evaluation constitutes grounds for decision-making regarding further policy fate. Depending on obtained outcomes, several scenarios are possible: continuation of policy implementation without changes, adjustment of its individual components, revision of the goal or complete termination of policy as one that has lost relevance or proved ineffective.

Thus, monitoring and evaluation do not complete the policy life cycle but rather close it within a managerial loop that ensures the transition to a new cycle of policy formulation or transformation. It is at this stage that the principle of institutional learning is realised, without which the long-term enhancement of the capacity of the defence management system is impossible.

Conclusion

Thus, the article substantiates the expediency of considering state policy in the defence domain as an integral life cycle covering the interconnected stages of goal-setting, initiation, formulation, decision-making, implementation, monitoring, and outcome evaluation. It is shown that the effectiveness of defence policy is determined not by individual managerial decisions but by the quality of the organisation of the entire cycle and the presence of feedback at each of its stages.

The proposed universal model of the state policy life cycle makes it possible to systematise the approaches to the formulation and implementation of the policies of the MoD of Ukraine, ensures the coherence between strategic objectives and resource capacities, and increases the manageability of the political process under the conditions of a dynamic security environment. The practical

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

significance of the obtained results lies in the possibility of using the proposed model as an analytical tool for the evaluation of current defence policies, their adjustment, and the development of new managerial decisions, taking into account the principles of adaptability and institutional learning.

Recommendations

The article materials may be of practical and scholarly interest to the officials of public administration bodies in the national security and defence domain, in particular to the senior leadership and specialists of the MoD of Ukraine and the General Staff of the Armed Forces of Ukraine involved in the formulation, implementation, and evaluation of state defence policies; to researchers and academic staff in the fields of public administration, military security, and defence management; as well as to the analysts of the security and defence sector, strategic planning experts, and the specialists in capability development and defence institution reform who use process- and results-oriented approaches in their activities.

Conflict of Interest

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

References

1. Howlett, M., Ramesh, M., & Perl, A. (2020). *Studying Public Policy: Principles and Processes*. 4th ed. Oxford University Press.
2. Wu, X., Ramesh, M., Howlett, M., & Fritzen, S. (2018). *The Public Policy Primer: Managing the Policy Process.* 2nd ed. Routledge.
3. Dunn, W. N. (2012). *Public Policy Analysis: An Integrated Approach.* 5th ed. Routledge.
4. Sabatier, P. A., & Weible, C. M. (2014). *Theories of the Policy Process*. 3rd ed. Westview Press.
5. Bardach, E., & Patashnik, E. M. (2020). *A Practical Guide for Policy Analysis: The Eightfold Path to More Effective Problem Solving. 6th ed*. CQ Press (SAGE).
6. Yarger, H. R. (2006). *Strategic Theory for the 21st Century: The Little Book on Big Strategy.* Strategic Studies Institute, U.S. Army War College.
7. Bartholomees, J. B. (ed.). (2012). *U.S. Army War College Guide to National Security Issues*. Vol. I: Theory of War and Strategy. 5th ed. Strategic Studies Institute.
8. *NATO Defence Planning Process*. NATO. https://www.nato.int/cps/en/natohq/topics_49202.htm
9. *NATO Comprehensive Operations Planning Directive (COPD)*. NATO Standardization Office.
10. Pressman, J. L., & Wildavsky, A. (1984). *Implementation*. 3rd ed. University of California Press.
11. *Recommendation of the Council on Public Policy Evaluation*. (2022). OECD. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0478
12. *Instrumentarii dlia analizu derzhavnoi polityky.* (2023). Ukrainskyi nezalezhnyi tsentr politychnykh doslidzhen.
13. *Derzhavna polityka*. Pidruchnyk. (2014). Nats. akad. derzh. upr. pry Prezydentovi Ukrainy. (Red. kol.: Yu. V. Kovbasiuk (holova), K. O. Vashchenko (zast. holovy), Yu. P. Surmin (zast. holovy) ta in.). NADU. https://ktpu.kpi.ua/wp-content/uploads/2014/02/DERZHAVNA-POLITIKA.pdf
14. *Metodolohiia opysu polityk: navch.-metod. Materialy.* (2025). Ministerstvo oborony Ukrainy.

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Життєвий цикл державної політики у сфері оборони

Андрій Зінченко
доктор технічних наук, професор
головний інспектор
Головна інспекція Міністерства оборони України
03168, проспект Повітряних Сил, 8, Київ, Україна
e-mail: zinchenko.andrei@ukr.net
ORCID: 0000-0002-4734-3401

Ігор Луньов
перший заступник генерального інспектора
Міністерства оборони України
Головна інспекція Міністерства оборони України
03168, проспект Повітряних Сил, 8, Київ, Україна
e-mail: igr.lunov@gmail.com
ORCID: 0009-0005-3028-1581

Віктор Козлов
старший науковий співробітник
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: vvkadet1@ukr.net
ORCID: 0000-0002-6737-212X

Олег Тарасов
кандидат військових наук, доцент
доцент кафедри військової підготовки
Державний університет “Київський авіаційний університет”
03048, вулиця Медова, 1, Київ, Україна
e-mail: tarasovo@ukr.net
ORCID: 0000-0002-6763-8653

Анотація. Актуальність дослідження зумовлена зростанням ролі державних політик у сфері оборони в умовах воєнного стану, динамічного безпекового середовища та обмежених ресурсів, що потребує підвищення якості управлінських рішень і забезпечення їхньої адаптивності. У таких умовах державна політика має розглядатися не як сукупність розрізнених рішень або нормативно-правових актів, а як цілісний, безперервний управлінський процес із чітко визначеною логікою розвитку та механізмами зворотного зв’язку. Метою статті є обґрунтування універсальної моделі життєвого циклу державної політики у сфері оборони та визначення її основних етапів з урахуванням особливостей формування і реалізації політик, що належать до компетенції Міністерства оборони України. У статті використано системний і процесний підходи, структурно-функціональний аналіз, методи аналізу та синтезу, індукції й дедукції, елементи порівняльного та ризик-орієнтованого аналізу, що дозволило розглянути державну політику у сфері оборони як багатоетапний життєвий цикл. Основні результати дослідження полягають в обґрунтуванні універсальної моделі життєвого циклу державної політики у сфері оборони, виокремленні його ключових етапів – від визначення мети та ініціювання політики до моніторингу й оцінювання

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

результатів – та доведенні визначальної ролі зворотного зв'язку для забезпечення результативності й стійкості оборонних політик. Показано, що ефективність політик Міністерства оборони України значною мірою залежить від узгодженості всіх етапів життєвого циклу та здатності системи управління до інституційного навчання і своєчасного коригування управлінських рішень. Результати дослідження можуть бути цікавими для посадових осіб органів державного управління у сфері національної безпеки і оборони, фахівців Міністерства оборони України та Генерального штабу Збройних Сил України, наукових і науково-педагогічних працівників у галузі державного управління та воєнної безпеки, а також для аналітиків і експертів, залучених до формування, реалізації та оцінювання оборонних політик.

Ключові слова: державна політика, життєвий цикл політики, оборонна політика, державне управління, Міністерство оборони України, моніторинг і оцінювання, зворотний зв'язок.

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Received: *September 16, 2025* | **Revisions Requested:** - | **Revision Received:** -
Accepted: *December 12, 2025* | **Published Online:** *April 10, 2026*

Licensed (C) by Creative Commons Attribution International License 4.0 (CC BY-NC-SA)

DOI: 10.62524/msj.2026.4.1.5

The Analysis of Global Trends in the Development of Operational (Operational-Strategic) Reconnaissance-Strike Complexes Based on Unmanned Aerial Vehicles

Dmytro Solomatin
Candidate of Military Sciences, Senior Researcher
Chief of Branch
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 Sciences, 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

Vadym Pasichnyk
Candidate of Military Sciences
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

Oleksandr Lutseviat
Senior Research Fellow
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.@gmail.com
ORCID: 0000-0003-4165-3908

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Serhii Popkov
Junior Research Fellow
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl Avenue, 28 B, Kyiv, Ukraine
e-mail: popkov3151@gmail.com
ORCID: 0009-0003-3152-8246

Abstract. The relevance of the research is determined by the growing role of reconnaissance–strike complexes of the operational and operational–strategic level under the conditions of modern armed conflicts, first of all under the conditions of the russian–Ukrainian war, which is accompanied by the rapid development of unmanned aerial technologies, network-centric command and control principles and high-precision strike means. In this regard, the article is aimed at a comprehensive analysis of global trends in the development of reconnaissance–strike complexes based on unmanned aerial vehicles, the identification of the main directions of the evolution of their components, and the formulation of scientifically substantiated proposals concerning the prospective development of such complexes with the aim of achieving an asymmetric military-technological advantage. The leading approach to the study of this issue is the system and structural-functional approaches in combination with comparative and critical-analytical analysis of open sources, which makes it possible to consider reconnaissance–strike complexes comprehensively as integrated multi-component systems, to assess the interrelationship of their elements and to identify the leading global technological trends. The article determines global trends in the development of reconnaissance–strike complexes of the operational (operational-strategic) level created on the basis of unmanned aerial vehicles (both with regard to such complexes as a whole and with regard to their components); reveals the directions for increasing the autonomy, network interaction and strike capabilities of reconnaissance–strike complexes; identifies the growing role of artificial intelligence, swarm technologies and mass expendable unmanned aerial vehicles; substantiates the expediency of transition to modular, serial and economically efficient solutions. The materials of the article have practical value for specialists in the field of defence planning, as well as for scientific and design organisations of the defence-industrial complex, and may be used in the formulation of requirements for prospective reconnaissance–strike complexes and in substantiating the directions of their further development.

Keywords: reconnaissance–strike complexes; unmanned aerial vehicles; unmanned aerial complexes; operational–strategic level; artificial intelligence; swarm technologies; network-centric systems; high-precision strike; defence technologies.

Introduction

Under the conditions of modern geopolitical challenges and military threats that have faced Ukraine over the past ten years, military-technological superiority over the adversary has become a key element in ensuring the state's defence capability and the effective conduct of combat operations. The war that has continued since 2014, especially in the phase of the full-scale invasion after 24 February 2022, has put forward new requirements for the Armed Forces of Ukraine regarding technological adaptation, the modernisation of armaments and the introduction of innovations.

The relevance of the research is determined by the need for a comprehensive analysis of contemporary global trends in the development of armaments, the assessment of technologies introduced by the aggressor state, the study of national experience in modernising samples of weapons and military equipment, as well as the identification of prospective directions for the development of the domestic defence-industrial complex.

The aim of the article is a comprehensive analysis of innovative solutions in the field of defence technologies, the assessment of existing technological developments in Ukraine, the identification of the main directions for the further development of high-technology armaments, as well as the formulation of proposals for technical solutions that ensure the achievement of an asymmetric advantage over the adversary.

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Issues concerning the development of reconnaissance–strike complexes (RSC) of the operational (operational–strategic) level created on the basis of unmanned aerial vehicles (UAVs) were considered in [1]. A retrospective analysis and development trends of unmanned aerial complexes (UACs), taking into account current programmes for their creation, are presented in [2]. A view on the development of RSC in accordance with trends in armed struggle is set out in [3]. An analysis of combat operations conducted by reconnaissance–fire complexes during the repulse and deterrence of the full-scale armed aggression of the russian federation against Ukraine is provided in [4]. Prospects for the development of strike UACs of the defence forces of Ukraine are considered in [5]. The necessity of introducing into armaments UAC command and decision-making systems based on artificial intelligence is emphasised in [6]. A methodology for the selection of UACs for the defence forces of Ukraine is proposed in [7]. Prospects for the development of UACs with UAVs of the "multicopter" type are examined in [8]. Trends in the development of UAVs with hybrid propulsion systems are highlighted in [9]. The peculiarities of the employment of UAVs in wars and methods of countering them are analysed in [10].

Methodological Framework

The methodological framework of the research is formed by a set of mutually complementary scientific approaches, methods and principles that ensure a systematic, objective and representative analysis of the development of RSC under modern conditions. The scientific approaches (Table 1), methods (Table 2) and principles (Table 3) that constitute this framework are presented below.

Table 1. Scientific approaches used to study global development trends of the specified RSC

Approaches	Purpose of use
System approach	For considering RSC as an integrated set of interdependent components – sensor subsystems, communication channels, information processing means, delivery platforms and strike means. This makes it possible to assess RSC not as a set of technologies but as a single multifunctional system in which a change in one element alters the overall capabilities of the complex.
Structural-functional approach	For determining the functional role of individual components of RSC and their contribution to the overall effectiveness of the processes of "detection–identification–strike"
Comparative approach	For comparing global practices, technological solutions and doctrinal approaches of different states (the United States, the United Kingdom, France, Türkiye, Israel, China, Ukraine, etc.). This provides an opportunity to identify general trends and specific development models.
Critical-analytical approach	For analysing information from open sources: scientific publications, data of analytical centres, defence industry materials, conclusions regarding the war in Ukraine, and assessments of NATO and other international structures. The application of this approach made it possible to avoid incorrect generalisations, to take into account different viewpoints and to formulate conclusions on the basis of verified data.

Table 2. Research methods used to study global development trends of the specified RSC

Approaches	Purpose of use
Method of analysis and synthesis	For structuring information on RSC technologies and concepts, identifying the main technical trends, and generalising the obtained data in the form of systematic conclusions
Content analysis	For processing a large body of sources (analytical reports of defence agencies, annual reports of military-industrial companies, military-technical reviews, scientific articles and official NATO documents).
Expert-analytical method	For interpreting complex technical data, assessing the results of the introduction of new technologies and the prospects for their practical application under the conditions of modern conflicts.
Scenario analysis method	For analysing the prospects for the development of RSC up to 2030–2035, and for assessing the impact of new technologies (AI, UAV swarms, software-defined munitions, edge computing) on the operational and strategic capabilities of the armed forces.

It should also be noted that the limitations of the research included the use only of open-source intelligence (OSINT) materials without access to classified military documents; the limited availability of precise technical characteristics of the latest systems, which is compensated for by the analysis of available patents, marketing materials and expert assessments; and the dependence of the

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

assessment of the operational effectiveness of UAVs and RSC in the war in Ukraine on fragmented data (due to information constraints of the parties).

Table 3. Principles of researching the development of the specified RSC

Principles	What validates the use
Objectivity	The analysis is based on the use of data confirmed by several information sources.
Comprehensiveness	The analysis covers technological, doctrinal, tactical, political and industrial aspects.
Relevance	The analysed sources include materials of 2020–2025 that reflect current trends.
Scientific justification	The analysis is based on a number of scientific research methods.
Interdisciplinarity	The analysis combines knowledge from different fields of science (technical, military).

Results

As a result of the conducted analysis, global trends in the development of RSC of the operational (operational-strategic) level, which are created on the basis of the UAV, have been identified. Such trends are conditionally divided into three components, which relate both to such RSC as a whole and to the UAC and UAV that form part of these RSC. The identified trends are considered below.

Global trends in the development of the specified RSC as a whole

Based on the analysis of the prospects for the development of unmanned aviation of the armed forces of the leading countries of the world, it has been determined that, in general, the main global trends in the development of the specified RSC are as follows:

ensuring the possibility of simultaneous control from the ground command post of the RSC of several reconnaissance-strike UACs, and from ground control stations of the UAC – of groups of UAV of different types (reconnaissance-strike (reconnaissance, strike), relay platforms) with minimal operator intervention, as well as ensuring the possibility of transferring UAV control functions from one UAC to another and to the ground command post of the RSC;

inclusion in the structure of the RSC of "mothership UAVs", which serve as carriers of smaller strike UAV (single-use or reusable), ensuring the possibility of their autonomous employment after release from the carrier and their return on board after completing combat missions (for reusable UAV);

ensuring capabilities for conducting continuous reconnaissance within the entire area of responsibility of the RSC, its processing and dissemination to external UAC crews and/or directly to strike the UAV in real time and in a form suitable for their immediate employment;

increasing capabilities for high-precision fire engagement of stationary and moving targets in the shortest possible time within the designated area of responsibility of the RSC under any meteorological conditions and at any time of day;

ensuring the possibility of combat control of the air elements of the RSC from ground command posts (control stations) in real time during their flight within the designated limits of the RSC area of responsibility through the use of satellite channels and airborne relay platforms;

ensuring interaction with external reconnaissance assets (radar, radio, radiotechnical, electro-optical) and command and control assets in a single information space in order to enhance the level of situational awareness and the possibility of selective dissemination of reconnaissance information both to own UAC (UAV) and to other combat platforms (strike assets) in real time;

ensuring the possibility of organising interaction with other RSC created on the situational principle of employment, or directly with other strike assets deployed on air, land and maritime platforms, in order to increase the power of fire impact on the enemy in designated areas of combat operations in real time;

ensuring the possibility of the mass employment of the UAV from the structure of the RSC (in groups or "swarms") and control of their group flights (in the future – in joint combat formations with

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

manned aircraft) in real time (as required) in order to overload and disorganise enemy air defence systems and increase the effectiveness of engagement of important enemy objects;

improvement of software and hardware support to ensure the possibility of information exchange and organisation of interaction between different control subsystems within the RSC (in particular, the creation of data-exchange interfaces between the automatic target recognition system and the weapon control system, between systems that ensure situational awareness of the ground and air environment, etc.);

enhancement of the capabilities of technical support units responsible for the operation of RSC components, including the incorporation into their structure of groups for employment support, repair and maintenance of UAC (UAV) and their command posts (ground control stations).

Global trends in the development of UAC within the specified RSC

As a result of the conducted analysis, the following main trends in the development of UAC within the specified RSC have been identified:

enhancement of the strike capabilities of UACs through equipping them with single-use strike UAVs with jet engines, as well as aerial target simulators developed on their basis, which will ensure the possibility of more rapid strikes against moving objects (targets) in the operational depth after receiving reconnaissance information about them and will create conditions for more effective deception and overloading of the enemy air defence system;

enhancement of the strike capabilities of UACs through equipping them with reconnaissance-strike (strike) reusable UAVs with long-range aviation munitions of the “air-to-surface” and “air-to-air” classes, which will ensure more effective overcoming of the enemy air defence system and engagement of objects located at considerable distances from the line of combat contact;

enhancement of the reconnaissance capabilities of UACs in terms of surveillance and imagery airborne reconnaissance (electro-optical in the visible and infrared spectrum, radiotechnical, radar) by day and by night under simple and complex meteorological conditions;

increasing the level of automation of UACs on the basis of artificial intelligence in order to ensure automated control of individual UAV, their groups (swarms) at all stages of flight (take-off, en-route flight, strike delivery, landing, etc.), as well as the possibility of their effective performance of combat and special tasks in the tactical, operational and strategic depth of the enemy;

increasing the effectiveness of control of group flights and swarms of UAV (in the future – in common combat formations with aircraft in order to master the forms and methods of joint employment with manned aviation);

enhancement of the resistance (resilience) of data transmission, command and control lines of UAVs under the influence of enemy electronic warfare assets (exposure to electromagnetic emissions of natural and artificial origin);

integration of UACs into automated command and control systems of troops (forces), ensuring their compatibility with UACs developed (employed) by partner countries within a common infrastructure (including the possibility of using unified communication and navigation systems (networks)) for the conduct of joint operations;

development of networked systems based on distributed artificial intelligence that will allow a group of UAVs to be employed as a single entity with automatic task distribution among the UAV in the group in real time in accordance with the evolving operational-tactical situation;

inclusion in the structure of UAC of relay UAV, aerostat-based relay platforms and satellite communication means in order to ensure information exchange between reconnaissance (strike) UAV and ground control stations beyond radio line-of-sight zones.

Global trends in the development of UAVs within the specified RSCs

The conducted analysis made it possible to identify the following main trends in the development of UAVs within the specified RSCs:

equipping reconnaissance UAVs with onboard compact multi-frequency radiotechnical suites

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

incorporating passive reconnaissance means, side-looking and all-round surveillance radars with active electronically scanned arrays (AESA), and high-resolution electro-optical systems;

implementation in onboard AESA radars of a wide range of operating modes enabling the identification of small-size ground objects by their radar signatures (in particular, SAR/ISAR modes (synthetic aperture / inverse synthetic aperture), which provide resolution at the level of 1–2 m), detection of moving ground and low-altitude air targets (including GMTI (Ground Moving Target Indication) mode), as well as acquisition of radar imagery of objects concealed by soil, snow, sand and forests (low-frequency subsurface radar mode);

increase in the detection range of onboard radars for ground objects in the active mode (up to 250 km);

enhancement of the capabilities of onboard passive radiotechnical means for target detection based on their own emissions (up to 400 km);

improvement of the resolution of electro-optical reconnaissance means (less than 1 angular minute) in the visible and infrared spectra (both in static image formation modes and in video streaming modes with wide-area and focused fields of view);

enhancement of the capabilities of onboard reconnaissance means in target selection, recognition and prioritisation against the background of the underlying surface, radio interference and high-intensity false signals;

equipping UAVs with electro-optical and infrared reconnaissance devices capable of detecting targets at low, medium and high altitudes with equal effectiveness and functioning both by day and by night;

ensuring the possibility of cueing electro-optical stations based on external preliminary target designation and/or their own algorithms (including localisation of a target by its radio emission detected by the onboard radar);

enhancing capabilities of single-use strike UAVs to engage mobile ground moving targets through equipping their warheads with their own homing seekers (radar, infrared, laser);

equipping reusable reconnaissance-strike UAVs with their own self-defence missile armament (in particular, “air-to-air” and “air-to-surface” missiles), as well as effective electronic warfare means to counter enemy air defence and electronic suppression assets, which will ensure the possibility of UAVs approaching reconnaissance objects at a distance corresponding to the maximum realisation of their reconnaissance capabilities;

equipping UAVs with communication and data transmission systems of the MP-CDL (Multi-Platform Common Data Link) type, which ensure the possibility of organising the exchange of reconnaissance information with other combat (reconnaissance, strike) platforms and their command posts within a single information space, as well as the provision (reception) of target designation during joint employment in designated areas of combat operations;

integration into the software and hardware of UAVs of elements of artificial intelligence and machine vision in order to automate navigation processes, target detection, their recognition (by category, type, condition), tracking, guidance to the target and its engagement;

ensuring the functioning of UAVs in an autonomous mode that does not require operator intervention after their launch (start), through the use of onboard integrated inertial-satellite navigation systems with different types of sensors;

improvement of onboard inertial systems in order to enhance the navigation accuracy of UAVs through the use of improved sensors and new algorithms for compensating time-dependent errors in the measurement of navigation parameters on the basis of artificial intelligence;

increasing the endurance of UAVs, development of compact modular-type observation equipment, ensuring the transmission of reconnaissance data in real time through the use of various communication channels;

increasing the flight range of UAVs, as well as reducing their thermal and acoustic signature

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

through the replacement of traditional internal combustion engines with new-type propulsion systems (in particular, liquid hydrogen engines, electric motors and hybrid versions);

introduction of technologies to reduce fuel consumption and increase the service life of compact turbogenerators and turbojet engines, development of new energy-efficient compact air-aluminium power sources for UAVs;

development of power converters and electrical installations of UAVs with intelligent self-diagnostics and failure compensation functions;

increasing the flight speed of UAVs through equipping them with turbojet and turboprop engines, as well as hybrid propulsion systems (turbojet (turboprop) engines integrated with electric motors);

development of hypersonic UAVs capable of reaching speeds exceeding Mach 5, which will significantly accelerate the process of engaging objects (targets) located in the operational and strategic depth of the enemy and will practically preclude the destruction of such UAVs by traditional air defence systems;

development of reconnaissance-strike UAVs based on the integration of two types of drones – reconnaissance and loitering strike – which ensures the detection of targets at long distances and the immediate direction of a loitering munition towards the target for its engagement;

development, on the basis of UAVs, of decoy aerial targets capable of imitating the signatures of various aircraft in order to deceive enemy air defence, as well as interceptor UAVs designed to engage aerial targets of different types (including FPV drones, helicopters and UAVs of the “Shahed” type);

reduction of radar and thermal signatures of UAVs through the manufacture of their airframes using new composite materials and stealth technologies (by analogy with the carrier-based variant of the fifth-generation fighter F-35C), the use of radar-absorbing and/or radar-scattering coatings, as well as the creation of plasma formations around the most powerful radar-reflective elements of UAVs, synchronised with radar emissions, which allows operations under conditions of strong enemy air defence;

use of new technologies for the miniaturisation and enhancement of onboard equipment capabilities, development on this basis of compact radio communication modules with increased range of command and telemetry channels, as well as high-capacity onboard batteries that extend the operating time of onboard equipment and the endurance of UAVs;

development of new optical odometry and stabilisation technologies enabling UAVs to fix their position on terrain using a specific marker, information about which is obtained from their onboard cameras (a key advantage of these technologies is independence from GPS connectivity, which increases the resistance of UAVs to electronic interference);

development of fibre-optic cables with improved properties (strength, flexibility, quality, etc.) to ensure stable control of UAVs in complex terrain conditions at maximum possible distances under conditions of active electronic countermeasures;

advancement of sensor technologies (research into the integration of various sensors (lidars, radars, cameras, etc.) in order to improve environmental perception accuracy and enhance the navigation capabilities of UAVs);

advancement of communication technologies (development of new protocols and standards for data transmission between UAVs and ground stations, including the use of 5G and other high-speed channels);

development of collision-avoidance systems (creation of technologies for detecting and preventing collisions with other objects in the air and on the ground, including algorithms for analysing sensor data);

development of energy-efficient systems (research aimed at improving the energy efficiency of UAVs through the use of new types of batteries, solar panels and other energy sources);

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

development of multi-antenna systems (creation of technologies for coordination and interaction of several UAVs within a single mission, enabling the performance of more complex tasks);

advancement of cyber security technologies (protection of UAVs against cyber threats in order to increase the effectiveness and safety of their employment during mission execution in operations (combat actions));

development of multi-channel technical vision systems capable of analysing information in the optical, radio and infrared spectra;

improvement of technical vision systems in order to ensure reliable detection and identification of objects (targets), taking into account their possible distortions under conditions of optical and radio interference;

improvement of algorithms for processing information on detected objects (targets) through the application of machine learning and artificial intelligence technologies;

ensuring multi-position monitoring of terrain on the basis of technical vision methods and integrated processing of radar frame streams, with the possibility of recognising and predicting the location of objects (targets);

implementation of technologies aimed at enhancing the quality and autonomy of navigation and solving positioning tasks, including improvement of the software and hardware of onboard optical navigation systems in order to increase their resolution through the use of convolutional neural networks;

implementation of technologies for cooperative monitoring and terrain mapping based on data from UAVs operating as a group;

development of intelligent onboard information-navigation complexes based on multispectral (multi-sensor) technical vision systems, ensuring the processing of heterogeneous measurement data using artificial intelligence;

development of integrated correlation-extreme onboard navigation systems with joint processing of information on objects (terrain) obtained in different spectra (visible, infrared and radar);

improvement of onboard software and hardware in order to ensure the possibility of autonomous control, navigation and interaction of individual UAVs (their groups) in flight through the development and implementation of effective neural-network algorithms of swarm interaction, elements of artificial intelligence, and technologies of learning and self-learning of UAV groups;

improvement of communication organisation systems and task-allocation algorithms within a UAV group;

development of an integrated system for group control, interaction and behavioural organisation of a UAV group during the execution of assigned tasks;

enhancement of the strength and service life of UAV structures through the development and use of polymer composite materials based on nanomodified infusion and adhesive compounds, as well as lattice composite load-bearing structures;

development of technical systems for safe thermal inspection (detection) of possible structural defects of UAVs, preventing damage to their composite skins during inspection;

development of technologies for the joint employmnt of UAVs and manned aircraft within the airspace;

enhancing resistance of UAV information channels to interference through ensuring their protection by means of quantum encryption technologies;

implementation of a modular design principle for UAVs, ensuring the compatibility of modules at structural, energy and information levels in order to provide UAVs with modernisation potential and maintain their required technical level during the operation phase with minimal costs.

Promising trends in UAV development (primarily single-use systems) should also include the

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

mastering and implementation of simplified manufacturing technologies (including the materials used), while preserving the main efficiency requirements in order to ensure mass production and the fastest possible delivery to the troops. This is expected to ensure the mass employment of UAVs as one of the key factors of their effectiveness (primarily due to the possibility of overloading the enemy air defence system and depleting its stocks of surface-to-air missiles as a result of prolonged attacks). One example is the domestically produced strike UAV "AQ 400 Scythe", "Kosa", developed by the company "Terminal Autonomy", the design of which is based on the concept of rapid and efficient production with minimised logistical costs while ensuring maximum functionality, making it a cost-effective instrument for military operations in terms of the "effectiveness–cost" criterion.

Discussions

For a comprehensive analysis, it is appropriate to consider relevant opinions and research findings of foreign specialists.

Sources [11], [12] provide data on the number of countries employing RSCs over a certain period. These data indicate a significant increase in unmanned and autonomous strike means (including UAVs) within RSCs employed at the operational level. For clarity of analysing these data, the authors of the article constructed a corresponding graph (Fig. 1) and diagrams (Fig. 2).

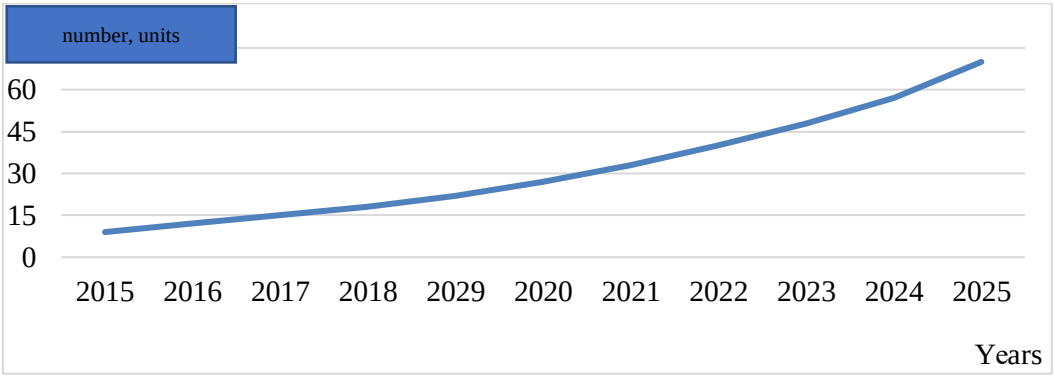


Figure 1. Dynamics of the increase in the number of states integrating RSCs into their armed forces during 2015–2025

The analysis of the data presented in Figs. 1 and 2 indicates a significant increase over the past 10 years in the number of states integrating RSCs into their armed forces, as well as a considerable growth in the share of strike UAVs and loitering munitions within these RSCs.

Researchers in [13] analyse the economic feasibility of single-use and reusable UAVs, which is important for shaping an effective composition of RSCs and optimising strike UAV systems. In publication [14], the authors consider the optimisation of task allocation among UAVs in multi-mission operations, which makes it possible to enhance the effectiveness of operational RSCs. Report [15] analyses the role of precision strikes in strategic confrontation, including the integration of UAVs, cruise missiles and information systems within operational-strategic RSCs. The authors in [16] developed a swarm control algorithm for UAVs intended for future highly autonomous RSCs, ensuring a high level of coordination. The current state of applying multi-agent models for the control of unmanned systems, which forms the basis for the development of autonomous RSCs, is presented by the author in [17]. Analytical review [18] provides an overview of global trends in the development of loitering munitions, which constitute one of the key strike components of modern RSCs. Study [19] offers an empirical analysis of the employment of russian loitering munitions, providing practical insight into the effectiveness of single-use strike UAVs under the conditions of modern warfare.

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

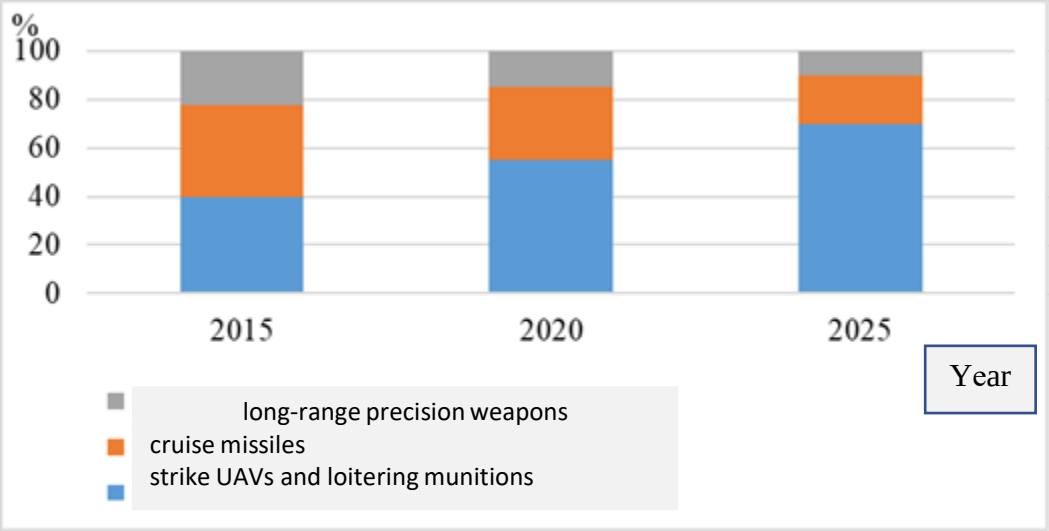


Figure 2. Proportion of strike means of different types (loitering munitions, cruise missiles, strike UAVs, long-range precision weapons) within RSCs

Conclusion

1. The conducted analysis confirmed that operational and operational-strategic level RSCs, created on the basis of UAVs, constitute one of the key elements of modern warfare and determine the character of armed struggle in the twenty-first century. Global trends indicate a transition from individual strike means to integrated network-centric systems in which UAVs of different classes, reconnaissance, command and control, and strike assets operate within a single information space. The obtained results make it possible to assert that the development of the specified RSCs should be based on the principles of asymmetric response to the enemy, priority of network-centric solutions, wide employment of artificial intelligence and swarm technologies, as well as close interaction between science, the defence-industrial complex and combat units.

2. It has been established that the dominant trend in the development of the specified RSCs is the increasing level of automation and autonomy through the implementation of elements of artificial intelligence, distributed control systems and swarm algorithms. This makes it possible to significantly shorten the “detection–identification–engagement” cycle, reduce the workload on operators and enhance the resilience of the complexes to the loss of individual elements under combat conditions. At the same time, the specified RSCs are developing in the direction of deep integration with automated troop command and control systems, as well as with other reconnaissance and fire engagement means of different basing (air, land and maritime). This increases the effectiveness of the employment of these RSCs and the flexibility of their use at the operational and operational-strategic levels.

3. The analysis of the development of UACs within the specified RSCs revealed a clear trend towards combining reusable strike platforms with single-use UAVs and loitering munitions. Such an approach ensures the possibility of employing RSCs in accordance with the operational-tactical situation based on an optimal “effectiveness–cost” ratio, creates conditions for overloading enemy air defence systems and increases the overall survivability of RSCs.

4. It has been determined that the development of UAVs within the specified RSCs is taking place along the lines of increasing range, speed, endurance and reduced detectability, as well as through a qualitative leap in the capabilities of onboard sensor systems. The integration of multispectral reconnaissance means, AESA radars, technical vision systems and machine learning

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

ensures increased target recognition accuracy and the effectiveness of UAV employment under conditions of active enemy electronic countermeasures. At the same time, it is important to ensure the simplification of UAV production technologies and the possibility of their rapid adaptation to changes in the operational-tactical situation. Examples of domestic developments demonstrate the expediency of focusing on serial production, modularity and rapid upgrading of UAV designs, taking into account real combat experience.

A further research direction may be the development of a methodological framework for substantiating the optimal composition of RSCs based on UAVs, taking into account their technological level, possible employment scenarios and economic constraints.

Recommendations

The practical value of the obtained results consists in the fact that they may be used for:

the development of state programmes for the advancement of armament and military equipment (in terms of the creation and modernisation of RSCs), the selection of priority topics for relevant research and development and experimental design work, and the formulation of appropriate technical solutions;

substantiation of operational-tactical and tactical-technical requirements for prospective RSCs created on the basis of UAVs, as well as for their components;

formation of the scientific and methodological basis of the educational process in higher military educational institutions and within the officer training system during the teaching of disciplines related to the development of armament and military equipment, etc.

Conflict of Interest

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

References

1. Substantiation of Operational and Tactical Requirements for a Reconnaissance-Strike Complex (Contour) Based on Unmanned Aerial Vehicles as Part of an Unmanned Aerial System. (2025). *Research Project Final Report. Central Research Institute of the Armed Forces of Ukraine.* Project Supervisor: D. O. Solomatin. Performers: A. A. Sedliar, O. I. Lutseviat, et al. Central Research Institute of the Armed Forces of Ukraine.
2. Hlushchenko, P. A., Samoilenko, O. V., & Zhevtiuk, O. A., et al. (2023). Retrospective Analysis and Trends in the Development of Unmanned Aerial Systems Considering Current Development Programs. *Collection of Scientific Papers of the State Aviation Research Institute, 19* (26), *231–244.* https://znp.dndia.org.ua.
3. Ishchenko, D. A., Strinada, V. V., & Levchenko, O. V. (2024). A Methodological Approach to Forming the Concept of a Reconnaissance–Strike Complex Based on the Analysis of Trends in Armed Struggle. *Collection of Scientific Papers of Zhytomyr Military Institute, 26* (11), *107–121.* https://znp.zvir.zt.ua.
4. Holovchenko, O. V., Stetsiuk, R. M., & Lisohor, B. V. (2024). Analysis of Lessons Learned from the Employment of Reconnaissance–Fire Complexes during the Repulsion and Deterrence of the Russian Federation's Large-Scale Armed Aggression against Ukraine. *International Scientific Journal Grail of Science, 37,* 114–121. https://archive.journal-grail.science.
5. Steshenko, P. M., Bohoslavets, S. O., Duzhyi, R. V., & Luzhbina, O. B. (2024). Scale of Combat Employment and Prospects for the Development of Strike Unmanned Aerial Systems of the Defense Forces of Ukraine. *Collection of Scientific Papers of the State Aviation Research Institute, 20* (27), 134–139. https://znp.dndia.org.ua.

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

6. Vishchun, I. V. (2021).The Need to Introduce Control and Decision-Making Systems Based on Artificial Intelligence into Unmanned Aerial Systems Armament. Proceedings of the All-Ukrainian Scientific and Technical Internet Conference, *Current Issues of Application, Operation, and Repair of Weapons and Military Equipment.* Department of Military Training. Vinnytsia National Technical University. https://conferences.vntu.edu.ua/index.php/apozbt/apozbt2021/paper/view/13980.
7. Yerylkin, A. H., Kruk, B. M., Korobetskyi, O. V., Puzhai-Chereda, S. K., & Kotliar, M. O. (2024). Substantiation of Proposals for Developing a Methodology for Selecting Unmanned Aerial Systems for the Defense Forces of Ukraine. *Collection of Scientific Papers of Ivan Kozhedub Kharkiv National Air Force University, 2* (80), 68–74. https://journal-hnups.com.ua.
8. Zhevtiuk, O. A., Samoilenko, O. V., & Mamonova, N. L. (2022). Prospects for the Development of Multicopter-Type Unmanned Aerial Systems in the Armed Forces of Ukraine. *Collection of Scientific Papers of the State Aviation Research Institute, 18* (25), 20–25. https://znp.dndia.org.ua.
9. Bezdelnyi, V. V., & Shevchenko, S. O. (2021). Analysis of Trends in the Development of Unmanned Aerial Vehicles with Hybrid Power Plants. *Air Power of Ukraine, Institute of Aviation and Air Defense, National Defence University of Ukraine, 1* (1), 83–84. https://sap.nuou.org.ua.
10. Kucherenko, Yu. F., Vlasik, S. M., Bespalko, O. V., & Salnyk, O. V. (2023). Analysis of the Use of Unmanned Aerial Vehicles in Modern Warfare and Key Measures for Countering Them. *Science and Technology of the Air Force of the Armed Forces of Ukraine, 2* (51), 38–45. https://journal-hnups.com.ua.
11. *The Military Balance 2024.* (2024). International Institute for Strategic Studies. https://www.iiss.org.
12. *The future of unmanned aerial systems in high-intensity conflict.* (2023). RAND Corporation. https://www.rand.org.
13. Dobbins, J., & Smith, A. (2021). *Comparing the cost-effectiveness of expendable versus reusable small unmanned aerial systems (RAND RR-2789).* RAND Corporation. https://www.rand.org/pubs/research_reports/RR2789.html. (rand.org).
14. Liu, B., et al. (2023). Task assignment of UAV swarms based on deep reinforcement learning. *Drones, 7* (5), 297. https://doi.org/10.3390/drones7050297. (MDPI).
15. Fayet, H., & Péria-Peigné, L. (2024). Deep precision strikes: A new tool for strategic competition? Focus stratégique, *121*. https://www.ifri.org/sites/default/files/2025-01/ifri_fayet_peria-peigne_deep_precision_strikes_2024.pdf. (IFRI).
16. Wei, Z., & Wei, R. (2024). UAV swarm rounding strategy based on deep reinforcement learning goal consistency with multi-head soft attention algorithm. *Drones, 8* (12), 731. https://doi.org/10.3390/drones8120731. (MDPI).
17. Ekechi, C. (2025). A survey on UAV control with multi-agent reinforcement learning: Trends and challenges. *Drones, 9* (7), 484. https://www.mdpi.com/2504-446X/9/7/484. (MDPI).
18. *Loitering munitions: Macroeconomic trends.* (2022). Army-Technology Analyst Comment. https://www.army-technology.com/analyst-comment/loitering-munitions-macroeconomic-trends/. (army-technology.com).
19. *Hit or miss: The Russian loitering munition kill list*. (2022). Oryx Open-Source Visual Verification. https://www.oryxspioenkop.com/2022/11/hit-or-miss-russian-loitering-munition.html. (Oryx).

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Аналіз світових тенденцій розвитку розвідувально-ударних комплексів оперативного (оперативно-стратегічного) рівня, що створюються на основі безпілотних літальних апаратів

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.@gmail.com
ORCID: 0000-0003-4165-3908

Сергій Попков
молодший науковий співробітник
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: popkov3151@gmail.com
ORCID: 0009-0003-3152-8246

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Анотація. Актуальність дослідження зумовлена зростанням ролі розвідувально-ударних комплексів оперативного та оперативно-стратегічного рівня в умовах сучасних збройних конфліктів, насамперед у контексті російсько-української війни, що супроводжується стрімким розвитком безпілотних авіаційних технологій, мережецентричних принципів управління та засобів високоточного ураження. У зв'язку із цим статтю спрямовано на комплексний аналіз світових тенденцій розвитку розвідувально-ударних комплексів на основі безпілотних літальних апаратів, визначення ключових напрямів еволюції їхніх складових та формування науково обґрунтованих пропозицій щодо перспектив розвитку таких комплексів з метою набуття асиметричної воєнно-технологічної переваги. Провідним підходом для дослідження зазначеної проблематики є системний та структурно-функціональний підходи у поєднанні з порівняльним і критично-аналітичним аналізом відкритих джерел, що дозволяє комплексно розглянути розвідувально-ударні комплекси як інтегровані багатокомпонентні системи, оцінити взаємозв'язок їхніх елементів і виявити провідні світові технологічні тренди. У статті визначено світові тенденції розвитку розвідувально-ударних комплексів оперативного (оперативно-стратегічного) рівня, що створюються на основі безпілотних літальних апаратів (як стосовно таких комплексів у цілому, так і стосовно їхніх складових); розкрито напрями підвищення автономності, мережевої взаємодії та ударних можливостей розвідувально-ударних комплексів; виявлено зростання ролі штучного інтелекту, ройових технологій і масових витратних безпілотних літальних апаратів; обґрунтовано доцільність переходу до модульних, серійних й економічно ефективних рішень. Матеріали статті становлять практичну цінність для фахівців у сфері оборонного планування, наукових і проєктних організацій оборонно-промислового комплексу, їх може бути використано під час формування вимог до перспективних розвідувально-ударних комплексів та обґрунтування напрямів їх подальшого розвитку.

Ключові слова: розвідувально-ударні комплекси; безпілотні літальні апарати; безпілотні авіаційні комплекси; оперативно-стратегічний рівень; штучний інтелект; ройові технології; мережецентричні системи; високоточне ураження; оборонні технології.

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Received: *December 4, 2025* | **Revisions Requested:** - | **Revision Received:** -
Accepted: *January 27, 2026* | **Published Online:** *April 10, 2026*

Licensed (C) by Creative Commons Attribution International License 4.0 (CC BY-NC-SA)

DOI: 10.62524/msj.2026.4.1.6

Визначення пріоритетних факторів впливу на ефективність функціонування системи кадрового менеджменту Збройних Сил України на основі методу інтерпретаційного структурного моделювання

Віктор Царинник
ад'юнкт
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: tsarynnykviktor@gmail.com
ORCID: 0009-0003-8638-6353

Сергій Баранов
начальник Головного управління розвитку спроможностей
ракетних військ і артилерії
Міністерство оборони України
003168, проспект Повітряних Сил, 6, Київ, Україна
e-mail: harada3699@gmail.com
ORCID: 0000-0002-3306-943X

Володимир Ремез
доктор філософії
доцент кафедри територіальної оборони
Національний університет оборони України
03049, проспект Повітряних Сил, 28, Київ, Україна
e-mail: remezv93145@gmail.com
ORCID: 0000-0002-2561-1081

Артем Васянович
начальник штабу 92 окремої штурмової бригади
імені кошового отамана Івана Сірка
63505, вул. Горішного, 142, Чугуїв, Харківська обл., Україна
e-mail: vas271296@ukr.net
ORCID: 0009-0004-3433-2035

Анотація. Актуальність дослідження зумовлена необхідністю підвищення ефективності функціонування системи кадрового менеджменту Збройних Сил України в умовах тривалої збройної агресії, обмеженості ресурсів і зростаючих вимог до якості підготовки та використання персоналу Збройних Сил України. Складність та багаторівневість зазначеної системи зумовлюють потребу в застосуванні сучасних методів стратегічного аналізу та структурування факторів впливу на її ефективність. Метою статті є визначення та ієрархізація факторів впливу на ефективність функціонування системи кадрового менеджменту Збройних

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Сил України на основі поєднання SWOT-аналізу та методу інтерпретаційного структурного моделювання. У статті здійснено аналіз існуючих підходів до оцінювання ефективності кадрового менеджменту, обґрунтовано доцільність використання SWOT-аналізу для формування множини факторів та методу інтерпретаційного структурного моделювання для встановлення структури взаємозв'язків між ними. Методологічну основу дослідження становлять системний аналіз, структурно-функціональний підхід, методи стратегічного аналізу та інтерпретаційного структурного моделювання. У результаті дослідження сформовано множину внутрішніх і зовнішніх факторів впливу, побудовано матрицю залежності та матрицю досяжності, а також визначено ранжовану ієрархію факторів. Встановлено, що ключовою системною проблемою функціонування системи кадрового менеджменту Збройних Сил України є відсутність інтегрованої методики оцінювання її ефективності, яка є фактором найвищого рівня в ієрархії. Отримані результати створюють методичну основу для подальшого розроблення інтегрованої системи показників оцінювання ефективності кадрового менеджменту. Матеріали статті можуть бути використані для удосконалення державної кадрової політики у секторі безпеки і оборони, а також розроблення методичних підходів до оцінювання ефективності функціонування системи кадрового менеджменту Збройних Сил України.

Ключові слова: кадровий менеджмент, персонал Збройних Сил України, ефективність функціонування, системний аналіз, SWOT-аналіз, інтерпретаційне структурне моделювання, ієрархія факторів.

Вступ (Introduction)

Ефективність функціонування системи кадрового менеджменту Збройних Сил України (СКМ ЗС України) є одним із ключових чинників забезпечення боєздатності військ, особливо в умовах тривалої збройної агресії та високої інтенсивності бойових дій. Водночас сучасні умови її функціонування характеризуються значною кількістю взаємопов'язаних внутрішніх і зовнішніх факторів, що суттєво впливають на результативність системи.

Підвищення ефективності функціонування СКМ ЗС України потребує системного підходу до визначення ключових факторів впливу та встановлення їхньої пріоритетності. Ідентифікація таких факторів дозволяє обґрунтовано визначити напрями удосконалення системи та сформувати методичну основу для оцінювання її ефективності.

Проблематика розвитку кадрового менеджменту у Збройних Силах України, удосконалення військової кадрової політики та підготовки персоналу знайшла відображення у працях вітчизняних науковців [1–5]. У зазначених дослідженнях розкрито підходи до правового забезпечення кадрових процесів, оцінювання ефективності діяльності кадрових органів, моніторингу функціонування системи, а також сформовано теоретичні засади та понятійно-термінологічний апарат кадрового менеджменту.

Разом із тим, відкриті наукові джерела не містять комплексних досліджень, спрямованих на визначення пріоритетних факторів впливу на ефективність функціонування СКМ ЗС України із застосуванням методів стратегічного аналізу, зокрема SWOT-аналізу у поєднанні з методом інтерпретаційного структурного моделювання (Interpretive Structural Modeling – ISM).

Отже, незважаючи на наявність значної кількості наукових праць, присвячених окремим аспектам функціонування СКМ ЗС України, питання системного визначення, структурування та ієрархізації факторів впливу залишаються недостатньо опрацьованими. Це зумовлює необхідність застосування методів стратегічного та структурного аналізу, які дозволяють не лише ідентифікувати ключові фактори, а й визначити характер взаємозв'язків між ними та рівень їхньої значущості для функціонування системи.

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Огляд літератури (Literature review)

Аналіз наукової літератури свідчить про наявність значної кількості досліджень, присвячених різним аспектам функціонування СКМ ЗС України, проте у них застосовуються різні методичні підходи до аналізу зазначеної проблематики.

Так, у роботі Ю. А. Гусака, Д. В. Кандуєва та Н. О. Корнейченка [1] проведено логіко-лінгвістичне моделювання процесу правового забезпечення кадрового менеджменту у Збройних Силах України в умовах правового режиму воєнного стану та сформовано систему логічних правил застосування правових норм. Водночас, дослідження зосереджене на формалізації правових процедур і не охоплює питання визначення пріоритетних факторів підвищення ефективності системи кадрового менеджменту. М. П. Думенко [2] пропонує методичний підхід до оцінювання ефективності функціонування системи кадрових органів Збройних Сил України, що базується на використанні системи показників і критеріїв оцінювання, однак у роботі не розглядається структурне моделювання взаємозв'язків факторів впливу. У дослідженні В. І. Гурковського, Є. О. Романенка, М. В. Андрусяка та Р. Ю. Русецького [3] розглянуто кадрову політику у Збройних Силах України крізь призму концепції управління інтелектуальним потенціалом та обґрунтовано необхідність раціонального використання фахівців із критичними компетенціями, проте не здійснюється формалізоване визначення пріоритетних факторів впливу. У роботі І. М. Половінкіна, А. В. Тристана, С. В. Сівкова та А. П. Мірончука [4] запропоновано підхід до визначення критеріїв і показників для моніторингу системи кадрового менеджменту в Міністерстві оборони України, однак дослідження обмежується формуванням системи показників і не враховує ієрархічну структуру взаємодії факторів. О. Семененко, В. Царинник, Л. Царинник та Н. Снапкова [5] досліджують понятійно-термінологічний апарат кадрового менеджменту Збройних Сил України та обґрунтовують теоретичні засади управління персоналом в умовах сучасних загроз, проте робота має переважно теоретичний характер і не передбачає аналізу структурних взаємозв'язків факторів.

Таким чином, проведений аналіз свідчить про те, що, попри ґрунтовне опрацювання окремих аспектів функціонування СКМ ЗС України, питання комплексного визначення, структурування та ієрархізації факторів впливу на її ефективність із застосуванням методу ISM залишаються недостатньо дослідженими. Це зумовлює актуальність подальших наукових досліджень у зазначеному напрямі. Водночас встановлено, що метод ISM уже застосовували у воєнній сфері, зокрема у дослідженні В. А. Горгуленка та Б. І. Коломійця [6], однак у контексті ведення кіберборотьби.

Методологічна основа (Methodological Framework)

Перш ніж визначати пріоритетні фактори впливу на ефективність функціонування системи кадрового менеджменту Збройних Сил України, доцільно уточнити сутність базового поняття "система", а також його інтерпретацію у контексті кадрового менеджменту.

Термін "система" походить від грецького systema – ціле, що складається з взаємопов'язаних частин. У загальному розумінні під системою слід розуміти сукупність елементів, об'єднаних стійкими зв'язками та взаємодіями, які забезпечують її цілісність, функціонування та розвиток [7]. Приклад системи наведено на рис. 1.

З огляду на це СКМ ЗС України може бути розглянуто як складну соціально-організаційну систему, що включає сукупність суб'єктів, процесів, ресурсів і механізмів управління персоналом, взаємопов'язаних між собою та спрямованих на забезпечення комплектування, розвитку, утримання і ефективного використання персоналу Збройних Сил України. Структурно-функціональну модель такої системи відображено на рис. 2.

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

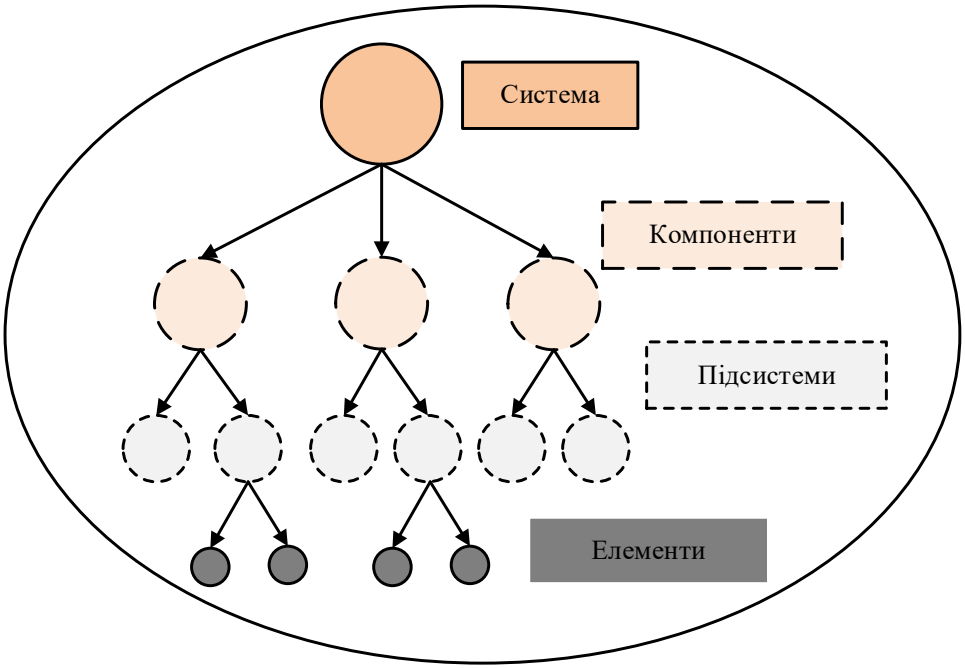


Рисунок 1. Приклад системи

Таким чином, СКМ ЗС України належить до класу складних (великих) систем. Визначальною ознакою таких систем є не їхній масштаб, а наявність сукупності взаємопов'язаних елементів, що функціонують як єдине ціле та утворюють інтегровану структуру управління. Особливістю складних систем є наявність багаторівневої структури, різнотипних зв'язків між елементами та їхня здатність до розвитку й адаптації під впливом зовнішніх і внутрішніх факторів. У цьому контексті СКМ ЗС України доцільно розглядати як динамічну систему, ефективність функціонування якої визначається не лише характеристиками окремих елементів, а й характером їхньої взаємодії.

У зв'язку із цим, ефективність функціонування СКМ ЗС України формується під впливом сукупності взаємопов'язаних факторів різної природи, які визначають як поточний стан системи, так і напрями її розвитку. До таких факторів належать організаційні, нормативно-правові, ресурсні, кадрові, освітні, соціально-психологічні, а також фактори зовнішнього середовища, зокрема безпекові та соціально-економічні умови функціонування держави.

Важливою особливістю зазначених факторів є їхній взаємозалежний характер: зміна одного із них може спричиняти трансформацію інших, що в цілому впливає на результативність функціонування СКМ ЗС України. Це зумовлює необхідність їх розгляду не як ізольованих елементів, а як складової єдиної системи впливів, що формують інтегральний ефект.

З огляду на це, для дослідження факторів впливу на ефективність функціонування СКМ ЗС України доцільним є застосування методів стратегічного аналізу, зокрема SWOT-аналізу, який дозволяє здійснити їх ідентифікацію та класифікацію, а також методу ISM, що забезпечує встановлення структури взаємозв'язків між факторами, визначення їхньої ієрархії та пріоритетності.

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

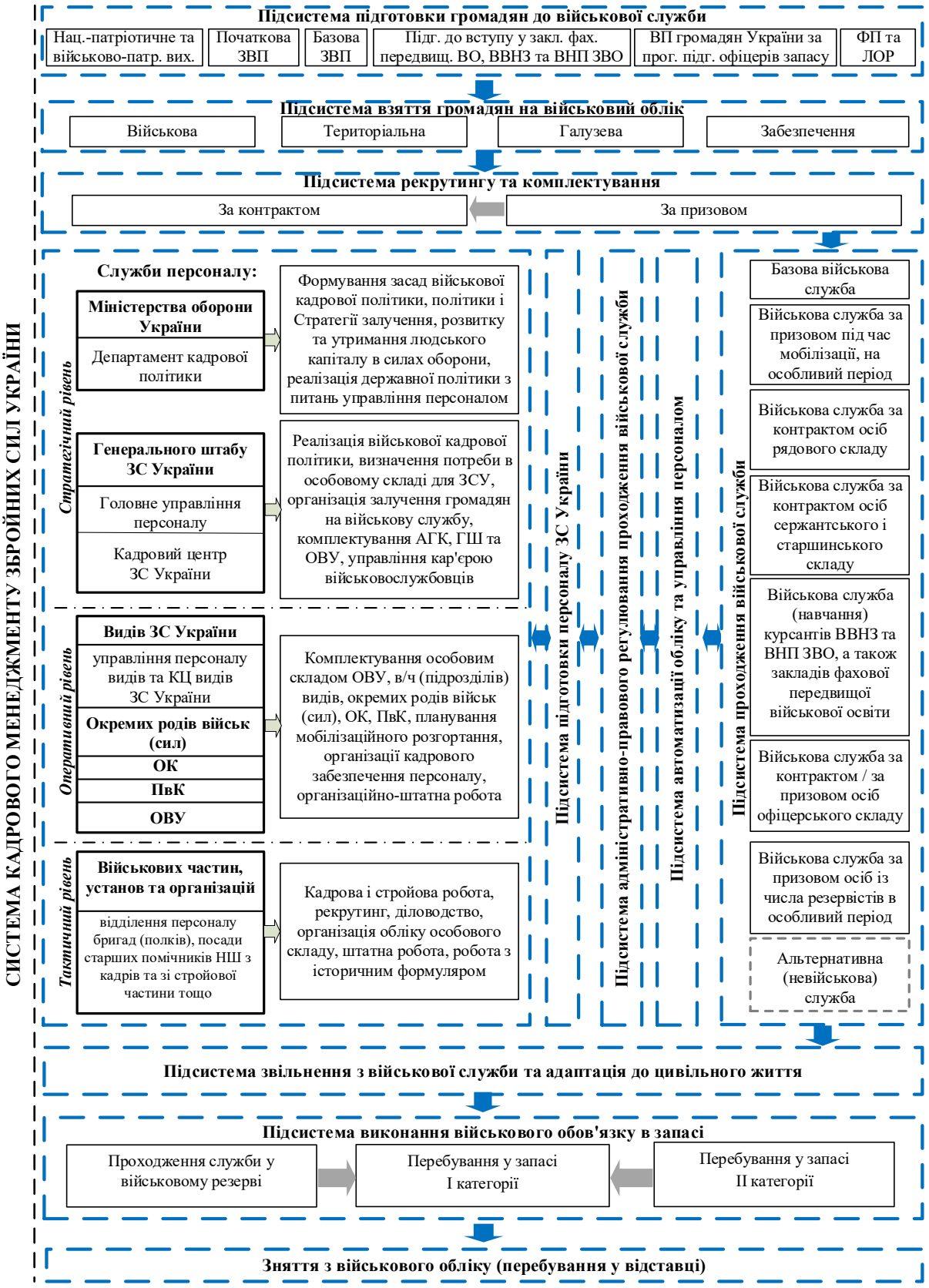


Рисунок 2. Структурно-функціональна модель СКМ ЗС України

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Застосування зазначених методів у комплексі дозволяє перейти від простого переліку факторів до їх системного упорядкування та формалізованого аналізу, що створює методичну основу для обґрунтування управлінських рішень щодо підвищення ефективності функціонування системи кадрового менеджменту Збройних Сил України.

Результати і обговорення (Results and Discussions)

Дослідження впливу факторів, зокрема визначення основних факторів та оцінювання їхньої пріоритетності, доцільно здійснювати у два етапи. На першому етапі необхідно сформувати множину факторів впливу на ефективність функціонування системи, насамперед тих, що відображають її проблемні аспекти. На другому етапі – виявити та розкрити фактори, вирішення яких є обґрунтовано першочерговим.

У межах першого етапу для пошуку та формулювання множини факторів пропонується застосувати метод SWOT-аналізу. Цей метод зарекомендував себе як дієвий інструмент стратегічного планування розвитку складних систем. Перевага SWOT-аналізу полягає в тому, що, на відміну від інших методів, які широко використовуються у дослідженні факторів впливу на ефективність функціонування систем, він передбачає диференціацію умов і чинників за категоріями: сильні (strengths) та слабкі (weaknesses) сторони – внутрішні фактори, можливості (opportunities) та загрози (threats) – зовнішні фактори. Така особливість дає змогу не лише сформувати перелік (множину) факторів, а й визначити характер їхнього впливу на ефективність функціонування СКМ ЗС України.

Результатом виконання другого етапу має стати ранжована ієрархія факторів впливу, в якій елементом найвищого рівня буде шуканий фактор (або фактори), усунення якого, з досить високою ймовірністю, є першочерговим для підвищення ефективності функціонування системи. Тобто йдеться про задачу ранжування та вибору альтернатив. Результативність і доцільність застосування для вирішення таких задач методу аналізу ієрархій (MAI), розробленого Т. Сааті [8–10], який за своєю сутністю є не лише одним із методів дослідження впливу факторів, а й потужним інструментом ранжування альтернатив та ухвалення складних багатокритеріальних рішень, підтверджується, зокрема, у роботах [11–13]. Разом із тим, у межах MAI ранжування альтернативних рішень здійснюється шляхом оцінювання ваги критеріїв, які, своєю чергою, є однаковими для кожної альтернативи. Альтернативами вирішення поставленого наукового завдання у цьому дослідженні є фактори впливу на ефективність функціонування СКМ ЗС України. Підібрати такі критерії оцінювання, які були б притаманні кожному із зазначених факторів, без викривлення та втрати їхнього змісту, є досить складно з огляду на їхню неоднорідність. Зважаючи на це, другий етап пропонується реалізувати за допомогою методу ISM [14–15].

Перший етап (SWOT-аналіз факторів). Загалом метод SWOT-аналізу використовується під час стратегічного планування для відповіді на три базових запитання, що виникають у процесі аналізу функціонування складної системи, а саме: з’ясування поточного стану системи шляхом оцінювання сильних і слабких сторін, можливостей та загроз; виокремлення сильних сторін і можливостей, які майбутній стан системи може використати, а також слабких сторін і загроз, які він може пом’якшити; ухвалення рішення щодо побудови стратегії зміни стану складної системи.

За результатами аналізу внутрішніх та зовнішніх факторів впливу на підвищення ефективності функціонування системи складено відповідну SWOT-матрицю (табл. 1).

Для визначення стратегії переведення СКМ ЗС України з поточного стану в необхідний, тобто у стан підвищеної ефективності, необхідно обрати одну з можливих стратегій, а саме:

стратегія S-O – акцент на сильні сторони для використання наявних можливостей;

стратегія W-O – подолання слабких сторін шляхом реалізації можливостей;

стратегія S-T – протидія загрозам за допомогою сильних сторін;

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

стратегія W-T – уникнення загроз і мінімізація слабких сторін.

Для подальшого дослідження факторів впливу на ефективність функціонування системи, з огляду на її раціональність, було обрано стратегію W-O.

Таблиця 1. SWOT-матриця факторів впливу на підвищення ефективності функціонування СКМ ЗС України

Внутрішні фактори	**Сильні сторони (Strengths)**		**Слабкі сторони (Weaknesses)**	
	S1	Наявність сформованої системи нормативно-правового регулювання кадрової політики у секторі безпеки і оборони	**W1**	Недостатня узгодженість військової кадрової політики з потребами військ
	S2	Наявність розгалуженої системи військової освіти та підготовки персоналу	**W2**	Недостатній рівень розвитку системи початкової загальновійськової підготовки громадян
	S3	Накопичений досвід кадрового забезпечення військ в умовах воєнного стану	**W3**	Дисбаланс структури підготовки військових фахівців
	S4	Функціонування системи управління кар'єрою персоналу Збройних Сил України	**W4**	Недостатня ефективність кадрового менеджменту у Збройних Силах України
	S5	Поступове впровадження стандартів НАТО у сфері управління персоналом	**W5**	Недостатня інтеграція інформаційних систем управління персоналом
	S6	Наявність інституційної бази для формування кадрового резерву	**W6**	Відсутність інтегрованої методики оцінювання ефективності СКМ
Зовнішні фактори	**Можливості (Opportunities)**		**Загрози (Threats)**	
	O1	Євроатлантична інтеграція України	**T1**	Висока інтенсивність бойових дій та втрати персоналу
	O2	Розвиток міжнародної військової освіти	**T2**	Демографічне скорочення мобілізаційного ресурсу держави
	O3	Цифровізація управління персоналом	**T3**	Висока конкуренція на ринку праці за висококваліфікованих фахівців
	O4	Розвиток військово-патріотичного виховання	**T4**	Тривалий характер війни та зростання навантаження на систему комплектування
	O5	Міжнародна допомога у підготовці персоналу	**T5**	Обмеженість фінансових ресурсів держави

Другий етап (побудова ранжованої ієрархії факторів). Вихідною множиною елементів для побудови ієрархії є внутрішні фактори – слабкі сторони поточного стану системи, а також зовнішні – можливості. Якщо зв'язки між елементами цієї множини H визначені, то описати її можна у вигляді спрямованого графа та квадратної бінарної матриці залежності B розмірністю $n \times n$, де n – кількість факторів, які є взаємозалежними між собою. Матриця B позначає наявність (або відсутність) залежності між складовими множини H факторів впливу на ефективність функціонування системи. Отже, елемент матриці залежності b_{ij}, $i = \overline{1,n}$ може приймати значення:

$$b_{ij} = \begin{cases} 1, \text{ якщо } i\text{-ий фактор впливає на } j\text{-ий;} \\ 0, \text{ якщо } i\text{-ий фактор не впливає на } j\text{-ий.} \end{cases} \quad (1)$$

Знаючи зв'язки між елементами множини H факторів впливу на підвищення ефективності функціонування системи та використовуючи вираз (1), можна сформувати матрицю залежності B (табл. 2).

Відповідно до побудованої матриці залежності складено спрямований граф

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

взаємозв'язків між елементами множини H факторів впливу на ефективність функціонування системи (рис. 3).

Таблиця 2. Матриця залежності факторів впливу на підвищення ефективності функціонування СКМ ЗС України

	W_1	W_2	W_3	W_4	W_5	W_6	O_1	O_2	O_3	O_4	O_5
W_1	0	0	0	0	0	1	0	0	0	0	0
W_2	0	0	0	0	0	1	0	0	0	0	0
W_3	0	0	0	0	0	1	0	0	0	0	0
W_4	0	0	0	0	0	1	0	0	0	0	0
W_5	0	0	0	1	0	0	0	0	0	0	0
W_6	0	0	0	0	0	0	0	0	0	0	0
O_1	1	1	0	0	0	0	0	0	0	0	0
O_2	0	0	1	1	0	0	0	0	0	0	0
O_3	0	0	0	0	1	0	0	0	0	0	0
O_4	0	0	0	0	0	0	1	0	0	0	0
O_5	0	0	0	0	0	0	0	1	0	0	0

Наступним кроком є побудова бінарної матриці досяжності (I+B) відповідній матриці B розмірності. Це можна реалізувати шляхом піднесення її у деякий степінь k, за якого виконуватиметься рівність:

$$(I + B)^{k-1} \leq (I + B)^k = (I + B)^{k+1}, \quad (2)$$

де: I – одинична матриця;

$(I + B)^k = (I + B)^{k+1}$ – матриця досяжності.

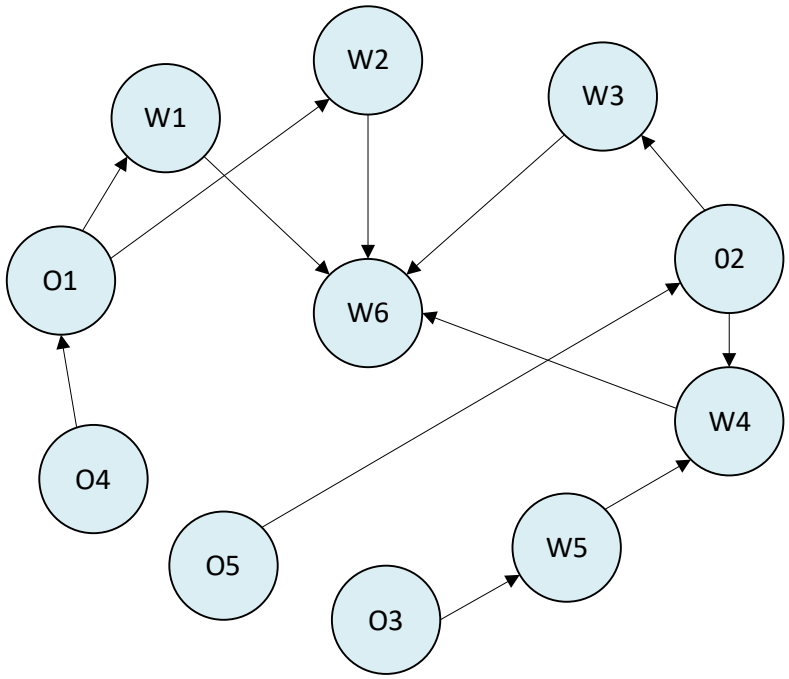


Рисунок 3. Спрямований граф взаємозв'язків між факторами

Сформувати матрицю досяжності можна й іншим шляхом, за допомогою спрямованого графа (рис. 3). У такому разі елементи матриці досяжності d_{ij}, $i = \overline{1,n}$, прийматимуть значення:

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

$$d_{ij} = \begin{cases} 1, \text{ якщо з } i\text{-го є маршрут до } j\text{-го;} \\ 0, \text{ якщо з } i\text{-го немає маршруту до } j\text{-го.} \end{cases} \quad (3)$$

За обома наведеними варіантами побудови матриці досяжності за незмінних вихідних даних її зміст буде однаковим (табл. 3).

Таблиця 3. Матриця досяжності факторів впливу на підвищення ефективності функціонування СКМ ЗС України

	W_1	W_2	W_3	W_4	W_5	W_6	O_1	O_2	O_3	O_4	O_5
W_1	1	0	0	0	0	1	0	0	0	0	0
W_2	0	1	0	0	0	1	0	0	0	0	0
W_3	0	0	1	0	0	1	0	0	0	0	0
W_4	0	0	0	1	0	1	0	0	0	0	0
W_5	0	0	0	1	1	1	0	0	0	0	0
W_6	0	0	0	0	0	1	0	0	0	0	0
O_1	1	1	0	0	0	1	1	0	0	0	0
O_2	0	0	1	1	0	1	0	1	0	0	0
O_3	0	0	0	1	1	1	0	0	1	0	0
O_4	1	1	0	0	0	1	1	0	0	1	0
O_5	0	0	1	1	0	1	0	1	0	0	1

Шукана ранжована ієрархія факторів впливу на ефективність функціонування системи може бути побудована на основі матриці досяжності шляхом поділу вершин спрямованого графа (факторів) на підмножини рівнів.

Для цього необхідно в ітеративному порядку визначати досяжні $R(h_i)$ й попередні $A(h_i)$ вершини для кожного фактора (табл. 4).

Таблиця 4. Перша ітерація побудови ранжованої ієрархії факторів впливу на підвищення ефективності функціонування СКМ ЗС України

h_i	$R(h_i)$	$A(h_i)$	$R(h_i) \cap A(h_i)$
W_1	W_1, W_6	W_1, O_1, O_4	W_1
W_2	W_2, W_6	W_2, O_1, O_4	W_2
W_3	W_3, W_6	W_3, O_2, O_5	W_3
W_4	W_4, W_6	W_4, W_5, O_2, O_3, O_5	W_4
W_5	W_4, W_5, W_6	W_5, O_3	W_5
W_6	W_6	$W_1, W_2, W_3, W_4, W_5, W_6, O_1, O_2, O_3, O_4, O_5$	W_6
O_1	W_1, W_2, W_6, O_1	O_1, O_4	O_1
O_2	W_3, W_4, W_6, O_2	O_2, O_5	O_2
O_3	W_4, W_5, W_6, O_3	O_3	O_3
O_4	W_1, W_2, W_6, O_1, O_4	O_4	O_4
O_5	W_3, W_4, W_6, O_2, O_5	O_5	O_5

До першої ітерації належать: O_3, O_4, O_5.

На кожному кроці ітерації факторами поточного рівня будуть ті, для яких виконуватиметься рівність:

$$A(h_i) = R(h_i) \cap A(h_i). \quad (4)$$

Тобто рівнем ієрархії вважатимемо множину тих вершин, які є недосяжними з решти вершин множини H.

Після вилучення O_3, O_4, O_5 залишаються $W_1, W_2, W_3, W_4, W_5, W_6, O_1, O_2$ (табл. 5).

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Таблиця 5. Друга ітерація побудови ранжованої ієрархії факторів впливу

h_i	$R(h_i)$	$A(h_i)$	$R(h_i) \cap A(h_i)$
W1	W_1, W_6	W_1, O_1	W_1
W2	W_2, W_6	W_2, O_1	W_2
W3	W_3, W_6	W_3, O_2	W_3
W4	W_4, W_6	W_4, W_5, O_2	W_4
W5	W_4, W_5, W_6	W_5	W_5
W6	W_6	$W_1, W_2, W_3, W_4, W_5, W_6, O_1, O_2$	W_6
O1	W_1, W_2, W_6, O_1	O_1	O_1
O2	W_3, W_4, W_6, O_2	O_2	O_2

До другої ітерації належать: W_5, O_1, O_2.

Третю та четверту ітерації побудови ранжованої ієрархії факторів впливу наведено, відповідно, у табл. 6 та 7.

Таблиця 6. Третя ітерація побудови ранжованої ієрархії факторів впливу

h_i	$R(h_i)$	$A(h_i)$	$R(h_i) \cap A(h_i)$
W1	W_1, W_6	W_1	W_1
W2	W_2, W_6	W_2	W_2
W3	W_3, W_6	W_3	W_3
W4	W_4, W_6	W_4	W_4
W6	W_6	W_1, W_2, W_3, W_4, W_6	W_6

До третьої ітерації належать: W_1, W_2, W_3, W_4.

Таблиця 7. Четверта ітерація побудови ранжованої ієрархії факторів впливу

h_i	$R(h_i)$	$A(h_i)$	$R(h_i) \cap A(h_i)$
W6	W_6	W_6	W_6

До четвертої ітерації належать: W_6.

За результатами ітераційної процедури побудови ранжованої ієрархії встановлено, що в порядку послідовного вилучення першими вилучаються фактори O_3, O_4, O_5, далі – W_5, O_1, O_2, після чого – W_1, W_2, W_3, W_4, а завершальним фактором є W_6. Водночас, методом ISM у процесі ітераційного аналізу першими визначаються фактори, які не мають подальших залежностей у межах розглядуваної системи. Тобто на кожному кроці алгоритм визначає фактори поточного рівня ієрархії, після чого вони вилучаються з подальшого аналізу. Тому для представлення підсумкової ієрархії в аналітичному вигляді рівні доцільно подати у зворотному порядку, тобто від узагальнювального системного фактора до базових факторів, що формують умови його виникнення (рис. 4).

Таким чином, на основі матриці залежності факторів побудовано спрямований граф взаємозв'язків та матрицю досяжності факторів впливу на підвищення ефективності функціонування СКМ ЗС України. Подальше застосування ітераційної процедури побудови ранжованої ієрархії дало змогу виділити чотири рівні факторів. До першого рівня належить фактор W_6 – відсутність інтегрованої методики оцінювання ефективності СКМ, який є узагальнювальним системним фактором. Другий рівень становлять фактори W_1, W_2, W_3, W_4, що безпосередньо характеризують проблемні аспекти функціонування підсистем СКМ. До третього рівня належать W_5, O_1, O_2, які формують проміжний рівень впливу на слабкі сторони

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

системи. Четвертий рівень представлено факторами O_3, O_4, O_5, що відображають зовнішні можливості та вихідні умови розвитку системи.

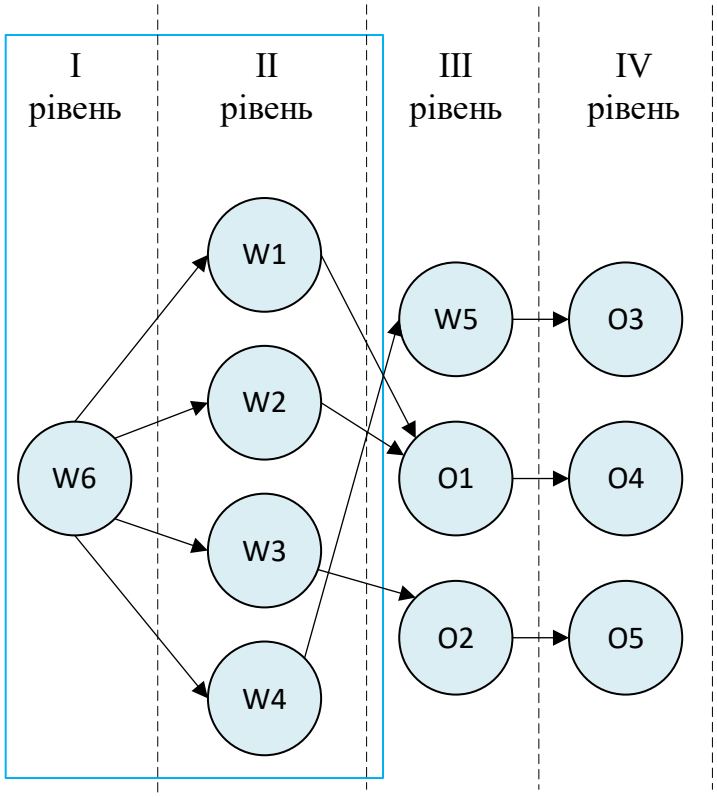


Рисунок 4. Ранжована ієрархія факторів впливу на підвищення ефективності функціонування СКМ ЗС України

Отримана ієрархія відображає причинно-наслідкову структуру факторів та створює логічне підґрунтя для подальшого розроблення інтегрованої методики оцінювання ефективності СКМ ЗС України.

Основною системною проблемою функціонування СКМ ЗС України є відсутність інтегрованої методики оцінювання її ефективності (фактор W6), що підтверджується результатами побудови ранжованої ієрархії факторів впливу. Разом із тим, встановлено, що до другого рівня ієрархії належать фактори W1, W2, W3, W4, які відображають ключові напрями функціонування системи кадрового менеджменту, зокрема реалізацію військової кадрової політики, розвиток системи початкової загальновійськової підготовки громадян, підготовку військових фахівців у системі військової освіти та ефективність кадрового менеджменту у Збройних Силах України.

Зазначені фактори формують основні проблемні напрями функціонування СКМ та безпосередньо впливають на рівень її ефективності. Тому саме їх має бути покладено в основу формування системи показників оцінювання ефективності функціонування СКМ ЗС України. У зв’язку із цим, у подальшому дослідженні акцент необхідно робити на розробленні інтегрованої методики оцінювання, яка передбачатиме визначення часткових інтегральних показників ефективності за відповідними напрямами функціонування системи.

Таким чином, на підставі результатів побудови ієрархії факторів не лише визначено ключову системну проблему функціонування СКМ ЗС України, а й обґрунтовано вибір основних напрямів формування системи показників оцінювання її ефективності.

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Висновок (Conclusion)

Наукова новизна дослідження полягає у тому, що вперше для системи кадрового менеджменту Збройних Сил України на основі поєднання SWOT-аналізу та методу ISM визначено, структуровано та ієрархізовано фактори впливу на ефективність її функціонування, що дало змогу виокремити системотвірний фактор та обґрунтувати напрями формування інтегрованої методики оцінювання.

У результаті застосування SWOT-аналізу сформовано множину внутрішніх і зовнішніх факторів, що відображають сильні та слабкі сторони системи, а також можливості й загрози її розвитку. Подальше використання методу ISM дало змогу встановити причинно-наслідкові зв'язки між факторами та побудувати їхню ранжовану ієрархію.

Визначено, що основною системною проблемою функціонування СКМ ЗС України є відсутність інтегрованої методики оцінювання її ефективності, яка є узагальнювальним фактором найвищого рівня. Водночас встановлено, що фактори другого рівня (узгодженість кадрової політики, розвиток системи підготовки персоналу, структура підготовки фахівців та ефективність кадрового менеджменту) формують ключові напрями впливу на результативність системи.

Отримані результати дозволяють обґрунтувати напрями подальшого удосконалення СКМ ЗС України та створюють методичну основу для формування системи показників оцінювання її ефективності.

Рекомендації (Recommendations)

Матеріали статті доцільно використовувати органами військового управління для обґрунтування та реалізації військової кадрової політики, а також ухвалення управлінських рішень щодо підвищення ефективності функціонування системи кадрового менеджменту Збройних Сил України. Отримані результати рекомендується застосовувати під час розроблення інтегрованої методики оцінювання ефективності системи кадрового менеджменту, зокрема під час формування системи часткових інтегральних показників за основними напрямами її функціонування. Запропонований підхід може бути використано у діяльності наукових установ та закладів військової освіти для проведення досліджень, розроблення методичного забезпечення та підготовки персоналу Збройних Сил України.

Реалізація результатів дослідження сприятиме підвищенню обґрунтованості управлінських рішень, удосконаленню кадрового забезпечення та зміцненню кадрового потенціалу Збройних Сил України.

Конфлікт інтересів (Conflict of Interest)

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

Використані джерела

1. Гусак, Ю. А., Кандуєв, Д. В. & Корнейченко, Н. О. (2025). Логіко-лінгвістична модель процесу правового забезпечення кадрового менеджменту у Збройних Силах України в умовах правового режиму воєнного стану. *Сучасні інформаційні технології у сфері безпеки та оборони, 3* (54), 62–74.
2. Думенко, М. П. (2024). Метод оцінювання ефективності функціонування системи кадрових органів Збройних Сил України. *Сучасні інформаційні технології у сфері безпеки та оборони, 1* (49), 128–140.
3. Гурковський, В. І., Романенко, Є. О., Андрусяк, М. В. & Русецький, Р. Ю. (2025). Кадрова політика у Збройних Силах України: концепція управління інтелектуальним потенціалом. *Military Strategy and Technology, 3* (3), 39–49.
4. Половінкін, І. М., Тристан, А. В., Сівков, С. В. & Мірончук, А. П. (2025). Визначення

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

критеріїв і показників для проведення моніторингу системи кадрового менеджменту в Міністерстві оборони України. *Зб. наук. пр. Центру воєнно-стратегічних досліджень Нац. ун-ту оборони України*, *1* (84), 118–125.
5. Семененко, О., Царинник, В., Царинник, Л. & Снапкова, Н. (2024). Кадровий менеджмент Збройних Сил України в контексті сучасних загроз та викликів: понятійно-термінологічний апарат. *Military Science*, *2* (3), 41–63.
6. Горгуленко, В. А. & Коломієць, Б. І. (2025). Фактори впливу на ефективність ведення кіберборотьби в інтересах застосування збройних сил. *Сучасні інформаційні технології у сфері безпеки та оборони*, *2* (53), 51–59.
7. Колектив авторів. (2024). *Основи теорії досліджень ефективності системи кадрового менеджменту у військовій сфері*. НУОУ.
8. Saaty, T. L. (1979). Applications of analytical hierarchies. *Mathematics and Computers in Simulation*, *21* (1), 1–20.
9. Saaty, T. L. (1991). Some mathematical concepts of the analytic hierarchy process. *Behaviormetrika*, *29* (18), 1–9.
10. Saaty, T. L. (2008). The analytic hierarchy and analytic network measurement processes: Applications to decisions under risk. *European Journal of Pure and Applied Mathematics*, *1* (1), 122–196.
11. Potomkin, M. M., Semenenko, O. M., Kliat, Y. O. & Sedliar, A. A. (2024). Comparing the results of alternative ranking obtained by several variants of the analytic hierarchy process. *Cybernetics and Systems Analysis*, *60*, 970–977.
12. Потьомкін, М. М., Седляр, А. А., Дейнега, О. В. & Зварич, А. О. (2021). Комплексне використання принципу Парето та методу аналізу ієрархій для підвищення обґрунтованості результатів ранжування альтернатив. *Кібернетика та системний аналіз*, *3* (57).
13. Вартанян, В. М. & Штейнбрехер, Д. О. (2019). Застосування методу аналізу ієрархій для побудови стратегії управління знаннями високотехнологічних проектів. *Радіоелектронні і комп'ютерні системи*, *2* (90).
14. Warfield, J. N. (1974). Developing interconnected matrices in structural modeling. *IEEE Transactions on Systems, Man and Cybernetics*, *4* (1), 81–87.
15. Warfield, J. N. (1976). *Societal systems: Planning, policy and complexity*. Wiley.

References

1. Husak, Yu. A., Kanduev, D. V., & Korneichenko, N. O. (2025). Logical-linguistic model of the legal support process of personnel management in the Armed Forces of Ukraine under martial law conditions. *Modern Information Technologies in the Sphere of Security and Defence*, *3* (54), 62–74.
2. Dumenko, M. P. (2024). Method for evaluating the effectiveness of the personnel bodies system functioning in the Armed Forces of Ukraine. *Modern Information Technologies in the Sphere of Security and Defence*, *1* (49), 128–140.
3. Hurkovskyi, V. I., Romanenko, Ye. O., Andrusiak, M. V., & Rusetskyi, R. Yu. (2025). Personnel policy in the Armed Forces of Ukraine: Concept of intellectual potential management. *Military Strategy and Technology*, *3* (3), 39–49.
4. Polovinkin, I. M., Trystan, A. V., Sivkov, S. V., & Mironchuk, A. P. (2025). Determination of criteria and indicators for monitoring the personnel management system in the Ministry of Defence of Ukraine. *Collection of Scientific Works of the Center for Military Strategic Studies of the National Defence University of Ukraine*, *1* (84), 118–125.
5. Semenenko, O., Tsarynnyk, V., Tsarynnyk, L., & Snapkova, N. (2024). Personnel management of the Armed Forces of Ukraine in the context of modern threats and challenges: Conceptual

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

and terminological framework. *Military Science, 2* (3), 41–63.
6. Horhulenko, V. A., & Kolomiiets, B. I. (2025). Factors influencing the effectiveness of cyber warfare in the interests of the use of the armed forces. *Modern Information Technologies in the Sphere of Security and Defence, 2* (53), 51–59.
7. Collective of authors. (2024). *Fundamentals of the theory of research on the effectiveness of personnel management systems in the military sphere*. National Defence University of Ukraine.
8. Saaty, T. L. (1979). Applications of analytical hierarchies. *Mathematics and Computers in Simulation, 21* (1), 1–20.
9. Saaty, T. L. (1991). Some mathematical concepts of the analytic hierarchy process. *Behaviormetrika, 29* (18), 1–9.
10. Saaty, T. L. (2008). The analytic hierarchy and analytic network measurement processes: Applications to decisions under risk. *European Journal of Pure and Applied Mathematics, 1* (1), 122–196.
11. Potomkin, M. M., Semenenko, O. M., Kliat, Y. O., & Sedliar, A. A. (2024). Comparing the results of alternative ranking obtained by several variants of the analytic hierarchy process. *Cybernetics and Systems Analysis, 60*, 970–977.
12. Potomkin, M. M., Sedliar, A. A., Deineha, O. V., & Zvarych, A. O. (2021). Complex use of the Pareto principle and the analytic hierarchy process for improving the validity of alternative ranking results. *Cybernetics and Systems Analysis, 3* (57).
13. Vartanian, V. M., & Shteinbrekher, D. O. (2019). Application of the analytic hierarchy process for building knowledge management strategy of high-tech projects. *Radioelectronic and Computer Systems, 2* (90).
14. Warfield, J. N. (1974). Developing interconnected matrices in structural modeling. *IEEE Transactions on Systems, Man and Cybernetics, 4* (1), 81–87.
15. Warfield, J. N. (1976). *Societal systems: Planning, policy and complexity*. Wiley.

Identification of priority factors influencing the functioning effectiveness of the personnel management system within the Armed Forces of Ukraine based on the interpretive structural modelling method

Viktor Tsarynnyk
Adjunct
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl Avenue, 28 B, Kyiv, Ukraine
e-mail: tsarynnykviktor@gmail.com
ORCID: 0009-0003-8638-6353

Serhii Baranov
Head of the Main Directorate for the
Development of Missile Forces and Artillery Capabilities
Ministry of Defense of Ukraine
03168, Povitrianykh syl avenue, 6, Kyiv, Ukraine
e-mail: harada3699@gmail.com
ORCID: 0000-0002-3306-943X

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Volodymyr Remez
Doctor of Philosophy
Associate Professor of the Territorial Defense Chair
National Defence University of Ukraine
03049, Povitrianykh Syl avenue, 28, Kyiv, Ukraine
e-mail: remezv93145@gmail.com
ORCID: 0000-0002-2561-1081

Artem Vasianovych
Chief of Staff of the 92nd Separate Assault Brigade
named after the Kosh Ataman Ivan Sirko
63505, Horishnogo St., 142, Chuguev, Kharkiv Oblast, Ukraine
e-mail: vas271296@ukr.net
ORCID: 0009-0004-3433-2035

Abstract. The relevance of the study is determined by the need to enhance the effectiveness of the personnel management system of the Armed Forces of Ukraine under the conditions of prolonged armed aggression, limited resources, and increasing requirements for the quality of training and deployment of personnel of the Armed Forces of Ukraine. The complexity and multi-level nature of this system determine the need to apply modern methods of strategic analysis and structuring of factors influencing its effectiveness. The aim of the article is to identify and hierarchise the factors influencing the effectiveness of the personnel management system of the Armed Forces of Ukraine based on a combination of SWOT analysis and the interpretive structural modelling (ISM) method. The article analyses existing approaches to assessing personnel management effectiveness and substantiates the expediency of using SWOT analysis to form a set of factors and the ISM method to establish the structure of interrelationships among them. The methodological basis of the study comprises system analysis, a structural-functional approach, methods of strategic analysis, and interpretive structural modelling. As a result of the study, a set of internal and external influencing factors has been formed, a dependency matrix and a reachability matrix have been constructed, and a ranked hierarchy of factors has been determined. It has been established that the key systemic problem in the functioning of the personnel management system of the Armed Forces of Ukraine is the absence of an integrated methodology for assessing its effectiveness, which constitutes the highest-level factor in the hierarchy. The obtained results provide a methodological basis for the further development of an integrated system of indicators for assessing personnel management effectiveness. The materials of the article may be used to improve state personnel policy in the security and defence sector, as well as in the development of methodological approaches to assessing the effectiveness of the functioning of the personnel management system of the Armed Forces of Ukraine.

Keywords: personnel management, personnel of the Armed Forces of Ukraine, functioning effectiveness, system analysis, SWOT analysis, interpretive structural modelling, ISM, factor hierarchy.

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Received: *October 8, 2025* | **Revisions Requested:** - | **Revision Received:** -
Accepted: *December 1, 2025* | **Published Online:** *April 10, 2026*

Licensed (C) by Creative Commons Attribution International License 4.0 (CC BY-NC-SA)

DOI: 10.62524/msj.2026.4.1.7

Methodological Approach to Creating a Cyber Defence Terminology System

Svitlana Zvarych
PhD of Technical Sciences, 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: zvarych.ss@gmail.com
ORCID: 0000-0002-0636-250X

Olexandr Trokhymenko
Senior Research Fellow
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl Avenue, 28 B, Kyiv, Ukraine
e-mail: tvo1978@ukr.net
ORCID: 0009-0008-8574-3757

Andrii Vorobyov
Senior Research Fellow
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl Avenue, 28 B, Kyiv, Ukraine
e-mail: atmssw@gmail.com
ORCID: 0000-0002-1689-3128

Tetiana Poberezhets
Senior Research Fellow
Military Institute of Telecommunications and Informatization
named after Heroes of Kruty
e-mail: tetiana.poberezhets@viti.edu.ua
ORCID: 0000-0001-8007-8614

Yuliia Kotiukh
Senior Research Fellow
Military Institute of Telecommunications and Informatization
named after Heroes of Kruty
e-mail: jul365@ukr.net
ORCID: 0009-0002-4511-9905

Abstract. The relevance of the study is determined by the recognised problem of heterogeneity and fragmentation of the cyber defence terminology in Ukraine. The lack of a unified, systematic terminology hinders effective interagency communication, the development of organizational and regulatory documentation, and operational coordination in countering cyber threats. The

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

interdisciplinary nature of cyber defence, which encompasses national security, technology, law, and other fields, reinforces the need to unify the conceptual apparatus. Until now, this area has been studied selectively, without considering terminology as a coherent system. The purpose of this article is to highlight a methodological approach to creating a cyber defense terminology system. The methodological basis of the work is the theoretical foundations of terminology, in particular the distinction between the concepts of "terminology" (as a spontaneously formed set of terms) and "terminology system" (as a consciously ordered, coherent, and structured system of concepts based on a specific concept). An analysis of the current state of cyber defence in Ukraine shows that, in parallel with the development of the cyber defence system itself, cyber defence terminology is in the process of active formation and is undergoing stages of coordination and consolidation in scientific publications and legislative acts. A methodological approach is proposed, which consists in systematising and structuring the existing terminological fund to give it the characteristics of a coherent terminology system. Following this approach, key components have been identified that form the basis of the terminology system structure. The proposed model consists of six main subsystems (groups of terms): fundamental terms and concepts, cyber defence objects, cyber threats and vulnerabilities, the functioning of the cyber defence system and its components, cyber defence entities, as well as the legal and regulatory environment. It is noted that the cyber defence terminology system is synthetic in nature, integrating concepts in the fields of information technology, politics, economics, law, and defence. The proposed methodological approach has made it possible to create a comprehensive and structured terminology system that allows for the unambiguous classification of any term related to cyber defence. It is emphasised that this system is not static and will evolve along with changes in technologies and forms of cyber warfare. The practical value of the research results lies in the development of methodological recommendations for the further formation and improvement of terms based on the principles of consistency and unambiguous interpretation, which will contribute to ensuring effective communication and cooperation between different sectors and their operational coordination in the field of cyber defence.

Keywords: term, terminology, terminological system, cyber defence.

Introduction

In the scientific and legal environment of the global community, debates have long persisted regarding the explanation of the phenomenon of cyberspace, its incorporation into the framework of international law, and the establishment of mechanisms for controlling its development and protection against negative manifestations. A key challenge remains the absence of a universally accepted terminological framework in the field of cyberspace, which should eliminate the possibility of "grey areas" in the forms and methods of employing its actors and means. Over recent decades, certain definitions of terms and concepts have already been formed and stabilised within the information space; however, their interpretation and understanding require harmonisation in accordance with unified standards.

The inconsistency of cybersecurity and cyber defence terminology is a recognised problem [1]. The lack of a unified terminology in the cyber domain hinders effective communication, the development of organisational and regulatory documentation, and operational coordination, which may potentially lead to ambiguity and misunderstandings, resulting in inadequate or ineffective response strategies. The interdisciplinary nature of cyber defence, encompassing national security (including cybersecurity), technology, law, and other domains, also necessitates the establishment of a unified terminological system.

At present, the terminological framework of cyber defence in Ukraine has been studied only fragmentarily. Certain aspects have been addressed by linguists [1]–[4] as well as by specialists in relevant fields [5]–[9]. At the same time, issues and theoretical foundations related to the development

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

of the terminological framework as an integrated system have not been comprehensively examined. Therefore, in our view, the study of the terminological system of cyber defence constitutes a relevant scientific task.

The aim of this article is to present a methodological approach to the development of a terminological system for cyber defence.

Methodological Framework

For a better understanding of the subsequent material, it is appropriate to provide an overview of terminology studies, which examine terms, terminologies, and terminological systems. These categories will be analysed specifically in the context of cyber defence.

The concept of "terminology" is understood as the entire set of terms that has developed "spontaneously" within a particular field of scientific knowledge [2]. Terminologies emerge simultaneously with the establishment of a field of knowledge or activity and evolve (expand) in parallel with it. At a certain stage of development, after the accumulation of a sufficient level of experience and/or knowledge, a period of stabilisation occurs. At the same time, the process of quantitative accumulation of terms ceases and transitions into a qualitative phase namely, their generalisation and organisation into a terminological system.

A terminological system is defined as a system of terms within a particular field (or subfield) of knowledge that serves a scientific theory or conceptual framework [2].

Terminological systems originate from terminologies. However, unlike terminology, a terminological system is formed discretely, as a result of the completion and achievements of a particular stage in the development of a theory or theories within a given field. At the same time, a terminological system does not necessarily have to be based strictly on a scientific theory; in some cases, a concept or a generalised idea may be sufficient [2,3]. Thus, it can be concluded that a terminological system is formed at a certain stage in the development of a field of scientific knowledge, when a scientific theory has been established and the objects and relationships between them have been defined.

Terminological systems are characterised by the presence of the following typical features [2]:

- integrity;
- correspondence between the sum of parts and the whole;
- a certain degree of stability;
- a structured nature.

Taken together, these features allow a terminological system to be considered complete.

Results

At present, the cyber defence system of Ukraine is only partially formed. Alongside its further development, its terminology is also evolving. It is being tested in practice, discussed in academic publications [6]–[9], and agreed terms and their definitions are formalised through legislative acts at various levels [10]–[12]. However, even at this stage, the existing terminological system provides opportunities for the systematisation and refinement of current terms, as well as for the creation of new ones.

In order to capture the current state of development of the cyber defence terminological system, it is proposed, at this stage, to utilise the existing terminology, classify it into groups according to specific characteristics, and subsequently integrate these groups to ensure the structured nature and integrity of the system being developed. This approach will ensure that the emerging system complies with the fundamental characteristics of a terminological system. New terms that arise in the future will be assigned to the relevant group or will form new ones. In this way, the cyber defence terminological system will be closely linked to the cyber defence system itself and will serve to describe it.

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Thus, in accordance with the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine" [11], cyber defence is defined as a set of political, economic, social, military, scientific, scientific-technical, informational, legal, organisational, and other measures implemented in cyberspace and aimed at ensuring the protection of state sovereignty and defence capability, preventing the outbreak of armed conflict, and repelling armed aggression.

An analysis of this definition indicates the presence of threats in/through cyberspace, the sources of such threats, the tools of cyber influence and cyber protection, the objects requiring cyber protection, and the actors responsible for providing it, as well as the possibility of their functioning in both peacetime and wartime conditions. Furthermore, this definition reflects the composition of the elements of the cyber defence system and the level of its functioning.

Based on the results of this analysis, within the framework of the proposed terminological system, key subsystems (or domains), which themselves are likely to represent systems, can be identified: **threats; actors of influence and protection; objects of protection; the tools employed; and the capabilities (functional capacities) of system components.** At the same time, the terminological system should describe both the internal interconnections between elements and the external regulatory relationships namely, the regulatory and legal environment. For completeness of the structure, it is also advisable to include a subsystem of basic (fundamental) terms that are common to all cyber domain systems.

It is evident that the cyber defence terminological system is synthetic in nature, as the system of concepts it encompasses integrates multiple domains, including information technology, communications, politics, economics, law, defence, as well as society and its relations.

Accordingly, in order to define the main subsystems of the cyber defence terminological system, an approach "from content to form" is applied, allowing for the identification of the principal groups of terminology.

Based on these conclusions, the proposed structure of the cyber defence terminological system may be represented as follows (Figure 1):

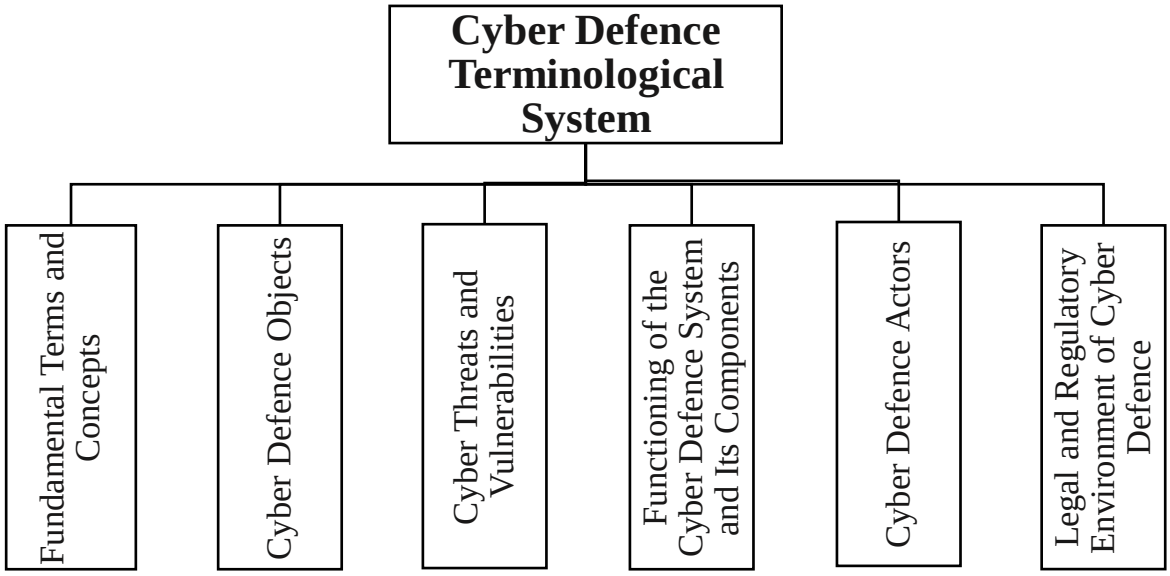


Figure 1. Generalised Scheme of the Cyber Defence Terminology System

Let us examine each of the subsystems in more detail

The fundamental terms and concepts subsystem includes the key general terms that describe cyberspace, cyber defence as a whole, and terms that cannot be assigned to more narrowly focused subsystems. These include, for example, cyberspace, cybersecurity, cyber resilience, cyber

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

protection, cyber defence, cyber operations, and others.

The **objects of cyber defence** subsystem describes all entities whose protection is the focus of cyber defence measures. This ranges from the sovereignty of the state and its governance systems to individual computers and their software products. Terms in this subsystem may include: critical information infrastructure and its components, government bodies, infrastructure objects, critical infrastructure, the National Bank of Ukraine (banking sector entity), institutions (organisations), target audiences, and individual citizens, among others.

The **cyber threats and vulnerabilities** subsystem encompasses terms that describe potential threats that the cyber defence system must counter. It is logical to divide this subsystem into two corresponding groups: threats and vulnerabilities.

Terms in the **cyber threats** group include concepts and/or names describing cyber impacts: DoS (Denial of Service) and DDoS (Distributed Denial of Service), Man-in-the-Middle, malware, social engineering, and many others.

The vulnerabilities group is primarily defined by the terminology of software and hardware tools, as well as factors associated with human error, external influence, and similar risks.

The functioning of the cyber defence system and its components subsystem, in turn, consists of lower-level subsystems containing terms related to organisational, technical, and practical measures implemented during the operation of the system.

Organisational measures terms – Cyber Defence Plan, cyber protection policy, incident response plan, disaster recovery plan, cybersecurity standards, etc.

Technical measures terms – firewall, antivirus software, encryption, multi-factor authentication (MFA), digital signature, etc.

Practical measures terms – all forms and methods of deploying cyber forces and their types, including cyber intelligence, OSINT, cyber reconnaissance, cyber counterintelligence, forensics, penetration testing, cyber training, cyber ranges, and more.

The **subjects of cyber defence** subsystem includes international, state, quasi-state, private entities, institutions, organisations, formations, and independent actors who may be directly or indirectly involved in the operation of the cyber defence system. Terms in this group include cyber forces, cybersecurity specialists, cybercriminals, cyberterrorists (groups), hacker groups, hackers, activists, and others.

The **legal and regulatory environment** subsystem, by topic, could technically be considered a component of the functioning subsystem. However, due to its unique nature and distinction from other components, it is advisable to highlight it as a separate direction. This group includes legislation, strategies, standards, departmental and interdepartmental regulatory documents, international agreements, and similar instruments.

The further development of cyber technologies is expected to alter the level of cyber threats, the degree of vulnerabilities, the scale, forms, and methods of cyber force deployment. This will necessitate new or updated terms to describe them, which, in turn, will require adjustments to the terminology system itself – including the introduction of new terms and subsystems or refinement of existing ones.

Discussions

Most of the key terms of the proposed cyber defence terminology system have already been described within other terminology systems [13]–[14]. For instance, in VST 01.114.001, definitions are provided for cyber attack, cyber operations, cyber influence, cyber threat, cyber protection, cyber weapon, cyber incident, cyber operation, and cyberspace. In VST 01.004.004, terms include cybernetic space (cyberspace), cybernetic attack, cyber strike, cybernetic threat, cybernetic security (cybersecurity), cybernetic protection, and cybernetic weapon. These terms were defined in earlier periods and reflected the level of cyber technology development at the time. However, they never became universally accepted or final. Since their definitions vary across different sources and sometimes even refer to repealed regulatory documents, they do not fully meet the requirements for

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

systematicity and coherence within the proposed terminology system. Consequently, they require revision and updating of their formulations.

Conclusion

In conclusion, the proposed methodological approach has enabled the creation of a coherent and structured cyber defence terminology system, which allows any term related to cyber defence to be unambiguously assigned to one of its subsystems. The described terminology system is not yet fully fixed. As the cyber defence system and its terminology continue to develop, the terminology system will also evolve and undergo corresponding changes.

Recommendations

Considering the described cyber defence terminology system and the requirements for terminology systems [3], the main rules for synthesising (creating and improving) new terms and their definitions can be defined as follows:

1. According to the rules of term formation [3], a term should be short and precise. Therefore, when creating a new term for the cyber defence system, it is advisable to use a word with the term-element “cyber-” rather than a multi-word phrase. For example, “cyber operation” is preferable to “cybernetic operation.”

2. Terminologies are not characterised by synonymy, so the principle of unambiguity must be observed: one object (subject, phenomenon, or event) – one term. If an established term already exists for an object or process in a related field, there is no need to create a new one. It is also inadvisable to rewrite the definition of an established term from a related field to describe another object of a different nature, as this may lead to ambiguity in understanding.

3. Following the principle of systematicity, similar concepts (processes, phenomena) that differ in terms of the level of involved subjects and objects, scale, intensity, etc., should be described according to the same rules, so that both their similarity and their fundamental differences are apparent from the definition.

For example, in the definitions of the terms cyber action, cyber strike, cyber attack, and cyber operation, it is advisable to indicate the purpose (goal), the object of influence, the acting subject, and the time.

Conflict of Interest

The authors declare that they have no competing interests regarding the subject matter of this article.

References

1. Nikolic, I. (2023). Nomination of cybersecurity terms in modern Ukrainian literary language. *Philological Journal*, *2* (22), 31–39.
2. Vashenko, L. A., Dubichynskyi, V. V., & Krymets, O. M. (2008). *Professional Ukrainian Language.* Center for Educational Literature.
3. Dyakov, A. S., Kiyak, T. R., & Kudelko, Z. B. (2000). *Fundamentals of Terminology: Semantic and Sociolinguistic Aspects*. KM Academia.
4. Kochan, I. (2016). Words with the Component “Cyber-” in Modern Ukrainian. *Bulletin of Lviv University*. *Series: Philological*, *63*, 277–285.
5. Kamchatnyi, M. V. Main features of the concept of “cyberwar” in modern international law. *Almanac of International Law*, *15*, 12–22.
6. Melnik, S. V. (2016). Conceptual and categorical apparatus in the system of professional training of future cybersecurity specialists. *Information technologies and teaching aids, 55* (5), 187–197.
7. Vdovenko, S. G., Danik, Yu. G., & Faraon, S. I. (2019). Definitive problems of the terms of the sphere of cyber security and cyber defense and the ways of their solution. *Computer Science*

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

and Cybersecurity, 1 (13), 17–29. https://doi.org/10.26565/2519-2310-2019-1-02.
8. Horhulenko, V. A. (2024). Military-theoretical justification of recommendations for the development of terminological apparatus in the sphere of cyber warfare. *Modern information technologies in the field of security and defense, 3* (51), 41–50. https://doi.org/10.33099/2311-7249/2024-51-3-41-50.
9. Mashtalir, V. V., & Gusak, Yu. A. (2025). Development of conceptual apparatus on cyber defense issues and approaches to creating cyber forces in Ukraine. *Science and Defense*, *1*, 36–46.
10. President of Ukraine. *Cybersecurity Strategy of Ukraine (96/2016).* (2016, 15 бер.). https://zakon.rada.gov.ua/laws/ show/96/2016/ed20160315#Text
11. *On the basic principles of ensuring cybersecurity in Ukraine*. Law of Ukraine No. 2163-VIII (2017, Oct. 5): as of April 20, 2025. https://zakon.rada.gov.ua/laws/show/2163-19.
12. *On the defense of Ukraine*. Law of Ukraine No. 1932-XII (1991, 6 груд.). https://zakon.rada.gov. ua/laws/show /1932-12#Text.
13. Military Standard 01.114.001 (Edit. 1). *Electromagnetic and cyber warfare. Glossary of terms and definitions. VST 01.114.001. 2023 (01).*
14. Military Standard 01.004.004 (Edit. 1). *Military Policy, Security, and Strategic Planning. State Information Security in the Military Sphere. Terms and Definitions. VST 01.004.004 – 2014 (01).*

Методичний підхід до створення термінологічної системи кібероборони

Світлана Зварич
кандидат технічних наук, старший дослідник
провідний науковий співробітник
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил України, 28 Б, Київ, Україна
e-mail: zvarych.ss@gmail.com
ORCID: 0000-0002-0636-250X

Олександр Трохименко
старший науковий співробітник
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил України, 28 Б, Київ, Україна
e-mail: tvo1978@ukr.net
ORCID: 0009-0008-8574-3757

Андрій Воробйов
старший науковий співробітник
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил України, 28 Б, Київ, Україна
e-mail: atmssw@gmail.com
ORCID: 0000-0002-1689-3128

Тетяна Побережець
старший науковий співробітник
Військовий інститут телекомунікацій та інформатизації
імені Героїв Крут
e-mail: tetiana.poberezhets@viti.edu.ua
ORCID: 0000-0001-8007-8614

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Юлія Котюх
старший науковий співробітник
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут
e-mail: jul365@ukr.net
ORCID: 0009-0002-4511-9905

Анотація. Актуальність дослідження зумовлена визнаною проблемою неоднорідності та фрагментарності термінологічного апарату кібероборони в Україні. Відсутність єдиної, систематизованої термінології перешкоджає ефективній міжвідомчій комунікації, розробці організаційної та нормативно-правової документації та оперативній координації з протидії кіберзагрозам. Міждисциплінарний характер кібероборони, що охоплює національну безпеку, технології, право та інші галузі, посилює потребу в уніфікації понятійного апарату. Досі ця сфера досліджувалася вибірково, без розгляду термінології як цілісної системи. Метою статті є висвітлення методичного підходу до створення термінологічної системи кібероборони. Методологічною основою роботи стали теоретичні засади термінознавства, зокрема розмежування понять «термінологія» (як стихійно сформована сукупність термінів) та «терміносистема» (як свідомо впорядкована, цілісна та структурована система понять, що базується на певній концепції). Аналіз сучасного стану кібероборони в Україні показує, що, паралельно з розвитком самої системи кібероборони, термінологія кібероборони перебуває на стадії активного формування та проходить етапи узгодження та закріплення у наукових публікаціях і законодавчих актах. Запропоновано методичний підхід, що полягає у систематизації та структуруванні вже існуючого термінологічного фонду для надання йому ознак цілісної терміносистеми. Слідуючи цьому підходу виділено ключові компоненти, які лягли в основу структури терміносистеми. Запропонована модель складається з шести основних підсистем (груп термінів): фундаментальні терміни та поняття, об’єкти кібероборони, кіберзагрози та вразливості, функціонування системи кібероборони та її складових, суб’єкти кібероборони, а також правове і регуляторне середовище. Зазначено, що терміносистема кібероборони має синтетичний характер, інтегруючи поняття у сферах інформаційних технологій, політики, економіки, юриспруденції, оборони .

Запропонований методичний підхід дозволив створити цілісну та структуровану терміносистему, яка дає можливість однозначно класифікувати будь-який термін, що належить до сфери кібероборони. Підкреслено, що ця система не є сталою і буде розвиватися разом зі змінами у технологіях та формах ведення кіберборотьби. Практична цінність результатів дослідження полягає у розробленні методичних рекомендацій для подальшого формування і удосконалення термінів, що базуються на принципах системності та однозначності трактування, що сприятиме забезпеченню ефективної комунікації та співпраці між різними секторами та їх оперативній координації у сфері кібероборони.

Ключові слова: термін, термінологія, термінологічна система, кібероборона.

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Received: *October 10, 2025* | **Revisions Requested:** - | **Revision Received:** -
Accepted: *December 12, 2025* | **Published Online:** *April 10, 2026*

Licensed (C) by Creative Commons Attribution International License 4.0 (CC BY-NC-SA)

DOI: 10.62524/msj.2026.4.1.8

Турецький досвід багаторівневої системи фізичних, інженерних та технічних засобів контролю і стримування “Стіна безпеки”: аналіз, результати та перспективи адаптації для Збройних Сил України

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

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

Артем Семененко
Курсант
Військовий інститут
Київського національного університету імені Тараса Шевченка
03189, вулиця Юлії Здановської, 81, Київ, Україна
e-mail: aretemsemen1612@gmail.com
ORCID: 0009-0006-2753-5648

Марія Ярмольчик
доктор філософії, доцент
начальник науково-дослідної лабораторії
Державний університет “Київський авіаційний університет”
03048, вулиця Медова, 1, Київ, Україна
e-mail: LinkinFan357@ukr.net
ORCID: 0000-0001-9917-0189

“Хто хоче миру, нехай готується до війни”
Publius Flavius Vegetius Renatus

“Стіна – це не перемога. Стіна – це час для перемоги”
Доктрина інтегрованої оборони периметру (NATO, AJP-3.15)

“Справжнє стримування – це не зброя. Це система, якій противник вірить”
Андрій Гнатов, Олег Семененко

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Анотація. Актуальність дослідження зумовлена необхідністю наукового осмислення міжнародного досвіду побудови багаторівневих інтегрованих систем безпеки кордонів в умовах сучасних асиметричних загроз та гібридної агресії. Турецький проєкт “Physical Border Security System” (“Стіна безпеки”) є одним із найбільш масштабних, технологічно насичених та доктринально обґрунтованих прикладів реалізації такої системи у сучасному світі. Аналіз цього досвіду набуває особливого значення для України в контексті тривалої російської агресії та необхідності формування ефективної, довготривалої системи захисту державних кордонів і зон демаркації. Метою публікації є системний науковий аналіз турецького досвіду побудови багаторівневої системи фізичних, інженерних та технічних засобів контролю і стримування кордону, виявлення її структурних компонентів, ефективності та обмежень, а також обґрунтування концептуальних засад адаптації зазначеного досвіду для потреб Збройних Сил України. Основними результатами дослідження є: систематизація архітектурних принципів турецької “Стіни безпеки”; аналіз чотирьох функціональних рівнів системи – фізичного, технічного, мобільного та командно-інформаційного; порівняльний аналіз ефективності системи за ключовими безпековими показниками; розроблення концептуальної моделі адаптації турецького досвіду для України з урахуванням воєнно-диверсійної специфіки загроз. У статті доведено, що для України доцільне не пряме копіювання турецької моделі, а її концептуальна еволюція у напрямі більш технологізованої, мобільної та воєнізованої системи безпекових поясів уздовж лінії розмежування та у зонах критичної інфраструктури. Матеріали статті можуть бути корисними для органів військового управління, аналітичних структур сектору безпеки і оборони, а також для фахівців з оборонного планування, воєнної доктрини та розвитку спроможностей Збройних Сил України.

Ключові слова: воєнна безпека, інтегрована система охорони кордону, багаторівнева система стримування, турецький безпековий досвід, інженерні загородження, сенсорні мережі, безпілотні системи, адаптація до умов України, система безпекових поясів, оборонне планування, Збройні Сили України, гібридні загрози, асиметричне стримування, командно-інформаційна інтеграція.

Вступ (Introduction)

Сучасний безпековий ландшафт характеризується зростанням асиметричних загроз, гібридної агресії та транскордонної нестабільності, які принципово змінюють підходи до захисту державних кордонів. Традиційні концепції прикордонної безпеки, засновані виключно на чисельності прикордонних підрозділів та патрулюванні, виявляються недостатніми перед обличчям сучасних викликів – організованої нелегальної міграції, транснаціонального тероризму, диверсійно-розвідувальних груп та контрабандних мереж. У цьому контексті особливого значення набуває науковий аналіз досвіду держав, які першими стикнулися з подібними викликами та сформували системні відповіді на них у вигляді інтегрованих багаторівневих систем охорони кордону [1–5].

Туреччина є унікальним прикладом держави, яка, перебуваючи в оточенні зон хронічної нестабільності, а саме: сирійського конфлікту, іракської нестабільності, вірмено-азербайджанської напруженості та курдського збройного руху, розробила та реалізувала один із найбільш масштабних і технологічно складних проєктів охорони кордону у світі – “Physical Border Security System”, відомий як “Стіна безпеки”, що є не просто інженерним об’єктом, а комплексною кіберфізичною системою, яка поєднує бетонні загородження, розгалужені сенсорні мережі, безпілотні авіаційні системи та централізовані командно-інформаційні центри в єдину архітектуру стримування [6–10].

Науковий інтерес до турецького проєкту “Стіни безпеки” визначається кількома взаємопов’язаними чинниками. По-перше, масштаб і тривалість реалізації проєкту (із 2014

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

року і дотепер) дозволяє провести всебічний аналіз не лише архітектурних рішень, а й їхньої практичної ефективності в реальних безпекових умовах. По-друге, турецький досвід є релевантним для низки держав, які стикаються з подібними геополітичними та безпековими викликами, зокрема для України. По-третє, проєкт демонструє практичний перехід від доктрини реагування до доктрини превенції, що є фундаментальним зрушенням у підходах до прикордонної безпеки [11–15].

Для України вивчення турецького досвіду набуває особливої гостроти в умовах широкомасштабного російського вторгнення 2022 року та необхідності стратегічного мислення щодо майбутнього лінії розмежування у будь-якому сценарії закінчення гострої фази конфлікту. Якщо внаслідок переговорного процесу або тимчасового зупинення вогню з'явиться демаркаційна лінія, Україна опиниться перед стратегічним завданням забезпечення її контролю в умовах збереженої загрози з боку держави-агресора. За цих обставин турецький досвід інтегрованої системи стримування може стати важливим концептуальним орієнтиром, хоча й потребує суттєвої адаптації до специфіки воєнно-диверсійних загроз, характерних для українського контексту [16–20].

У сучасній науковій літературі питання фізичних систем охорони кордонів розглядається переважно у контексті управління міграцією або контртерористичної діяльності. Водночас синтез цих підходів з доктриною інтегрованого стримування в умовах замороженого або низькоінтенсивного конфлікту залишається недостатньо дослідженим. Особливо мало уваги приділяється трансферу відповідного досвіду в умови держав, які перебувають у стані активного або потенційно поновлюваного збройного конфлікту [21–25].

Отже, головною метою статті є системний науковий аналіз турецького досвіду побудови багаторівневої системи фізичних, інженерних та технічних засобів контролю і стримування кордону, виявлення її ефективності та обмежень, а також обґрунтування концептуальної моделі адаптації зазначеного досвіду для потреб Збройних Сил України (ЗС України) в умовах сучасних безпекових загроз.

Матеріали та методи (Materials and Methods)

Проблематика інтегрованих систем охорони кордону та їхньої ролі в системі національної безпеки сучасних держав має виражений міждисциплінарний характер і розглядається на перетині військової науки, стратегічних досліджень, геополітики та прикладної безпекології. Науковий доробок у цій галузі охоплює широкий спектр підходів, від класичних теорій стратегічного стримування до сучасних концепцій інтегрованого управління кордонами та кіберфізичних безпекових систем [1–25].

Теоретичним підґрунтям сучасних підходів до фізичного стримування є концепції класиків стратегічної думки. Карл фон Клаузевіц [6] визначив фундаментальний принцип перевищення витрат противника над його потенційними здобутками як основу успішного стримування. Цей принцип отримав нову інтерпретацію в контексті фізичних прикордонних систем: бар'єр є ефективним не тоді, коли він фізично непереборний, а тоді, коли витрати на його подолання перевищують цінність очікуваного результату, Ентоні Генрі Хед [7] розробив принципи операційної лінії та управління простором, які безпосередньо застосовуються в сучасному проєктуванні прикордонних систем. Сунь Цзи [8], своєю чергою, запровадив концепцію *"примушення противника до розкриття"* як альтернативу прямому силовому протистоянню – це підхід, що знайшов відображення в сучасних сенсорно-орієнтованих системах виявлення.

У сучасній зарубіжній науці питання ефективності фізичних прикордонних систем вивчали такі дослідники, як Різ Джонс [26], який провів порівняльний аналіз більш як 70 прикордонних бар'єрів у світі та дійшов висновку про їхню обмежену ефективність без технічного доповнення та мобільних компонентів реагування. Рон Хеснер та Джейсон

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Вітенберг [27] на основі кількісного аналізу довели, що технологічно оснащені бар'єри суттєво ефективніші за прості фізичні загородження за порівнянних витрат. Доктринальна база систем охорони кордонів у контексті НАТО сформована насамперед у документах AJP-3.15 та Allied Land Doctrine ALP-3.2, що визначають принципи інтегрованого контролю периметра [11–15].

Турецький проєкт "Physical Border Security System" у науковій літературі розглядається переважно у контексті управління міграційними потоками (Hürriyet Daily News [28]; Türkiye Today [29]) та протидії тероризму (Anadolu Agency [30]). Офіційна статистика та програмні параметри визначаються Presidential Annual Program 2025 [31] – нормативним документом Адміністрації Президента Туреччини, що є головним офіційним джерелом даних про стан реалізації проєкту. Водночас синтетичного дослідження турецької системи як доктринальної моделі для держав, які перебувають в умовах активної або потенційно поновлюваної збройної агресії, у науковій літературі фактично немає.

Проблематика захисту лінії розмежування та її трансформації в систему управління безпековим простором в умовах замороженого конфлікту розглядається в роботах українських дослідників. Горбулін та Качинський [32] запропонували концепцію "зони безпекового управління" як альтернативи традиційній прикордонній смузі. Руснак та Телелим [33–35] розробили методологію оборонного планування в умовах триваючої гібридної агресії. Однак питання безпосередньої адаптації досвіду "Physical Border Security System" для потреб ЗС України в науковій літературі системно не досліджувалося.

Порівняльний аналіз підходів до формування систем безпеки кордонів у різних державах свідчить про наявність спільного архітектурного принципу щодо багаторівневості системи, що поєднує пасивні фізичні бар'єри, активні технічні засоби виявлення та мобільні компоненти реагування. Водночас конкретна реалізація цього принципу суттєво відрізняється залежно від характеру загрози, географічних умов, фінансових можливостей та доктринальних установок. Ізраїльська система безпеки кордонів [36], іспанська система "Система Інтегральної Зовнішньої Спостереженості" (SIVE) [37] та американська система "Інтегроване фіксоване спостереження" (IFSS) [38] демонструють різні відповіді на цей спільний виклик.

Для вирішення завдань дослідження застосовано комплекс загальнонаукових і спеціальних методів. Системний аналіз дозволив розглянути турецьку "Стіну безпеки" як цілісну систему взаємопов'язаних елементів. Структурно-функціональний аналіз забезпечив виявлення функціонального призначення кожного компонента системи та їхньої взаємодії. Порівняльний аналіз дав змогу зіставити турецький досвід з іншими прикладами інтегрованих систем охорони кордонів. Метод морфологічного аналізу застосовано для формування концептуальної моделі адаптації турецького досвіду для України. Дескриптивний аналіз офіційних документів забезпечив верифікацію фактологічної основи дослідження. Прогностичний метод використано для оцінювання можливих сценаріїв застосування адаптованої системи.

Результати та обговорення (Results and Discussions)

Розуміння турецького проєкту "Physical Border Security System" неможливе без усвідомлення специфічного безпекового середовища, в якому перебуває Туреччина. Ця країна межує з вісьмома державами, а саме: Грецією, Болгарією, Грузією, Вірменією, Азербайджаном (ексклав Нахічевань), Іраном, Іраком та Сирією, з яких більшість або самі є зонами нестабільності, або межують з такими зонами. Загальна довжина сухопутних кордонів Туреччини становить 2 949 км, що саме собою є масштабною безпековою задачею. Після початку громадянської війни в Сирії у 2011 році Туреччина опинилась у принципово новій безпековій ситуації: на її кордоні матеріалізувалась не абстрактна, а цілком реальна загроза масового незаконного перетину і людьми, і збройними формуваннями [1, 6].

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Дослідники Türkiye Today [29] та Hürriyet Daily News [28] виділяють три взаємопов'язаних першопричини, що сформували запит на реалізацію масштабного проєкту: міграційна криза після 2011 р., яка перетворила Туреччину на головний транзитний маршрут для мільйонів вимушених переселенців; зростання активності збройних угруповань, насамперед Робітничої партії Курдистану (РПК), на східних кордонах; системне посилення контрабандних мереж, що скористалися послабленням прикордонного контролю в умовах хаосу сирійського конфлікту. Ці три фактори сформували унікальний тиск, який не дозволяв обмежитися традиційними заходами реагування і вимагав системного архітектурного рішення [2, 3].

Принципово важливим є те, що турецька влада обрала шлях не нарощування чисельності прикордонних підрозділів (що в умовах 2 949 км кордону означало б астрономічне фінансове навантаження), а технологічного переозброєння прикордонної безпеки. Саме цей вибір між "людиноємним" та "технологоємним" підходами став визначальним для подальшої архітектури системи [4, 5].

Проєкт "Physical Border Security System" реалізовувався поетапно, і кожен етап відображав зміну безпекових пріоритетів та накопичений досвід попередніх фаз.

Перший етап (2014–2015 рр.) було ініційовано насамперед різким збільшенням потоку біженців із Сирії та Іраку. На цьому етапі розпочалось будівництво перших бетонних секцій на сирійському кордоні, тобто фактично як вимушена тактична відповідь на безпосередню загрозу. Рішення здавалось тимчасовим, проте стало початком стратегічної програми.

Другий етап (2016–2018 рр.) став найінтенсивнішим за темпами реалізації. Цей період характеризується масштабним розширенням будівництва одночасно на кількох прикордонних ділянках: станом на кінець 2018 р. понад 764 км стіни вздовж 911 км сухопутного кордону з Сирією було збудовано. Водночас розпочалось спорудження бар'єру на кордоні з Іраном. На цьому ж етапі відбулась суттєва технологічна модернізація системи: до бетонної інфраструктури почали масово інтегруватися сенсорні мережі та оптико-електронні системи спостереження [8, 9].

Третій етап (2018–2025 рр.) характеризується географічним розширенням проєкту та його технічним поглибленням. Будівництво охопило кордон з Іраком, а також кордони з Грецією та Болгарією, де зростання міграційного тиску набуло нового виміру. Ключовою особливістю цього етапу стала більш глибока інтеграція системи: від паралельного існування фізичних і технічних компонентів, до їхньої справжньої функціональної інтеграції в рамках єдиних центрів управління. Станом на осінь 2025 р., за даними Presidential Annual Program 2025 [31], побудовано 1 304 км стін та загороджень, що становить приблизно 44% від загальної довжини сухопутних кордонів, а патрульні дороги прокладені на близько 1 700 км кордону [10].

Архітектура та компонентна структура системи.

Загальна архітектурна логіка

Турецька "Стіна безпеки" є системою не лінійного, а просторового контролю. Це принципова відмінність від класичних прикордонних бар'єрів так званого "берлінського типу" чи ізраїльського "зеленого кордону" 1960-х рр. Архітектурна логіка системи ґрунтується на концепції "примусового виявлення": кожен суб'єкт, що намагається несанкціоновано перетнути кордон, під впливом різноманітних фізичних і технічних перешкод змушений або уповільнитися та стати видимим, або витратити занадто великі зусилля на подолання системи, або обрати контрольовані точки перетину [11, 12]. Ця логіка, по суті, реалізує принцип Сунь Цзи [8] про "примушення противника діяти в умовах, вигідних для захисника".

Система організована за чотирма рівнями: фізичним (пасивне стримування), технічним (сенсори та спостереження), мобільним (активне реагування) і командно-інформаційним (управління та аналітика). Жоден із цих рівнів не функціонує ізольовано: вони утворюють

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

взаємопосилюючу мережу, де ефективність кожного рівня залежить від функціонування інших [13, 14]. Саме ця інтегрованість, а не окремі технологічні рішення, є головним архітектурним досягненням турецького проєкту.

Фізичний рівень (пасивне стримування).

Бетонні модульні секції є базовим і найбільш видимим компонентом системи. За даними Presidential Annual Program 2025 [31], станом на осінь 2025 р. збудовано 1 304 км стін та загороджень, причому на кордоні з Сирією їхня довжина сягає 764 км, з Іраном — понад 204 км (ще близько 91 км перебуває у стадії будівництва). Конструктивно бетонні секції є збірними залізобетонними модулями заввишки 2,5–3,0 м із антипідкопним фундаментом та верхніми елементами загородження типу concertina. Ключовими конструктивними принципами є: модульність, що забезпечує швидке нарощування або адаптацію; адаптивність до гірського та нерівного рельєфу; конструктивна сумісність із системами сенсорів та оптичного спостереження [15].

Рови, траншеї та земляні вали є доповнювальним інженерним елементом, що суттєво посилює ефективність бетонних секцій. Рови глибиною до 3–4 м перед фізичним бар'єром унеможливлюють під'їзд транспортних засобів до стіни та ускладнюють прорив організованих груп. Важливою характеристикою цих елементів є їхня функціональна подвійність: вони є і фізичною перешкодою, і засобом "видимості" – у зоні рову потенційний порушник стає надзвичайно вразливим для технічних систем спостереження [16].

Технічний рівень (сенсорні системи та спостереження).

Оптико-електронні системи спостереження є центральним технічним компонентом системи. Вони включають: денні відеосистеми з роздільною здатністю HD та 4K для документування та ідентифікації; тепловізійні камери, що забезпечують виявлення теплових слідів на дальніх відстанях навіть у повній темряві; панорамні камери 360° для безперервного охоплення простору; автоматизовані системи відстеження з алгоритмами детектування руху. Станом на 2025 р. в систему введено 341 спостережну вежу, зокрема близько 250 на східному кордоні [28–31]. Ці вежі слугують водночас і платформами для сенсорів, і структурними опорними точками системи управління.

Радіолокаційні та акустичні сенсорні системи забезпечують виявлення руху за межами прямої видимості та у складних погодних умовах. Наземні радари короткого радіуса дії охоплюють ділянки між вежами і компенсують "мертві зони" оптичних систем. Сейсмічні та інфрачервоні датчики, вбудовані в ґрунт поблизу стіни, фіксують підземні коливання та теплові аномалії. Системи автоматичного оповіщення забезпечують миттєву передачу сигналів тривоги в центри управління з прив'язкою до координат події [17]. Значущість цього рівня полягає в тому, що він фактично усуває необхідність постійної присутності людини безпосередньо біля стіни, замінюючи людський ресурс технічним.

Безпілотні авіаційні системи як елемент просторового контролю.

Безпілотні авіаційні системи (БпЛА) трансформують "стіну" з лінійної фізичної перешкоди у тривимірну систему просторового контролю. Застосування тактичних БпЛА типу Bayraktar mini та ANKA для патрулювання кордону забезпечує широкозонний огляд, недосяжний для стаціонарних систем спостереження. БпЛА виконують три ключових функції: первинний широкозонний огляд великих ділянок кордону; підтвердження сигналів від наземних сенсорів та визначення характеру загрози; оперативна розвідка в реальному часі з передачею даних до центрів управління [18, 19]. Саме завдяки БпЛА система набуває здатності до динамічної реорганізації ресурсів спостереження у відповідь на ситуацію, що змінюється.

Командно-інформаційний рівень (управління та інтеграція).

Командно-інформаційний рівень є мозком системи, що перетворює масиви даних від різнорідних джерел на своєчасні управлінські рішення. Центри управління та аналізу

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

забезпечують: збирання та оброблення даних від усіх сенсорних систем у режимі реального часу; пріоритизацію загроз на основі алгоритмічного аналізу; координацію дій мобільних підрозділів реагування; документування інцидентів для аналітичного опрацювання. Аналіз поведінкових шаблонів дозволяє системі не просто реагувати на інциденти, а й передбачати ймовірні місця та часові вікна спроб порушення [20]. Цей рівень перетворює набір технічних засобів на інтелектуальну систему ситуаційної обізнаності.

Аналіз ефективності та порівняльна оцінка.

Ефективність за ключовими безпековими показниками.

Оцінка ефективності "Physical Border Security System" потребує застосування системи показників, що охоплює як кількісні, так і якісні виміри. За даними Міністерства внутрішніх справ Туреччини [39] та аналітичних публікацій Türkiye Today [29], реалізація системи сприяла суттєвому скороченню кількості несанкціонованих перетинів кордону на укріплених ділянках, у деяких зонах скорочення досягає 70–80% порівняно з доінфраструктурним рівнем. Разом із тим, ефективність є нерівномірною: на ділянках, де технічне оснащення не відповідає рівню фізичної інфраструктури, або в гірських районах зі складним рельєфом показники значно нижчі [28, 29]. Якісний вимір ефективності виявляється у трьох напрямах. По-перше, суттєво зросла ситуаційна обізнаність прикордонних сил: система забезпечує виявлення та фіксацію загроз на стадії підготовки до перетину, а не в момент безпосереднього прориву. По-друге, скоротилось операційне навантаження на особовий склад, бо значна частина спостереження перенесена з людей на технічні засоби, що дозволяє оптимальніше розподіляти людські ресурси. По-третє, система створила документальну базу інцидентів, яка дозволяє виявляти поведінкові шаблони та прогнозувати ймовірні спроби прориву [30, 31].

Таблиця 1. Компонентна структура турецької "Стіни безпеки"

Рівень системи	Основні елементи	Функціональне призначення	Характер дії
Фізичний	Бетонні секції, рови, вали	Фізичне стримування, затримка, канолізація потоків	Пасивний
Технічний	Оптоелектроніка, радари, сенсори	Виявлення, фіксація, раннє попередження	Активний / цілодобовий
БпЛА	Тактичні дрони, аеростати	Просторовий контроль, підтвердження загроз	Динамічний
Мобільний	Патрулі, пункти реагування	Перехоплення, нейтралізація загроз	Реактивний
Командний	Центри управління, аналітика	Інтеграція даних, прийняття рішень	Системний

Обмеження та критичні залежності системи.

Аналіз турецької системи виявив низку структурних обмежень, важливих для наукового осмислення. Перша критична залежність – це залежність від безперервного технічного обслуговування. Сенсорні мережі та оптико-електронні системи вимагають регулярного технічного обслуговування, а їхній вихід із ладу в окремих зонах тимчасово перетворює бетонні секції на пасивні загородження без аналітичної підтримки. Друга – це залежність від кваліфікованого персоналу для центрів управління: система генерує значний масив даних, ефективне оброблення яких потребує підготовленого аналітичного ресурсу [16, 17]. Третє обмеження – це природний рельєф. Гірські та важкодоступні ділянки на кордонах з Іраном та Іраком суттєво ускладнюють як будівництво, так і обслуговування інфраструктури. На таких ділянках щільність контролю нижча, що створює "уразливі вікна" в системі. Четверте

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

обмеження – це методологічна адаптація загрози: аналіз свідчить, що суб'єкти, які здійснюють незаконні перетини, поступово адаптують свою тактику до логіки системи, обираючи ділянки зі слабшим технічним оснащенням або часові вікна технічних збоїв [18, 19].

Порівняльний аналіз із іншими прикордонними системами.

У контексті глобального досвіду побудови інтегрованих систем охорони кордонів турецький проєкт посідає унікальне місце. Порівняно з ізраїльською системою безпеки кордонів [36], турецька демонструє більшу масштабність охоплення за меншої питомої технологічної насиченості. Ізраїльська система є більш насиченою технологічно на кожний кілометр, однак охоплює значно менші абсолютні відстані. Американська система IFSS [38] є більш технологічно складною, але реалізована у принципово інших географічних умовах, частково напівпустельних, де природний рельєф "сам по собі" є додатковим бар'єром.

Від більшості європейських прикордонних систем (іспанської SIVE [37], грецьких та угорських бар'єрів) турецька відрізняється своїм системним, а не фрагментарним характером. Тоді як більшість європейських держав реалізували локальні відповіді на конкретні міграційні тиски, Туреччина від самого початку орієнтувалась на стратегічну довгострокову програму. Це принципово змінює і масштаб системи, і глибину її доктринального обґрунтування [20].

Таблиця 2. Порівняльна характеристика провідних інтегрованих систем охорони кордонів

Параметр	Туреччина	Ізраїль	США (IFSS)	ЄС (локальні)
Довжина (км)	~1 304	~800	~700	Фрагм.
Тип загрози	Гібридна	Тероризм	Міграція	Міграція
Рівень технологій	Середній	Високий	Високий	Низький
Характер системи	Стратегічний	Стратегічний	Тактичний	Реактивний
Воєнізація	Середня	Висока	Низька	Низька

Концептуальна модель адаптації для України.

Відмінність українського контексту від турецького.

Концептуальна адаптація турецького досвіду для України вимагає передусім чіткого розуміння принципових відмінностей безпекового контексту. Туреччина будувала свою систему в умовах гібридних загроз із помірним рівнем інтенсивності: міграційний тиск, контрабанда, терористична активність. Ці загрози характеризуються великою кількістю малих суб'єктів із обмеженим технічним оснащенням і відсутністю державної підтримки. Натомість Україна у будь-якому сценарії постконфліктного врегулювання стикатиметься із загрозою, що має принципово іншу природу: державно-підтримувана диверсійна та розвідувальна активність, оснащена військовою технікою, координована на стратегічному рівні та орієнтована не лише на інфільтрацію, а й на дестабілізацію [1–5].

З огляду на це, трансфер турецького досвіду не може бути механічним. Йдеться про адаптацію архітектурної логіки, а не конкретних технічних рішень: принцип багаторівневості та інтеграції компонентів є цілком релевантним; принцип заміни "людиноємного" підходу "технологоємним" є не просто прийнятним, а критично необхідним; принцип просторового (а не лінійного) контролю є єдино ефективним для умов постконфліктного розмежування.

П'ятирівнева концептуальна модель для України.

На основі аналізу турецького досвіду та специфіки українських безпекових умов пропонується п'ятирівнева концептуальна модель системи стримування і контролю для України.

Рівень 1 – інженерно-ландшафтний (пасивний). На відміну від турецьких бетонних

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

секцій, орієнтованих на стримування мігрантів, в Україні інженерні елементи мають бути орієнтовані на стримування воєнно-технічних засобів противника. Це означає більш масивні протитанкові рови глибиною 4–5 м та шириною до 6 м, земляні вали, що перешкоджають прямій видимості противника, системи керованих мінних загороджень, що активуються у разі виявлення загрози, та модульні загородження у "сліпих зонах" рельєфу [6, 7].

Рівень 2 – сенсорно-технічний (ключовий). Цей рівень є найважливішим з огляду на досвід турецького проєкту. В українських умовах він потребує суттєвого технологічного поглиблення: масштабне розгортання розподілених сейсмічних сенсорних мереж з автономним живленням; тепловізійні системи спостереження з дальністю до 10 км; РЛС ближньої та середньої дальності для виявлення техніки і груп в умовах обмеженої видимості; акустичні системи розпізнавання характеристик пострілів та двигунів. Критичним принципом є масовість і дешевизна за рахунок децентралізації, а не точкове розміщення дорогих систем [8, 9].

Рівень 3 – безпілотний (домінуючий). Беручи до уваги масштабний досвід, набутий ЗС України у застосуванні БпЛА в ході широкомасштабного вторгнення, цей рівень може стати унікальною конкурентною перевагою української системи. Пропонується організація постійного безпілотного патрулювання за допомогою малих автономних дронів із автоматичним обміном даними; розгортання прив'язних аеростатів для довготривалого спостереження над критичними ділянками; формування резерву БпЛА з ударним потенціалом для реагування на виявлені загрози. В українських умовах "стіна" має бути повітряною, а не лише наземною [10–14].

Рівень 4 – мобільно-вогневий (активний). Ключова відмінність від турецької моделі полягає у воєнізованому характері цього рівня. В Україні мобільний компонент є не поліцейськими патрулями, а бойовими підрозділами з летальним потенціалом. Структура цього рівня передбачає: мобільні бойові групи реагування із часом прибуття до будь-якої точки лінії розмежування не більше 15–20 хвилин; дистанційно керовані бойові модулі на ключових ділянках; системи нелетального та летального ураження для різних типів загроз [15, 16].

Рівень 5 – командно-аналітичний (управління та розвідка). В українських умовах цей рівень має бути глибоко інтегрованим з розвідувальними структурами та системами кіберзахисту. Архітектура рівня включає: єдину цифрову платформу управління ситуацією вздовж лінії розмежування; інтеграцію з даними ГРУ ЗС України, СБ України та ДПСУ; алгоритмічне прогнозування активності на основі поведінкових шаблонів; автоматичне оповіщення та пріоритизацію загроз [17–20].

Пріоритетні зони реалізації.

На відміну від Туреччини, яка прагне до суцільного охоплення своїх кордонів, Україна в умовах постконфліктного врегулювання не потребує і не може реалізувати суцільну систему безпекових заходів уздовж усієї потенційної лінії розмежування. Доцільна вибіркова, зональна модель, що концентрує ресурси у трьох пріоритетних категоріях зон: ділянки лінії розмежування з підтвердженою або прогнозованою активністю ДРГ противника; підходи до великих міст – Харківський, Запорізький, Херсонський та Дніпровський напрямки; зони критичної інфраструктури, насамперед енергетика, водопостачання та залізничні вузли [21–25].

Стратегічний сенс для України.

Реалізація системи безпекових поясів для України має п'ять взаємопов'язаних стратегічних ефектів.

Перший – зрив сценарію "повзучої війни": наявність системи стримування, видимої для противника та підтвердженої практикою виявлення і знищення порушників, суттєво ускладнює стратегію підтримки постійного напруження без прямої відповідальності.

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Другий – зменшення навантаження на особовий склад: заміна частини людського ресурсу технічними засобами дозволяє вивільнити боєздатні підрозділи для інших завдань і зменшити кількість втрат серед особового складу прикордонних підрозділів.

Третій – "фіксація" де-факто межі без її юридичного визнання: система стримування матеріально позначає лінію розмежування без необхідності її дипломатичного оформлення [22–25].

Четвертий ефект – виграш часу для стратегічного відновлення: збереження контролю над лінією розмежування без виснажливих бойових зіткнень дозволяє Україні зосередитися на відновленні, переозброєнні та підготовці до можливих нових фаз конфронтації.

П'ятий – сигнальна функція для партнерів та противника: демонстрація здатності самостійно контролювати власні кордони посилює позиціонування України як надійного суб'єкта міжнародної безпеки та знижує сприйняття її як "слабкої ланки", що потребує постійного зовнішнього забезпечення [18–20].

Таблиця 3. Порівняльна характеристика турецької та пропонованої української моделей

Параметр	Туреччина	Україна (пропозиція)
Характер загрози	Міграційно-терористична	Воєнно-диверсійна (державна)
Тип стримування	Пасивне (бетон)	Активне (технологія + мобільність)
Основа системи	Фізична інфраструктура	Сенсорно-безпілотний контроль
Логіка дій	Поліцейська	Військова
Географія охоплення	Суцільна лінія	Зональні безпекові пояси
Рівень воєнізації	Середній	Максимальний

Висновки та рекомендації (Conclusion and Recommendations)

У результаті проведеного дослідження систематизовано науковий аналіз турецького досвіду побудови багаторівневої системи фізичних, інженерних та технічних засобів контролю і стримування кордону. Встановлено, що "Physical Border Security System" є принципово новим явищем у сучасній практиці безпеки кордонів – кіберфізичною системою, яка перетворює "стіну" з пасивного інженерного об'єкта на активну інтелектуальну систему ситуаційного контролю. Ключовою архітектурною особливістю є не якесь конкретне технічне рішення, а принцип функціональної інтеграції чотирьох рівнів – фізичного стримування, технічного виявлення, безпілотного просторового контролю та мобільного реагування – в єдину командно-інформаційну систему управління.

Аналіз ефективності системи виявив її структурні сильні сторони та обмеження. До сильних сторін належать: суттєве скорочення несанкціонованих перетинів на укріплених ділянках; зростання ситуаційної обізнаності без відповідного зростання чисельності персоналу; формування стратегічно керованого та прогнозованого безпекового простору. Обмеженнями є: нерівномірна ефективність через різний рівень технічного оснащення різних ділянок; критична залежність від безперервного технічного обслуговування; складність повноцінного покриття гірського рельєфу та адаптаційна активність суб'єктів загрози.

Порівняльний аналіз виявив, що турецька система є найбільш масштабним за протяжністю та найбільш доктринально обґрунтованим прикладом інтегрованої прикордонної безпеки серед сучасних аналогів. На відміну від переважно реактивних та фрагментарних підходів більшості держав, турецька програма реалізується як стратегічна довгострокова ініціатива з усвідомленою архітектурою та фазованістю впровадження.

Обґрунтована концептуальна модель адаптації для України базується на принципі

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

“еволюції, а не копіювання”: запозиченні архітектурної логіки багаторівневості та інтеграції за радикальної адаптації конкретних рішень до специфіки воєнно-диверсійних загроз. Запропонована п’ятирівнева модель (інженерно-ландшафтний, сенсорно-технічний, безпілотний, мобільно-вогневий та командно-аналітичний рівні) відображає українські реалії значно глибше, ніж будь-яке механічне запозичення. Особливою відмінністю є воєнізований характер системи від початку: на відміну від поліцейської логіки турецького проєкту, українська система визначається як бойова.

Матеріали статті можуть бути корисними для органів військового управління, структур оборонного планування, аналітичних центрів сектору безпеки і оборони, а також для фахівців у сфері воєнної доктрини та розвитку спроможностей ЗС України. Практична реалізація запропонованої моделі доцільна після закінчення гострої фази конфлікту і має бути включена до системи доктринальних документів ЗС України як елемент національної стратегії безпеки. Подальші дослідження за напрямом статті варто зосередити на: розробленні детальних технічних специфікацій елементів системи з урахуванням доступних технологічних ресурсів України; аналізі досвіду постконфліктних демаркаційних ліній (Корея, Кіпр, Косово) для виявлення уроків щодо управління безпековим простором в умовах замороженого конфлікту; розробленні методичного апарату оцінювання ефективності системи та критеріїв модернізації її окремих компонентів.

Конфлікт інтересів (Conflict of Interest)

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

Використані джерела

1. Горбулін, В. (2017). *Світова гібридна війна: український фронт*. НІСД.
2. Watling, J., & Reynolds, N. (2023). *Meatgrinder: Russian tactics in the second year of its invasion of Ukraine*. Royal United Services Institute. https://www.rusi.org
3. Kofman, M., & Lee, R. (2022). Not built for purpose: The Russian military's ill-fated force design. *War on the Rocks*. https://warontherocks.com
4. Freedman, L. (2022). Ukraine and the art of strategy. *Survival, 64* (2), 7–22.
5. Cordesman, A. (2023). *The Russian–Ukrainian war and the changing character of war*. Center for Strategic and International Studies.
6. Clausewitz, C. von. (1984). *On war*. Princeton University Press.
7. Jomini, A.-H. (1971). *The art of war*. Greenwood Press.
8. Sun Tzu. (2013). *The art of war*. Oxford University Press.
9. Gray, C. S. (1999). *Modern strategy*. Oxford University Press.
10. Warden, J. (1988). *The air campaign: Planning for combat*. National Defense University Press.
11. North Atlantic Treaty Organization. (2022). *NATO 2022 strategic concept*. Brussels.
12. North Atlantic Treaty Organization. (2017). *Allied joint doctrine (AJP-01)*. NATO Standardization Office.
13. North Atlantic Treaty Organization. (2019). *Allied joint doctrine for the conduct of operations (AJP-3)*. NATO Standardization Office.
14. North Atlantic Treaty Organization. (2020). *Allied joint doctrine for countering improvised explosive devices (AJP-3.15)*.
15. North Atlantic Treaty Organization. (2021). *NATO glossary of terms and definitions (AAP-06)*.
16. Руснак, І. (2016). *Оборонне планування в системі забезпечення воєнної безпеки держави*. НУОУ.
17. Телелим, В. (2012). *Основи стратегічного управління у сфері воєнної безпеки держави*. НУОУ.
18. Кузьо, Т. (2023). Питання безпеки лінії розмежування. *Atlantic Council*.

19. Президент України. (2021). *Стратегія воєнної безпеки України*.
20. Кабінет Міністрів України. (2020). *Стратегія національної безпеки України*.
21. Міністерство оборони України. (2021). *Стратегічний оборонний бюлетень України*.
22. Міністерство оборони України. (2020). *Доктрина застосування сил оборони України*.
23. Збройні Сили України. (2022). *Доктринальні документи*. Генеральний штаб ЗС України.
24. Booth, K. (1979). *Strategy and ethnocentrism*. Routledge.
25. Freedman, L. (2013). *Strategy: A history*. Oxford University Press.
26. Jones, R. (2016). *Violent borders: Refugees and the right to move*. Verso Books.
27. Hassner, R., & Wittenberg, J. (2015). Barriers to entry: Who builds fortified boundaries and why? *International Security*, *40* (1), 157–190.
28. Hürriyet Daily News. (n.d.). *Turkey builds security walls on nearly half of land borders.* https://www.hurriyetdailynews.com/turkiye-builds-security-walls-on-nearly-half-of-land-borders-215218
29. Türkiye Today. (n.d.). *Türkiye completes security wall across 44% of land borders.* https://www.turkiyetoday.com/nation/turkiye-completes-security-wall-across-44-of-land-borders-report-shows-3209253
30. Anadolu Agency. (n.d.). *Turkey installs 764 km security wall on Syria border.* https://www.aa.com.tr/en/middle-east/turkey-installs-764-km-security-wall-on-syria-border/1170257
31. Presidency of the Republic of Türkiye. (2025). *Presidential annual program 2025*. https://www.sbb.gov.tr/annual-programmes/
32. Горбулін, В., & Качинський, А. (2017). Концептуальні засади формування системи стратегічного планування у сфері національної безпеки України. *Стратегічна панорама*, *1*, 5–12.
33. Руснак, І., & Телелим, В. (2018). Система оборонного планування в Україні: сучасний стан та напрями розвитку. *Наука і оборона*, ***3***, 3–10.
34. Руснак, І., & Лобко, М. (2020). Проблеми узгодження стратегічних і доктринальних документів. *Воєнно-науковий вісник*, *34*, 27–35.
35. Телелим, В., & Загорка, О. (2019). Методологічні підходи до формування системи керівних документів. *Зб. наук. пр. НУОУ*, *2*, 15–23.
36. Yadin, A. (2022). *The Israeli border system: Technology, fencing, and strategic deterrence*. Israel Defense.
37. Guardia Civil. (2020). *Sistema integrado de vigilancia exterior (SIVE)*. Ministerio del Interior de España.
38. U.S. Customs and Border Protection. (2021). *Integrated fixed tower (IFT) program*. DHS.
39. T.C. İçişleri Bakanlığı. (2024). *Sınır güvenliği istatistikleri 2024*. https://www.icisleri.gov.tr

References

1. Horbulin, V. (2017). *World hybrid war: The Ukrainian front*. NISS.
2. Watling, J., & Reynolds, N. (2023). *Meatgrinder: Russian tactics in the second year of its invasion of Ukraine*. Royal United Services Institute. https://www.rusi.org
3. Kofman, M., & Lee, R. (2022). Not built for purpose: The Russian military's ill-fated force design. *War on the Rocks*. https://warontherocks.com
4. Freedman, L. (2022). Ukraine and the art of strategy. *Survival, 64* (2), 7–22.
5. Cordesman, A. (2023). *The Russian–Ukrainian war and the changing character of war*. Center for Strategic and International Studies.
6. Clausewitz, C. von. (1984). *On war*. Princeton University Press.
7. Jomini, A.-H. (1971). *The art of war*. Greenwood Press.
8. Sun Tzu. (2013). *The art of war*. Oxford University Press.

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

9. Gray, C. S. (1999). *Modern strategy*. Oxford University Press.
10. Warden, J. (1988). *The air campaign: Planning for combat*. National Defense University Press.
11. North Atlantic Treaty Organization. (2022). *NATO 2022 strategic concept*. Brussels.
12. North Atlantic Treaty Organization. (2017). *Allied joint doctrine (AJP-01)*. NATO Standardization Office.
13. North Atlantic Treaty Organization. (2019). *Allied joint doctrine for the conduct of operations (AJP-3)*. NATO Standardization Office.
14. North Atlantic Treaty Organization. (2020). *Allied joint doctrine for countering improvised explosive devices (AJP-3.15)*.
15. North Atlantic Treaty Organization. (2021). *NATO glossary of terms and definitions (AAP-06)*.
16. Rusnak, I. (2016). *Defense planning in the system of ensuring the military security of the state*. NDUU.
17. Telelym, V. (2012). *Fundamentals of strategic management in the field of military security of the state*. NDUU.
18. Kuzio, T. (2023). Issues of security of the line of contact. *Atlantic Council*.
19. President of Ukraine. (2021). *Military security strategy of Ukraine*.
20. Cabinet of Ministers of Ukraine. (2020). *National security strategy of Ukraine*.
21. Ministry of Defense of Ukraine. (2021). *Strategic defense bulletin of Ukraine*.
22. Ministry of Defense of Ukraine. (2020). *Doctrine on the employment of the defense forces of Ukraine*.
23. Armed Forces of Ukraine. (2022). *Doctrinal documents*. General Staff of the Armed Forces of Ukraine.
24. Booth, K. (1979). *Strategy and ethnocentrism*. Routledge.
25. Freedman, L. (2013). *Strategy: A history*. Oxford University Press.
26. Jones, R. (2016). *Violent borders: Refugees and the right to move*. Verso Books.
27. Hassner, R., & Wittenberg, J. (2015). Barriers to entry: Who builds fortified boundaries and why? *International Security, 40* (1), 157–190.
28. Hürriyet Daily News. (n.d.). *Turkey builds security walls on nearly half of land borders.* https://www.hurriyetdailynews.com/turkiye-builds-security-walls-on-nearly-half-of-land-borders-215218
29. Türkiye Today. (n.d.). *Türkiye completes security wall across 44% of land borders*. https://www.turkiyetoday.com/nation/turkiye-completes-security-wall-across-44-of-land-borders-report-shows-3209253
30. Anadolu Agency. (n.d.). *Turkey installs 764 km security wall on Syria border*. https://www.aa.com.tr/en/middle-east/turkey-installs-764-km-security-wall-on-syria-border/1170257
31. Presidency of the Republic of Türkiye. (2025). *Presidential annual program 2025*. https://www.sbb.gov.tr/annual-programmes/
32. Horbulin, V., & Kachynskyi, A. (2017). Conceptual foundations of the formation of a strategic planning system in the field of national security of Ukraine. *Strategic Panorama*, *1*, 5–12.
33. Rusnak, I., & Telelym, V. (2018). The defense planning system in Ukraine: Current state and development directions. *Science and Defense*, *3*, 3–10.
34. Rusnak, I., & Lobko, M. (2020). Problems of harmonization of strategic and doctrinal documents. *Military Scientific Bulletin*, *34*, 27–35.
35. Telelym, V., & Zahorka, O. (2019). Methodological approaches to the formation of a system of guiding documents. *Collection of Scientific Works of NDUU*, *2*, 15–23.
36. Yadin, A. (2022). *The Israeli border system: Technology, fencing, and strategic deterrence*. Israel Defense.
37. Guardia Civil. (2020). *Integrated external surveillance system (SIVE)*. Ministry of the Interior of Spain.

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

38. U.S. Customs and Border Protection. (2021). *Integrated fixed tower (IFT) program*. Department of Homeland Security.
39. Ministry of Interior of Türkiye. (2024). *Border security statistics 2024*. https://www.icisleri.gov.tr

Turkish experience of a multi-level system of physical, engineering and technical means of control and containment "Security Wall": analysis, results and adaptation prospects for the Armed Forces of Ukraine

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

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

Artem Semenenko
Cadet
Military Institute of Taras Shevchenko National University of Kyiv
03189, Yulii Zdanovskaya St., 81, Kyiv,Ukraine
e-mail: aretemsemen1612@gmail.com
ORCID: 0009-0006-2753-5648

Mariia Yarmolchyk
PhD, docent
Head of Research Laboratory
State University "Kyiv Aviation University"
03048, Medova Street, 1, Kyiv, Ukraine
e-mail: LinkinFan357@ukr.net
ORCID: 0000-0001-9917-0189

"Whoever wants peace, let him prepare for war"
Publius Flavius Vegetius Renatus

"A wall is not victory. A wall is a time for victory"
The Doctrine of Integrated Perimeter Defense (NATO, AJP-3.15)

"Real deterrence is not a weapon. It is a system that the enemy believes in"
Andriy Gnatov, Oleh Semeneko

Abstract. The relevance of the study is due to the need for scientific understanding of the international experience of building multi-level integrated border security systems in the conditions

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

of modern asymmetric threats and hybrid aggression. The Turkish project “Physical Border Security System” (“Security Wall”) is one of the most large-scale, technologically rich and doctrinally justified examples of the implementation of such a system in the modern world. The analysis of this experience is of particular importance for Ukraine in the context of the ongoing Russian aggression and the need to form an effective, long-term system for protecting state borders and demarcation zones. The purpose of the article is a systematic scientific analysis of the Turkish experience in building a multi-level system of physical, engineering and technical means of border control and containment, identifying its structural components, effectiveness and limitations, as well as substantiating the conceptual principles of adapting the aforementioned experience for the needs of the Armed Forces of Ukraine. The main results of the study are: systematization of the architectural principles of the Turkish “Security Wall”; analysis of the four functional levels of the system – physical, technical, mobile and command and information; comparative analysis of the system’s effectiveness according to key security indicators; development of a conceptual model for adapting the Turkish experience for Ukraine, taking into account the military-sabotage specifics of threats. The article proves that for Ukraine it is not advisable to directly copy the Turkish model, but rather its conceptual evolution towards a more technological, mobile and militarized system of security belts along the contact line and in critical infrastructure areas. The materials of the article can be useful for military command bodies, analytical structures of the security and defense sector, as well as for specialists in defense planning, military doctrine and development of capabilities of the Armed Forces of Ukraine.

Keywords: military security, integrated border protection system, multi-level deterrence system, Turkish security experience, engineering barriers, sensor networks, unmanned systems, adaptation to the conditions of Ukraine, security belt system, defense planning, Armed Forces of Ukraine, hybrid threats, asymmetric deterrence, command and information integration.

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Received: *October 8, 2025* | **Revisions Requested:** - | **Revision Received:** -
Accepted: *December 1, 2025* | **Published Online:** *April 10, 2026*

Licensed (C) by Creative Commons Attribution International License 4.0 (CC BY-NC-SA)

DOI: 10.62524/msj.2026.4.1.9

Метод оцінювання стану воєнно-економічної безпеки держави на основі нечітких оцінок ресурсних можливостей

Поліна Толок
кандидат економічних наук, старший науковий співробітник
старший науковий співробітник
Державний науково-дослідний інститут випробувань і сертифікації
озброєння та військової техніки
e-mail: tolok100@meta.ua
ORCID: 0000-0002-2481-8152

Анотація. Забезпечення воєнно-економічної безпеки держави в умовах сучасних воєнних конфліктів є ключовим завданням системи національної безпеки. Ресурсні можливості держави, а саме: людські, матеріальні та фінансові ресурси, визначають її здатність до виконання завдань оборони. Однак традиційні методи кількісного оцінювання стану воєнно-економічної безпеки не повною мірою враховують невизначеність та неточність вхідних даних, притаманних умовам бойового застосування. Метою статті є розроблення та детальний опис методу оцінювання стану воєнно-економічної безпеки держави, що ґрунтується на використанні нечітких оцінок ресурсних можливостей. Метод реалізується в чотири послідовні етапи: перший – визначення необхідного рівня воєнно-економічної безпеки та вимог до ресурсного забезпечення; другий – оцінювання стану ресурсних можливостей держави за складовими ресурсної забезпеченості; третій – формування нечіткої шкали оцінювання рівня воєнно-економічної безпеки та оцінювання чутливості отриманих оцінок; четвертий – оцінювання достатності ресурсних можливостей держави для забезпечення необхідного показника воєнно-економічної безпеки. Запропонований метод дозволяє кількісно оцінити рівень воєнно-економічної безпеки з урахуванням нечіткості вхідних даних, визначити відхилення фактичних показників ресурсного забезпечення від необхідних, а також сформувати рекомендації для органів державного управління. Метод пройшов апробацію на прикладі оцінювання ресурсних можливостей України, що підтверджує його практичну значущість для планування оборонних ресурсів та вироблення управлінських рішень.

Ключові слова: воєнно-економічна безпека, ресурсні можливості держави, нечіткі множини, нечіткі оцінки, метод оцінювання, людські ресурси, матеріальні ресурси, фінансові ресурси, рівень безпеки, оборонний потенціал, ступінь напруженості обстановки, парні порівняння.

Вступ (Introduction)

Воєнно-економічна безпека (ВЕБ) держави є однією із найважливіших складових системи національної безпеки та визначає здатність держави протистояти зовнішнім та внутрішнім загрозам завдяки ефективному використанню наявних ресурсних можливостей. Проблематика оцінювання стану ВЕБ набуває особливої актуальності в умовах тривалих

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

воєнних конфліктів, зокрема широкомасштабного вторгнення російської федерації в Україну, розпочатого у 2022 році, яке демонструє, що здатність держави мобілізувати та ефективно використати наявні ресурси безпосередньо визначає результат збройного протистояння [1–5].

Традиційний підхід до оцінювання ВЕБ базується на порівнянні фактичних показників ресурсного забезпечення з нормативно визначеними або плановими. Водночас в умовах реального застосування збройних сил вхідні дані щодо стану ресурсів характеризуються суттєвою невизначеністю, а процес ухвалення рішень відбувається в умовах дефіциту часу та інформаційної неповноти. Це зумовлює необхідність розроблення методів оцінювання, що враховують нечіткість інформації та забезпечують отримання стійких оцінок навіть за умов варіативності вхідних даних [6–9]. Методологічну основу нечіткого моделювання заклали праці Л. Заде [10], розвинені для задач воєнно-економічного аналізу у роботах вітчизняних та зарубіжних дослідників [11–15]. Застосування апарату нечітких множин дозволяє формалізувати якісні експертні оцінки, враховувати розмитість меж між рівнями безпеки та забезпечувати розроблення аналітично обґрунтованих управлінських рекомендацій [16–20].

Метою статті є розроблення та детальний опис методу оцінювання стану воєнно-економічної безпеки держави на основі нечітких оцінок ресурсних можливостей, що включає визначення необхідного рівня ВЕБ, оцінювання стану ресурсних можливостей за всіма складовими, формування нечіткої шкали оцінювання та визначення достатності ресурсних можливостей для забезпечення заданого рівня безпеки.

Матеріали та методи (Materials and Methods)

Теоретичною основою розробленого методу є апарат нечітких множин та нечіткої логіки [10, 11], методи багатокритеріального аналізу та попарного порівняння [21], теорія ієрархій Сааті [22], а також методологія оцінювання ресурсного забезпечення оборонної сфери [1–5]. Інформаційну базу методу формують: статистичні дані Державної служби статистики України щодо стану людських, матеріальних і фінансових ресурсів; нормативно-правові акти у сфері оборонного планування та визначення показників ВЕБ; результати експертного оцінювання складових ресурсного забезпечення; аналітичні матеріали Центрального науково-дослідного інституту Збройних Сил України. Метод будується на принципах системності (врахування всіх видів ресурсного забезпечення), комплексності (інтеграція кількісних та якісних показників), нечіткості (використання функцій належності для опису невизначеності), адаптивності (можливість коригування вимог до ресурсів відповідно до зміни воєнно-політичної обстановки) та верифікованості (оцінка чутливості результатів до варіації вхідних даних). Структурно метод реалізується у чотири послідовні взаємопов’язані етапи, що охоплюють весь цикл: від визначення цільових показників ВЕБ до оцінювання відповідності фактичного стану встановленим вимогам і формування управлінських рекомендацій.

Результати (Results)

Розроблений метод оцінювання стану воєнно-економічної безпеки держави складається з чотирьох основних етапів. Загальну структуру методу за першим та другим етапами відображено на рис. 1, за третім та четвертим – на рис. 2. Нижче наведено детальний опис кожного етапу.

Етап 1. Визначення необхідного рівня воєнно-економічної безпеки держави та вимог до його ресурсного забезпечення.

Перший етап є вихідним для всього методу й спрямований на формалізацію вимог до рівня ВЕБ та ресурсного забезпечення, необхідного для реалізації завдань оборони на визначений час або плановий період *T*.

Блок 1.1. Формування вимог до рівня ВЕБ на час (t), період (T).

На основі аналізу воєнно-політичної обстановки (ВПО) в державі та навколо неї

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

визначається перелік найбільш імовірних загроз національній безпеці України та оцінюються коефіцієнти степеня напруженості обстановки *k(t)* для кожного часового зрізу *t* впродовж планового горизонту *T*. Ці коефіцієнти відображають відносну інтенсивність потреб у ресурсному забезпеченні та є функцією прогнозованої динаміки конфлікту.

Необхідний рівень ВЕБ на час *t* визначається за формулою:

$$W_{ВЕБ}^{необх}(t) = k(t) \cdot W_{ВЕБ}^{необх}(T),$$

де *k(t)* – характеристика степеня напруженості обстановки на час *t*; $W_{ВЕБ}^{необх}(T)$ –максимально необхідний рівень ВЕБ для виконання максимальної кількості завдань протягом усього планового горизонту *T*, $W_{ВЕБ}^{необх}(T) \in [0;1]$.

Максимально необхідний рівень ВЕБ визначається, виходячи з аналізу найбільш несприятливих сценаріїв розвитку воєнно-стратегічної обстановки, та задається нормативно або на підставі результатів стратегічного планування. Характеристика степеня напруженості *k(t)* описується функцією, що враховує прогнозовану динаміку конфлікту, сезонні фактори, ресурсні цикли та зовнішні чинники впливу, при цьому $k(t) \in [0;1]$, де значення 1 відповідає максимальній напруженості.

Блок 1.2. Формування вимог до ресурсного забезпечення визначеного рівня ВЕБ на час (t), період (T).

На підставі визначеного необхідного рівня ВЕБ здійснюється уточнення вимог до ресурсного забезпечення за складовими різних видів ресурсів: людських (i=1), матеріальних (i=2) та фінансових (i=3).

Для кожного виду ресурсів виділяються *j*-і (людські: $j \in [1; J]$), *l*-і (матеріальні: $l \in [1;L]$) та *d*-і (фінансові: $d \in [1; D]$) складові ресурсного забезпечення. Кожній складовій відповідає запланований (необхідний) рівень забезпеченості $E_i^{необх} \in [0;1]$, що розраховується на час *t* або плановий горизонт *T*.

Визначення вимог до ресурсного забезпечення виконується в такій послідовності:

1) Аналізуються складові людських, матеріальних та фінансових ресурсів (наприклад: чисельність особового складу різних вікових категорій, запаси боєприпасів, паливно-мастильних матеріалів, медичних засобів, фінансові резерви, оборонні витрати).

2) Для кожної складової встановлюються ваги $w_j^{необ}, w_l^{необ}, w_k^{необ}$, що відображають її відносну важливість для забезпечення заданого рівня ВЕБ у певній операційній обстановці. Суми ваг за кожним видом ресурсів нормуються до одиниці.

3) Формуються референтні таблиці вимог до ресурсної забезпеченості складових усіх трьох видів ресурсів на визначений час *t* або плановий горизонт *T*, що є основою для подальшого порівняння з фактичним станом.

Таблиця 1. Структура та параметри необхідного ресурсного забезпечення рівня ВЕБ

№	Складові людських ресурсів / Показники	Вимоги $w_j^{необх}$	№	Складові матеріальних ресурсів / Показники	Вимоги $w_l^{необх}$	№	Складові фінансових ресурсів / Показники	Вимоги $w_k^{необх}$
1	від 18 до 27 років, млн чол	14,67	1	Технічні	0,9	1	Запаси національної валюти, трл грн	13,5
2	від 27 до 45 років, млн чол	9,86	2	Матеріальні	0,9	2	Валютні запаси, млрд дол США	39,67
3	від 45 до 60 років, млн чол	2,35	3	Продовольчі	0,95	3	Запаси цінних металів, тон	31,2
4	чисельність ЗС України, тис чол	854,54	4	Медичні	0,85	4	Запаси цінних паперів, млрд дол	15,67
5	чисельність підготовленого резерву, тис чол	967,34	5	Інші	0,95	5	Обронні витрати, млрд дол	11,7

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

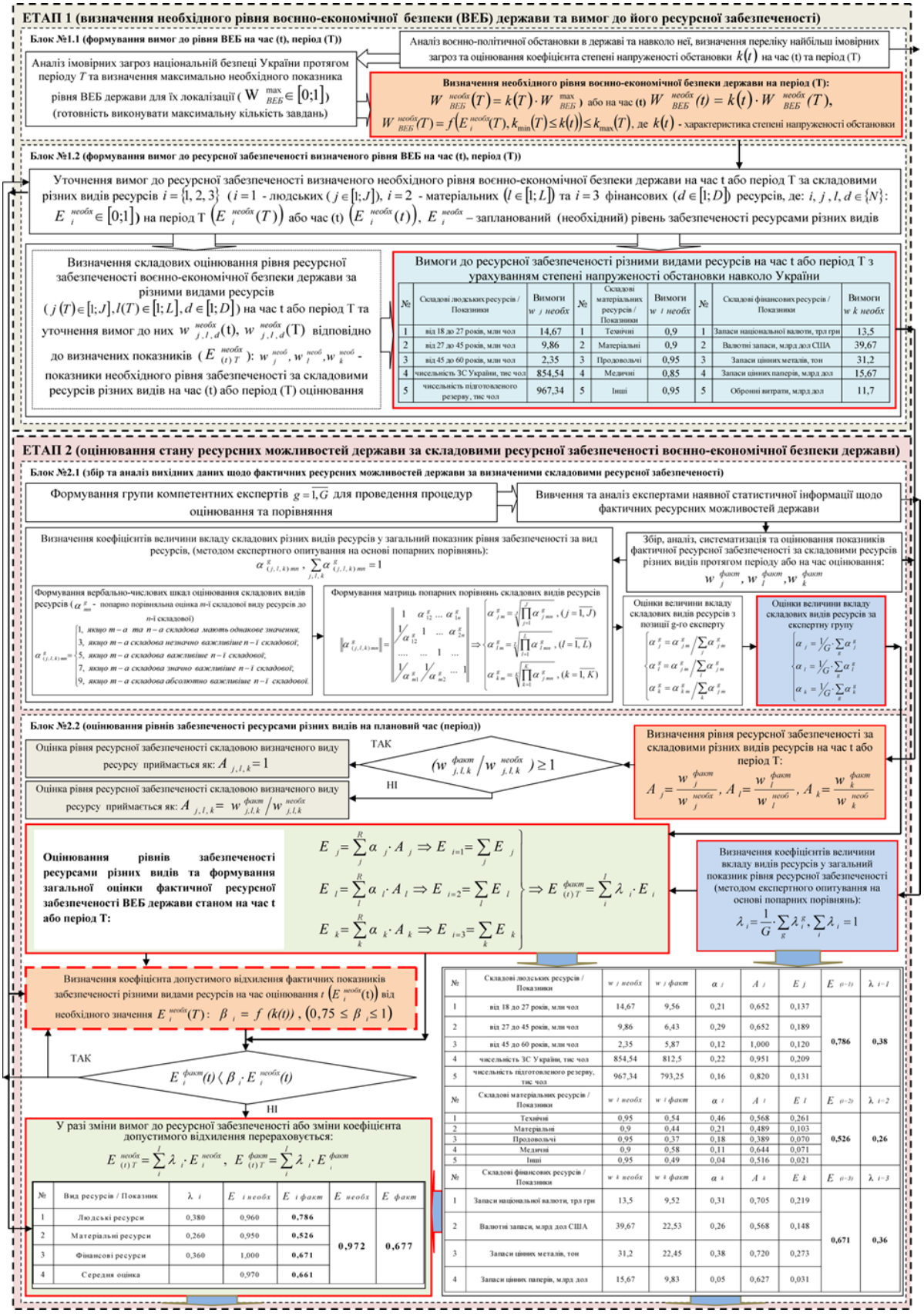


Рисунок 1. Загальна структура методу оцінювання стану ВЕБ держави (етапи 1–2)

The Central Research institute
of the Armed Forces of Ukraine

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

Military Science. Vol. 4 No.1 (2026)

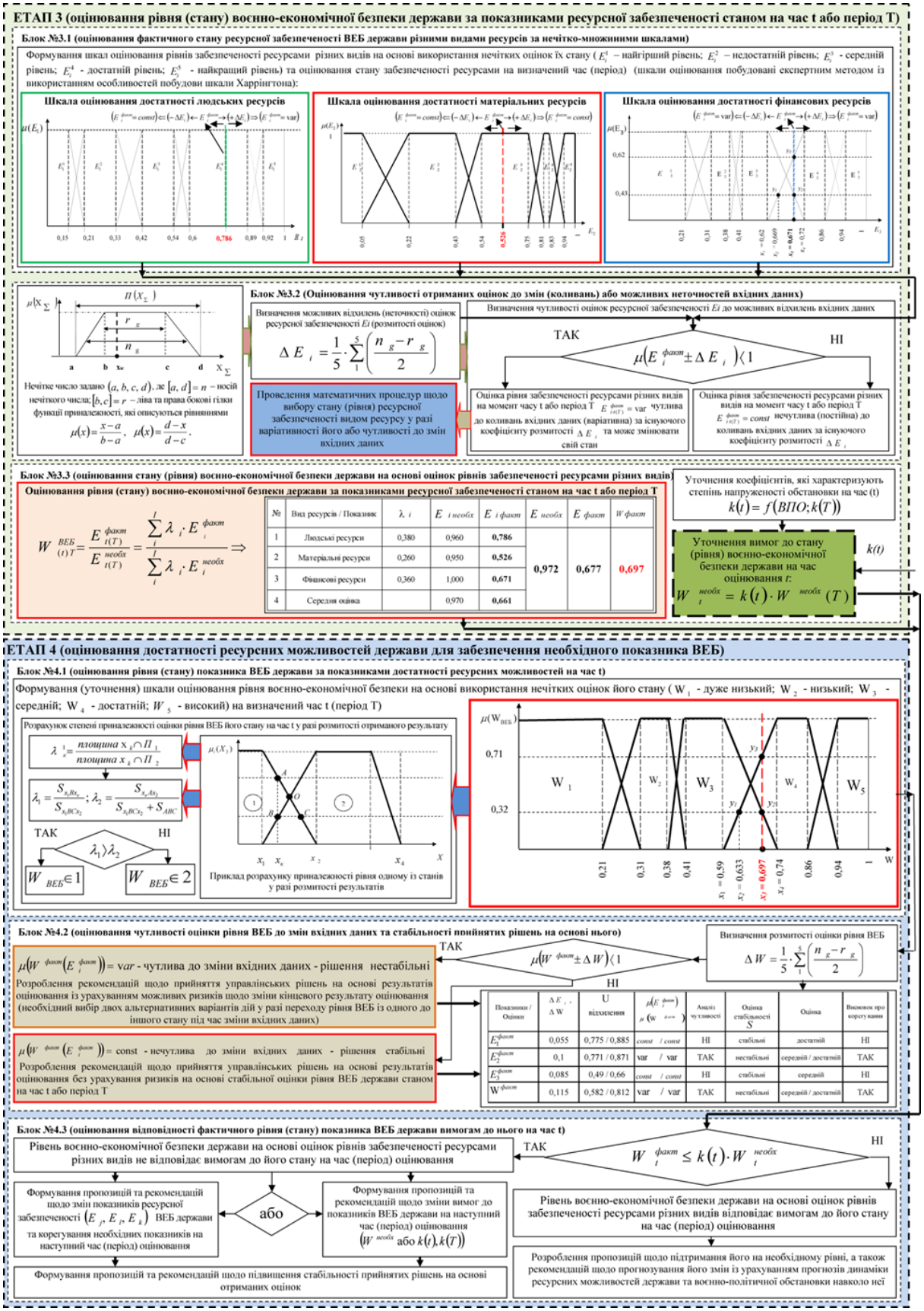


Рисунок 2. Загальна структура методу оцінювання стану ВЕБ держави (етапи 3–4)

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Етап 2. Оцінювання стану ресурсних можливостей держави за складовими ресурсної забезпеченості воєнно-економічної безпеки держави.

Другий етап спрямований на збирання, систематизацію та оцінювання фактичного стану ресурсних можливостей держави за всіма складовими трьох видів ресурсів: людських, матеріальних і фінансових. Етап складається з двох основних блоків.

Блок 2.1. Збирання та аналізування вихідних даних щодо фактичних ресурсних можливостей держави за визначеними складовими ресурсної забезпеченості.

Формується *група компетентних експертів* $g = \overline{1,G}$ для проведення процедур оцінювання та порівняння. Склад групи включає фахівців у галузі воєнної економіки, оборонного планування та управління ресурсами. Паралельно здійснюється збирання та аналіз наявної статистичної інформації щодо фактичних ресурсних можливостей держави.

Для визначення ваг складових кожного виду ресурсів застосовується метод попарних порівнянь. Формується матриця попарних порівнянь складових виду ресурсів, елементи якої α^{g}_{mn} відповідають оцінці відносної важливості *m*-ї складової порівняно з *n*-ю у формалізованій вербально-числовій шкалі:

$$\alpha^{g}_{(j,l,k)mn} = \begin{cases} 1, \text{ якщо } m-а \text{ та } n-а \text{ складова мають однакове значення}; \\ 3, \text{ якщо } m-а \text{ складова незначно важливіше } n-ї \text{ складової}; \\ 5, \text{ якщо } m-а \text{ складова важливіше } n-ї \text{ складової}; \\ 7, \text{ якщо } m-а \text{ складова значно важливіше } n-ї \text{ складової}; \\ 9, \text{ якщо } m-а \text{ складова абсолютно важливіше } n-ї \text{ складової}. \end{cases}$$

Коефіцієнти вкладу (ваги) α кожної складової виду ресурсів у загальний показник рівня забезпеченості за цим видом ресурсів визначаються на основі нормалізованих результатів попарних порівнянь, причому $\alpha^{g}_{(j,l,k)mn}$, $\sum_{j,l,k} \alpha^{g}_{(j,l,k)mn} = 1$.

Збирання, аналізування, систематизація та оцінювання фактичних показників ресурсної забезпеченості за складовими ресурсів виконується протягом планового горизонту або на час оцінювання. Фактичні значення показників записуються як $w^{факт}_{j}, w^{факт}_{l}, w^{факт}_{k}$ та порівнюються з необхідними $w^{необх}_{j,l,k}$.

Блок 2.2. Оцінювання рівнів забезпеченості ресурсами різних видів на плановий час (період).

Оцінка рівня ресурсної забезпеченості *j*-ї складової людських ресурсів (аналогічно – *l*-ї матеріальної та *d*-ї фінансової складової) визначається шляхом порівняння фактичних і необхідних показників:

якщо $(w^{факт}_{j,l,k} / w^{необх}_{j,l,k}) \geq 1$, тоді $A_{j,l,k} = 1$;

якщо $(w^{факт}_{j,l,k} / w^{необх}_{j,l,k}) < 1$, тоді $A_{j,l,k} = w^{факт}_{j,l,k} / w^{необх}_{j,l,k}$.

Загальний показник рівня ресурсної забезпеченості за складовими кожного виду ресурсів розраховується як зважена сума оцінок відповідних складових:

$$\left.\begin{aligned} E_j &= \sum_{j}^{R} \alpha_j \cdot A_j \Rightarrow E_{i=1} = \sum_{j} E_j \\ E_l &= \sum_{l}^{R} \alpha_l \cdot A_l \Rightarrow E_{i=2} = \sum_{l} E_l \\ E_k &= \sum_{k}^{R} \alpha_k \cdot A_k \Rightarrow E_{i=3} = \sum_{k} E_k \end{aligned}\right\} \Rightarrow E^{факт}_{(t)T} = \sum_{i}^{I} \lambda_i \cdot E_i .$$

Для формування інтегрального (загального) показника фактичного рівня ресурсної забезпеченості ВЕБ держави застосовується адитивна згортка з ваговими коефіцієнтами

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

$\lambda_i = \frac{1}{G} \cdot \sum_g \lambda_i^g$, $\sum_i \lambda_i = 1$ видів ресурсів:

$$E_{(t)T}^{необх} = \sum_i^I \lambda_i \cdot E_i^{необх}, \quad E_{(t)T}^{факт} = \sum_i^I \lambda_i \cdot E_i^{факт},$$

де λ_i – вагові коефіцієнти трьох видів ресурсів у загальному показнику рівня ресурсної забезпеченості ВЕБ, що визначаються методом попарних порівнянь та нормуються так, що $\sum_i \lambda_i = 1$.

Рекомендовані значення вагових коефіцієнтів видів ресурсів:

для людських – $\lambda_1 = 0{,}38$, для матеріальних – $\lambda_2 = 0{,}26$, для фінансових – $\lambda_3 = 0{,}36$.

Якщо фактичний показник забезпеченості окремим видом ресурсів знижується нижче допустимої межі, визначається коефіцієнт допустимого відхилення, і здійснюється перерахунок вимог до ресурсного забезпечення з урахуванням поточної обстановки. Приклад результатів розрахунку показано у таблицях на рис. 1 та рис. 2.

Етап 3. Оцінювання рівня (стану) воєнно-економічної безпеки держави за показниками ресурсної забезпеченості станом на час t або період T.

Третій етап є ключовим для отримання кількісної оцінки рівня ВЕБ з урахуванням нечіткості вхідних даних. Він складається з трьох блоків.

Блок 3.1. Оцінювання фактичного стану ресурсної забезпеченості ВЕБ держави за різними видами ресурсів за нечітко-множинними шкалами.

Для оцінювання рівнів ресурсної забезпеченості застосовуються нечіткі множини з функціями належності *μ(E)*. Визначаються п’ять рівнів стану ресурсної забезпеченості ВЕБ держави:

E^1 – найгірший рівень: критично низький рівень ресурсного забезпечення, при якому виконання основних завдань оборони практично неможливе;

E^2 – недостатній рівень: ресурсне забезпечення значно нижче необхідного, завдання оборони можуть виконуватися лише частково;

E^3 – середній рівень: ресурсне забезпечення відповідає мінімально допустимому, завдання оборони виконуються з суттєвими обмеженнями;

E^4 – достатній рівень: ресурсне забезпечення відповідає визначеним вимогам, завдання оборони виконуються в повному обсязі;

E^5 – найкращий рівень: ресурсне забезпечення перевищує необхідний рівень, держава має резервний потенціал для нарощування зусиль.

Шкали оцінювання достатності ресурсної забезпеченості для кожного виду ресурсів будуються на основі трапецієподібних або трикутних функцій належності нечіткого числа. Нечітке число задається параметрами *(a, b, c, d)*, де *[a, d] = n* – носій нечіткого числа, *[b, c] = r* – ліва та права бокові гілки функції приналежності. Функції приналежності визначаються за формулами:

$$\mu(x) = \frac{x-a}{b-a}, \quad \mu(x) = \frac{d-x}{d-c}.$$

Шкали оцінювання є специфічними для кожного виду ресурсів (людських, матеріальних, фінансових) та будуються методом експертного опитування з урахуванням особливостей побудови шкал Харрінгтона. Параметри функцій приналежності для кожного рівня визначаються на основі статистичних даних, нормативних документів та експертних оцінок.

Блок 3.2. Оцінювання чутливості отриманих оцінок до змін (коливань) або можливих неточностей вхідних даних.

Визначення можливих відхилень (неточностей) оцінок ресурсної забезпеченості ΔE_i

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

здійснюється за формулою: $\Delta E_i = \frac{1}{5} \cdot \sum_1^5 \left(\frac{n_g - r_g}{2} \right)$, де n_g – носій нечіткого числа, r_g – бокові гілки функції приналежності для g-ї складової.

Далі перевіряється умова $\mu\left(E_i^{факт} \pm \Delta E_i\right) \langle 1$. Якщо умова виконується, тоді оцінка рівня ресурсної забезпеченості нечутлива до коливань вхідних даних (розмита), тобто може змінювати свій стан. Якщо умова не виконується, тоді оцінка нечутлива (стала), тобто результат не зміниться за наявного коефіцієнта розмитості ΔE_i.

На підставі отриманих результатів проводиться процедура математичного вибору рівня (стану) ресурсної забезпеченості різних видів на час t або плановий горизонт T при варіативності коефіцієнта розмитості або його чутливості до змін вхідних даних.

Блок 3.3. Визначення стану (рівня) воєнно-економічної безпеки держави на основі оцінок рівнів забезпеченості ресурсами різних видів.

Загальний рівень (стан) ВЕБ держави на час t або плановий горизонт T визначається як відношення зваженої суми фактичних показників забезпеченості до відповідної зваженої суми необхідних показників: $W_{(t)T}^{ВЕБ} = \frac{E_{t(T)}^{факт}}{E_{t(T)}^{необх}} = \frac{\sum_i^I \lambda_i \cdot E_i^{факт}}{\sum_i^I \lambda_i \cdot E_i^{необх}}$, де $E_{t(T)}^{факт}$ та $E_{t(T)}^{необх}$ – фактичний та необхідний інтегральні показники ресурсної забезпеченості відповідно; λ_i – вагові коефіцієнти видів ресурсів.

Отримане значення $W^{необх}(T)$ інтерпретується відповідно до нечіткої шкали оцінювання стану ВЕБ держави (блок 4.1). У разі необхідності уточнення коефіцієнтів степеня напруженості обстановки здійснюється перерахунок необхідного рівня ВЕБ на час оцінювання: $W_t^{необх} = k(t) \cdot W^{необх}(T)$.

Етап 4. Оцінювання достатності ресурсних можливостей держави для забезпечення необхідного показника ВЕБ.

Четвертий, завершальний етап методу, спрямований на формування висновку щодо відповідності фактичного рівня ВЕБ необхідному та вироблення рекомендацій для органів державного управління.

Блок 4.1. Оцінювання (уточнення) шкали показника ВЕБ держави за показниками достатності ресурсних можливостей на час t.

Формується шкала оцінювання показника ВЕБ держави на основі нечітких оцінок його стану (рівня). Визначаються п’ять градацій стану ВЕБ: W_1 – дуже низький, W_2 – низький, W_3 – середній, W_4 – достатній, W_5 – високий. Відповідні функції приналежності нечітких множин будуються як трапецієподібні функції у просторі значень $W \in [0;1]$.

Розрахунок ступеня належності отриманого значення $W^{необх}(T)$ до одного зі станів виконується за формулою:

$$\lambda_к^1 = \frac{площина\ x_k \cap П_1}{площина\ x_k \cap П_2},$$

де $П_1$ та $П_2$ – функції приналежності двох суміжних рівнів ВЕБ, між якими розташоване розраховане значення W.

Якщо $\lambda_1 > \lambda_2$ – рівень ВЕБ відповідає стану та $W_{ВЕБ} \in 1$ (нижчий рівень); якщо $\lambda_1 \le \lambda_2$ – рівень ВЕБ відповідає стану тоді $W_{ВЕБ} \in 2$ (вищий рівень).

Блок 4.2. Оцінювання чутливості оцінки рівня ВЕБ до змін вхідних даних та стабільності ухвалення рішень на основі нього.

Визначається розмитість оцінки рівня ВЕБ держави за формулою:

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

$$\Delta W = \frac{1}{5} \cdot \sum_{1}^{5} \left(\frac{n_g - r_g}{2} \right).$$

Далі перевіряється умова $\mu\left(W^{факт} \pm \Delta W\right) \langle 1$:

- $\mu\left(W^{факт}\left(E_i^{факт}\right)\right) = \text{var}$ – чутлива до змін вхідних даних, тобто рішення нестабільне. Розробляються рекомендації щодо ухвалення управлінських рішень з урахуванням можливих ризиків зміни кінцевого результату оцінювання (необхідний вибір двох альтернативних варіантів дій у разі переходу рівня ВЕБ з одного в інший стан при зміні вхідних даних).
- $\mu\left(W^{факт}\left(E_i^{факт}\right)\right) = \text{const}$ – нечутлива до змін вхідних даних, тобто рішення стабільне. Розробляються рекомендації щодо ухвалення управлінських рішень без урахування ризиків на основі стабільної оцінки рівня ВЕБ держави станом на час *t* або плановий горизонт *T*.

Блок 4.3. Оцінювання відповідності фактичного рівня (стану) показника ВЕБ держави вимогам до нього на час t.

Перевіряється умова відповідності фактичного рівня ВЕБ необхідному:

$$W_t^{факт} \le k(t) \cdot W_t^{необх}.$$

Якщо умова виконується (ТАК), тобто фактичний рівень ВЕБ за оцінками рівнів забезпеченості ресурсами різних видів *відповідає вимогам до нього на час (період) оцінювання,* тоді розробляються пропозиції щодо підтримання рівня ВЕБ на необхідному рівні, а також щодо прогнозування його змін з урахуванням динаміки ресурсних можливостей держави та воєнно-політичної обстановки.

Якщо умова не виконується (НІ), тобто фактичний рівень ВЕБ за оцінками рівнів забезпеченості ресурсами різних видів *не відповідає вимогам,* тоді формуються такі пропозиції та рекомендації:

пропозиції щодо зміни показників ресурсної забезпеченості $\left(E_j, E_l, E_k\right)$ ВЕБ держави та коригування відповідних показників на наступний час (період) оцінювання;

пропозиції та рекомендації щодо зміни вимог до показників ВЕБ на наступний час (період) оцінювання $\left(W^{необх}\right.$ або $\left.k(t), k(T)\right)$;

рекомендації щодо підвищення стабільності ухвалених рішень на основі отриманих оцінок.

Обговорення (Discussion)

Розроблений метод оцінювання стану ВЕБ держави на основі нечітких оцінок ресурсних можливостей має низку суттєвих переваг порівняно з традиційними детермінованими підходами. По-перше, метод забезпечує об'єктивну кількісну оцінку рівня ВЕБ з урахуванням реальної невизначеності вхідних даних, що є критично важливим в умовах активних бойових дій та постійних змін оперативної обстановки. По-друге, апарат нечітких множин дозволяє формалізувати якісні експертні судження та перевести їх у кількісні оцінки без втрати інформативності.

Результати апробації методу на прикладі України, але наведений приклад відповідає стану на кінець 2021 року, бо, з огляду на триваючу війну, слід враховувати під час оцінювання ВЕБ держави додаткові воєнно-економічні обмеження. Але необхідність врахування цих обмежень, пов'язаних з вимогами до необхідного рівня ВЕБ (вимоги повинні мати особливу структуру розрахунку в умовах війни), свідчить про те, що запропонований метод є працездатним й може застосовуватися в будь-яких умовах розвитку держави.

Важливою властивістю методу є оцінювання чутливості отриманих результатів до змін вхідних даних. Як показує аналіз (рис. 2), оцінка загального рівня ВЕБ є чутливою до варіацій даних щодо матеріального забезпечення, що обумовлює необхідність ухвалення

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

управлінських рішень з урахуванням ризику зміни оцінки зі “середнього” на “достатній” рівень. Це дозволяє особам, що ухвалюють рішення, завчасно планувати два альтернативні варіанти дій відповідно до можливого розвитку ситуації.

Серед обмежень методу слід відзначити залежність якості результатів від достовірності вхідних статистичних даних та кваліфікації групи експертів. В умовах воєнного конфлікту отримання повних статистичних даних може бути ускладненим, що зумовлює потребу в розробленні методів верифікації та корекції вхідних даних. Крім того, параметри нечітких функцій приналежності потребують регулярного перегляду відповідно до змін операційного середовища.

Перспективними напрямами розвитку методу є: інтеграція з системами підтримки ухвалення рішень на основі штучного інтелекту; розширення переліку показників ресурсного забезпечення (зокрема, цифрових та технологічних ресурсів); адаптація методу для оцінювання ВЕБ коаліційних формувань та міжнародних партнерств у сфері колективної оборони.

Висновок (Conclusions)

У результаті проведеного дослідження розроблено метод оцінювання стану воєнно-економічної безпеки держави на основі нечітких оцінок ресурсних можливостей, що передбачає чотири взаємопов’язані етапи:

1) перший етап – визначення необхідного рівня ВЕБ та формалізація вимог до ресурсного забезпечення, що дозволяє встановити цільові показники ВЕБ з урахуванням динаміки воєнно-політичної обстановки та коефіцієнтів степеня напруженості;

2) другий етап – оцінювання стану ресурсних можливостей держави, що забезпечує систематизацію та кількісну оцінку фактичного рівня людських, матеріальних і фінансових ресурсів у зіставленні з необхідними за допомогою методу попарних порівнянь;

3) третій етап – оцінювання рівня ВЕБ за нечіткими шкалами, що реалізує апарат нечітких множин для формування лінгвістично інтерпретованих оцінок та аналізу їх чутливості до невизначеності вхідних даних;

4) четвертий етап – оцінювання достатності ресурсних можливостей, що завершує цикл оцінювання формуванням висновку про відповідність рівня ВЕБ вимогам та виробленням управлінських рекомендацій.

Метод апробовано на прикладі оцінювання ресурсних можливостей України, що підтвердило його практичну значущість. Практична значущість методу полягає в тому, що його результати можуть бути використані: органами державної влади та Міністерством оборони для стратегічного планування оборонних ресурсів; Генеральним штабом Збройних Сил України для поточного контролю рівня ВЕБ; аналітичними центрами та науковими установами для прогнозування змін ресурсних можливостей держави в умовах воєнного конфлікту.

Перспективними напрямами подальших досліджень є розширення переліку складових ресурсного забезпечення, розроблення автоматизованих систем збирання та верифікації вхідних даних, а також інтеграція методу з системами підтримки ухвалення рішень на основі штучного інтелекту в контексті цифровізації оборонного планування.

Конфлікт інтересів (Conflict of Interest)

Авторка заявляє, що у неї немає конкуруючих інтересів за тематикою статті.

Подяки (Acknowledgments)

Дослідження виконано в рамках науково-дослідних робіт Центрального науково-дослідного інституту Збройних Сил України.

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Використані джерела

1. Семененко, О. М., Водчиць, О. Г., & Кремешний, О. І. (2021). Методичний підхід до оцінювання воєнно-економічної безпеки держави. *Збірник наукових праць ЦНДІ ЗС України*, *4* (97), 6–18.
2. Семененко, О. М., & Воронченко, І. О. (2022). Методологія оцінювання стану воєнно-економічної безпеки та оборонного потенціалу держави. *Системи озброєння і військова техніка*, *2* (70), 3–12.
3. Горбулін, В. П., & Качинський, А. Б. (2020). *Стратегічне планування: вирішення проблем національної безпеки*. НІСД.
4. Лопатін, О. Л., & Семененко, О. М. (2021). *Оборонне планування на основі спроможностей: методологія та практика*. ЦНДІ ЗС України.
5. Гаврилюк, І., Клят, Ю., Водчиць, О., Добровольський, Ю., Гетьман, А., & Фомкін, Д. (2025). Щодо оцінки військово-економічної безпеки України в контексті сучасних військових конфліктів. *Соціальний розвиток і безпека*, *15* (1), 19–25. https://doi.org/10.33445/sds.2025.15.1.3
6. Заде, Л. А. (1976). *Понятие лингвистической переменной и его применение к принятию приближённых решений*. Мир.
7. Zadeh, L. A. (1965). Fuzzy sets. *Information and Control*, *8*, 338–353. https://doi.org/10.1016/S0019-9958(65)90241-X
8. Ротштейн, А. П. (1999). *Интеллектуальные технологии идентификации: нечёткая логика, генетические алгоритмы, нейронные сети*. УНИВЕРСУМ-Вінниця.
9. Рибачок, В. Л. (2020). Застосування методів нечіткої логіки для оцінювання інтегральних показників у військово-економічному аналізі. *Системи озброєння і військова техніка*, *1* (61), 67–74.
10. Беллман, Р., & Заде, Л. (1976). Принятие решений в расплывчатых условиях. In *Вопросы анализа и процедуры принятия решений* (с. 172–215). Мир.
11. Harrington, E. C. (1965). The desirability functions. *Industrial Quality Control*, *21* (10), 494–498.
12. Saaty, T. L. (1980). *The analytic hierarchy process*. McGraw-Hill.
13. Борисенко, М. В., & Семененко, О. М. (2023). Метод оцінювання рівня ресурсного забезпечення воєнно-економічної безпеки із застосуванням нечітких множин. *Науковий вісник Херсонського державного університету. Серія: Економічні науки*, *49*, 15–22.
14. Ярош, В. О., & Семененко, О. М. (2022). Аналіз достатності ресурсних можливостей держави для забезпечення заданого рівня воєнно-економічної безпеки. *Збірник наукових праць ЦНДІ ЗС України*, *1* (98), 32–41.
15. Клименко, В. А., & Гречко, А. В. (2021). *Методи нечіткого моделювання в системах підтримки прийняття рішень у сфері оборони*. ХУПС ім. І. Кожедуба.
16. Петренко, А. В., & Семененко, О. М. (2023). Оцінювання чутливості нечітких оцінок рівня воєнно-економічної безпеки до змін вхідних даних. *Вісник НТУУ «КПІ». Серія: Інформатика, управління та обчислювальна техніка*, *78*, 45–53.
17. Рубець, М. В. (2022). Нечіткі моделі оцінювання оборонного потенціалу держави в умовах неповноти інформації. *Проблеми програмування*, *2–3*, 115–123.
18. Грінченко, Т. А. (2023). Застосування теорії нечітких множин для аналізу фінансової складової воєнно-економічної безпеки. *Фінанси України*, *6*, 87–96.
19. Водчиць, О. Г., & Семененко, О. М. (2021). Методика побудови шкал оцінювання ресурсної забезпеченості воєнно-економічної безпеки держави. *Наука і техніка Повітряних Сил ЗС України*, *4* (45), 58–66.

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

20. Кремешний, О. І., & Борисенко, М. В. (2022). Формування показників достатності ресурсних можливостей держави для планування оборонних потреб. *Збірник наукових праць Національного університету оборони України*, *3* (32), 29–38.

References

1. Semenenko, O. M., Vodchyts, O. H., Kremeshnyi, O. I. (2021). Methodical approach to assessing the military-economic security of the state. *Collection of Scientific Works of the Central Research Institute of the Armed Forces of Ukraine*, *4* (97), 6–18.
2. Semenenko, O. M., & Voronchenko, I. O. (2022). Methodology for assessing the state of military-economic security and defense potential of the state. *Systems of Arms and Military Equipment*, *2* (70), 3–12.
3. Horbulin, V. P., & Kachynskyi, A. B. (2020). *Strategic planning: Solving national security problems*. NISS.
4. Lopatin, O. L., & Semenenko, O. M. (2021). *Capability-based defense planning: Methodology and practice*. Central Research Institute of the Armed Forces of Ukraine.
5. Havryliuk, I., Kliat, Y., Vodchyts, O., Dobrovolskyi, Y., Hetman, A., & Fomkin, D. (2025). On the assessment of Ukraine's military-economic security in the context of modern military conflicts. *Social Development and Security*, *15* (1), 19–25. https://doi.org/10.33445/sds.2025.15.1.3
6. Zadeh, L. A. (1976). *The concept of a linguistic variable and its application to approximate reasoning*. Mir.
7. Zadeh, L. A. (1965). Fuzzy sets. *Information and Control*, *8*, 338–353. https://doi.org/10.1016/S0019-9958(65)90241-X
8. Rotshtein, A. P. (1999). *Intelligent identification technologies: Fuzzy logic, genetic algorithms, neural networks*. Universum-Vinnytsia.
9. Rybachok, V. L. (2020). Application of fuzzy logic methods for evaluating integral indicators in military-economic analysis. *Systems of Arms and Military Equipment*, *1* (61), 67–74.
10. Bellman, R., & Zadeh, L. A. (1976). Decision-making in a fuzzy environment. In *Problems of analysis and decision-making procedures* (pp. 172–215). Mir.
11. Harrington, E. C. (1965). The desirability functions. *Industrial Quality Control, 21*(10), 494–498.
12. Saaty, T. L. (1980). *The analytic hierarchy process*. McGraw-Hill.
13. Borysenko, M. V., & Semenenko, O. M. (2023). Method for assessing the level of resource provision of military-economic security using fuzzy sets. *Scientific Bulletin of Kherson State University. Series: Economic Sciences*, *49*, 15–22.
14. Yarosh, V. O., & Semenenko, O. M. (2022). Analysis of the sufficiency of state resource capabilities to ensure a given level of military-economic security. *Collection of Scientific Works of the Central Research Institute of the Armed Forces of Ukraine*, *1* (98), 32–41.
15. Klymenko, V. A., & Hrechko, A. V. (2021). *Methods of fuzzy modeling in decision support systems in the defense sector*. Ivan Kozhedub Kharkiv National Air Force University.
16. Petrenko, A. V., & Semenenko, O. M. (2023). Sensitivity assessment of fuzzy evaluations of the level of military-economic security to changes in input data. *Bulletin of NTUU "KPI". Series: Informatics, Control and Computer Engineering*, *78*, 45–53.
17. Rubets, M. V. (2022). Fuzzy models for assessing the defense potential of the state under conditions of incomplete information. *Problems in Programming*, *2–3*, 115–123.
18. Hrinchenko, T. A. (2023). Application of fuzzy set theory for analyzing the financial component of military-economic security. *Finance of Ukraine*, *6*, 87–96.
19. Vodchyts, O. H., & Semenenko, O. M. (2021). Methodology for constructing evaluation scales of resource provision for military-economic security of the state. *Science and Technology of*

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

the Air Force of Ukraine, *4* (45), 58–66.
20. Kremeshnyi, O. I., & Borysenko, M. V. (2022). Formation of indicators of sufficiency of state resource capabilities for defense planning. *Collection of Scientific Works of the National Defense University of Ukraine*, *3* (32), 29–38.

Method of Assessing the State of Military-Economic Security of the State Based on Fuzzy Estimates of Resource Capabilities

Polina Tolok
Candidate of Economic Sciences, Senior Researcher
Senior Research Fellow
State Research Institute for Testing and Certification of
Armaments and Military Equipment
e-mail: tolok100@meta.ua
ORCID: 0000-0002-2481-8152

Abstract. Ensuring the military-economic security (VES) of the state in the conditions of modern military conflicts is a key task of the national security system. The resource capabilities of the state, namely: human, material and financial resources, determine its ability to perform defense tasks. However, traditional methods of quantitative assessment of the state of VES do not fully take into account the uncertainty and inaccuracy of input data inherent in the conditions of combat use. The purpose of the article is to develop and provide a detailed description of a method for assessing the state of military-economic security of the state, which is based on the use of fuzzy estimates of resource capabilities. The method is implemented in four consecutive stages: the first is the determination of the required level of VEB and requirements for resource provision; the second is the assessment of the state's resource capabilities by the components of resource provision; the third is the formation of a fuzzy scale for assessing the level of VEB and assessing the sensitivity of the obtained estimates; the fourth is the assessment of the sufficiency of the state's resource capabilities to ensure the required VEB indicator. The proposed method allows for a quantitative assessment of the level of VEB taking into account the vagueness of the input data, to determine the deviation of the actual indicators of resource provision from the required ones, and to formulate recommendations for state administration bodies. The method was tested on the example of assessing the resource capabilities of Ukraine, which confirms its practical significance for planning defense resources and making management decisions.

Keywords: military-economic security, resource capabilities of the state, fuzzy sets, fuzzy estimates, assessment method, human resources, material resources, financial resources, level of security, defense potential, degree of tension of the situation, paired comparisons.

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Received: *May 21, 2025*| **Revisions Requested:** - | **Revision Received:** -
Accepted: *October 28, 2025* | **Published Online:** *April 10, 2026*

Licensed (C) by Creative Commons Attribution International License 4.0 (CC BY-NC-SA)

DOI: 10.62524/msj.2026.4.1.10

The Foresight of the russian federation's Mobilisation Potential: Structure, Mechanisms and Development Scenarios for 2025–2026 years

Volodymyr Hurkovskyi
Doctor of Public Administration, Professor
Chief of Branch
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

Robert Ovanesian
Leading Research Fellow
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl Avenue, 28 B, Kyiv, Ukraine
e-mail: bober1609@gmail.com
ORCID: 0009-0008-6761-2059

Denys Kalashnikov
Research Fellow
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl Avenue, 28 B, Kyiv, Ukraine
e-mail: kalash179@gmail.com
ORCID: 0009-0003-4625-6191

Andrii Tsybizov
Candidate of Military 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: Enigma_007@ukr.net
ORCID: 0000-0001-6555-5005

Karel Nedbalek
Doctor of Law, Professor
European Professional Doctorate
Zlín, Czech Republic
e-mail: slusovice@motelgolg.cz
ORCID: 0000-0002-1010-2460

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Abstract. Relevance of the study is due to the need to anticipate how the russian federation will compensate for its losses under the conditions of a protracted war. For example, analysis of open sources from July 2025 indicates russia's plans to expand conscription through reforms of the military administration, which may change the dynamics of the war. For Ukraine, this means a need for accurate data and forecasts in order to effectively allocate its own resources. The article is dedicated to a systematic analysis and foresight of the mobilisation potential of the russian federation under the conditions of full-scale war against Ukraine. The study reveals the structure, troop generation mechanisms, and limitations of the russian mobilisation system, proposing a forecast of its development for 2025–2026. The aim of the article – is to conduct a systematic analysis of the organisation of russia's mobilisation resource in the context of its war against Ukraine and to develop a forecast of its mobilisation capabilities for 2025–2026. The article outlines the structure and characteristics of russia's mobilisation resource, including the legal framework and recruitment mechanisms; it examines the specifics of partial mobilisation, contract service, recruitment of foreigners, and forced conscription in the occupied territories; it identifies key limitations of the system based on verified data; it formulates a forecast based on current trends and historical examples; and it offers conclusions to support Ukraine's strategic defence planning. A systemic approach is the basis of the study, as mobilisation in russia represents a complex system encompassing the legislative framework, administrative mechanisms, socio-economic conditions, and the ideological apparatus. For the analysis, the model of general systems theory by Ludwig von Bertalanffy is used, which considers a system as a set of interconnected elements, where a change in one component, for example, the demographic reserve, affects others, such as military effectiveness or economic stability. Based on empirical and theoretical methods, including the analysis of official documents, reports by ISW, RAND, Human Rights Watch, and other open sources, it has been established that mobilisation in russia relies on a centralised repressive system, but faces a demographic crisis (a 10% decrease in the working-age population by 2030), economic sanctions (a 3.5% decrease in GDP in 2023–2024), and organisational problems (corruption, lack of equipment). Partial mobilisation, contract service, recruitment of foreigners (including from North Korea and Nepal), and forced conscription in the temporarily occupied territories of Ukraine are the key mechanisms, but their effectiveness is decreasing due to low training levels and resistance. The forecast for 2025–2026 anticipates the continuation of hybrid mobilisation (150–200 thousand people annually), but with the risk of exhaustion due to economic and social constraints. Historical examples (Japan 1941–1945, the USSR in Afghanistan) highlight the vulnerability of such systems. For Ukraine, information operations, strikes on logistics, and strengthening of sanctions are recommended. The study offers strategic leverage points to weaken the enemy, which is of critical importance for state defence.

Keywords: mobilisation resource, russian federation, mobilisation potential, russian-Ukrainian war, foresight, partial mobilisation, contract service, occupied territories, demographic crisis, economic sanctions, strategic planning.

Introduction

The war of russia against Ukraine, which has been ongoing since 2014 and escalated sharply with the full-scale invasion on 24 February 2022, imposes new requirements on the analysis of russia's military capabilities, in particular its mobilisation resources. Against the backdrop of significant losses, which, according to estimates by the Institute for the Study of War (ISW), amount to hundreds of thousands of killed and wounded as of 2025, russia is forced to continuously adapt its force generation system in order to maintain its offensive potential.

The losses of the russian army, together with the need for troop rotation and the creation of reserves, have created an urgent demand for replenishing human resources to sustain the war effort.

Since the conflict has officially been referred to as a "special military operation", full

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

mobilisation has not been declared in russia. Instead, alternative methods of force generation have been employed, including partial mobilisation, forced conscription in occupied territories, recruitment of so-called volunteers into regular forces and "private military companies", the use of prisoners, foreign nationals, and the transfer of conscripts to contract service. However, these methods have faced serious organisational, logistical, and social challenges, complicating the provision of sufficient personnel. This process includes partial mobilisation, contract-based service, forced recruitment of residents in the temporarily occupied territories of Ukraine, and the enlistment of foreign mercenaries. For Ukraine, which is resisting aggression, understanding these mechanisms is critical for forecasting enemy actions and developing effective counter-strategies.

The mobilisation resource of russia is a complex system dependent on demographic, economic, and political factors. The totalitarian regime, which has intensified since 2022, effectively suppresses any attempts at public resistance by employing repressive legislation, such as the amendments to the Criminal Code of the russian federation of 3 March 2022, which предусматривают (provide for) up to 15 years of imprisonment for "disseminating false information" about the actions of the russian armed forces. At the same time, russia faces internal challenges: a demographic crisis, economic sanctions, and the loss of skilled personnel complicate efforts to expand its military. For example, according to ISW data, russia is planning reforms to expand the recruitment of reservists and contract soldiers to compensate for losses; however, these measures have limited effectiveness due to low public motivation and economic constraints.

The analysis of russia's mobilisation resource is important not only for assessing its current capabilities but also for forecasting its actions in the medium term (2025–2026). The historical example of France's mobilisation during the Napoleonic Wars (1799–1815), when the "levée en masse" system enabled the rapid formation of a large army but led to resource exhaustion, illustrates the limits of coercive mobilisation models. Today, russia, similarly to historical empires, is balancing between coercion and attempts to stimulate voluntary recruitment, creating both opportunities and vulnerabilities.

The aim of this article is to conduct a systematic analysis of the organisation of russia's mobilisation resource in the context of the war against Ukraine and to develop a forecast of its mobilisation capabilities for 2025–2026. The objectives are as follows:

to characterise the structure and features of russia's mobilisation resource, including the legislative framework and recruitment mechanisms;

to examine the specifics of partial mobilisation, contract service, recruitment of foreigners, and forced conscription in occupied territories;

to identify key limitations of the system based on verified data;

to formulate a forecast based on current trends and historical examples;

to provide conclusions that will support Ukraine's defence planning.

The relevance of this study is determined by the need to anticipate how russia will compensate for its losses in the context of a protracted war. For instance, the analysis of open sources from July 2025 indicates russia's plans to expand conscription through reforms of its military administration, which may alter the dynamics of the war. For Ukraine, this implies the need for accurate data and forecasts in order to effectively allocate its own resources. The following section, devoted to methodology, will outline the analytical approach ensuring the validity and reliability of the conclusions.

Methodological Framework

The study of the mobilisation resource of the russian federation in the context of the full-scale war against Ukraine requires a systematic approach that integrates empirical and theoretical methods to analyse the interconnections between demographic, economic, political, and military factors. This section outlines the methodological framework used for the analysis, explains the selection of sources

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

and methods, and substantiates the relevance of the topic for Ukraine's defence planning.

A systems approach forms the basis of this study, as mobilisation in russia represents a complex system encompassing the legislative framework, administrative mechanisms, socio-economic conditions, and ideological apparatus. The analysis employs the general systems theory model of Ludwig von Bertalanffy, which considers a system as a set of interconnected elements, where changes in one component, such as the demographic reserve, affect others, including military effectiveness and economic stability [1]. This approach makes it possible to identify leverage points — vulnerabilities within the system that may be exploited for strategic influence.

Empirical methods include the analysis of primary and secondary sources. Primary sources comprise official documents, in particular Presidential Decree of the russian federation No. 647 of 21 September 2022 on partial mobilisation [2]. Secondary sources include analytical reports of international organisations such as ISW and the RAND Corporation, as well as publications in academic databases (JSTOR, Springer) and media outlets such as Euromaidan Press and Texty.org.ua. In particular, the ISW report of 22 December 2024 on the militarisation of youth in russia and in the temporarily occupied territories of Ukraine was used to analyse military-patriotic training programmes [3]. To ensure relevance, data from posts on the X platform from July 2025 were used, indicating russia's plans to reform its conscription system [4].

Theoretical methods include comparative analysis and forecasting. Comparative analysis was applied to compare contemporary russian mobilisation with historical examples, in particular the "levée en masse" system in France during the Napoleonic Wars, which demonstrated both the effectiveness of forced mobilisation and its limits due to resource exhaustion [5]. Forecasting is based on a qualitative approach that takes into account demographic trends, such as the projected decline of russia's working-age population by 2030 according to Rosstat [6], economic constraints caused by sanctions [7], and political factors, including the strengthening of the repressive apparatus through amendments to the Criminal Code of the russian federation [8]. Scenario analysis is used to assess possible developments, enabling the modelling of different trajectories for 2025–2026, such as the continuation of partial mobilisation or a transition to full mobilisation.

The selection of sources is determined by their relevance and reliability. Academic databases such as JSTOR provide access to studies on mobilisation systems in authoritarian regimes [9], while reports by ISW and RAND offer up-to-date data on russian military strategy [3, 10]. Media outlets such as Euromaidan Press are used to analyse developments in the occupied territories [11], while posts on the X platform are employed to track current trends, including statements on reforms of military administration in russia [4].

The choice of the research topic is based on its critical importance for Ukraine's national security. russia's mobilisation resource directly affects the course of the war, as its effectiveness determines the ability to compensate for losses, which, according to estimates by Forbes Ukraine, may reach up to 30,000 personnel per month [12]. These data suggest that the russian federation may sustain its mobilisation reserve until 2032 under current conditions, making the forecasting of its capabilities strategically essential. For Ukraine, which is confronting a numerically superior adversary, understanding these processes enables the development of countermeasures, such as strikes on logistical centres or information campaigns aimed at demoralising russian recruits.

The proposed methodology ensures a comprehensive and substantiated approach to the analysis by combining empirical data with theoretical models. The following section, devoted to the results of the study, will examine in detail the structure of russia's mobilisation resource, the mechanisms of force generation, and the key limitations of the system, thereby providing a foundation for forecasting developments in 2025–2026.

Results and Discussions

The methodological framework outlined in the previous section has enabled a systematic

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

approach to analysing the mobilisation resource of the russian federation, considering it as a complex system operating under the conditions of a full-scale war against Ukraine. This section examines the specific features of mobilisation organisation, the structure of the mobilisation resource, force generation mechanisms, and the key constraints affecting the effectiveness of the russian military system. The findings are based on the analysis of official documents, reports by international organisations, academic sources, and up-to-date data reflecting the situation as of July 2025.

Features of mobilisation organisation in russia

Mobilisation in russia is a centralised system regulated by a number of legislative acts, in particular the Federal Law "On Mobilisation Preparation and Mobilisation in the russian federation" No. 31-FZ of 1997, supplemented by amendments introduced after 2022 [13]. These amendments, inter alia, expanded the powers of military commissariats and introduced electronic draft notices, enabling the automation of conscription processes [14]. The system relies on a totalitarian state apparatus which, akin to a "web", encompasses regional administrations, security structures, and propaganda media, ensuring the coercive involvement of citizens. However, this centralisation also has a downside: bureaucratic inertia and corruption complicate the rapid deployment of forces.

A key feature is the hybrid approach, combining forced mobilisation with voluntary contract-based service. For example, following the announcement of partial mobilisation in September 2022, russia reportedly mobilised 300,000 personnel; however, actual figures are likely higher than officially declared, as the kremlin continues to employ covert mobilisation practices. Against this background, recruitment is further complicated by draft evasion and logistical challenges [15]. At the same time, the state has intensified propaganda campaigns aimed at "patriotic" indoctrination, particularly through programmes such as "Yunarmiya" and the militarisation of schools, which, according to ISW data, involved up to 1.5 million adolescents in 2024 [3].

Structure of the mobilisation resource

russia's mobilisation resource is based on the country's demographic structure, which comprises approximately 146 million people, of whom the working-age population (15–59 years) accounts for around 80 million [6]. However, the actual mobilisation potential is limited: according to expert estimates, the working-age population will decrease by 10% by 2030 due to low birth rates and emigration [16].

At the same time, russia's mobilisation potential is significantly larger in theoretical terms due to its population size. Estimates suggest that the total mobilisation potential amounts to approximately 20–25 million people. However, this figure is purely theoretical and does not account for the actual capacity or willingness of these citizens to serve. The practical ability to mobilise such numbers is constrained by economic, logistical, and social barriers, which hinder the rapid formation of large military contingents.

The core mobilisation reserve includes:

conscription-age individuals – men aged 18 to 30 subject to mandatory military service;

reservists – citizens who have previously completed military service and remain in reserve, forming the main component of the mobilisation reserve (approximately 2 million individuals with prior conscription experience) [17];

contract soldiers – approximately 500,000 personnel in the russian armed forces as of 2025 [18];

volunteers – individuals who join the armed forces voluntarily;

conscripts – up to 250,000 annually through regular conscription cycles [19];

women – individuals with relevant military specialisations who may also be mobilised.

Losses in Ukraine, which, according to the General Staff of the Armed Forces of Ukraine, exceeded 700,000 killed and wounded as of July 2025, have significantly reduced this reserve [20]. For comparison, during the Second Chechen War (1999–2009), russia lost approximately 25,000 personnel over ten years, highlighting the unprecedented scale of current losses [21].

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Mechanisms for Manning the Armed Forces

At the outset of its full-scale aggression against Ukraine, the russian federation deployed approximately 200,000 troops. By the end of 2023, according to statements by the russian dictator, around 617,000 military personnel were already involved in the so-called "special military operation", with 244,000 directly engaged in combat operations [22]. In the context of a war of attrition, manpower requirements are not limited to compensating losses but also include the accumulation of reserves for future military operations and the rotation of personnel.

To maintain the necessary level of personnel, russia employs several approaches:

Mobilisation in the occupied territories:

In the occupied territories of Ukraine (Donetsk, Luhansk, Kherson, and Zaporizhzhia regions), russia conducts forced mobilisation. According to available data, starting from 19 February 2022, the russian federation carried out mobilisation in the occupied parts of Donetsk and Luhansk regions. Within this framework, supporters of the so-called "russian world" were recruited voluntarily, while other citizens were forcibly conscripted, including full-time students and cadets of the Donetsk and Luhansk academies of the Ministry of Internal Affairs. These measures were accompanied by mass "round-ups" of men of conscription age. According to estimates by the Eastern Human Rights Group, as of June 2022, around 140,000 individuals had been mobilised, with an additional 80,000 mobilised during the so-called partial mobilisation. By summer 2024, this number had risen to 300,000. The mobilisation of human resources in the occupied territories continues to this day [23].

The involvement of personnel who previously served in the so-called "people's militias", the use of mobilised individuals from these regions, and the recruitment of russian volunteers partially compensated for losses and the growing demand for manpower; however, significant problems remained unresolved.

According to Human Rights Watch, between 2022 and 2024 up to 100,000 individuals were mobilised in the so-called DPR and LPR, often under the threat of execution [28]. These units are frequently used as expendable forces, which reduces their combat effectiveness and provokes local resistance.

Partial mobilisation:

The russian federation first faced an acute need to reinforce its armed forces in early autumn 2022. This was a consequence of the successful Ukrainian counteroffensive in the Kharkiv region. As a result, in late September 2022 the kremlin was forced to announce a partial mobilisation, which formally lasted until January 2023. This measure enabled a rapid increase in troop numbers by approximately 300,000 personnel. However, the process revealed systemic challenges: ineffective accounting of mobilisation resources, insufficient infrastructure, and logistical shortcomings in equipping recruits. To partially mitigate these issues, russia began using the territory of belarus as a training ground for newly mobilised personnel.

The partial mobilisation announced in September 2022 became a key instrument for replenishing the armed forces. According to official figures, 300,000 individuals were planned to be mobilised, but the actual number was lower due to widespread draft evasion: according to BBC estimates, up to one million men left russia in 2022–2023 [15]. The mobilisation process exposed systemic deficiencies, including inadequate training of reservists, corruption in military enlistment offices, and shortages of equipment. For example, mobilised personnel from Dagestan reported a lack of body armour and modern weapons [25].

At the time of the full-scale invasion of Ukraine, the strength of the armed forces of the russian federation amounted to 1,902,758 personnel, including 1,013,628 military servicemen. However, since January 2023, the kremlin has been forced to increase the size of its armed forces three times. As a result, the authorised strength rose by 12.5% to 2,039,758 personnel, including 1,150,628 military servicemen. From December 2023, the authorised strength was further increased by 14.7% to 2,209,130 personnel, including 1,320,000 military servicemen. From 1 December 2024, the size

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

of the armed forces increased by a further 13.6%, reaching 2,389,130 personnel, including 1,500,000 military servicemen.

The dynamics of the growth in the size of the armed forces of the russian federation are illustrated in Figures 1–5.

It should be noted that the announcement of partial mobilisation did not trigger critical internal upheaval for the kremlin, although public dissatisfaction increased. According to data from the Levada Center, in August 48% supported the continuation of military actions, while 44% supported the initiation of peace negotiations. In September, the figures shifted to 44% and 48% respectively. October polling showed a more pronounced change: 57% supported peace negotiations, while 36% supported the continuation of military actions. However, it would be premature to interpret these figures as evidence of growing pacifism among russians. On the contrary, according to the same surveys, the proportion of russians supporting the war against Ukraine remains very high: 76% in August, 72% in September, and 73% in October.

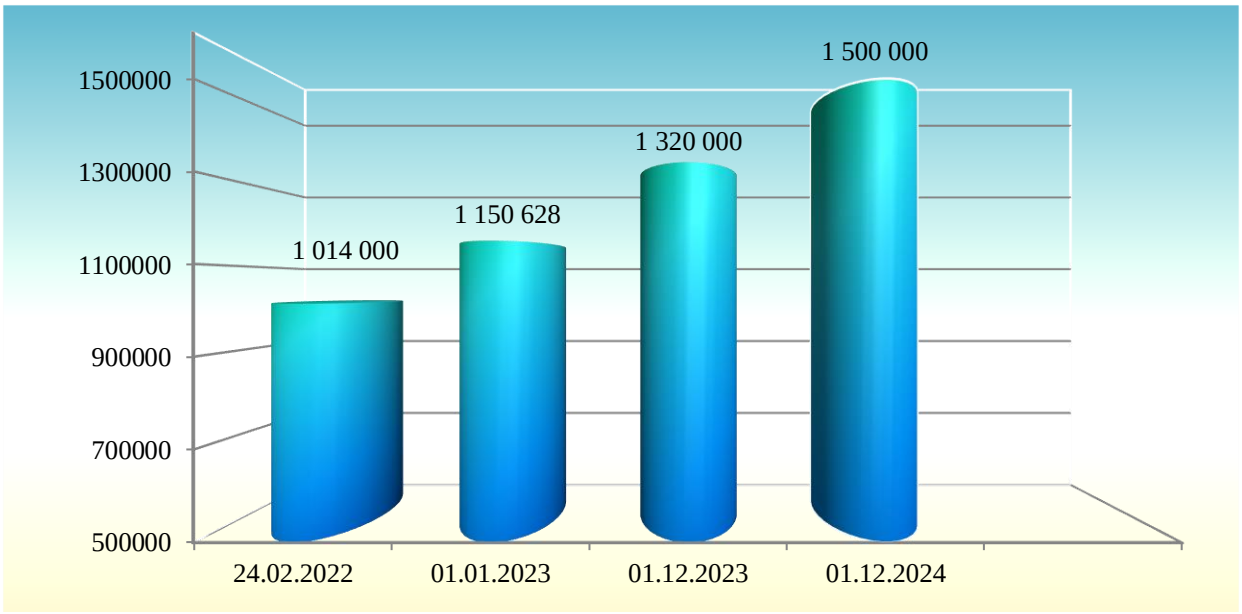


Figure 1. Dynamics of the growth in the number of military personnel of the armed forces of the russian federation

At the same time, according to various estimates, between 500,000 and 1 million people left the country. In order to avoid further escalation of social tensions, the kremlin was forced to revise its military recruitment strategy.

Contract service:

At present, the most widespread official method of recruitment is the signing of contracts with russians who join the army predominantly not as volunteers but as mercenaries. Contract service forms the basis of so-called “voluntary” recruitment. There is a continuous effort by the authorities to encourage the population to join the russian army. The most effective incentive for recruitment is the comparatively high salary (relative to the national average in russia), as well as substantial one-off payments upon signing a contract.

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

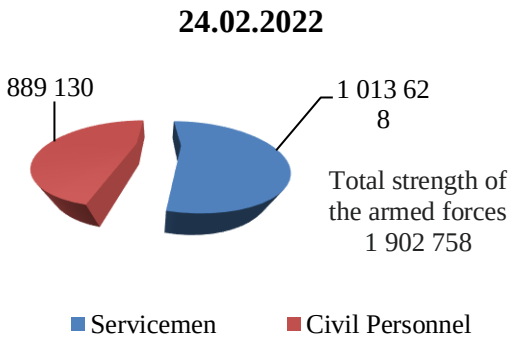


Figure 2. Strength of the armed forces of the russian federation as of 24 February 2022

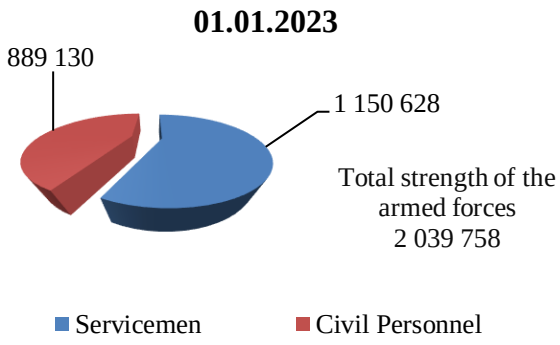


Figure 3. Strength of the armed forces of the russian federation as of 01.January 2023

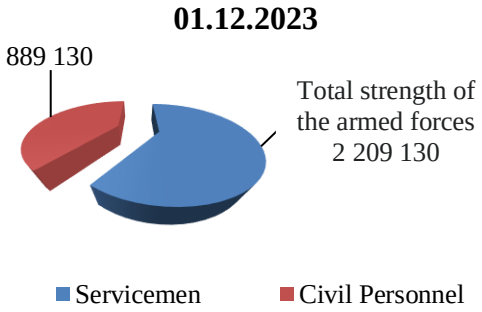


Figure 4. Strength of the armed forces of the russian federation as of 1 December 2023

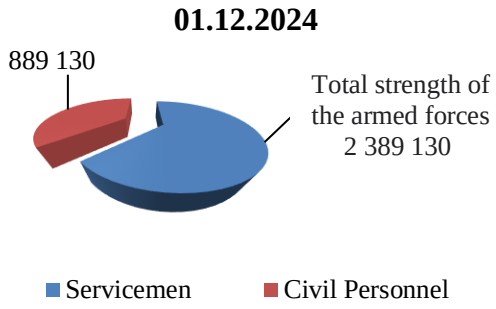


Figure 5. Strength of the armed forces of the russian federation as of 1 December 2024

Thus, in 2023, prior to the spring conscription campaign, a media campaign promoting contract service with the ministry of defence of the russian federation was launched. Mobile recruitment points for contract military service were deployed in city streets, while managers of enterprises and educational institutions received recommendations to promote contract service among employees and students. In addition to the informational component, there was also a financial one: the russian federal authorities offered a one-off payment upon signing, salaries significantly higher than the national average, and numerous benefits for both the servicemen and their families. This became an attractive factor for a portion of recruits and also reduced the financial burden on regional authorities, which were often unable to adequately support the formation and functioning of volunteer battalions.

russia offers high financial incentives (up to 200,000 roubles per month), but motivation remains low due to high casualty rates. According to RAND, in 2024 russia recruited approximately 100,000 contract soldiers, primarily from economically disadvantaged regions such as Buryatia and Tuva [10]. Coercive methods are also used in recruitment, including threats of imprisonment for economic debts [26].

From July 2024, at the federal level, every citizen who signs a contract for military service in the russian army receives:

400,000 roubles – a one-off payment;

from 204,000 roubles – monthly salary;

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

40,000–50,000 roubles – monthly payment during the training period.

In addition, all constituent entities of the russian federation have introduced one-off payments for signing military service contracts under regional programmes. Between 2023 and 2024, there was a clear upward trend in financial "incentives" for contract signing across the russian federation, although since the beginning of 2025 a reverse trend has been observed. At present, these payments range from 300,000 to 2,600,000 roubles, depending on the region.

In December 2023, putin, for the first time since the beginning of the full-scale invasion, announced the number of contract servicemen in the russian army — 640,000. dmitry medvedev stated that in 2023 alone, 410,000 russians signed contracts, while since the beginning of 2024 this figure has increased by a further 53,000. At the same time, according to viktor sobolev, a member of the defence committee of the state duma of russia, as of 4 February 2025, the total number of individuals who had signed contracts for military service in the russian army amounted to approximately 740,000.

Despite this, according to ISW, since late 2024 the monthly "recruitment" rate into the russian army has likely been equal to or lower than the number required to replace monthly losses on a one-to-one basis. Moreover, certain regions of the russian federation are unable to meet their monthly recruitment quotas, as citizens are increasingly reluctant to participate in the war.

Significantly greater attention has also been paid by the defence establishment to conscripts. Since early 2023, active recruitment campaigns targeting young men have been conducted and continued throughout the year. Unit commanders and senior servicemen have applied various methods of influence, ranging from individual conversations to threats and intimidation. The combination of incentives and coercion allows recruitment targets for contract service to be met through conscripts.

To improve the effectiveness of conscription followed by transition to contract service, the russian state duma adopted legislative amendments that increased the conscription age to 30, thereby expanding the pool of eligible men. In addition, a reformed system of military registration was introduced, covering all persons liable for military service. Electronic draft notices were also implemented; these are considered legally served from the moment they appear in the personal electronic account of a conscript on the "Gosuslugi" portal. Failure to report to the military commissariat may result in restrictive measures, including bans on leaving the country, driving vehicles, conducting real estate transactions, or obtaining loans.

Since 2022, there has also been a steady increase in the number of citizens conscripted for compulsory military service into the armed forces of the russian federation (see Figure 2). In spring 2025, the kremlin conscripted approximately 160,000 men, marking the largest conscription campaign in three and a half years of the war against Ukraine. According to official russian statements, these conscripts are not intended to be deployed to the so-called "special military operation". However, in practice, many recruits are compelled — formally or informally — to sign contracts after entering service and are subsequently deployed to the front lines as part of the occupying forces. This mechanism has become one of the key means for the kremlin to compensate for substantial wartime losses.

Recruitment of Foreign Nationals:

One of the key aspects of the formation of the armed forces of the russian federation is the involvement of foreign nationals. The russian authorities employ an extensive system for recruiting foreigners and facilitating their participation in military operations.

The primary focus is placed on countries with low income levels and relatively favourable attitudes towards russia. Foreign recruits are offered high remuneration, service in rear areas, and the prospect of obtaining russian citizenship. The most active recruitment efforts are conducted in Syria, India, Nepal, as well as in countries of Africa and Central Asia. In addition, there is confirmed evidence of the participation of citizens of North Korea in the war against Ukraine on the side of

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

russia.

According to Euromaidan Press, in 2024 up to 10,000 Nepalese citizens and up to 15,000 North Korean soldiers took part in hostilities [11]. Recruitment relies on both economic incentives and coercion; however, the effectiveness of such units remains low due to language barriers and inadequate training [27].

According to intelligence assessments from South Korea and the United States, the DPRK deployed between 10,000 and 12,000 military personnel, including special units, who participated in combat operations in the Kursk region. On 26 April 2025, the Chief of the General Staff of the russian federation, Valery Gerasimov, officially acknowledged their participation in hostilities in the region, and on 27 April 2025, Pyongyang confirmed the deployment, stating that it had been carried out under a mutual defence agreement signed with russia in June 2024 [24]. Thus, North Korea is actively involved in the war, and it is assumed that it may expand its military presence, although the scale and timing of further deployments remain uncertain.

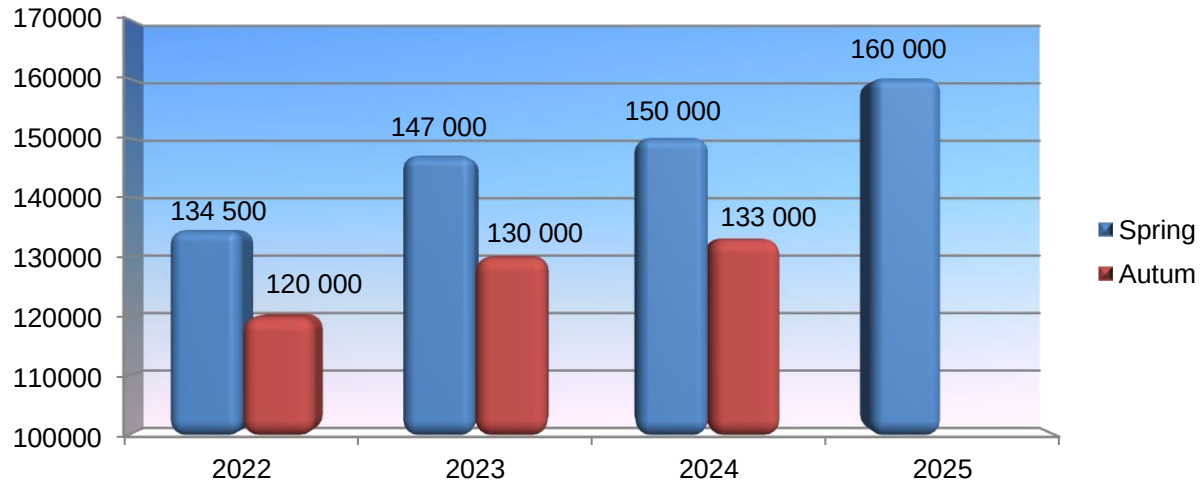


Figure 2. The dynamics of the increasing number of citizens conscripted for compulsory military service in the russian federation

In March 2024, a scheme involving the forced recruitment of Indian citizens was uncovered, whereby individuals were lured with offers of education at private russian universities and subsequently sent to the front. It is estimated that at least 180 Indian nationals were affected by this scheme.

A typical method of recruiting foreign nationals involves offering employment in the rear of the russian army, followed by reassignment to frontline positions. For instance, in 2023 more than 100 Indian citizens signed contracts with the russian army. A similar scheme was used to recruit Nepalese citizens, and in early 2024 the Nepalese authorities began countering this practice by suspending the issuance of work visas to russia following reports of the deaths of 10 Nepalese nationals.

Furthermore, in September 2023, Cuban authorities dismantled a network engaged in recruiting Cuban citizens. It is likely that some Cubans were incorporated into the 106th Airborne Division. In total, more than one hundred Cuban nationals signed contracts with the russian army.

At the same time, the russian mobilisation system faces a number of constraints:

Demographic crisis: The decline in the working-age population and population ageing reduce

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

the available reserve [6].

Economic sanctions: According to IMF data, russia's GDP declined by 3.5% in 2023–2024, limiting military financing [7].

Corruption: Reports of equipment shortages and embezzlement of funds are systemic [23].

Social demotivation: While the repressive apparatus suppresses dissent, low public trust in the authorities reduces the effectiveness of voluntary recruitment [26].

These constraints resemble the experience of the Soviet Union during the Soviet–Afghan War (1979–1989), when economic difficulties and public dissatisfaction, combined with the large-scale deployment of both professional and conscripted personnel, ultimately led to a gradual depletion of resources [30].

The findings of the study indicate that the russian mobilisation system, despite its centralisation and reliance on a repressive apparatus, remains vulnerable due to demographic, economic, and organisational constraints. These conclusions provide a foundation for forecasting russia's mobilisation capabilities for the period 2025–2026, which will be presented in the following section.

Forecast for 2025–2026

The findings presented in the previous section have identified both the strengths and weaknesses of the russian mobilisation system, enabling an assessment of its capabilities in the medium-term perspective (2025–2026).

This forecast is based on qualitative scenario analysis, taking into account demographic, economic, political, and military factors, as well as historical precedents. Much like a large-scale mechanism operating at the limits of its capacity, the russian mobilisation system exhibits signs of strain, yet retains the potential to sustain the war effort through totalitarian control and adaptive responses to emerging challenges.

In the short term, russia is likely to continue relying on contract service and the coercive involvement of conscripts, as the declaration of full mobilisation could trigger significant public discontent and mass emigration. Financial incentives will remain a key recruitment tool, although their effectiveness is declining due to economic constraints and decreasing public willingness to engage in military service. Recruitment of foreign nationals is also likely to intensify, particularly in countries demonstrating favourable attitudes towards russia, such as North Korea, where participation of military personnel in hostilities against Ukraine has already been confirmed. At the same time, forced mobilisation in the temporarily occupied territories of Ukraine will continue, although its potential remains limited due to local resistance, logistical challenges, and broader demographic and economic constraints.

Demographic and Economic Constraints

The demographic crisis remains a key factor constraining russia's mobilisation potential. According to forecasts by Rosstat, the working-age population is expected to decline by approximately 10% by 2030, amounting to a reduction of around 8 million individuals aged 15–59 [6]. High losses in Ukraine, which, according to estimates by the General Staff of the Armed Forces of Ukraine, reached 1,052,190 killed and wounded as of July 2025, further exacerbate this pressure [7]. For example, data from ISW indicate that russia loses on average 1,251 military personnel per day in 2025, exceeding the rate of replenishment through conscription and contract service [7]. This creates a deficit of human resources, particularly among qualified specialists such as drone operators and artillery personnel.

In the medium term (2025–2026), russia may face increasing difficulties in maintaining troop numbers due to declining willingness among citizens to serve in the military and growing social tensions associated with sustained high casualty rates. Economic sanctions and logistical constraints will further complicate the provision and sustainment of the armed forces, potentially forcing the kremlin to consider more radical measures, such as full mobilisation or an expansion of the conscription age. However, such steps are likely to intensify internal instability, thereby limiting their

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

practical implementation.

Economic sanctions, which, according to the International Monetary Fund, resulted in a 3.5% decline in russia's GDP in 2023–2024, will continue to constrain military financing [8]. War expenditures, estimated at USD 250 billion by the end of 2024, impose additional pressure on the economy, which, much like a vessel in a storm, remains afloat largely due to energy exports [9]. However, the termination of russian gas transit through Ukraine after 1 January 2025, as noted by the Prime Minister of Ukraine Denys Shmyhal, may further reduce russia's revenues, thereby limiting its capacity to finance contract payments or procure military equipment [22].

Political and Social Factors

putin's totalitarian regime, reinforced by repressive legislation such as the 2022 amendments to the criminal code of the russian federation, effectively suppresses any form of dissent [10]. However, low public motivation remains a significant challenge. According to The moscow Times, in 2024 only 20% of contract soldiers signed agreements voluntarily, while the remainder were subjected to economic or administrative pressure [27]. In 2025–2026, russia is likely to continue employing propaganda campaigns, such as the "Year of the Defender of the Fatherland", declared by putin for 2025, in order to further militarise society [22]. This approach resembles the experience of Nazi Germany in 1943–1945, when "total war" campaigns sought to mobilise the population despite economic exhaustion, ultimately resulting in reduced combat effectiveness due to insufficient training and resources [28].

Mechanisms of Force Generation

Mobilisation in the occupied territories. Forced mobilisation in the temporarily occupied territories of Ukraine is expected to continue, although its scale will gradually decline due to local resistance and the depletion of human resources. According to Human Rights Watch, in 2024 russia mobilised up to 100,000 individuals in the so-called DPR and LPR, most of whom were assigned to unskilled tasks, thereby reducing their operational effectiveness [26]. In 2025–2026, russia may intensify repressive measures to recruit additional personnel; however, this could provoke local uprisings similar to those observed in Kherson in 2022 [11].

Partial mobilisation. russia will likely continue its policy of partial mobilisation, as full mobilisation could trigger social instability even under repressive conditions. According to Forbes Ukraine, the current rate of losses allows russia to sustain its reserve until 2032, but only under the condition of recruiting 200,000–300,000 personnel annually [12]. In 2025–2026, russia may expand conscription through the use of electronic summonses and automated databases, simplifying the process but failing to address the issue of inadequate training among recruits [14].

Contract service. Contract service will remain the primary source of force replenishment; however, its effectiveness is expected to decline due to economic constraints. A reduction in financial incentives caused by budgetary pressures will likely lead to a decrease in voluntary enlistment. According to RAND, in 2024 russia already faced a shortage of contract soldiers in central regions, prompting increased recruitment from economically disadvantaged areas such as Dagestan and Chechnya [10]. This trend is likely to persist.

Recruitment of foreign nationals. russia will continue to recruit foreign nationals, particularly from North Korea, Nepal, and Central Asian states. According to Reuters, in 2025 russia may recruit up to 20,000 foreign fighters; however, their limited training and low motivation will constrain their effectiveness [28]. For instance, North Korean units involved in the war against Ukraine have demonstrated low combat effectiveness due to language barriers and poor coordination [7].

Development Scenarios

Baseline scenario (most probable): russia will continue its hybrid mobilisation model, combining partial conscription, contract service, and recruitment of foreign nationals. It is estimated that 150,000–200,000 personnel may be recruited annually, which would allow the continuation of current levels of combat operations but would not enable major breakthroughs due to insufficient

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

training and logistical constraints. Demographic decline and economic sanctions will gradually weaken the system.

Pessimistic scenario: in the event of significant successes by the Armed Forces of Ukraine, such as the liberation of key territories (e.g., the Kursk operation of 2024), russia may declare full mobilisation. This could enable the recruitment of up to 500,000 personnel; however, it would likely trigger economic collapse and internal instability, similar to the crisis experienced by the Soviet Union during the Afghan War [30].

Optimistic scenario (for Ukraine): intensified sanctions, reduced energy exports, and increased resistance in the occupied territories may force russia to reduce mobilisation to approximately 100,000 personnel annually, thereby rendering its armed forces more vulnerable to Ukrainian counteroffensives.

The historical example of Japan's mobilisation during the Second World War (1941–1945) illustrates how economic constraints and sustained losses can undermine mobilisation capacity. Despite mass conscription and societal militarisation, Japan faced shortages of resources and trained personnel, ultimately leading to defeat [32]. Similar challenges may confront russia if economic pressure and battlefield losses continue to increase.

The forecast indicates that russia is capable of sustaining the war against Ukraine until 2026; however, its mobilisation system is approaching its limits due to demographic, economic, political, and social factors. These findings provide a basis for Ukraine's strategic planning, which will be examined in detail in the following section.

Conclusion

The analysis of russia's mobilisation resources in the context of the large-scale war against Ukraine, conducted in this study, has achieved its objective: a systematic examination of the organisation, structure, and force-generation mechanisms of russian armed forces, as well as the development of a foresight assessment for 2025–2026.

The findings, based on open sources, allow for the formulation of key conclusions that correspond to the study's objectives and possess practical significance for Ukraine's strategic defence planning.

Firstly, the organisation of mobilisation in russia is characterised by a centralised approach, relying on a repressive apparatus and legislative framework, including Federal Law No. 31-FZ and amendments to the criminal code of the russian federation [13, 10]. The aggressor state possesses significant mobilisation potential (20–25 million individuals); however, economic, logistical, and organisational constraints complicate its implementation. This system ensures a relatively stable replenishment of forces but suffers from bureaucratic inefficiency and corruption. For instance, logistical and equipment challenges observed during the 2022 partial mobilisation remain relevant in 2025, thereby reducing unit combat effectiveness [15, 26].

Secondly, the structure of russia's mobilisation resource is constrained by the demographic crisis and economic sanctions. The working-age population is projected by Rosstat to decline by 10% by 2030, and combined with losses in Ukraine (over 1 million personnel as of July 2025), this creates a significant human resource deficit [6, 7]. This situation resembles the historical example of Japan during the Second World War, where resource depletion led to reduced military effectiveness [32]. For Ukraine, this presents opportunities for targeted actions to further weaken russian reserves.

Thirdly, the mechanisms for force generation—partial mobilisation, contract service, recruitment of foreign nationals, and forced conscription in the occupied territories—demonstrate mixed effectiveness. The 2022 partial mobilisation enabled the conscription of more than 300,000 individuals into the russian armed forces but also revealed systemic issues, provoking social discontent and the emigration of approximately 500,000 citizens. In other words, despite ambitious plans (300,000 individuals in 2022), russia faced evasion and organisational challenges [15].

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Simultaneously, in the occupied territories of Donetsk and Luhansk, about 220,000 people were mobilised by July 2022, partially compensating for losses but failing to fully address the replenishment of units that had suffered combat casualties.

To mitigate social tension, russia has intensified the recruitment of contract soldiers, offering high payments (ranging from 300,000 to 2,600,000 rubles) and various benefits, while also forcibly mobilising conscripts, prisoners, and debtors. The russian authorities employ multiple networks to recruit foreign nationals from low-income countries (Syria, India, Nepal, Cuba, DPRK) for subsequent participation in the war.

Although contract service recruits up to 100,000 individuals annually, it remains dependent on economic incentives, which have become less accessible due to sanctions [10, 27]. The recruitment of foreign nationals, such as North Korean or Nepali mercenaries, does not resolve issues related to training quality [28]. The most problematic mechanism is forced conscription in the occupied territories, which provokes resistance and reduces unit combat effectiveness [11, 29]. These vulnerabilities represent leverage points that Ukraine can exploit, for instance through information campaigns to demoralise recruits or by supporting local resistance.

russia employs a broad spectrum of methods to maintain its armed forces, but systemic problems, social discontent, and high casualties complicate the maintenance of necessary troop levels, forcing reliance on coercive and deceptive recruitment practices.

Since 2022, there has been a trend of increased conscription for compulsory military service (up to 160,000 individuals by spring 2025), an increase of the conscription age to 30, the introduction of electronic summons, and restrictions on draft evaders. Various methods of influence are applied to conscripts, compelling them to sign contracts. Despite these measures, since late 2024, russia has faced difficulties in meeting recruitment quotas, as citizens are increasingly reluctant to participate in the war, and monthly conscription often fails to offset losses.

Foresight for 2025–2026 indicates a likely continuation of the hybrid mobilisation model, which would enable russia to recruit 150,000–200,000 individuals annually, but with gradually declining efficiency due to economic and demographic constraints [12]. In the event of intensified sanctions or successes by the Armed Forces of Ukraine, such as the Kursk operation in 2024, russia might resort to full mobilisation, but this would risk economic collapse and internal instability, similar to the USSR's crisis during the Afghan war [30]. For Ukraine, this underscores the need to strengthen pressure on russia's logistical chains and to use diplomatic instruments to isolate its economy.

Based on these findings, Ukraine can develop strategies that maximise the impact on the vulnerabilities of russia's mobilisation system.

Recommendations

Intensify information campaigns to create conditions for the demoralisation of russian recruits and to support resistance in the occupied territories, as observed in Kherson in 2022 [11].

Focus military efforts on the destruction of logistics hubs, depots, and enterprises involved in arms production, thereby complicating the supply of mobilised units [25].

Enhance diplomatic efforts to strengthen sanctions, particularly targeting russia's energy sector, which would reduce its financial capacity for mobilisation [8].

These findings emphasise that, despite its apparent strength, russia's mobilisation system is vulnerable to systematic pressure. For Ukraine, which is defending its sovereignty, understanding these vulnerabilities is not merely a theoretical achievement but also a practical instrument for achieving victory. As the Chinese strategist Sun Tzu noted in his famous treatise The Art of War, obtaining a strategic advantage over an adversary requires knowledge of their weaknesses.

Conflict of Interest

The authors declare that they have no competing interests regarding the subject of this article.

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

References

1. Bertalanffy, L. (1974). General system theory: Critical overview. In Problems of methodology of systemic research (pp. 12–35). Naukova Dumka.
2. President of the russian federation. (2022). On the announcement of partial mobilisation in the russian federation." (647/2022). http://kremlin.ru/acts/news/69391
3. Harward, C., Wolkov, N., Mappes, G., Runkel, W., & Barros, G. (2024, Dec. 22). russian offensive campaign assessment. Institute for the Study of War. https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-december-22-2024
4. Posts on platform X regarding the reform of the conscription system in russia. (2025, July). Various authors. https://x.com
5. Bell, D. A. (2007). The first total war: Napoleon's Europe and the birth of warfare as we know it. Houghton Mifflin.
6. Forecast of demographic development of the russian federation until 2030. Rosstat. (n.d.). https://rosstat.gov.ru/population/demography
7. russia's war against Ukraine. All news at this time. (2025, July 30). Radio Svoboda. https://www.radiosvoboda.org/a/rosiya-ukrayina-zahroza-viyny/31703318/lbl0lbi420651.html
8. Siluanov, A. (2024, Oct. 25). IMFC statement by Anton Siluanov, Minister of Finance, russian federation. International Monetary Fund. https://meetings.imf.org/-/media/AMSM/Files/AM2024/IMFC/Russia.ashx
9. russian invasion of Ukraine. In Wikipedia. The Free Encyclopedia. Wikipedia contributors. (n.d.). https://en.wikipedia.org/wiki/russian_invasion_of_Ukraine
10. Federal Law of the russian federation "On amendments to the Criminal Code of the russian federation" No. 32-FZ (2022, March 3). http://kremlin.ru/acts/news/67890
11. Intel: russia intensifies forced mobilisation in occupied territories of Ukraine. (2024, Jan. 9). Euromaidan Press. https://euromaidanpress.com/2024/01/09/intel-russia-intensifies-forced-mobilisation-in-occupied-territories-of-ukraine/
12. Analysis of losses of the russian army and their impact on mobilisation potential. (2024). Forbes Ukraine. https://forbes.ua/war-in-ukraine
13. Federal Law of the russian federation "On mobilisation preparation and mobilisation in the Russian Federation." No. 31-FZ (1997, Febr. 26). http://www.consultant.ru/document/cons_doc_LAW_13551/
14. Sudimykh i ogranichenno godnykh na front [Convicted and limited fit to the front] [Post on X]. (2023, May 31). Mobilizationews [@mobilizationews]. https://x.com/mobilizationews/status/1663930799148740610
15. "Zhizn' otdat', poluchit' uvech'ya". Budet li v Rossii novaya mobilizatsiya? ["Give life, get injuries". Will there be a new mobilisation in russia?]. (2023, Sept. 26). BBC News russian. https://www.bbc.com/russian/articles/c4nvxd54931o
16. Vishnevsky, A. (2023). Demographic challenges in russia: 2020–2030. Higher School of Economics.
17. Gressel, G. (2024, Jan. 18). Beyond the counter-offensive: Attrition, stalemate, and the future of the war in Ukraine. European Council on Foreign Relations. https://ecfr.eu/publication/beyond-the-counter-offensive-attrition-stalemate-and-the-future-of-the-war-in-ukraine/
18. Assault detachments of Zapad Group complete combat training in rear area. (2025, July 18). Ministry of Defence of the russian federation. https://eng.mil.ru/news/7f137eaf-a4e5-400f-a425-b9724716d6d7
19. russia's General Staff reports on 133,000 conscripts drafted in 2024 fall campaign. (2024). TASS. https://tass.com/defense/1936783

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

20. General Staff of the Armed Forces of Ukraine. (2025, July). Information materials. https://ivms.mil.gov.ua/wp-content/uploads/2025/07/08.07.-14.07.2025.pdf
21. Lyall, J. (2020). Chechnya: russia's forgotten war. Cambridge University Press.
22. Aksenov, P. (2023, Dec. 14). putin nazval chislennost' voyuyushchey v Ukraine armii. O chem govoryat eti tsifry? [putin named the size of the army fighting in Ukraine. What do these figures say?]. BBC News russian. https://www.bbc.com/russian/articles/cpw3qq6j0y2o
23. russia mobilised over 300,000 people in occupied Donetsk, report reveals. (2024, Oct. 2). NV the new voice of Ukraine. https://english.nv.ua/nation/russia-mobilised-over-300-000-people-in-occupied-donetsk-since-invasion-says-new-report-50455331.html
24. Why did the russian federation officially recognise the participation of DPRK troops in the war. Center for Countering Disinformation. (n.d.). https://cpd.gov.ua/international-direction/yevropa/dlya-chogo-rf-oficzijno-vyznala-uchast-vijsk-kndr-u-vijni
25. russia's war against Ukraine. Resistance. All news at this time. (2024, Dec. 23). Radio Svoboda. https://www.radiosvoboda.org/a/rosiya-ukrayina-zahroza-viyny/31703318.html
26. In Dagestan, locals fight police on day two of mass protests against mobilisation. (2022, Sept. 26). Meduza. https://meduza.io/en/news/2022/09/26/in-dagestan-locals-fight-police-on-day-two-of-mass-protests-against-mobilization
27. russian regions hike military sign-up payments in bid to boost manpower for Ukraine war. (2024, July 30). The moscow Times. https://www.themoscowtimes.com/2024/07/30/russian-regions-hike-military-sign-up-payments-in-bid-to-boost-manpower-for-ukraine-war-a85864
28. putin offers citizenship to foreigners who fight for russia. (2024, Jan. 4). Reuters. https://www.reuters.com/world/europe/putin-offers-citizenship-foreigners-who-fight-russia-2024-01-04/
29. russia forces Ukrainians in occupied areas into military. (2023, Dec. 20). Human Rights Watch. https://www.hrw.org/news/2023/12/20/russia-forces-ukrainians-occupied-areas-military
30. Grau, L. W. (2000). The Soviet-Afghan war: How a superpower fought and lost. University Press of Kansas.
31. Tooze, A. (2006). The wages of destruction: The making and breaking of the Nazi economy. Penguin Books.
32. Drea, E. J. (2009). Japan's imperial army: Its rise and fall, 1853–1945. University Press of Kansas.

Форсайт мобілізаційного потенціалу російської федерації в умовах війни проти України: структура, механізми та сценарії розвитку на 2025–2026 роки

Володимир Гурковський
доктор наук з державного управління, професор
начальник відділу
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: volodymyrgurkovskyi@gmail.com
ORCID: 0000-0003-2021-5204

Роберт Ованесян
провідний науковий співробітник
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: bober1609@gmail.com
ORCID: 0009-0008-6761-2059

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Денис Калашников
науковий співробітник
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: kalash179@gmail.com
ORCID: 0009-0003-4625-6191

Андрій Цибізов
кандидат військових наук, старший дослідник
старший науковий співробітник
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: Enigma_007@ukr.net
ORCID: 0000-0001-6555-5005

Карел Недбалек
доктор юридичних наук, професор
Європейський професійний докторат
Злін, Чеська Республіка
e-mail: slusovice@motelgolg.cz
ORCID: 0000-0002-1010-2460

Анотація. Актуальність дослідження зумовлена необхідністю передбачити, як рф компенсуватиме свої втрати в умовах затяжної війни. Наприклад, аналіз відкритих джерел від липня 2025 року вказує на плани росії щодо розширення призову через реформи військової адміністрації, що може змінити динаміку війни. Для України це означає потребу в точних даних і прогнозах, щоб ефективно розподіляти власні ресурси. Стаття присвячена системному аналізу та форсайту мобілізаційного потенціалу російської федерації в умовах широкомасштабної війни проти України. Дослідження розкриває структуру, механізми комплектування військ і обмеження російської мобілізаційної системи, пропонуючи прогноз її розвитку на 2025–2026 роки. Мета статті – провести системний аналіз організації мобілізаційного ресурсу росії в умовах війни проти України та розробити прогноз її мобілізаційних можливостей на 2025–2026 роки. У статті охарактеризовано структуру та особливості мобілізаційного ресурсу росії, включаючи законодавчу базу та механізми комплектування; досліджено специфіку часткової мобілізації, контрактної служби, вербування іноземців і примусового призову на окупованих територіях; виявлено ключові обмеження системи на основі верифікованих даних; сформульовано прогноз на основі сучасних трендів та історичних прикладів і запропоновано висновки, які сприятимуть стратегічному плануванню оборони України. Системний підхід є основою дослідження, оскільки мобілізація в росії являє собою складну систему, що охоплює законодавчу базу, адміністративні механізми, соціально-економічні умови та ідеологічний апарат. Для аналізу використано модель загальної теорії систем Людвіга фон Берталанфі, яка розглядає систему як сукупність взаємопов'язаних елементів, де зміна одного компонента, наприклад, демографічного резерву, впливає на інші, такі як військова ефективність чи економічна стабільність. На основі емпіричних і теоретичних методів, включаючи аналіз офіційних документів, звітів ISW, RAND, Human Rights Watch, інших відкритих джерел, встановлено, що мобілізація в росії спирається на централізовану репресивну систему, але стикається з демографічною кризою (скорочення працездатного населення на 10% до 2030 року), економічними санкціями (зменшення ВВП на 3,5% у 2023–2024 роках) і організаційними

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

проблемами (корупція, брак спорядження). Часткова мобілізація, контрактна служба, вербування іноземців (зокрема з Північної Кореї та Непалу) та примусовий призов на окупованих територіях України є ключовими механізмами, але їхня ефективність знижується через низьку підготовку та спротив. Прогноз на 2025–2026 роки передбачає продовження гібридної мобілізації (150–200 тис. осіб щорічно), але з ризиком виснаження через економічні та соціальні обмеження. Історичні приклади (Японія 1941–1945, срср в Афганістані) підкреслюють вразливість подібних систем. Для України рекомендуються інформаційні операції, удари по логістиці та посилення санкцій. Дослідження пропонує стратегічні точки важеля для ослаблення ворога, що має критичне значення для оборони держави.

Ключові слова: мобілізаційний ресурс, російська федерація, мобілізаційний потенціал, російсько-українська війна, форсайт, часткова мобілізація, контрактна служба, окуповані території, демографічна криза, економічні санкції, стратегічне планування.

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Received: *January 8, 2026* | **Revisions Requested:** - | **Revision Received:** -
Accepted: *March 5, 2026* | **Published Online:** *April 10, 2026*

Licensed (C) by Creative Commons Attribution International License 4.0 (CC BY-NC-SA)

DOI: 10.62524/msj.2026.4.1.11

Методика пріоритезації та оцінювання впливу когнітивних загроз на ефективність системи стратегічних комунікацій Збройних Сил України

Олег Темний
ад'юнкт
кафедра інформаційної боротьби інституту стратегічних комунікацій
Національний університет оборони України
03049, проспект Повітряних Сил, 28, Київ, Україна
e-mail: o.temnyi@edu.nuou.org.ua
ORCID: 0009-0009-3173-094X

Анотація. Актуальність дослідження зумовлена тим, що в умовах широкомасштабної агресії російської федерації проти України когнітивні загрози набули системного, комплексного та цілеспрямованого характеру, що безпосередньо впливає на ефективність функціонування системи стратегічних комунікацій Збройних Сил України. Посилення інформаційно-психологічного впливу противника, зростання ролі дезінформації, маніпулятивних наративів та когнітивних операцій вимагають розроблення науково обґрунтованих підходів до їх ідентифікації, оцінювання та пріоритизації. У зв'язку з цим особливої значущості набуває формування методичного апарату, який дозволяє комплексно оцінювати вплив когнітивних загроз на систему стратегічних комунікацій та забезпечувати ухвалення обґрунтованих управлінських рішень у сфері когнітивної безпеки. Отже, метою статті є розроблення методики пріоритизації та оцінювання впливу когнітивних загроз на ефективність системи стратегічних комунікацій Збройних Сил України, яка враховує багатокритеріальний характер таких загроз та специфіку їх реалізації в умовах сучасної війни. Основними результатами проведеного дослідження є розроблення комплексної методики, що складається з двох взаємопов'язаних часткових методик. Перша часткова методика базується на застосуванні методу аналізу ієрархій та передбачає попарне порівняння когнітивних загроз за визначеними критеріями (інтенсивність, масштаб, темп та стійкість впливу), що дозволяє здійснити їх обґрунтовану пріоритизацію. Друга часткова методика спрямована на оцінювання впливу пріоритетних загроз на ефективність системи стратегічних комунікацій і передбачає використання апарату теорії ймовірностей, адитивного та мультиплікативного згортання показників, а також елементів теорії ігор. У статті запропоновано структурно-логічну схему методики, яка складається з шести послідовних етапів із деталізацією процедурних блоків на кожному з них, що забезпечує її практичну реалізованість. Проведений практичний розрахунок для актуальних когнітивних загроз у період 2025–2026 років дозволив продемонструвати ефективність запропонованого підходу та його придатність до використання в умовах російсько-української війни, що триває. Матеріали статті можуть бути корисними для органів військового управління, підрозділів стратегічних комунікацій, аналітичних і наукових установ сектору безпеки і оборони, а також для фахівців у сфері інформаційної та когнітивної безпеки. Запропонована методика може бути використана під час оцінювання загроз, планування заходів протидії та підвищення ефективності стратегічних

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

комунікацій Збройних Сил України. Подальші дослідження за напрямом статті доцільно зосередити на вдосконаленні математичного апарату оцінювання когнітивних загроз, розширенні переліку критеріїв їх аналізу, інтеграції розробленої методики в систему підтримки ухвалення рішень органів військового управління, а також адаптації підходів до стандартів держав – членів НАТО з урахуванням досвіду ведення сучасних гібридних та когнітивних війн.

Ключові слова: когнітивні загрози; стратегічні комунікації; Збройні Сили України; пріоритизація загроз; метод аналізу ієрархій; теорія ймовірностей; теорія ігор; адитивне та мультиплікативне згортання; ефективність системи; когнітивна безпека; російсько-українська війна.

Вступ (Introduction)

Широкомасштабне вторгнення російської федерації в Україну у лютому 2022 року зумовило якісно нові умови функціонування системи стратегічних комунікацій (ССК) Збройних Сил України (ЗС України). Сучасна війна набула ознак комплексного протистояння, у якому поряд із застосуванням традиційних військових засобів дедалі більшого значення набуває інформаційно-когнітивний вимір. В умовах тривалого збройного протистояння росія цілеспрямовано застосовує широкий спектр когнітивних операцій, спрямованих на деморалізацію українського суспільства та особового складу ЗС України, підрив міжнародної підтримки України, формування деструктивних наративів і зниження рівня довіри до офіційних джерел інформації [1, 2]. Такі дії охоплюють поширення дезінформації, маніпулювання суспільною свідомістю, використання психологічного тиску та створення інформаційного шуму, що ускладнює процес ухвалення рішень як на стратегічному, так і на оперативному рівнях.

За цих умов система стратегічних комунікацій ЗС України перетворюється на один із ключових інструментів забезпечення стійкості держави, підтримання морально-психологічного стану військ і населення, а також формування сприятливого міжнародного інформаційного середовища. Водночас ефективність ССК значною мірою залежить від здатності своєчасно виявляти, ідентифікувати та оцінювати когнітивні загрози, визначати їх пріоритетність і вплив на досягнення цілей стратегічних комунікацій.

Актуальність дослідження зумовлена необхідністю розроблення науково обґрунтованих методичних підходів до оцінювання та пріоритизації когнітивних загроз в умовах сучасної війни. Наявні підходи здебільшого не враховують комплексного, динамічного та багатокритеріального характеру когнітивного впливу, що ускладнює формування ефективних управлінських рішень у сфері стратегічних комунікацій. Крім того, зростає потреба у створенні універсального інструментарію, який дозволив би інтегрувати кількісні та якісні показники оцінювання загроз, враховувати їх взаємозв’язок та прогнозувати наслідки їх реалізації.

Отже, дослідження, спрямоване на розроблення методики пріоритизації та оцінювання впливу когнітивних загроз на ефективність системи стратегічних комунікацій ЗС України, є своєчасним і має важливе теоретичне та практичне значення для підвищення когнітивної стійкості держави в умовах російсько-української війни, що триває.

Матеріали та методи (Materials and Methods)

Аналіз наявних наукових праць свідчить про те, що в українській військовій науці ще недостатньо розроблені формалізовані методичні підходи до пріоритизації когнітивних загроз та кількісного оцінювання їх впливу на ефективність ССК ЗС України. Переважна більшість досліджень має описовий характер без чіткого математичного апарату, який дозволяв би

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

порівнювати загрози між собою та визначати найбільш критичні напрями протидії [3–5].

Метою статті є розроблення методики пріоритизації та оцінювання впливу когнітивних загроз на ефективність системи стратегічних комунікацій ЗС України в умовах продовження збройного протистояння з росією, яка забезпечує науково обґрунтоване ранжування загроз та кількісне оцінювання їх впливу на ключові показники функціонування ССК.

Результати та Обговорення (Results and Discussion)

Сформуємо погляди щодо визначення когнітивних загроз ССК ЗС України та проведемо класифікацію актуальних когнітивних загроз.

Станом на 2025–2026 роки в умовах російсько-української війни, що триває, система стратегічних комунікацій ЗС України зазнає систематичного впливу таких основних когнітивних загроз [1, 3, 6] (табл. 1).

Загальну структурно-логічну схему методики можна представити, як на рис. 1.

Розроблена методика являє собою двоетапну систему (рис. 2): перший рівень – це часткова методика пріоритизації когнітивних загроз; другий рівень – це часткова методика оцінювання їх впливу на ефективність ССК ЗС України.

Загальна структурно-логічна схема методики охоплює шість послідовних етапів.

Таблиця 1. Класифікація актуальних когнітивних загроз системі стратегічних комунікацій ЗС України (2025–2026 рр.)

Код	Найменування загрози	Характеристика
$З_1$	Дезінформаційні кампанії та фейкові наративи	Цілеспрямоване поширення неправдивої інформації про дії ЗСУ, втрати, рішення командування з метою підриву довіри суспільства та союзників
$З_2$	Маніпулювання суспільними настроями щодо мобілізації	Когнітивні операції, спрямовані на нагнітання страху та невдоволення мобілізаційними заходами, формування ухильницьких настроїв
$З_3$	Підрив міжнародної підтримки та коаліційної єдності	Цілеспрямований вплив на суспільну думку в країнах-партнерах для зменшення підтримки України, поширення «втоми від війни»
$З_4$	Інформаційні атаки на моральний дух особового складу	Психологічні операції, спрямовані безпосередньо на військовослужбовців ЗСУ: листівки, соцмережі, перехоплені канали зв'язку
$З_5$	Дискредитація командування та інститутів ЗСУ	Поширення дискредитуючих матеріалів щодо вищого командування, формування образу некомпетентності та корумпованості
$З_6$	Когнітивні атаки через штучний інтелект та діпфейки	Застосування ШІ-генерованого контенту (відео, аудіо, тексти) для створення правдоподібних фейків з мінімальним виявленням
$З_7$	Маніпулювання інформаційним простором у зонах бойових дій	Захоплення інформаційного поля на ТВД, поширення дезорієнтуючих повідомлень серед мирного населення окупованих/прифронтових районів

Визначимо зміст першої часткової методики пріоритизації когнітивних загроз.

Як основні процедури проведення розрахунків щодо пріоритизації когнітивних загроз можна визначити:

1. *Формування матриць попарних порівнянь.*

Основним методом під час формування та пріоритизації загроз є метод аналізу ієрархій (MAI) Т. Сааті [7]. Він є одним з найбільш ефективних формалізованих методів ухвалення рішень в умовах багатокритеріального вибору, зокрема для задач пріоритизації. Для кожного

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

критерію k (де $k = 1, ..., K$) формується матриця попарних порівнянь розміром ($n \times n$), де n – кількість когнітивних загроз:

$$A^{(k)} = \|a_{ij}^{(k)}\|, \; i, j = 1, ..., n, \quad (1)$$

де $a_{ij}^{(k)}$ – оцінка переваги загрози $З_i$ над загрозою $З_j$ за критерієм k за шкалою Сааті (1–9), $a_{ij}^{(k)} = 1 / a_{ji}^{(k)}$ — умова оберненосиметричності матриці.

ЕТАП I: ПРІОРИТИЗАЦІЯ КОГНІТИВНИХ ЗАГРОЗ (МАІ Сааті)	
Блок 1	Блок 1.1. Формування вихідного переліку когнітивних загроз
Блок 2	Блок 1.2. Визначення критеріїв оцінювання: інтенсивність (I), масштаб охоплення (M), темп впливу (T), стійкість (C)
Блок 3	Блок 1.3. Формування групи експертів ($n \geq 7$) та узгодження їх компетентності
Блок 4	Блок 1.4. Проведення процедури попарного порівняння загроз за кожним критерієм
ЕТАП II: ОБЧИСЛЕННЯ ПРІОРИТЕТІВ (СИНТЕЗ МАІ)	
Блок 1	Блок 2.1. Перевірка узгодженості матриць попарних порівнянь ($ВУ \leq 0,10$)
Блок 2	Блок 2.2. Обчислення локальних пріоритетів (власних векторів матриць)
Блок 3	Блок 2.3. Обчислення глобальних пріоритетів загроз на основі вагових коефіцієнтів критеріїв
Блок 4	Блок 2.4. Ранжування загроз та формування переліку пріоритетних
ЕТАП III: ФОРМУВАННЯ СИСТЕМИ ПОКАЗНИКІВ ЕФЕКТИВНОСТІ ССК	
Блок 1	Блок 3.1. Визначення ключових показників ефективності (KPI) ССК ЗСУ
Блок 2	Блок 3.2. Побудова матриці відповідності “загрози – показники ефективності”
Блок 3	Блок 3.3. Визначення базових рівнів показників ефективності у відсутності загроз
ЕТАП IV: ОЦІНЮВАННЯ ВПЛИВУ ЗАГРОЗ НА KPI (ТЕОРІЯ ЙМОВІРНОСТІ + ТЕОРІЯ ІГОР)	
Блок 1	Блок 4.1. Оцінювання імовірності реалізації кожної пріоритетної загрози $P(З_i)$
Блок 2	Блок 4.2. Оцінювання умовних імовірностей деградації j-го показника ефективності за умови реалізації загрози $З_i$
Блок 3	Блок 4.3. Визначення коефіцієнтів деградації показників ефективності δ_{ij}
Блок 4	Блок 4.4. Застосування теорії ігор для визначення оптимальної стратегії протидії
ЕТАП V: ІНТЕГРАЛЬНЕ ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ССК	
Блок 1	Блок 5.1. Адитивне згортання часткових показників у комплексний показник ефективності
Блок 2	Блок 5.2. Мультиплікативне згортання для критично важливих показників
Блок 3	Блок 5.3. Визначення інтегрального показника ефективності ССК ЗСУ в умовах когнітивних загроз
ЕТАП VI: АНАЛІЗ РЕЗУЛЬТАТІВ ТА ВИРОБЛЕННЯ РЕКОМЕНДАЦІЙ	
Блок 1	Блок 6.1. Порівняння з пороговими значеннями та шкалою оцінювання
Блок 2	Блок 6.2. Ідентифікація критичних точок деградації ССК
Блок 3	Блок 6.3. Формування рекомендацій щодо пріоритетних заходів протидії когнітивним загрозам

Рисунок 1. Загальна структурно-логічна схема методики пріоритизації та оцінювання впливу когнітивних загроз

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

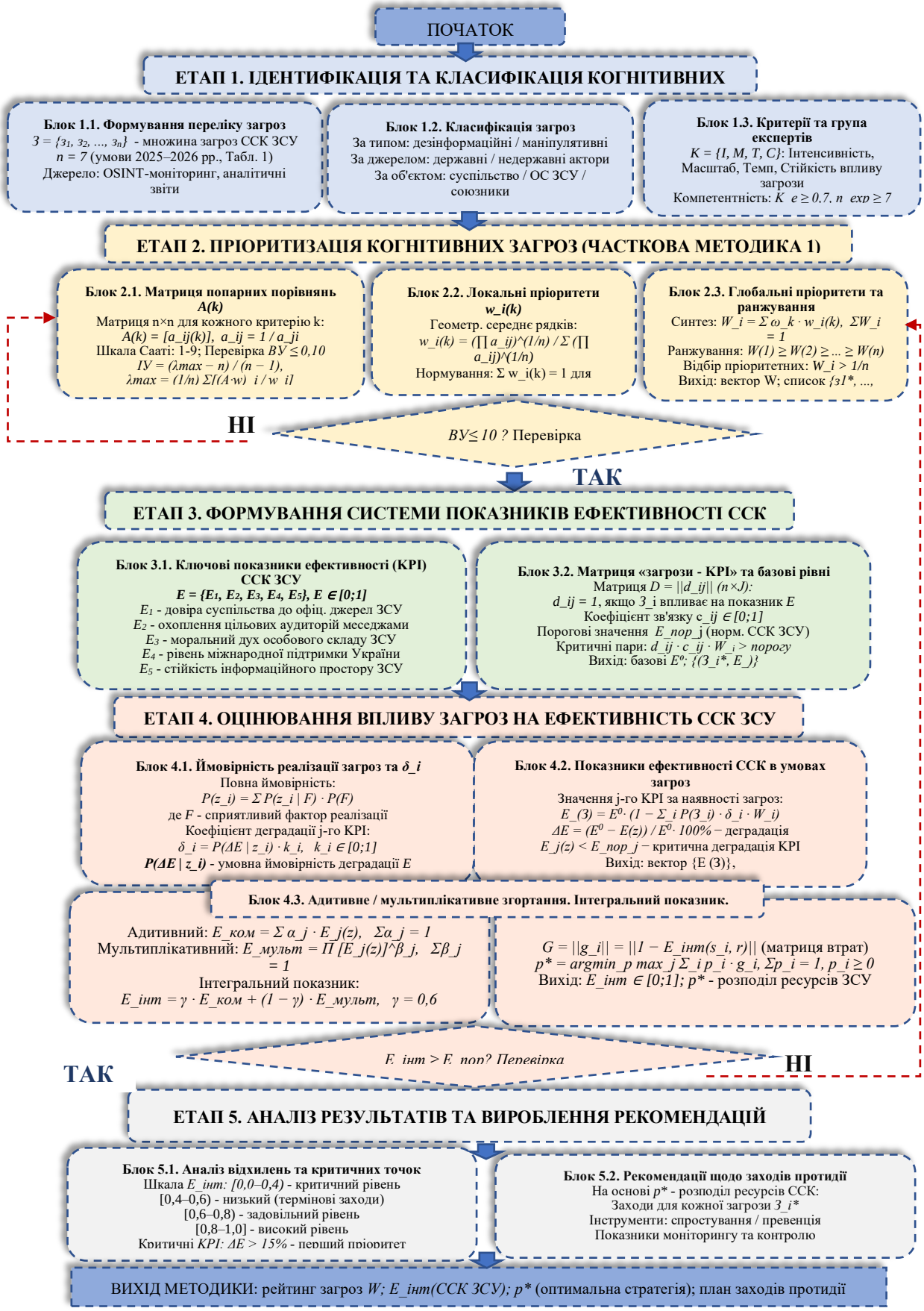


Рисунок 2. Загальна блок-схема методики пріоритезації та оцінювання впливу когнітивних загроз на ефективність функціонування системи стратегічних комунікацій ЗС України

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

2. *Обчислення локальних пріоритетів.*

Для кожної матриці $A^{(k)}$ обчислюються локальні пріоритети $w_i^{(k)}$ як нормовані компоненти головного власного вектора. Практичне наближення локального пріоритету i-ї загрози за критерієм k:

$$w_i^{(k)} = \sqrt[n]{(\prod_j a_{ij}^{(k)})} / \Sigma_l \sqrt[n]{(\prod_j a_{lj}^{(k)})} \quad (2)$$

3. *Перевірка узгодженості матриці.*

Відношення узгодженості (ВУ) обчислюється за формулою:

$$ВУ = ІУ / ВВ, \quad (3)$$

де ІУ – індекс узгодженості: $ІУ = (\lambda_{max} - n) / (n - 1)$; ВВ – випадкова узгодженість (табличне значення). Умова прийнятної узгодженості: $ВУ \leq 0{,}1$.

Максимальне власне значення матриці знаходиться як:

$$\lambda_{max} = (1/n) \cdot \Sigma_i [(A^{(k)} \cdot w^{(k)})_i / w_i^{(k)}]. \quad (4)$$

4. *Визначення вагових коефіцієнтів критеріїв.*

Аналогічно формується матриця попарних порівнянь самих критеріїв, яка визначає вагові коефіцієнти υ_k $(k=1, ..., K)$. У нашому випадку $K=4$ критерії: Інтенсивність (I), Масштаб (M), Темп (T), Стійкість (C).

5. *Обчислення глобальних пріоритетів та ранжування.*

Глобальний пріоритет (інтегральна оцінка пріоритетності) i-ї когнітивної загрози:

$$W_i = \Sigma_k \upsilon_k \cdot w_i^{(k)}, \ \Sigma_i W_i = 1. \quad (5)$$

Загрози ранжуються за спаданням W_i. Загрози, для яких виконується умова $W_i > 1/n$, належать до групи пріоритетних та підлягають першочерговому аналізу в рамках другої часткової методики.

Визначимо зміст другої часткової методики оцінювання впливу когнітивних загроз.

Як основні процедури проведення розрахунків щодо пріоритизації когнітивних загроз можна визначити:

1. *Система показників ефективності ССК ЗС України.*

Ефективність системи стратегічних комунікацій ЗС України оцінюється через систему ключових показників: E_1 – довіра суспільства до офіційних джерел ЗС України; E_2 – охоплення цільових аудиторій ключовими меседжами; E_3 – моральний дух особового складу; E_4 – рівень міжнародної підтримки; E_5 – стійкість інформаційного простору (рівень спростувань фейків). Кожен показник нормується: $E_j \in [0; 1]$, де 1 – максимальна ефективність.

2. *Оцінювання імовірності реалізації загроз та коефіцієнтів деградації.*

Імовірність реалізації i-ї когнітивної загрози $P(З_i)$ оцінюється експертним методом або на основі аналізу статистики подій інформаційного простору. Для складових загроз застосовується формула повної ймовірності:

$$P(З_i) = \Sigma_m P(З_i \mid F_m) \cdot P(F_m), \quad (6)$$

де F_m – m-та умова (сприятливий фактор реалізації загрози). Коефіцієнт деградації j-го показника ефективності під впливом i-ї загрози:

$$\delta_{ij} = P(\Delta E_j \mid З_i) \cdot \kappa_{ij}, \quad (7)$$

де $P(\Delta E_j \mid З_i)$ – умовна імовірність значного зниження j-го показника за умови реалізації загрози $З_i$; $\kappa_{ij} \in [0; 1]$ – коефіцієнт, що характеризує максимальну глибину можливої деградації показника.

3. *Адитивне згортання показників ефективності.*

Комплексний (агрегований) показник ефективності ССК ЗС України в умовах реалізації множини когнітивних загроз обчислюється через адитивне згортання:

$$E_ком = \Sigma_j \alpha_j \cdot E_j(З), \ \Sigma_j \alpha_j = 1, \quad (8)$$

де α_j – вагові коефіцієнти показників, що визначаються методом MAI або методом рангової кореляції; $E_j(З)$ – значення j-го показника ефективності в умовах дії виявлених загроз:

$$E_j(З) = E°_j \cdot (1 - \Sigma_i P(З_i) \cdot \delta_{ij} \cdot W_i), \quad (9)$$

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

де $E°_j$ – базовий рівень j-го показника у відсутності загроз. Адитивне згортання застосовується за умови компенсаційності показників (низьке значення одного може компенсуватися високим іншого).

4. *Мультиплікативне згортання для критичних показників.*

Для критично важливих некомпенсаційних показників (моральний дух, довіра) застосовується мультиплікативне згортання:

$$E_мульт = \prod_j [E_j(З)]^{\beta_j},\ \ \Sigma_j \beta_j = 1, \qquad (10)$$

де β_j – показники степеня, що відображають відносну важливість j-го показника. Інтегральне (комплексне) оцінювання рекомендується виконувати через зважену середню адитивного та мультиплікативного показників:

$$E_інт = \gamma \cdot E_ком + (1 - \gamma) \cdot E_мульт,\ \ \gamma \in [0; 1]. \qquad (11)$$

5. *Застосування теорії ігор для визначення оптимальної стратегії.*

Вибір оптимальної стратегії протидії когнітивним загрозам моделюється як матрична гра двох гравців: ЗС України (захисник) та противник (агресор). Матриця виграшів (втрат ефективності ССК) має вигляд:

$$G = \|g_{ij}\|,\ \ i \in \{стратегії\ ЗСУ\},\ \ j \in \{стратегії\ противника\}, \qquad (12)$$

де $g_{ij} = 1 - E_інт(s_i, r_j)$ – втрати ефективності ССК ЗС України при застосуванні стратегії s_i (ЗС України) та r_j (противник). Оптимальна змішана стратегія ЗС України $p^* = (p_1^*, ..., p_m^*)$ знаходиться з умови мінімаксу:

$$p^* = arg\ min_\{p\}\ max_\{j\}\ \Sigma_i p_i \cdot g_{ij},\ \ \Sigma_i p_i = 1,\ \ p_i \geq 0. \qquad (13)$$

Для підтвердження працездатності методики проведемо чисельний експеримент щодо практичних розрахунків за етапами та процедурами методики.

1. *Сформуємо матрицю попарних порівнянь за критерієм "Інтенсивність" (табл. 2).*

Розглянемо приклад пріоритизації для чотирьох найбільш актуальних загроз (скорочений перелік для наочності): $З_1$ – дезінформаційні кампанії, $З_2$ – маніпулювання настроями щодо мобілізації, $З_3$ – підрив міжнародної підтримки, $З_4$ – атаки на моральний дух ОС. Матриця попарних порівнянь за критерієм "Інтенсивність впливу":

Таблиця 2. Матриця попарних порівнянь за критерієм "Інтенсивність" та обчислення локальних пріоритетів

Загроза	$З_1$	$З_2$	$З_3$	$З_4$	$\prod a_{ij}^{(1/n)}$	$w_i^{(I)}$
$З_1$	1	3	2	4	2,213	0,440
$З_2$	1/3	1	1/2	2	0,760	0,151
$З_3$	1/2	2	1	3	1,316	0,262
$З_4$	1/4	1/2	1/3	1	0,745	0,148
Сума	—	—	—	—	5,034	1,000

Перевірка узгодженості: $\lambda_{max} \approx 4{,}03$; ІУ = (4,03 − 4) / 3 = 0,010; $ВВ_4 = 0{,}90$; ВУ = 0,010 / 0,90 = 0,011 ≤ 0,10 – **матриця узгоджена.**

2. *Глобальні пріоритети після синтезу за всіма критеріями.*

Після проведення аналогічних розрахунків за критеріями "Масштаб" (M), "Темп" (T), "Стійкість" (C) та визначення вагових коефіцієнтів критеріїв υ = (0,35; 0,25; 0,20; 0,20), глобальні пріоритети загроз (табл. 3).

Висновок: пріоритетними загрозами є $З_1$ (дезінформаційні кампанії, $W_1 = 0{,}401 > 1/4 = 0{,}25$) та $З_3$ (підрив міжнародної підтримки, $W_3 = 0{,}261 > 0{,}25$). Саме ці загрози підлягають детальному аналізу в другій частковій методиці.

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Таблиця 3. Результати ранжування когнітивних загроз за методом MAI

Загроза	*w_i^(I)*	*w_i^(M)*	*w_i^(T)*	*w_i^(C)*	W_i *(global)*	Ранг
$З_1$ – Дезінформ. кампанії	0,440	0,420	0,380	0,350	**0,401**	1
$З_2$ – Маніп. мобілізацією	0,151	0,180	0,260	0,200	**0,191**	3
$З_3$ — Підрив міжн. підтримки	0,262	0,270	0,200	0,320	**0,261**	2
$З_4$ – Атаки на мор. дух ОС	0,148	0,130	0,160	0,130	**0,142**	4

3. *Оцінювання впливу на показники ефективності ССК ЗС України.*

Для двох пріоритетних загроз визначено: $P(З_1)$ = 0,85; $P(З_3)$ = 0,70. Базові показники ефективності: $E°_1$ = 0,72 (довіра), $E°_2$ = 0,68 (охоплення аудиторій), $E°_3$ = 0,75 (моральний дух), $E°_4$ = 0,65 (міжнародна підтримка), $E°_5$ = 0,60 (стійкість інформ. простору).

Матриця коефіцієнтів деградації δ_{ij} наведена у табл. 4.

Розрахунок значень показників ефективності за формулою (9), де вагові коефіцієнти W_1 = 0,401; W_3 = 0,261 (табл. 5):

$$E_1(З) = 0,72 \cdot (1 - 0,85 \cdot 0,35 \cdot 0,401 - 0,70 \cdot 0,15 \cdot 0,261) = 0,72 \cdot (1 - 0,1193 - 0,0274) = 0,72 \cdot 0,8533 \approx 0,615$$

$$E_2(З) = 0,68 \cdot (1 - 0,85 \cdot 0,20 \cdot 0,401 - 0,70 \cdot 0,10 \cdot 0,261) = 0,68 \cdot (1 - 0,0682 - 0,0183) = 0,68 \cdot 0,9135 \approx 0,621$$

$$E_3(З) = 0,75 \cdot (1 - 0,85 \cdot 0,25 \cdot 0,401 - 0,70 \cdot 0,05 \cdot 0,261) = 0,75 \cdot (1 - 0,0852 - 0,0091) = 0,75 \cdot 0,9057 \approx 0,679$$

$$E_4(З) = 0,65 \cdot (1 - 0,85 \cdot 0,30 \cdot 0,401 - 0,70 \cdot 0,45 \cdot 0,261) = 0,65 \cdot (1 - 0,1023 - 0,0822) = 0,65 \cdot 0,8155 \approx 0,530$$

$$E_5(З) = 0,60 \cdot (1 - 0,85 \cdot 0,40 \cdot 0,401 - 0,70 \cdot 0,20 \cdot 0,261) = 0,60 \cdot (1 - 0,1363 - 0,0365) = 0,60 \cdot 0,8272 \approx 0,496$$

Таблиця 4. Матриця коефіцієнтів деградації показників ефективності ССК ЗС України

Загроза \ KPI	E_1 (довіра)	E_2 (охоплення)	E_3 (мор.дух)	E_4 (міжн.підтр.)	E_5 (стійкість)
$З_1$ (дезінформ.)	0,35	0,20	0,25	0,30	0,40
$З_3$ (підрив підтр.)	0,15	0,10	0,05	0,45	0,20

4. *Адитивне та мультиплікативне згортання. Інтегральна оцінка.*

При вагових коефіцієнтах α = (0,25; 0,20; 0,25; 0,20; 0,10) адитивний комплексний показник:

$$E_ком = 0,25 \cdot 0,615 + 0,20 \cdot 0,621 + 0,25 \cdot 0,679 + 0,20 \cdot 0,530 + 0,10 \cdot 0,496$$

$$E_ком = 0,154 + 0,124 + 0,170 + 0,106 + 0,050 = 0,604$$

При β = (0,30; 0,20; 0,30; 0,15; 0,05) мультиплікативний показник:

$$E_мульт = 0,615^{0,30} \cdot 0,621^{0,20} \cdot 0,679^{0,30} \cdot 0,530^{0,15} \cdot 0,496^{0,05} \approx 0,615^{0,30} \cdot 0,621^{0,20} \cdot 0,679^{0,30} \cdot 0,530^{0,15} \cdot 0,496^{0,05}$$

$$E_мульт \approx 0,868 \cdot 0,904 \cdot 0,893 \cdot 0,905 \cdot 0,986 \approx 0,591$$

Інтегральний показник при γ = 0,6:

$$E_інт = 0,6 \cdot 0,604 + 0,4 \cdot 0,591 = 0,362 + 0,236 = 0,598$$

Таблиця 5. Результати оцінювання ефективності ССК ЗС України в умовах пріоритетних когнітивних загроз

Показник	Базовий рівень $E°_j$	Рівень в умовах загроз $E_j(3)$	Відносне зниження, %
E_1 – Довіра суспільства	0,720	0,615	−14,6 %
E_2 – Охоплення аудиторій	0,680	0,621	−8,7 %
E_3 – Моральний дух ОС	0,750	0,679	−9,5 %
E_4 – Міжнародна підтримка	0,650	0,530	−18,5 %
E_5 – Стійкість інформ. простору	0,600	0,496	−17,3 %
E_ком (адитивний)	**0,686**	**0,604**	**−12,0 %**
E_інт (інтегральний)	**~0,680**	**0,598**	**−12,1 %**

5. *Аналіз оптимальної стратегії протидії (фрагмент теорії ігор).*

ЗС України мають три стратегії протидії: *sA* – активне спростування (фактчекінг + кіберпротидія), *sB* – медіапревенція (проактивне наративоутворення), *sC* – комбінована. Противник (росія) застосовує: *rI* – концентровані дезінформаційні атаки, *rII* – розпорошений вплив через соцмережі. Матриця втрат ефективності (1 − E_інт):

$$G = \begin{matrix} & rI & rII \\ sA: & [0{,}32 & 0{,}45] \\ sB: & [0{,}48 & 0{,}25] \\ sC: & [0{,}35 & 0{,}32] \end{matrix}$$

Аналіз матриці показує відсутність сідлової точки в чистих стратегіях. Оптимальна змішана стратегія ЗС Україна, отримана методом лінійного програмування: $p^* = (0{,}42;\ 0{,}31;\ 0{,}27)$, тобто 42% ресурсів – на активне спростування, 31% – на проактивне наративоутворення, 27% – на комбіновані заходи. Ціна гри (мінімальне гарантоване значення втрат ефективності): $v^* \approx 0{,}37$, що відповідає гарантованому рівню ефективності ССК ЗС України ≥ 0,63.

Висновки та рекомендації (Conclusion and Recommendations)

У статті розроблено методику пріоритизації та оцінювання впливу когнітивних загроз на ефективність системи стратегічних комунікацій ЗС України, яка складається з двох взаємопов'язаних часткових методик. Основні результати:

1. Запропонована загальна структурно-логічна схема методики охоплює шість послідовних етапів та конкретні процедурні блоки, що забезпечують повний цикл аналізу, від ідентифікації загроз до вироблення рекомендацій щодо оптимальної стратегії протидії.

2. Перша часткова методика (пріоритизація) базується на MAI Сааті з чотирма критеріями оцінювання (інтенсивність, масштаб, темп, стійкість) та забезпечує кількісне ранжування загроз з перевіркою узгодженості суджень експертів.

3. Друга часткова методика (оцінювання впливу) інтегрує апарат теорії ймовірності для оцінювання ймовірності реалізації загроз та коефіцієнтів деградації показників, адитивне та мультиплікативне згортання для визначення комплексного та інтегрального показника ефективності ССК, а також елементи теорії ігор для пошуку оптимальної стратегії протидії.

4. Практичний приклад підтвердив працездатність методики: для умов 2025–2026 рр. пріоритетними визначено загрози $З_1$ (дезінформаційні кампанії) та $З_3$ (підрив міжнародної підтримки). Сукупний вплив цих загроз знижує інтегральний показник ефективності ССК ЗС України на ≈12%, передусім за рахунок деградації показника міжнародної підтримки (−18,5%) та довіри суспільства (−14,6%).

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

5. Оптимальна стратегія протидії ЗС України, визначена за допомогою матричної гри, передбачає виділення 42% ресурсів на активне спростування та кіберпротидію, що гарантує рівень ефективності ССК не нижче ніж 0,63 за будь-якої стратегії противника.

Подальші дослідження доцільно спрямувати на: верифікацію запропонованої методики на реальних даних моніторингу інформаційного простору; розширення переліку когнітивних загроз з урахуванням новітніх технологій (діпфейки, ШІ-генерований контент); розроблення автоматизованого інструментарію підтримки ухвалення рішень на основі запропонованого математичного апарату; а також адаптацію методики до рівня оперативного командування ЗС України.

Конфлікт інтересів (Conflict of Interest)

Автор заявляє, що у нього немає конкуруючих інтересів за тематикою статті.

Використані джерела

1. Семененко, О. М. (2024). Когнітивні операції в сучасній гібридній війні: загрози та методи протидії. *Зб. наук. пр. ЦНДІ ЗС України, 2* (111), 12–28.
2. Taranenko, A. (2024). Когнітивна безпека як вимір російсько-української війни. *Політологічний вісник, 92*, 371–382. https://doi.org/10.17721/2415-881x.2024.92.371-382.
3. Максименко, С., & Деркач, Л. (2024). Сучасна когнітивно-інформаційна війна: роль маніпуляцій свідомістю українців у трансформації особистості. *Проблеми сучасної психології, 64*, 157–181.
4. Горбулін, В. П. (2022). *Як перемогти Росію у війні майбутнього*. Брайт Букс.
5. Стрельбицький М., & Гринь М. (2023). Когнітивна війна Росії проти України. *Наукові праці МАУП. Юридичні науки.* https://doi.org/10.32689/2522-4603.2023.1.7.
6. Сирський, О. С., Семененко, О. М., Лебеденко, А. В., & Кінь, О. В. (2025). Свідомість як поле бою – еволюція когнітивної війни у системі глобальної безпеки. *Зб. наук. пр. ЦНДІ ЗС України, 3* (114), 6–20.
7. Saaty, T. L. (1980). *The Analytic Hierarchy Process: Planning, Priority Setting, Resource Allocation*. McGraw-Hill.
8. Giles, K. (2023). *Russian Cyber and Information Warfare in Practice: Lessons from the War on Ukraine*. Chatham House.
9. Frontiers in Artificial Intelligence. (2025). *Decoding manipulative narratives in cognitive warfare: a case study of the Russia-Ukraine conflict*. https://doi.org/10.3389/frai.2025.1566022.
10. *Біла книга. Стратегічні комунікації та інформаційна безпека*. (2021). Міністерство оборони України. https://www.mil.gov.ua/.
11. Вентцель, Е. С. (2017). *Теорія ймовірностей*. (12-те вид.). КноРус.
12. Ларичев, О. І. (2006). *Теорія і методи прийняття рішень*. (3-тє вид.). Логос.
13. Льюс, Р. Д., & Райффа, Х. *Ігри та рішення: вступ і критичний огляд*. (Пер. з англ.).

References

1. Semenenko, O. M. (2024). Cognitive operations in modern hybrid warfare: Threats and countermeasures. *Collection of Scientific Works of the Central Research Institute of the Armed Forces of Ukraine, 2* (111), 12–28.
2. Taranenko, A. (2024). Cognitive security as a dimension of the Russian-Ukrainian war. *Political Science Bulletin, 92*, 371–382. https://doi.org/10.17721/2415-881x.2024.92.371-382
3. Maksymenko, S., & Derkach, L. (2024). Modern cognitive-information warfare: The role of manipulating Ukrainian consciousness in personality transformation. *Problems of Modern Psychology, 64*, 157–181.

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

4. Horbulin, V. P. (2022). *How to defeat Russia in the war of the future*. Bright Books.
5. Strelbytskyi, M., & Hryn, M. (2023). Russia's cognitive warfare against Ukraine. *Scientific Works of MAUP. Legal Sciences*. https://doi.org/10.32689/2522-4603.2023.1.7
6. Syrskyi, O. S., Semenenko, O. M., Lebedenko, A. V., & Kin, O. V. (2025). Consciousness as a battlefield – the evolution of cognitive warfare in the global security system. *Collection of Scientific Works of the Central Research Institute of the Armed Forces of Ukraine*, *3* (114), 6–20.
7. Saaty, T. L. (1980). *The analytic hierarchy process: Planning, priority setting, resource allocation*. McGraw-Hill.
8. Giles, K. (2023). *Russian cyber and information warfare in practice: Lessons from the war on Ukraine*. Chatham House.
9. *Frontiers in Artificial Intelligence*. (2025). Decoding manipulative narratives in cognitive warfare: A case study of the Russia-Ukraine conflict. https://doi.org/10.3389/frai.2025.1566022
10. Ministry of Defense of Ukraine. (2021). *White paper: Strategic communications and information security*. https://www.mil.gov.ua/
11. Venttsel, E. S. (2017). *Probability theory* (12th ed.). KnoRus.
12. Larichev, O. I. (2006). *Theory and methods of decision making* (3rd ed.). Logos.
13. Luce, R. D., & Raiffa, H. (1957). *Games and decisions: Introduction and critical survey*. John Wiley & Sons. (Original work published in English).

Methodology for prioritizing and assessing the impact of cognitive threats on the effectiveness of the strategic communications system of the Armed Forces of Ukraine

Oleh Temnyi
postgraduate
Department of Information Warfare, Institute of Strategic Communications
National Defense University of Ukraine
03049, Povitrianykh Syl avenue, 28, Kyiv, Ukraine
e-mail: o.temnyi@edu.nuou.org.ua
ORCID: 0009-0009-3173-094X

Abstract. The relevance of the study is due to the fact that in the conditions of full-scale aggression of the Russian Federation against Ukraine, cognitive threats have acquired a systemic, complex and targeted nature, which directly affects the effectiveness of the functioning of the strategic communications system of the Armed Forces of Ukraine. The strengthening of the information and psychological influence of the enemy, the growth of the role of disinformation, manipulative narratives and cognitive operations require the development of scientifically sound approaches to their identification, assessment and prioritization. In this regard, the formation of a methodological apparatus that allows for a comprehensive assessment of the impact of cognitive threats on the strategic communications system and ensuring the adoption of justified management decisions in the field of cognitive security is of particular importance. Therefore, the purpose of the article is to develop a methodology for prioritizing and assessing the impact of cognitive threats on the effectiveness of the strategic communications system of the Armed Forces of Ukraine, which takes into account the multi-criteria nature of such threats and the specifics of their implementation in the conditions of modern warfare. The main results of the research are the development of a

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

comprehensive methodology consisting of two interconnected partial methodologies. The first partial methodology is based on the application of the hierarchy analysis method and involves a pairwise comparison of cognitive threats according to certain criteria (intensity, scale, pace and stability of impact), which allows for their reasonable prioritization. The second partial methodology is aimed at assessing the impact of priority threats on the effectiveness of the strategic communications system and involves the use of the apparatus of probability theory, additive and multiplicative folding of indicators, as well as elements of game theory. The article proposes a structural and logical scheme of the methodology, which includes six consecutive stages with a detailing of procedural blocks in each of them, which ensures its practical feasibility. The practical calculation carried out for current cognitive threats in the period 2025–2026 allowed demonstrating the effectiveness of the proposed approach and its suitability for use in the conditions of the ongoing Russian-Ukrainian war. The materials of the article can be useful for military command bodies, strategic communications units, analytical and scientific institutions of the security and defense sector, as well as for specialists in the field of information and cognitive security. The proposed methodology can be used when assessing threats, planning countermeasures and increasing the effectiveness of strategic communications of the Armed Forces of Ukraine. Further research in the direction of the article should be focused on improving the mathematical apparatus for assessing cognitive threats, expanding the list of criteria for their analysis, integrating the developed methodology into the decision-making support system of military command bodies, as well as adapting approaches to the standards of NATO member states, taking into account the experience of conducting modern hybrid and cognitive wars.

Keywords: cognitive threats; strategic communications; Armed Forces of Ukraine; threat prioritization; method of hierarchy analysis; probability theory; game theory; additive and multiplicative convolution; system efficiency; cognitive security; russian-Ukrainian war.

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Received: *January 8, 2026* | **Revisions Requested:** - | **Revision Received:** -
Accepted: *March 28, 2026* | **Published Online:** *April 10, 2026*

Licensed (C) by Creative Commons Attribution International License 4.0 (CC BY-NC-SA)

DOI: 10.62524/msj.2026.4.1.12

Методика планування порядку оновлення озброєння, військової та спеціальної техніки військових формувань

Володимир Ткаченко
кандидат військових наук, старший дослідник
начальник управління
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: cvsdnaou@i.ua
ORCID: 0000-0002-9625-2434

Олег Тимків
кандидат військових наук, старший дослідник
начальник відділу – заступник начальника управління
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: tumkivoa@ukr.net
ORCID: 0000-0002-2248-382X

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: zps20022017@gmail.com
ORCID: 0000-0003-0421-7736

Василь Харченко
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: vasaxar1957@gmail.com
ORCID: 0000-0001-7160-7385

Наталія Ткаченко
молодший науковий співробітник
Національний університет оборони України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: cvsdnaou@i.ua
ORCID: 0009-0008-4706-813X

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Анотація. Оновлення озброєння – це процес заміни застарілих, зношених або частково застарілих зразків озброєння, військової та спеціальної техніки на більш сучасні, спрямований на підтримання або покращення бойових можливостей військових формувань. Для підтримання Збройних Сил України в боєздатному стані важливе значення має своєчасне оснащення їх новітніми зразками озброєння, військової та спеціальної техніки, що забезпечить захист державного суверенітету і територіальної цілісності держави. Оновлення озброєння наразі відбувається не за планом, а за наявності фінансових ресурсів на підставі рішення відповідних керівників. Методичного апарату обґрунтування порядку оновлення озброєння, військової та спеціальної техніки у військах практично немає. Це ускладнює порядок визначення військових формувань, у яких потрібно оновити озброєння, а також визначення зразків озброєння, військової та спеціальної техніки, які слід замінити новими. Таким чином, розроблення методики планування порядку оновлення озброєння, військової та спеціальної техніки військових формувань є актуальним питанням. Мета статті полягає в розробленні основних положень методичного підходу до планування порядку оновлення озброєння, військової та спеціальної техніки військових формувань. Методика передбачає обґрунтоване визначення потреби в оновленні озброєння, військової та спеціальної техніки, ранжування заходів оновлення, формування потреби в ресурсах на оновлення та оптимізацію планів оновлення в умовах обмеження ресурсів. Вона охоплює основні етапи процесу оновлення – від оцінювання поточного стану зразків озброєння, військової та спеціальної техніки до формування збалансованого Плану оновлення та моніторингу його подальшої реалізації. Статтю присвячено дослідженню основних етапів планування порядку оновлення озброєння. Кожний із представлених етапів методики є, по суті, окремим науковим методом. Методика є складною та багатофункціональною. Оскільки дослідження є багатокритеріальним, то у статті використовується багато коефіцієнтів, які враховують вплив різних факторів на процес планування оновлення озброєння, зокрема коефіцієнт технічної готовності, коефіцієнт морального старіння, коефіцієнт технічного рівня, коефіцієнт укомплектованості, коефіцієнт залишкового ресурсу тощо. Методика спрямована на впорядкування процесу планування порядку оновлення озброєння, військової та спеціальної техніки військових формувань, що сприятиме підвищенню їхньої боєздатності.

Ключові слова: коефіцієнт, методика, метод, оптимізація, оцінювання, оновлення, озброєння, військова та спеціальна техніка, показник, пріоритет, спроможності.

Вступ (Introduction)

Забезпечення державного суверенітету і територіальної цілісності держави в умовах збройної агресії потребує перебування Збройних Сил України (ЗС України) у стані високої та постійної бойової готовності. Однією з ключових складових цього процесу є своєчасне оновлення озброєння, військової та спеціальної техніки (ОВСТ), що передбачає заміну морально й фізично застарілих зразків ОВСТ сучасними, модернізованими та перспективними. Раціонально організований процес оновлення ОВСТ забезпечує нарощування бойових спроможностей без істотної зміни організаційно-штатної структури військових формувань, що є критично важливим в умовах тривалих бойових дій.

Аналіз сучасних загроз національній безпеці демонструє, що оновлення ЗС України новими високотехнологічними зразками (високоточними засобами ураження, безпілотними системами, засобами РЕБ та автоматизації управління) є безальтернативним шляхом зміцнення оборонного потенціалу держави.

На сьогодні процес оновлення парку ОВСТ військових формувань ЗС України стикається з низкою важливих факторів:

– швидке старіння парку ОВСТ. Значна кількість ОВСТ мають тривалі строки

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

експлуатації, є морально та фізично застарілими, а також потребують модернізації або заміни;

– проблема різнорідності ОВСТ. У з'єднаннях та частинах одночасно експлуатуються радянські зразки ОВСТ, ОВСТ вітчизняного виробництва різних років, трофейні зразки та численні зразки, отримані в рамках міжнародної технічної допомоги;

– недосконаліть системи постачання ОВСТ. Поставки ОВСТ нерідко організовано за принципом "постачання того що є", а не того "що необхідно". Темпи планового оновлення ОВСТ суттєво відстають від потреб;

– катастрофічний дефіцит ресурсів. Головною проблемою залишаються невідповідність бюджетних асигнувань реальним потребам на оновлення ОВСТ.

Попри гостроту зазначених факторів, нині у ЗС України методично обґрунтованого планування оновлення ОВСТ у військових формуваннях фактично немає.

Відсутність єдиного механізму, який би дозволив в умовах обмеженого фінансування визначити чітку пріоритетність зразків ОВСТ та збалансувати потреби з виділеними ресурсами, зумовлює актуальність цього дослідження.

Наприкінці минулого століття порядок технічного переозброєння активно обговорювали. Зокрема, йшлося про такі аспекти [1]:

– технічне переозброєння розглядали з економічних міркувань, зокрема стосовно фінансових затрат на оновлення техніки, затрат на нове будівництво виробничих будівель та приміщень. При цьому про освоєння нових технологій, про підвищення ефективності виробництва не йшлося;

– технічне переозброєння не пов'язували ні з розвитком науково-технічного прогресу, ні з можливими перевагами, які можуть бути досягнуті завдяки оновленню техніки.

Також багато уваги приділяється питанням щодо визначення поняття життєвого циклу зразків технічних засобів [2–5]. При цьому здебільшого звертається увага на економічний бік питання. Необхідність технічного переозброєння розглядається як економічно доцільний процес [6–8].

Порядок оновлення ОВСТ почали висвітлювати в останні роки [9], [10]. Пропонується два підходи. У [9] розглянуто метод планування процесу оновлення ОВСТ у військових формуваннях. При цьому вважається, що ресурси майже необмежені, а всі процеси детерміновані. У [10] розглянуто питання щодо оновлення ОВСТ на основі критерію приросту економічності виконання ними завдань за призначенням та обґрунтування граничних обсягів оновлення зразків ОВСТ одного типу. Водночас не аналізується питання щодо впливу оновлення на бойові можливості військового формування, в якому здійснюється оновлення ОВСТ. Крім того, оновлення зразків ОВСТ розглядається як процес приросту економічності виконання ними завдань за призначенням.

Питання щодо визначення номенклатури ОВСТ, які виробляються і постачаються країнами-партнерами для комплектування ЗС України, досліджується в [11].

Таким чином, у результаті аналізу досліджень щодо оновлення ОВСТ виявлено відсутність публікацій, які присвячені обґрунтуванню процесу планування оновлення ОВСТ у військових формуваннях, що свідчить про актуальність досліджуваного питання.

Метою статті є розроблення методики планування порядку оновлення озброєння та військової техніки військових формувань.

Матеріали та методи (Materials and Methods)

Під час розроблення методики застосовано низку кількісних та якісних методів:

– кількісні методи – під час розрахунків інтегральних коефіцієнтів (K_0, *ІП*): математичне моделювання (методи дослідження операцій, аналіз розриву спроможностей), статистичний аналіз даних;

– якісні методи – під час визначення вагових коефіцієнтів та оцінювання параметрів, які

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

не підпадають під пряме вимірювання.

Методи дослідження – системний аналіз (для побудови структури методики); метод експертного оцінювання (для визначення коефіцієнтів бойової важливості); математичне моделювання та лінійна нормалізація (для розрахунку пріоритетності та ризиків); сценарний аналіз та методи багатокритеріального оцінювання (для оптимізації планів в умовах ресурсних обмежень).

Таким чином, у дослідженні вирішено завдання щодо розроблення та формалізації науково-методичного апарату для планування оновлення озброєння.

Необхідність розроблення методики планування порядку оновлення ОВСТ військових формувань зумовлена кількома ключовими факторами, які впливають на здатність військ (сил) ефективно забезпечувати суверенітет і територіальну цілісність України в умовах швидкозмінного зовнішнього середовища. До таких факторів належать: зростання непередбачуваних загроз, швидкий розвиток військових технологій, необхідність довгострокового бачення та узгодженості між цілями, стратегіями та діями ЗС України тощо.

Результати дослідження вказують на те, що методичний апарат, який застосовується під час оборонного планування на довгострокову перспективу, має певні обмеження. До таких обмежень належать труднощі щодо прогнозування технологічного розвитку, військових загроз та глобальних тенденцій на 10–15 років, відсутність єдиних підходів до визначення показників, які використовуються під час визначення пріоритетних напрямів переозброєння. Крім того, нині немає достатньої бази даних щодо показників визначення перспективних напрямів переозброєння ЗС України.

Запропонована методика дозволяє досягти більш обґрунтованого і гнучкого підходу до визначення пріоритетних напрямів переозброєння ЗС України на довгострокову перспективу, зменшуючи ризики, пов’язані з динамічним середовищем та обмеженими ресурсами.

Як базовий показник визначення пріоритетних напрямів переозброєння ЗС України на довгострокову перспективу пропонується використовувати рівень пріоритету, що має ясний фізичний зміст, є чутливим до змін заходів розвитку, простим і зручним для проведення аналізу (розрахунків) та об’єктивно характеризує вплив розглядуваних заходів на напрями переозброєння ЗС України.

Особливостями відпрацьованої методики є те, що в ній:

– формалізовано процедуру оцінювання та пріоритизації оновлення ОВСТ;

– розроблено математичний апарат для об’єктивного ранжування потреб в оновленні ОВСТ;

– розроблено алгоритм розрахунку потреб в оновленні ОВСТ: визначено методичні підходи до розрахунку необхідних обсягів оновлення та формування фінансових потреб;

– створено механізм оптимізації оновлення ОВСТ в умовах обмежень. Ключовим результатом розділу є розроблення алгоритму балансування планів;

– забезпечено практичну придатність методики шляхом підготовлених уніфікованих форм вхідних та вихідних документів (матриці оцінювання, підсумкові таблиці тощо).

Новизна розробленої методики полягає у поєднанні адаптивних, комплексних і міждисциплінарних підходів до визначення пріоритетних напрямів переозброєння ЗС України, що дозволяє ефективно вирішувати завдання щодо довгострокового планування і підвищувати готовність до швидких змін у військово-стратегічній обстановці.

Таким чином, у дослідженні розроблено методику планування порядку оновлення ОВСТ у військових формуваннях, яка дає можливість перевести процес планування оновлення ОВСТ із суб’єктивної площини у формат системного, прозорого та науково обґрунтованого аналізу.

Результати (Results)

Розроблена методика планування порядку оновлення ОВСТ військових формувань

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

визначає єдиний системний підхід до планування оновлення ОВСТ у військових формуваннях. Вона спрямована на забезпечення обґрунтованого визначення потреби в оновленні ОВСТ, ранжування заходів, формування потреби в ресурсах та оптимізацію планів оновлення в умовах обмежених ресурсів. Методика базується на принципах комплексності, об'єктивності, системності, наукової обґрунтованості, пріоритетності, реалістичності та ітеративності. Вона охоплює ключові аспекти процесу: від оцінювання поточного стану ОВСТ до формування збалансованого Плану оновлення та моніторингу його реалізації.

Розроблена методика є аналітичною та планувальною ланкою в загальнодержавному циклі оборонного планування. Схему методики наведено на рис.1.

Підготовчий етап.

Визначаються та затверджуються організаційні, методологічні та інформаційні засади для запуску циклу планування оновлення ОВСТ.

Одним із головних завдань цього етапу є затвердження створеною постійною робочою групою (ПРГ) специфічних параметрів для поточного циклу планування, що включає:

– вагові коефіцієнти (w_i, β_i) визначення та обґрунтування важливості кожного критерію у формулах;

– критичні порогові значення**.** Встановлення порогових значень для індивідуальних коефіцієнтів стану ($K_{тг}$, $K_{ресурс}$ тощо);

– шкали оцінювання.

Одним із ключових завдань цього етапу є визначення та затвердження методологічних підходів до проведення експертних оцінювань, які будуть використовуватися на подальших етапах методики.

Для забезпечення стандартизації та порівнянності експертних оцінок розробляються уніфіковані інструменти (анкети, опитувальні листи, таблиці оцінювання).

Етап 1. Аналіз стану зразків ОВСТ військових формувань та формування потреби.

Оцінювання стану ОВСТ, що перебуває на озброєнні військових формувань, є фундаментальним етапом процесу планування оновлення ОВСТ. Цей етап методики спрямований на об'єктивне і системне діагностування рівня технічної справності, відповідності тактико-технічним вимогам, ступеня морального та фізичного зносу (вичерпання ресурсу) зразків ОВСТ, що експлуатуються у військах.

Робоча група, використовуючи затверджені на підготовчому етапі форми, збирає та систематизує дані щодо кількісних та якісних характеристик наявних зразків ОВСТ. На основі зібраних даних для кожного зразка ОВСТ визначаються ряд коефіцієнтів, нормалізованих до шкали від 0 до 1.

Для кожного зразка визначаються ключові коефіцієнти стану в інтервалі від 0 до 1. До таких коефіцієнтів належать коефіцієнт технічної готовності ($K_{тг}$), коефіцієнт морального старіння ($K_{мс}$), коефіцієнт технічного рівня ($K_{тр}$), коефіцієнт укомплектованості ($K_{ук}$), коефіцієнт залишкового ресурсу ($K_{ресурс}$). Після отримання всіх п'яти коефіцієнтів та визначення вагових коефіцієнтів w_i розраховується інтегральний коефіцієнт потреби в оновленні K_0 для кожного зразка ОВСТ.

Інтегральний коефіцієнт потреби в оновленні (K_o) – комплексний (узагальнюючий) показник, що кількісно характеризує ступінь обґрунтованої необхідності оновлення конкретного зразка ОВСТ на основі аналізу його поточного стану. Для розрахунку K_o використовуються значення коефіцієнтів $K_{тг}$, $K_{мс}$, $K_{тр}$, $K_{ук}$, $K_{ресурс}$ та вагових коефіцієнтів w_i.

The Central Research institute
of the Armed Forces of Ukraine

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

Military Science. Vol. 4 No.1 (2026)

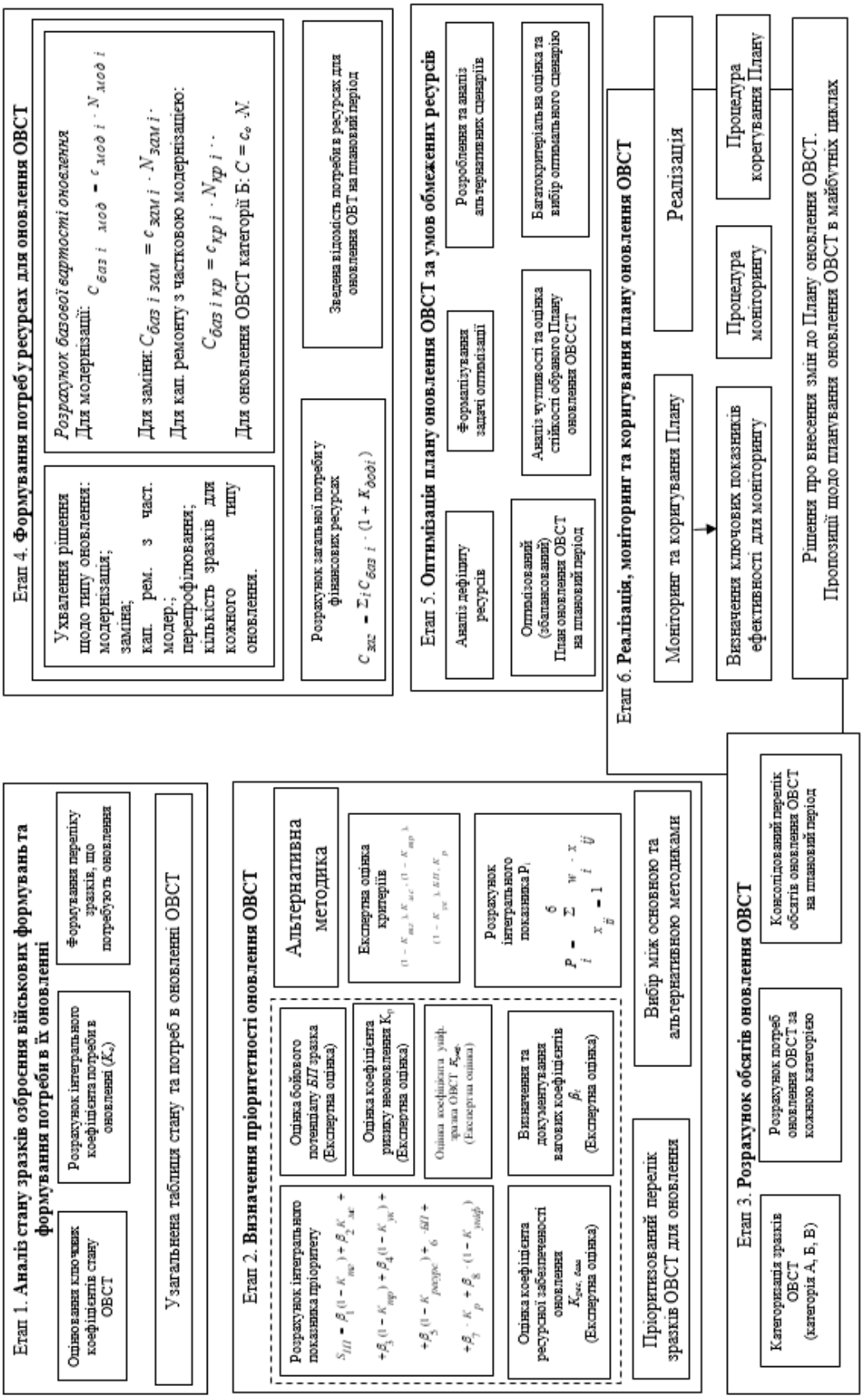


Рисунок 1. Схема методики планування порядку оновлення ОВТ у військових формуваннях

The Central Research institute
of the Armed Forces of Ukraine
ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Коефіцієнт технічної готовності ($K_{тг}$) – показник, що характеризує частку технічно справних зразків ОВСТ даного типу, готових до бойового застосування за призначенням, від загальної фактичної наявності зразків цього типу у військових формуваннях. Він відображає поточний рівень боєздатності парку ОВСТ з точки зору його технічної справності. Коефіцієнт $K_{тг}$ розраховується на основі даних служб експлуатації та озброєння:

$$K_{тг} = \frac{N_{техспр}}{N_{наявн}}, \quad (1)$$

Коефіцієнт морального старіння ($K_{мс}$) – показник, що характеризує ступінь відставання тактико-технічних характеристик (ТТХ) та функціональних можливостей зразка ОВСТ від сучасних вимог, що висуваються до ОВСТ цього класу, або від характеристик кращих вітчизняних і зарубіжних аналогів. Відображає технологічне та концептуальне відставання зразка ОВСТ, його нездатність ефективно протидіяти сучасним загрозам або виконувати завдання на належному рівні. Коефіцієнт морального старіння оцінюється експертами.
Джерелами даних для розрахунків є висновки експертних груп, результати науково-дослідних робіт, дані про ТТХ сучасних аналогів, доктринальні документи.

Коефіцієнт технічного рівня ($K_{тр}$) – відносна характеристика якості зразка ОВСТ, яка ґрунтується на порівнянні значень показників ТТХ зразка, який оцінюється, з еталонними значеннями відповідних ТТХ.

Джерелами даних для розрахунку коефіцієнта є експертні висновки, технічна документація на зразок ОВСТ та еталонні зразки, результати випробувань, дані про надійність та ремонтопридатність, аналіз вартості життєвого циклу.

Коефіцієнт укомплектованості ($K_{ук}$) – показник, що характеризує відношення фактичної наявності справних та готових до застосування зразків ОВСТ даного типу до штатної кількості зразків у військових формуваннях. У формулі K_o використовується як $(1 - K_{ук})$ – показник неукомплектованості. Розраховується за даними органів логістики та кадрових (мобілізаційних) органів:

$$К_{ук} = \frac{N_{наявн}}{N_{штат}}. \quad (2)$$

Джерелами даних є штатно-посадові розписи, табелі до штату, дані обліку ОВСТ, звіти органів логістики.

Коефіцієнт залишкового ресурсу ($K_{ресурс}$) – показник, що характеризує частку невипрацюваного технічного ресурсу зразка ОВСТ (за основними агрегатами або за інтегральним показником – мотогодинами, настрілом, календарним строком служби тощо) відносно встановленого нормативного (граничного) ресурсу до списання або капітального ремонту. Коефіцієнт відображає ступінь фізичного зносу ОВСТ та близькість до необхідності проведення капітального ремонту або списання. При розрахунку K_o використовується як $(1-K_{ресурс})$ – показник вичерпання ресурсу.

Коефіцієнт залишкового ресурсу розраховується на основі даних експлуатації та нормативно-технічної документації:

$$K_{ресурс} = \frac{R_{факт}}{R_{норм}} = \frac{R_{норм} - R_{відпр.}}{R_{норм}} = 1 - \frac{R_{відпр.}}{R_{норм}}. \quad (3)$$

Джерелами даних для коефіцієнта є формуляри (паспорти) зразків ОВСТ, дані автоматизованих систем обліку напрацювання, нормативно-технічна документація на ОВСТ, накази про встановлення норм ресурсу.

Розрахунок інтегрального коефіцієнта потреби в оновленні (K_o).

Інтегральний коефіцієнт потреби в оновленні *(K_o)* обчислюється як зважена сума нормованих показників, що характеризують різні аспекти стану зразка:

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

$$K_o = w_1 \cdot (1 - K_{тг}) + w_2 \cdot K_{мс} + w_3 \cdot (1 - K_{тр}) + w_4 \cdot (1 - K_{ук}) + w_5 \cdot (1 - K_{ресурс}), \quad (4)$$

де w_i – вагові числові коефіцієнти, що відображають відносну важливість (вагу) кожного з п'яти ключових коефіцієнтів стану ($(1-K_{тг})$, $K_{мс}$, $(1-K_{тр})$, $(1-K_{ук})$, $(1-K_{ресурс})$) під час розрахунку інтегрального коефіцієнта потреби в оновленні (K_o).

Значення вагових коефіцієнтів варіюються в діапазоні від 0 до 1. Вони визначаються експертами згідно з процедурами, затвердженими на підготовчому етапі.

Умова нормалізації: сума всіх вагових коефіцієнтів має дорівнювати одиниці:

$$\sum_{i=1}^{5} \omega_i = 1. \quad (5)$$

На основі розрахованого значення K_o визначається загальний рівень потреби (табл. 1).

Таблиця 1. Показники рівня потреби в оновленні ОВСТ (варіант)

Значення K_o	Рівень потреби в оновленні
≥ 0,7	високий (критичний)
0,5–0,69	середній (значний)
< 0,5	низький (незначний)

Результати оцінювання для всіх зразків ОВСТ зводяться в "Узагальнену таблицю стану та потреб в оновленні", яка містить такі стовпці, як: назва зразка ОВСТ, тип / клас, загальна кількість / укомплектованість ($K_{ук}$), значення $K_{тг}$, $K_{мс}$, $K_{тр}$, $K_{ресурс}$, розраховане значення K_o; рівень потреби в оновленні (*високий / середній / низький*) та пріоритет оновлення.

Етап 2. Визначення пріоритетності оновлення ОВСТ.

Цей етап спрямований на об'єктивне оцінювання та ранжування (впорядкування) зразків ОВСТ, відібраних на етапі 1.

Вхідні дані до етапу базуються на результатах етапу 1 та доповнюються новими експертними оцінками.

Розрахунок інтегрального показника пріоритету S.

Для кожного зразка ОВСТ, що підлягає оновленню, розраховується інтегральний показник пріоритету за наступною формулою:

$$S_{\text{ІП}} = \beta_1(1 - \text{К}_{\text{тг}}) + \beta_2\text{К}_{\text{мс}} + \beta_3(1 - \text{К}_{\text{тр}}) + \beta_4(1 - \text{К}_{\text{ук}}) + \beta_5(1 - \text{К}_{\text{ресурс}}) + \\ + \beta_6 \cdot \text{БП} + \beta_7 \cdot \text{К}_{\text{р}} + \beta_8 \cdot (1 - \text{К}_{\text{уніф}}), \quad (6)$$

де $S_{ІП}$ – інтегральний показник пріоритету оновлення зразків ОВСТ (чим вище значення, тим вищий пріоритет);

$K_{тг}$, $K_{мс}$, $K_{тр}$, $K_{ук}$, $K_{ресурс}$ – ключові коефіцієнти стану зразків ОВСТ, визначені на етапі 1.

β_1, β_2, …, β_8 – вагові коефіцієнти значущості відповідних критеріїв для визначення пріоритетності оновлення.

Оцінка бойового потенціалу (*БП*) зразка – це єдиний комплексний, нормалізований показник від 0 до 1, що характеризує важливість, критичність та ефективність зразка ОВСТ для виконання бойових завдань і його внесок у загальну бойову спроможність та відповідність оперативно-стратегічним потребам. Оцінюється експертною комісією на основі аналізу оперативних завдань, доктринальних документів, ролі зразка в системі ОВСТ.

Коефіцієнт ризику неоновлення ($K_р$) – нормалізована [від 0 до 1] оцінка рівня негативних наслідків (технічних, технологічних, логістичних, фінансових, оперативних), пов'язаних із подальшою експлуатацією (застосуванням за призначенням) зразка ОВСТ без оновлення у планові терміни. Оцінюється експертно.

Коефіцієнт уніфікації зразка ОВСТ ($K_{уніф}$) – нормалізована [від 0…1] оцінка рівня технічної сумісності та взаємозамінності даного зразка ОВСТ у межах частини (підрозділу), а також стандартизації за експлуатаційними параметрами, технічним обслуговуванням, ЗІП,

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

навчанням особового складу. Оцінюється експертно. Вищий $K_{уніф}$ (ближче до 1) свідчить про кращу уніфікацію. У формулі визначення S використовується $(1 - K_{уніф})$, оскільки низька уніфікація (високе значення $(1 - K_{уніф})$) може підвищити пріоритет оновлення (наприклад, на більш уніфікований зразок).

Тобто, чим вище значення $K_{уніфік}$, тим менш витратним та ризикованим буде забезпечення, обслуговування та введення зразка у військові формування. На коефіцієнт впливають ступінь використання у військах (масовість), наявність спільних комплектувальних з іншими зразками, сумісність з існуючою матеріально-технічною базою.

Коефіцієнт ресурсної забезпеченості оновлення ($K_{рес\ база}$) – відображає наявність фінансових, виробничих, логістичних та кадрових ресурсів для оновлення. $K_{рес\ база}$ оцінюється за даними табл. 2.

Таблиця 2. Шкала значень $K_{рес\ база}$ (варіант)

Рівень	Значення $K_{рес\ база}$	Опис
Високий	0.71 – 1.0	Усі ресурси (фінансові, виробничі, логістичні, кадрові) повністю доступні.
Середній	0.41 – 0.7	Більшість ресурсів доступні, реалізація оновлення можлива з уточненнями.
Низький	0.21 – 0.4	Часткова доступність ресурсів, реалізація оновлення ОВСТ можлива лише після доопрацювання.
Критичний	0.2	Практична відсутність ресурсів, оновлення неможливе без зовнішнього втручання.

Хоча він є важливим, його пряме включення до формули $S_{ІП}$ може призвести до зниження пріоритету для критично необхідних, але ресурсоємних зразків ОВСТ. Рекомендується збирати дані по $K_{рес\ база}$, але враховувати цей коефіцієнт переважно на етапі 5 під час аналізу реалістичності виконання Плану оновлення.

Після визначення вагових коефіцієнтів та розрахунку інтегрального показника пріоритету $S_{ІП}$ для кожного зразка ОВСТ його числове значення використовується для визначення рівня пріоритетності.

Альтернативна методика – експертне оцінювання (для розрахунку P_i).

Цей підхід застосовується в умовах обмеженості точних кількісних даних, браку часу для детальних розрахунків, або для експрес-оцінювання на оперативно-тактичному рівні.

Порядок застосування.

Крок 1. Експертне оцінювання критеріїв.

Формується група компетентних експертів, яка для кожного зразка ОВСТ оцінює шість ключових критеріїв:

1. Технічна готовність (оцінка корелює з високим значенням $1-K_{тг}$);
2. Моральне старіння (оцінка корелює з високим значенням $K_{мс}$);
3. Технічний рівень (оцінка корелює з високим значенням $1-K_{тр}$);
4. Укомплектованість (оцінка корелює з високим значенням $1-K_{ук}$);
5. Рівень бойового потенціалу (*БП*);
6. Ризик неоновлення ($K_р$).

Наведені критерії оцінюють за 5-бальною шкалою критичності / потреби в оновленні (де 1 – мінімальна, 5 – максимальна).

При цьому:

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

1 – мінімальна критичність / низька потреба;
2 – помірна критичність / потреба;
3 – середня критичність / потреба;
4 – висока критичність / потреба;
5 – максимальна (нагальна) критичність / потреба.

Крок 2. Розрахунок інтегрального показника P_i.

Після збирання та усереднення оцінок експертів сумарний пріоритет *Pi* для кожного зразка обчислюється за формулою:

$$P_i = \sum_{x_{ij}=1}^{6} w_i \cdot x_{ij}, \quad (7)$$

де P_i – сумарний пріоритет *i*-го зразка ОВСТ;

w_j – вагові коефіцієнти для шести критеріїв ($\sum W_j = 1$);

X_{ij} – усереднена експертна оцінка (від 1 до 5) *j*-го критерію для *i*-го зразка ОВСТ.

Для інтерпретації розрахованого значення P_i використовується наступна шкала (табл. 3).

Таблиця 3. Градація пріоритетів за значенням P_i

Значення P_i	Рівень пріоритету	Рекомендації щодо оновлення
> 4.0	Високий	Оновлення є першочерговим завданням
3.0 – 4.0	Середній	Оновлення доцільне при наявності ресурсів
2.0 – 2.9	Низький	Оновлення можливе, але може бути відтерміноване
< 2.0	Неактуальний	Оновлення не потребується найближчим часом

Градація пріоритетів за значенням P_i: (Примітка: наведені діапазони є орієнтовними і базуються на шкалі оцінок 1–5 та сумі ваг $\sum W_j = 1$. Максимально можливе значення $P_i = 5$).

Вибір між основною та альтернативною методиками залежить від конкретних умов та мети оцінювання, як зазначено в табл. 4.

Таблиця 4. Використання основної та альтернативної методик

Умови застосування	Рекомендована методика
Наявні повні та достовірні технічні та логістичні дані	Основна (розрахунок ІП)
Обмежені дані, необхідність швидкої оцінки, тактичний рівень	Альтернативна (експертна оцінка)
Проведення стратегічного аналізу, НДР, обґрунтування ДОЗ	Основна (розрахунок ІП)
Оперативно-тактичне планування у військах	Альтернативна (експертна оцінка)

В обох випадках ключовим є забезпечення компетентності експертів та прозорості процесу визначення як самих оцінок / коефіцієнтів, так і їхніх вагових коефіцієнтів.

Результати другого етапу представляються у вигляді табл. 5. Ця таблиця відображає ранжований перелік зразків із зазначенням розрахованого *ІП* (або P_i) та відповідного рівня пріоритетності.

У таблиці чітко візуалізовано результати ранжування, вона слугує основним вихідним документом етапу 2 для переходу до етапу 3.

Етап 3. Розрахунок обсягів оновлення ОВСТ.

Визначається найбільш доцільна стратегія оновлення кожного пріоритетного типу ОВСТ

Завдання етапу:

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

– категоризація пріоритизованих зразків ОВСТ;
– вибір та застосування відповідного методу розрахунку потреби в оновленні ОВСТ;
– розрахунок конкретної кількості зразків ОВСТ (N_i) для кожного заходу;
– формування консолідованого переліку обсягів оновлення ОВСТ для переходу до етапу формування потреби в ресурсах.

Таблиця 5. Пріоритизований перелік зразків ОВСТ для оновлення

№ з/п (місце в рейтингу)	Найменування зразка ОВСТ	Ідентифікатор зразка ОВСТ з етапу 1)	Розрахований інтегральний показник пріоритету (*ІП* або *Рі*)	Рівень пріоритетності оновлення (на основі *ІП* або *Рі*)	Ключові критерії, що визначили високий пріоритет	Примітки (наприклад, рекомендований тип оновлення, якщо вже попередньо визначено)
1	Зразок А	ID001	0.85	Високий	Критичний бойовий потенціал (*БП* = 0.9), високий ризик неоновлення (K_p=0.8)	Рекомендовано: заміна
2	Зразок Б	ID005	0.78	Високий	Значне моральне старіння (*Кмс=0.85*), високий K_o	Рекомендовано: модернізація або заміна
3	Зразок В	ID002	0.65	Середній	Низька технічна готовність ($1-K_{тг}$) = 0.7, значний K_o	Рекомендовано: капітальний ремонт з модернізацією
…						
N	Зразок N	ID0XX	0.35	Низький		Оновлення не є пріоритетним

Основним результатом етапу є обчислення ключових параметрів, що визначають темпи, обсяги та періодичність оновлення ОВСТ та формування “Консолідованого переліку обсягів оновлення ОВСТ на плановий період” (табл. 6), який є вхідним документом під час визначення потреби в ресурсах (етап 4) та оптимізації Плану оновлення (етап 5).

Таблиця 6. Консолідований перелік обсягів оновлення ОВСТ на плановий період

№ з/п (за пріоритетом)	Найменування зразка ОВСТ	Категорія	Метод розрахунку	Розрахована кількість до оновлення	Коротке обґрунтування кількості
1	ЗРК Тип-1	А	За спроможністю	2	Закриття розриву спроможностей ΔC_{ap} = X од. Внесок однієї нової системи *ГПЕі* $_{од.}$ = *Y* одиниць N_i = [X/Y] = 2
2	Танк тип Б	Б	Циклічний	30	Планове оновлення в рамках циклу. Обсяг одного циклу ($N_{зам}$) згідно з розрахунками
3	АТ КрАЗ	В	За станом	50	35 од. вже досягли критичного стану $N_i^{крит}$; 15 од. досягнуть критичного стану протягом наступних 2 років $N_i^{прогноз}$

The Central Research institute
of the Armed Forces of Ukraine
ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Етап 4. Формування потреб у ресурсах для оновлення ОВСТ.

Вхідні дані етапу доцільно представити у вигляді єдиної зведеної таблиці, що консолідує інформацію про зразки ОВСТ, їхній поточний стан (з етапу 1) та пріоритетність оновлення (з етапу 2). Вона слугуватиме основою для подальших розрахунків та ухвалення рішень. Варіант такої зведеної таблиці вхідних даних для етапу 4 наведено в табл. 7.

Таблиця 7. Зведений перелік зразків ОВСТ для планування ресурсів на оновлення (за результатами етапів 1 і 2 та, за потреби, етапу 3)

№ з/п (Відповідає місцю в рейтингу пріоритетності з етапу 2)	Найменування зразка ОВСТ	Ідентифікатор зразка ОВСТ (з етапу 1)	Розрахований *Ко* (інтегральний коефіцієнт потреби в оновленні, з етапу 1)	Рівень потреби в оновленні (за *Ко*, з етапу 1)	Ключові індивідуальні коефіцієнти стану (з етапу 1, напр., $K_{тг}$, $K_{мс}$, $K_{ресурс}$)	Розрахований інтегральний показник пріоритету (ІП або Рі, з етапу 2)	Рівень пріоритетності оновлення (з етапу 2)	Коротке обґрунтування пріоритету / ключові фактори (з етапу 2)
1	Зразок А	ID001	0,75	Високий	$K_{тг}$=0,6, $K_{мс}$=0,8, $K_{ресурс}$=0,2	0.85	Високий	Критичний *БП*, високий *Кр*
2	Зразок Б	ID005	0,68	Середній	$K_{мс}$=0,85 $K_{тр}$=0,5	0.78	Високий	Значне моральне старіння
…	…	…	…	…	…	…	…	…

Етап 5. Оптимізація Плану оновлення ОВСТ за умов обмежених ресурсів.

Проводиться визначення оптимальної стратегії розподілу обмежених ресурсів для реалізації Плану оновлення ОВСТ. Мета полягає в формуванні збалансованого Плану, який максимізує приріст бойових спроможностей та мінімізує ризики в межах встановлених фінансових, виробничих та інших обмежень.

Основним вхідним масивом даних є результати етапу 4, тобто “Зведена відомість потреби у ресурсах для оновлення ОВСТ”.

На основі аналізу або пропозицій, що виникли на етапі 4 або спеціально для етапу 5, розробляються альтернативні (менш затратні) варіанти оновлення.

Проводиться деталізація ризиків, пов’язаних зі скороченням або перенесенням термінів оновлення, що розглядаються в сценаріях оптимізації (для пріоритетних зразків ОВСТ).

Оптимізація Плану оновлення ОВСТ за умов обмежених ресурсів є складним завданням, що вимагає збалансованого підходу. Запропоновані нижче методи можуть застосовуватися окремо або, що частіше буває на практиці, у комбінації для розроблення найбільш прийнятного сценарію.

Вибір конкретного методу або їх поєднання залежить від величини дефіциту ресурсів, стратегічних пріоритетів та специфіки ОВСТ, що оновлюється.

Стратегічна мета – отримати максимальну бойову віддачу від реалізованих коштів, зосереджуючись на тих заходах, що найбільше посилюють боєздатність.

Формуються декілька потенційно ефективних сценаріїв скороченого Плану.

Сценарій 1 (Пріоритет понад усе). Цей сценарій формується на основі методу пріоритетного скорочення “зверху – вниз”, де заходи фінансуються тільки за показниками пріоритизації *ІП*, отриманими на етапі 2. Він передбачає фінансування заходів у суворій

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

відповідності до їхньої важливості до моменту вичерпання бюджетних лімітів.

Сценарій 2 (Максимальна ефективність витрат). Формується на основі ранжування.

Сценарій 3 (Математичний оптимум). Формується як розв'язок задачі оптимізації.

Сценарій 4 ("Стратегічний компроміс"). Розробляється експертною групою та може включати елементи інших підходів (відтермінування, зміна типу оновлення, фокус на спроможностях).

Процес вибору. Розроблені сценарії порівнюються між собою за допомогою запропонованих критеріїв. Для цього розробляється матриця рішень для багатокритеріального оцінювання сценаріїв оптимізації Плану оновлення на плановий період. Обирається не той сценарій, що є найкращим за одним математичним показником, а той, що демонструє найкращий збалансований результат за всією сукупністю критеріїв.

Результати п'ятого етапу – це комбінація структурованого табличного плану та детальних текстових аналітичних і обґрунтовуючих документів, які в сукупності складуть План оновлення озброєння на плановий період.

Після проходження відповідної процедури узгодження та затвердження компетентним органом військового управління (або вищим керівництвом) цей документ набуває статусу "Затвердженого Плану оновлення озброєння на певний період".

Етап 6. Реалізація, моніторинг та коригування Плану оновлення ОВСТ.

Відбувається забезпечення своєчасного та повного виконання затвердженого "Плану оновлення ОВСТ на плановий період", здійснення систематичного контролю за досягненням поставлених цілей та ефективним використанням ресурсів, а також оперативне реагування на зміни в обстановці або виявлені проблеми шляхом своєчасного коригування Плану.

Для проведення моніторингу виконання Плану оновлення ОВСТ встановлюються контрольні точки та періодичність звітності, здійснюється регулярний збір та аналіз даних за визначеними ПЕ від відповідальних виконавців. З метою отримання об'єктивних даних проводяться періодичні огляди виконання Плану за участю відповідальних осіб, з використанням механізмів зворотного зв'язку від військових формувань.

У разі суттєвих відхилень або змін умов – ініціюють процес перегляду та коригування Плану (повернення до попередніх етапів методики за потреби).

Підставою для коригування "Плану оновлення ОВСТ на плановий період" є суттєві відхилення фактичних показників від планових KPI_s, значні зміни в ситуації навколо України або поява нових загроз, що потребують перегляду пріоритетів.

Крім того, підставами для коригування Плану можуть стати зміни в обсягах фінансування або інших ресурсних обмежень та (або) у виробничих можливостях підприємств ОПК.

Корегування Плану може викликати поява нових, більш ефективних технологій або зразків ОВСТ чи, навпаки, виявлення суттєвих недоліків у оновлених зразках ОВСТ під час їхньої експлуатації (застосування за призначенням).

Ініціює процес коригування Плану оновлення ОВСТ на плановий період робоча група з планування оновлення ОВСТ у збройних силах, керівництво МО та ГШ ЗС України, командування видів / родів військ (сил).

Системний моніторинг та гнучке коригування Плану оновлення ОВСТ є запорукою його успішної реалізації та досягнення поставлених цілей щодо підтримання та підвищення обороноздатності військових формувань.

Висновки (Conclusion)

Таким чином, у статті вирішено наукове завдання щодо розроблення та формалізації науково-методичного апарату для планування оновлення озброєння.

Запропонована методика дозволяє досягти більш обґрунтованого і гнучкого підходу до

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

визначення пріоритетних напрямів переозброєння ЗС України на довгострокову перспективу, зменшуючи ризики, пов'язані з динамічним середовищем та обмеженими ресурсами.

Особливостями запропонованої методики є те, що в ній:

– формалізовано процедуру оцінювання та пріоритизації оновлення ОВСТ;

– розроблено математичний апарат для об'єктивного ранжування потреб в оновленні ОВСТ;

– розроблено алгоритм розрахунку потреб в оновленні ОВСТ. Визначено методичні підходи до розрахунку необхідних обсягів оновлення та формування фінансових потреб;

– запропоновано алгоритм оптимізації оновлення ОВСТ в умовах обмежень. Ключовим результатом є розроблення алгоритму балансування планів;

– забезпечено практичну придатність методики шляхом підготовлених уніфікованих форм вхідних та вихідних документів (матриці оцінювання, підсумкові таблиці тощо).

Новизна розробленої методики полягає у поєднанні адаптивних, комплексних і міждисциплінарних підходів до визначення пріоритетних напрямів переозброєння ЗС України, що дозволяє ефективно вирішувати завдання щодо довгострокового планування і підвищувати готовність до швидких змін у стратегічній обстановці.

Перспективами подальших досліджень може бути удосконалення методичного апарату обґрунтування порядку оновлення ОВСТ військових формувань з урахуванням аналізу результатів виробництва на вітчизняному ОПК.

Рекомендації (Recommendations)

Матеріали публікації пропонується використовувати для обґрунтування бюджетних запитів та ефективного використання оборонних ресурсів під час переходу до планування оновлення ОВСТ на основі спроможностей.

Розроблену методику, що забезпечує перехід від ситуативного ухвалення рішення до об'єктивного визначення пріоритетів оновлення ОВСТ та раціонального розподілу ресурсів, пропонується впровадити в систему нормативно-правових документів, а запропонований математичний апарат використати як основу для автоматизації процесів планування оновлення ОВСТ.

Конфлікт інтересів (Conflict of Interest)

Автори заявляють, що у них немає конфлікту інтересів.

Використані джерела

1. Аргинбеков, А. У. (2000). *Оновлення парку машин і обладнання на промисловому підприємстві* [Дис. канд. екон. наук].
2. Демідов, Б. О., Величко, О. Ф., & Волощук, І. В. (2006). *Системно-концептуальні основи діяльності у військово-технічній сфері: Кн. 2. Організаційно-методичні основи діяльності у військово-технічній сфері. Технологічний парк.*
3. Ковтуненко, А. П., & Зубарев, В. В. (2009). *Основы анализа сложных технических систем. Теория и приложения.* [Монографія]. ЦНДІ ОВТ ЗСУ.
4. Крыжный, А. В. (1994). *Основы решения проблемы долговечности вооружения войск ПВО Сухопутных войск*. [Дис. докт. техн. наук].
5. Романченко, І. С., Шуєнкін, В. О., Хомчак, Р. Б., Трегубенко, С. С., Марко, І. Ю., Закусило, П. С., & Хазанович, О. І. (2019). *Розвиток теорії матеріально-технічного забезпечення військ*. [Монографія]. НАСВ.
6. Бояринова, К. О., & Данильченко, К. О. (2010). *Управління процесом технічного переозброєння в контексті інноваційного розвитку підприємства*. http://www.nbuv.gov.ua/e-journals/PSPE/2010_2/Boyarinova_210.htm
7. Петрович, Й. М., Кіт, А. Ф., & Кулішов, В. В. *Оновлення техніко-технологічної бази*

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

шляхом проведення технічного переозброєння й реконструкції підприємства. http://poglyad.com/students/item/15599/.
8. Кушніренко, О. М. (2007). *Управління інноваційним оновленням матеріально-технічної бази виробництва* [Автореф. дис. канд. екон. наук]. (с. 22).
9. Закусило, П. С. (2016). *Розвиток теоретичних основ забезпечення боєздатності з'єднань (частин) збройних сил України за рахунок комплексного обґрунтування строку служби, міжремонтних строків експлуатації та тривалості планового ремонту озброєння і військової техніки.* [Дис. докт. військ. наук, ЦНДІ ЗС України].
10. Семененко, О. М., Іванов, В. Л., Колчін, Р. В., & Зарицький, О. І. (2015). Методика обґрунтування граничних обсягів оновлення зразків озброєння та військової техніки одного типу. *Зб. наук. праць ВА*, *2* (4), 34–39.
11. Довгополий, А. С., & Дихановський, А. М. (2022). Військово-технічна політика України як основа співробітництва з державами-партнерами в процесах розроблення, виробництва і постачання озброєння. *Озброєння та військова техніка*, *1* (33), 22–28. https://doi.org/10.34169/2414-0651.2022.1(33).22-28.

References

1. Argynbekov, A. U. (2000). *Renewal of the fleet of machines and equipment at an industrial enterprise* [Candidate of Economic Sciences dissertation].
2. Demidov, B. O., Velychko, O. F., & Voloshchuk, I. V. (2006). *System and conceptual foundations of activity in the military-technical sphere: Book 2. Organizational and methodological foundations of activity in the military-technical sphere*. Tekhnolohichnyi Park.
3. Kovtunenko, A. P., & Zubarev, V. V. (2009). *Fundamentals of the analysis of complex technical systems: Theory and applications* [Monograph]. Central Research Institute of Armaments and Military Equipment of the Armed Forces of Ukraine.
4. Kryzhnyi, A. V. (1994). *Fundamentals of solving the service life problem of air defense weapons of the Army Air Defense troops* [Doctor of Technical Sciences dissertation].
5. Romanchenko, I. S., Shuienkin, V. O., Khomchak, R. B., Trehubenko, S. S., Marko, I. Yu., Zakusylo, P. S., & Khazanovych, O. I. (2019). *Development of the theory of material and technical support of troops* [Monograph]. NASV.
6. Boiarynova, K. O., & Danylchenko, K. O. (2010). *Management of the technical re-equipment process in the context of the enterprise's innovative development*. http://www.nbuv.gov.ua/e-journals/PSPE/2010_2/Boyarinova_210.htm
7. Petrovych, Y. M., Kit, A. F., & Kulishov, V. V. (n. d.). *Renewal of the technical and technological base through technical re-equipment and reconstruction of an enterprise*. http://poglyad.com/students/item/15599/
8. Kushnirenko, O. M. (2007). *Management of innovative renewal of the material and technical base of production* [Abstract of the Candidate of Economic Sciences dissertation]. (p. 22).
9. Zakusylo, P. S. (2016). *Development of the theoretical foundations for ensuring the combat capability of formations (units) of the Armed Forces of Ukraine through comprehensive substantiation of service life, between-repair operating intervals, and the duration of planned repair of weapons and military equipment* [Doctor of Military Sciences dissertation. The Central Research Institute of the Armed Forces of Ukraine].
10. Semenenko, O. M., Ivanov, V. L., Kolchin, R. V., & Zarytskyi, O. I. (2015). Methodology for substantiating the limiting volumes of modernization of weapons and military equipment samples of one type. *Collection of Scientific Papers of the Military Academy, 2* (4), 34–39.
11. Dovhopolyi, A. S., & Dykhanovskyi, A. M. (2022). Ukraine's military-technical policy as a basis for cooperation with partner states in the processes of development, production, and supply of armaments. *Armament and Military Equipment, 1* (33), 22–28. https://doi.org/10.34169/2414-0651.2022.1(33).22-28

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Methodology for Planning the Procedure for Modernizing Weapons and Military (Special) Equipment of Military Formations

Volodymyr Tkachenko
Candidate of Military Sciences, Senior Researcher
Head of Directorate
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl avenue, 28 B, Kyiv, Ukraine
e-mail: cvsdnaou@i.ua
ORCID: 0000-0002-9625-2434

Oleh Tymkiv
Candidate of Military Sciences, Senior Researcher
Head of Department – Deputy Head of Directorate
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl avenue, 28 B, Kyiv, Ukraine
e-mail: tumkivoa@ukr.net
ORCID: 0000-0002-2248-382X

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: zps20022017@gmail.com
ORCID: 0000-0003-0421-7736

Vasyl Kharchenko
Candidate of Military Sciences, 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: vasaxar1957@gmail.com
ORCID: 0000-0001-7160-7385

Nataliia Tkachenko
Junior Research Fellow
National Defence University of Ukraine
03049, Povitrianykh Syl avenue, 28 B, Kyiv, Ukraine
e-mail: cvsdnaou@i.ua
ORCID: 0009-0008-4706-813X

Abstract. Weapons modernization is the process of replacing obsolete, worn, or partially outdated items of weapons and military (special) equipment (WMSE) with more advanced ones, aimed at maintaining or enhancing the combat capabilities of military formations. To maintain the Armed Forces of Ukraine (AFU) in a combat-capable state, timely equipping them with the latest WMSE is of particular importance, as it ensures the protection of the state's sovereignty and territorial integrity. At present, weapons modernization is carried out not according to a plan, but subject to the

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

availability of financial resources and based on decisions of the relevant commanders. A methodological framework for substantiating the procedure for WMSE modernization within the troops is practically absent. This complicates the identification of military formations in which weapons modernization is required, as well as the determination of WMSE items that should be replaced with new ones. Therefore, developing a methodology for planning the modernization procedure for WMSE of military formations is a relevant issue. The purpose of the article is to develop the key provisions of a methodological approach to planning the procedure for modernizing WMSE of military formations. The methodology provides for a substantiated determination of the need for WMSE modernization, the prioritization of modernization measures, the formation of resource requirements for modernization, and the optimization of modernization plans under resource constraints. It covers the main stages of the modernization process—from assessing the current condition of WMSE items to forming a balanced Modernization Plan and monitoring its further implementation. The article is devoted to studying the main stages of planning the procedure for weapons modernization. Each stage of the proposed methodology is, in essence, a separate scientific method. The methodology is complex and multifunctional. Since the research is multi-criteria, the article uses a significant number of coefficients that take into account the influence of various factors on the weapons modernization planning process, including the technical readiness coefficient, the obsolescence coefficient, the technical level coefficient, the manning (equipment fill) coefficient, the residual service life coefficient, and others. The methodology is aimed at streamlining the process of planning the procedure for modernizing WMSE of military formations, which will contribute to increasing their combat capability.

Keywords: coefficient; methodology; method; optimization; assessment; modernization; weapons; military and special equipment; indicator; priority; capabilities.

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Received: *November 11, 2025* | **Revisions Requested:** - | **Revision Received:** -
Accepted: *January 21, 2026* | **Published Online:** *April 10, 2026*

Licensed (C) by Creative Commons Attribution International License 4.0 (CC BY-NC-SA)

DOI: 10.62524/msj.2026.4.1.13

Аналіз підходів НАТО до системи моделювання та імітації, перспективи їх адаптації й упровадження в Україні

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, професор
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

Дмитро Нелінь
начальник науково-дослідного відділу
Харківський національний університет Повітряних Сил імені Івана Кожедуба
61023, вул. Сумська, 77/79, Харків, Україна
e-mail: nelindima35@gmail.com
ORCID: 0009-0003-9448-392X

Андрій Лук'янчиков
провідний науковий співробітник науково-дослідного відділу
Харківський національний університет Повітряних Сил імені Івана Кожедуба
61023, вул. Сумська, 77/79, Харків, Україна
e-mail: laa1968@ukr.net
ORCID: 0000-0002-3584-7901

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Анотація. Актуальність дослідження зумовлена потребою у трансформації систем підготовки та управління військ в умовах нових типів загроз, що проявилися під час російсько-української війни. Масоване застосування безпілотних систем, високоточного озброєння, засобів радіоелектронної боротьби і кібератак висвітлило обмеження традиційних підходів до навчання військ та аналізу результатів операцій. У зв'язку із цим зростає роль систем моделювання та імітації, які у НАТО розглядаються як стратегічний ресурс для підготовки, планування, дослідження та проведення операцій у багатодоменному середовищі. Метою роботи є аналіз структури, методологічних засад і ключових напрямів розвитку системи моделювання та імітації у НАТО, а також виявлення можливостей адаптації цих підходів у Збройних Силах України. У статті розкрито діяльність інституційних компонентів системи, підходи до стандартизації та технологічні ініціативи. Показано, що ефективність систем моделювання та імітації визначається рівнем інтеграції, стандартизації та доступності синтетичних середовищ. Обґрунтовано, що у вітчизняній практиці потенціал таких систем залишається недооціненим, термін "навчально-тренажерна база" не охоплює аналітично-дослідницьку функцію, яка є ключовою для підтримки прийняття рішень і дослідження операцій. Основними методами дослідження є системний і порівняльний аналіз, контент-аналіз нормативних документів НАТО, наукових публікацій українських дослідників та національних керівних документів у сфері підготовки військ і розвитку тренажерно-імітаційних систем. Результати статті можуть бути використані під час формування національної концепції розвитку систем моделювання та імітації, розроблення стандартів валідації тренажерів і моделей, створення єдиного інформаційно-аналітичного простору підготовки Збройних Сил України.

Ключові слова: моделювання та імітація, НАТО, симулятори, тренажери, підготовка військ, Збройні Сили України.

Вступ (Introduction)

Сучасне безпекове середовище характеризується високим рівнем невизначеності, багатодоменністю та зростаючою динамікою розвитку загроз, що суттєво ускладнює процеси підготовки, планування та ведення операцій. У цьому контексті традиційні методи військового навчання та аналізу мають обмежені можливості щодо відтворення реалістичних сценаріїв майбутніх подій. Як рішення розглядаються варіанти синтетичних середовищ, під якими розуміють штучно створені інтегровані простори, що об'єднують моделі, імітатори, інформаційні системи та реальні дані для відпрацювання навчальних сценаріїв, військових ігор і дослідження альтернативних варіантів розвитку подій.

З науково-методологічної точки зору терміни "modelling and simulation", "моделювання і симуляція", а також українські відповідники "моделювання" та "імітація" є функціонально рівнозначними. У стандартах НАТО (зокрема AMSP-01C, MSG-123) під "modelling" мають на увазі побудову абстрактної моделі об'єкта чи процесу, а під "simulation" – практичне застосування цієї моделі для експериментів або навчання. У військовій термінології країн НАТО ці обидва поняття розглядають як елементи єдиного процесу, що взаємно доповнюють один одного. Відповідно, скорочення M&S охоплює їх разом та застосовується як узагальнений рівнозначний термін "Modelling and Simulation" (моделювання (імітація)), який і будемо надалі використовувати у цьому значенні.

Підхід НАТО у сфері M&S є доцільним для України з огляду на його комплексність, стандартизованість і спрямованість на інтеграцію навчальних, аналітичних та управлінських процесів у єдиному інформаційному середовищі. Протягом останніх десятиліть країни – члени НАТО сформували розгалужену систему M&S, яка поєднує методологічні стандарти, інституційну підтримку та інструменти спільного навчання, аналізу й оцінювання операцій.

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Розвиток M&S у НАТО має стратегічне значення, оскільки дозволяє проводити військові ігри, програвання сценаріїв операцій, аналітичні дослідження та оцінювання ризиків без залучення значних матеріальних ресурсів. Особливу роль у цьому процесі відіграє Командування з питань трансформації (Allied Command Transformation, ACT), яке розглядає формування інтегрованого синтетичного середовища НАТО як пріоритетне завдання.

Такі середовища охоплюють наземний, морський, повітряний, космічний та кіберпростір, створюючи умови для безризикового випробування варіантів дій і багатопрофільної підготовки. Важливим чинником є їхня економічна доцільність: використання синтетичних середовищ дозволяє суттєво зменшити витрати на проведення реальних навчань, маневрів і випробувань озброєнь, скорочує потребу у витраті матеріальних ресурсів і водночас знижує ризики для особового складу та техніки.

Для України, що переходить на принципи НАТО у підготовці та управлінні, впровадження цих підходів є необхідною умовою створення сучасної, взаємосумісної системи моделювання та імітації, здатної забезпечити ефективну бойову підготовку, аналіз і планування операцій.

Центральним елементом у сфері M&S є впровадження підходу, який орієнтується на наявні дані. Він передбачає використання реальних оперативних, розвідувальних, логістичних та технічних даних як основи для побудови моделей і проведення імітацій. На відміну від традиційних сценарних методів, що значною мірою спиралися на експертні припущення, такий підхід забезпечує підвищену достовірність результатів, знижує рівень суб'єктивності та дозволяє формувати більш реалістичні прогнози розвитку ситуації. Це створює передумови для більш точного планування багатодоменних операцій та підвищення їхньої ефективності.

Досвід російсько-української війни наочно продемонстрував критичне значення таких підходів. Масштабне застосування безпілотних систем, засобів радіоелектронної боротьби, кібероперацій і високотехнологічних засобів ураження створює середовище, яке важко відтворити у традиційних навчаннях [1–4]. Українська практика підтвердила необхідність швидкої адаптації M&S до нових загроз, інтеграції даних з різнорідних джерел, а також проведення випробувань у синтетичних середовищах для перевірки ефективності нових тактик і технологій. Потенційно моделювання та імітація дають змогу не лише підвищити якість підготовки, а й стати елементом оперативної підтримки прийняття рішень у реальному часі.

Ефективне застосування засобів M&S неможливе без єдиних стандартів, які виконують роль "спільної мови" для взаємодії різнорідних систем. Значний внесок у цій сфері здійснили міжнародні організації IEEE, ISO та SISO, ключовим кроком для НАТО стало ухвалення у 1998 році архітектури HLA (High Level Architecture), яку закріплено у STANAG 4603. HLA забезпечує універсальний підхід до створення розподілених інтерактивних середовищ, у яких підсистеми взаємодіють через обмін повідомленнями, зберігаючи узгодженість функціонування.

Таким чином, системи M&S у діяльності НАТО виходять за межі інструментів технічної імітації суто для навчання. Вони постають як стратегічний ресурс, який інтегрує аналітичні, навчальні та управлінські функції, сприяючи підтримці оборонної спроможності, й розглядаються як стратегічні переваги НАТО у складному багатодоменному середовищі.

Метою роботи є аналіз структури, методологічних засад і ключових напрямів розвитку системи моделювання та імітації у НАТО, а також виявлення можливостей адаптації цих підходів у Збройних Силах України (ЗС України). Наукова новизна роботи полягає у комплексному розгляді системи M&S НАТО як інтегрованого інструменту підготовки військ, аналізу операцій і підтримки прийняття рішень у багатодоменному середовищі. У дослідженні узагальнено зміст ключових керівних документів НАТО з урахуванням їхньої потенційної адаптації до національної системи підготовки, а також висвітлено відмінності між навчально-

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

тренажерним і дослідницько-аналітичним використанням систем M&S. Теоретичне значення роботи полягає у розширенні наукових уявлень про роль моделювання та імітації у формуванні спільного інформаційного простору управління й навчання військ, що сприяє розвитку сучасної теорії військової підготовки та управління. Практичне значення результатів визначається можливістю їх використання під час розроблення національної концепції розвитку систем M&S, створення нормативно-методичної бази сертифікації тренажерних засобів і поступової інтеграції українських розробок у спільні програми НАТО. Отримані висновки можуть бути корисними для органів військового управління, наукових установ та підприємств оборонно-промислового комплексу, що працюють над створенням і впровадженням тренажерно-імітаційних систем.

Методологічна основа (Methodological Framework)

Дослідження ґрунтується на комплексному підході, що поєднує аналіз військових, технологічних та організаційно-методичних аспектів розвитку систем M&S у структурах НАТО і визначення можливостей адаптації цих підходів до потреб ЗС країни. Такий підхід дозволяє розглядати M&S не лише як навчальний інструмент, а як важливий елемент єдиної системи управління знаннями, що підтримує процеси підготовки, планування та аналізу операцій.

Методологічну основу дослідження становлять системний, порівняльний і структурно-функціональний аналіз, а також контент-аналіз та елементи прогнозування. Інформаційну базу склали офіційні документи НАТО, матеріали Командування з трансформації (АСТ), Групи моделювання та імітації, Центру передового досвіду M&S, звіти Об'єднаного центру аналізу та уроків, а також наукові праці українських дослідників і відкриті матеріали, присвячені розвитку тренажерно-імітаційних систем та імітаційних технологій у військовій сфері.

Метод системного аналізу використано для розгляду системи M&S НАТО як цілісного утворення зі взаємопов'язаними організаційними, технологічними та нормативними складовими. Порівняльний підхід дав змогу зіставити підходи НАТО та України до розроблення і застосування імітаційних систем, визначити спільні риси та відмінності. Контент-аналіз документів НАТО, українських наукових публікацій і відкритих джерел дозволив узагальнити ключові принципи побудови синтетичних навчальних середовищ і оцінити можливості їх адаптації у національній практиці. Елементи прогнозування застосовано для визначення тенденцій розвитку системи M&S в Україні у контексті інтеграції у спільний інформаційний простір НАТО.

Дослідження має певні обмеження, зокрема використано лише відкриті джерела, що не дають повного доступу до даних щодо організації бойової підготовки ЗС України, а також до технічних характеристик і результатів випробувань M&S-систем НАТО, які могли б деталізувати оцінку їхніх функціональних можливостей.

Результати (Results)

Війна в Україні наочно довела, що традиційні підходи до підготовки військ більше не відповідають викликам сучасного бою. Реалістичне навчання має враховувати дію в електромагнітно насичених і ворожих середовищах, гібридних загроз та "підпорогових" впливів у кількох доменах одразу [1, 2], а також функціонування систем в умовах логістичних збоїв і нестабільного зв'язку. Це вимагає відмови від "спрощених сценаріїв" та переходу до тренувань, що відтворюють складні оперативні проблеми. На думку провідних військових експертів США та НАТО [2], лише систематичне відпрацювання подібних ситуацій у мирний час здатне забезпечити ефективність військ у кризових і бойових умовах. Відтак майбутня система підготовки має інтегрувати багатодоменні загрози, фактори електронної боротьби та кібероперацій, роблячи головний акцент на стійкості та адаптивності військових структур.

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

При цьому слід враховувати, що сучасне покоління навчально-тренувальних засобів і систем імітації здатне забезпечити до 70–80% завдань бойової підготовки, передбачених програмами [5, 6].

Загальний підхід НАТО до систем M&S у систематизованому вигляді наведено на рис. 1, ключовими принципами є взаємосумісність, модульність, реалістичність, інтеграція з C4ISR (Command and Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance / Командування, управління, комп'ютери, зв'язок, розвідка, спостереження і рекогносцирування) та мультирівневе застосування – від індивідуального тренінгу до багатонаціональних операцій. Такі системи призначені для підвищення готовності, тестування тактик і підтримки прийняття оперативних рішень.



Рисунок 1. Загальний підхід НАТО до систем моделювання та імітації

НАТО надає моделюванню та імітаторам бойових систем надзвичайно важливе значення в контексті трансформації сил і модернізації підготовки персоналу, відзначається, що сучасні синтетичні середовища не в змозі повною мірою відтворити майбутні складні умови бойових дій, тому розроблення нових засобів M&S є пріоритетним [7]. Задля виконання цього завдання у НАТО створено певні організаційні структури. До найважливіших із них, які відповідають за моделювання й імітацію бойових дій, належать:

1. *Об'єднане командування з трансформації НАТО* (ACT), яке очолює стратегічні дослідження та розроблення концепцій, пов'язаних із багатодоменними операціями та імітацією бойових дій. ACT підтримує тісну співпрацю з Центром передового досвіду з M&S, а також з іншими структурами НАТО, впроваджуючи інновації в програми навчань і досліджень.

2. *Центр передового досвіду з M&S НАТО* (NATO Modelling & Simulation Centre of

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Excellence, M&S CoE), який, відповідно до "Основних принципів Центрів досвіду НАТО" (освіта та навчання; аналіз та отримані уроки; розроблення концепцій та апробація; розроблення доктрин та стандартів), спеціалізується на навчанні, обміні досвідом і розробленні методик у сфері M&S. Центр проводить комплексні курси (в тому числі базовий курс з моделювання, сертифікацію фахівців з комп'ютерних вправ тощо), які охоплюють як імітацію бойових дій, так і суміжну підтримку [9, 10]. Крім того, Центр є об'єднуючим хабом для спільноти фахівців: військових, науковців та представників оборонної промисловості [7]. Під егідою центру проводяться регулярні конференції й форуми, зокрема центр організовує та проводить щорічний Форум НАТО з комп'ютерного аналізу, навчання та досліджень (Computer Assisted Analysis, Exercise, Experimentation Forum, CA²X² Forum), який об'єднує більше 300 експертів з понад 30 країн. За словами керівника центру, він тісно взаємодіє з АСТ і збройними силами союзників, спільно розробляючи наступні покоління сервісів моделювання для навчання та досліджень [10, 11].

3. *Об'єднаний центр ведення бойових дій* (Joint Warfare Centre, JWC) – підпорядкований Союзному командуванню операцій НАТО (Allied Command Operations, ACO), на операційному рівні центр виконує роль моста між командуваннями трансформації (АСТ) і операцій (ACO) та відповідає за організацію командно-штабних навчань оперативного та стратегічного рівня з використанням розподіленої імітації. JWC має потужні обчислювальні та імітаційні інфраструктури, включно із мобільними ситуаційними центрами, системами управління сценаріями та мережевими тренажерами.

У звіті JWC відзначається, що центр активно застосовує "інноваційні методики навчань та передові технології імітації" для підвищення готовності й сумісності сил НАТО [12]. Командування JWC повідомляє про впровадження нових, дуже реалістичних середовищ (наприклад, 360-градусне відеоформування) та відкриття окремого відділу військових ігор для розроблення сценаріїв, що імітують реальні або ймовірні у майбутньому бойові умови. Усі ці ініціативи спрямовані на підготовку "наступного покоління сил НАТО" через складні вправи, які відтворюють реальні конфліктні ситуації [12].

4. *Об'єднаний центр підготовки сил* (Joint Force Training Centre, JFTC) – спеціалізується на підготовці сил для спільних (мультинаціональних) операцій на тактичному та оперативному рівнях. Центр проводить навчання, тренування радників і забезпечує підтримку командирів під час підготовки до місій. Для своїх заходів JFTC використовує вправи з комп'ютерною підтримкою (Computer Assisted Exercise, CAX) та інтегровані тренажери-імітатори, поєднуючи сухопутні, повітряні й кібернетичні компоненти. Згідно з інформацією з відкритих джерел, JFTC має сертифікованих інструкторів та власну навчальну мережу [12].

5. *Група моделювання та імітації НАТО* (NATO Modelling and Simulation Group, NMSG), яка входить до Організації НАТО з науки та технологій (NATO Science and Technology Organization, STO) – це спеціалізована група експертів, яка координує дослідження і стандарти в сфері моделювання та імітації, до її складу входить понад 500 фахівців із союзних і партнерських країн у численних робочих групах. Вона координує виконання Генерального плану моделювання та імітації НАТО (NATO M&S Master Plan), формує технічні стандарти і проводить сертифікацію сумісності систем імітації. Група також курує дослідні проєкти, зокрема за концепціями "Моделювання та імітація як послуга" (Modelling & Simulation as a Service. M&SaaS), тактичної підготовки в урбанізованому середовищі тощо [7, 11]. Її діяльність спрямована на створення простору для співпраці експертів держав – членів НАТО, країн-партнерів і представників промисловості задля обміну знаннями та визначення стратегічних напрямів розвитку симуляцій у військовій та безпековій галузях.

Запроваджені NMSG стандарти дозволяють різним імітаційним системам і програмному забезпеченню взаємодіяти між собою без технічних бар'єрів. Уніфіковані рамкові документи NMSG пропонують розробникам чіткі орієнтири та найкращі практики. Це скорочує потребу

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

у створенні базових рішень "з нуля" та дозволяє зосередити зусилля на інноваційності й удосконаленні продуктів. Як наслідок, цикл розроблення пришвидшується, а практичні рішення виходять на ринок у коротші терміни та з вищим рівнем надійності. Це, своєю чергою, посилює ефективність навчання, підготовки та прийняття рішень у військових і безпекових структурах.

6. *Агентство з питань обслуговування систем інформації та зв'язку НАТО* (англ. NATO Communications and Information Agency, NCIA), основна роль цієї структури – підтримка мереж і систем командування, вона також створює інфраструктуру для розподілених тренувань. Наприклад, NCIA координує спільні мережі (Federated Mission Networking), що підключають навчальні центри союзників, та розробляє програмні засоби для візуалізації даних під час навчальних ігор.

Під егідою цих інституційних органів у сфері M&S впроваджується багато ініціатив, найбільш вагомими з них є:

1. *Генеральний план моделювання та імітації НАТО* (NATO M&S Master Plan) [8]. Це стратегічний документ НАТО, який визначає бачення, цілі та підхід до використання моделювання й імітації в Альянсі, до його основних завдань належать:

– формування єдиної політики НАТО у сфері моделювання та імітації;

– визначення стандартів для забезпечення сумісності систем держав-членів;

– узгодження використання імітаційних технологій у навчанні, плануванні операцій, дослідженнях і розвитку озброєнь;

– оптимізація витрат завдяки спільному використанню рішень у сфері M&S;

– підтримка взаємосумісності сил НАТО.

2. *Ініціатива "Next Generation of Modelling & Simulation"* (NexGen M&S), яка спрямована на створення сталого середовища "імітації як послуги" (MSaaS) – єдиного модульного синтетичного простору з розподіленими можливостями планування, аналізу, розіграшу бойових дій (wargaming) і навчання на стратегічному та операційному рівнях. Інструменти та середовища M&S надаються користувачам (командуванням, навчальним центрам, дослідникам) як сервіс через мережеві або хмарні платформи без необхідності локальної інсталяції чи обслуговування складних систем. Командування трансформації також залучає до проєкту промисловість і наукові кола через Консультаційну групу промисловців НАТО (NATO Industry Advisory Group, NIAG), у тому числі представників близько 55 компаній з 15 країн – членів НАТО [7].

Проєкт вже переходить у фазу практичної реалізації, на зустрічі міністрів оборони країн – членів НАТО (15 жовтня 2025 року) 13 учасників підписали меморандум про створення "Distributed Synthetic Training High Visibility Project" ("Високопріоритетний проєкт з розподіленої синтетичної підготовки"). Меморандум визначає організаційні рамки, технічні стандарти та мінімальні вимоги до участі у розподілених тренуваннях. Відповідно до його положень кожна держава-учасниця зобов'язана брати участь у визначеній кількості тренувальних заходів щороку, що сприяє підтриманню належного рівня взаємосумісності та готовності сил у межах єдиного синтетичного навчального простору.

Ключовою особливістю проєкту є створення постійно діючого середовища, яке спирається на існуючу інфраструктуру, персонал та стандарти, що забезпечать можливість державам-учасницям "підключатися" до мережі для проведення регулярних спільних тренувань. Для реалізації цього завдання передбачається використання вже наявних симуляційних систем. Наголошується, що одним із ключових уроків, отриманих з українського досвіду, є усвідомлення ризиків централізованого навчання. Збирання особового складу в єдиному навчальному центрі створює загрозу безпеці в умовах сучасних високоточних ударів. Натомість розподілені тренувальні центри, у яких підрозділи можуть працювати з власних баз, забезпечують значно вищу гнучкість, стійкість і безперервність

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

підготовки [36].

3. *Особливої уваги заслуговує узагальнена методологія перевірки та валідації* Generic Methodology for Verification and Validation (GM-VV), яку розроблено SISO (Simulation Interoperability Standards Organization – міжнародною неприбутковою організацією, яка займається розробленням, узгодженням та впровадженням стандартів взаємосумісності у сфері M&S) спільно з НАТО. Вона забезпечує системний підхід до перевірки та валідації M&S-засобів, орієнтований на прозорість, відтворюваність та документованість усіх дій і рішень [13, 14]. Методологія складається з трьох рівнів – технічного, проєктного та організаційного, поєднує концептуальну основу, рамкові вимоги до реалізації й налаштування. Для НАТО GM-VV є ключовим інструментом у багатонаціональних навчаннях та розподілених синтетичних середовищах, оскільки вона створює довіру до результатів моделювання (імітації) і забезпечує їхню взаємосумісність [15]. Для України впровадження цієї методології могло б вирішити проблему відсутності єдиних критеріїв оцінювання тренажерів, що нині ускладнює процес закупівель і впровадження нових систем [16]. Таким чином, GM-VV слід розглядати не лише як технічний стандарт, а й як механізм управління якістю у сфері M&S.

Ще однією важливою структурою є Об'єднаний центр аналізу та засвоєння досвіду (Joint Analysis and Lessons Learned Centre, JALLC), який підпорядковано ACT. Участь JALLC у сфері M&S має опосередкований характер, центр не створює самі імітаційні системи, але здійснює підготовку матеріалів для розроблення моделей та сценаріїв застосування імітаторів, аналізує їх використання та збирає досвід навчань і операцій. JALLC оцінює ефективність існуючих рішень, виявляє обмеження та розробляє рекомендації щодо вдосконалення процедур, стандартів і доктрин НАТО. Таким чином, центр підтримує реалізацію стратегічних планів, зокрема NATO M&S Master Plan, сприяючи сумісності та узгодженій взаємодії сил NATO без безпосередньої участі у створенні або експлуатації імітаторів.

У 2024 році НАТО започаткувало ініціативу JALLC-UKR, спрямовану на систематизацію та аналіз уроків війни росії проти України. Для цього було сформовано аналітичну групу JURLAT (Joint Ukraine and russia Lessons Analysis Team – Група аналізу уроків України та росії), яка розробляє аналітичні матеріали, розміщує їх на Порталі отриманих уроків НАТО та видає щоквартальний бюлетень із ключовими висновками. Хоча основна діяльність здійснюється в режимі обмеженого доступу, створено також несекретну версію порталу, що забезпечує відкритий доступ до аналітичних матеріалів і ресурсів для користувачів.

Зазначимо, що у 2025 році країни НАТО та Україна додатково створили Спільний центр з аналізу, підготовки та освіти JATEC (NATO-Ukraine Joint Analysis, Training and Education Centre), метою якого є розбудова спроможностей сил оборони України, аналіз досвіду російсько-української війни, розвиток освіти та підготовки, досягнення взаємосумісності між Україною і НАТО. Внесок України включає надання аналітичних матеріалів та даних з практичного досвіду бойових дій, участь у розробленні навчальних програм і сценаріїв, а також спільне проведення тренінгів та навчань із силами НАТО. Це дозволяє враховувати національний досвід у спільних навчальних і аналітичних ініціативах.

Узагальнені результати проведеного аналізу системи M&S у НАТО подано в табл. 1, яка відображає ключові рівні, структури та ініціативи, їхні функції та призначення. Такий підхід дозволяє не лише окреслити ієрархію структур та ініціатив, а й виявити їхню взаємодоповнюваність у забезпеченні сумісності, підвищенні ефективності підготовки багатонаціональних сил та інтеграції передових технологій у військову практику НАТО.

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Таблиця 1. Основні рівні, структури та ініціативи НАТО у сфері моделювання та імітації

Структури / ініціативи	Функції	Призначення
Стратегічний рівень		
NATO M&S Master Plan	Визначає цілі, напрями та стандарти розвитку моделювання та імітації у НАТО.	Служить стратегічною рамкою для інтеграції моделювання та імітації у діяльність Альянсу.
Allied Command Operations (ACO)	Планування та проведення операцій НАТО; застосування моделювання та імітації для підтримки рішень.	Забезпечення ефективності та готовності багатонаціональних сил у реальних операціях.
Allied Command Transformation (ACT)	Розвиток концепцій, доктрин і навчальних підходів; впровадження моделювання та імітації у підготовку військ.	Підтримка трансформації Альянсу до багатодоменних операцій та майбутніх сценаріїв бойових дій.
Науково-технологічний рівень		
NATO Science and Technology Organization (STO)	Координує наукові дослідження у сфері оборони.	Генерує інноваційні рішення для підвищення спроможностей НАТО.
Generic Methodology for Verification and Validation (GM-VV)	Визначає концептуальні принципи; надає архітектурні шаблони та інструменти; дозволяє адаптацію методології під конкретний проєкт або організацію.	Стандартизований підхід до перевірки та валідації моделей і симуляцій; забезпечення довіри до результатів; уніфікація вимог до M&S-засобів.
Тренувально-експериментальний і консультаційний рівень		
NATO Modelling and Simulation Group (NMSG)	Розроблення стандартів, рекомендацій і технологій у сфері моделювання та імітації.	Забезпечення сумісності систем і узгодженості підходів у країнах НАТО та партнерів.
Joint Warfare Centre (JWC)	Організація та проведення командно-штабних і комп'ютерно-підтримуваних навчань.	Тренування штабів і підрозділів на оперативному та стратегічному рівнях.
Joint Force Training Centre (JFTC)	Проведення комп'ютерно-підтримуваних навчань та тренувань радників перед розгортанням.	Забезпечення готовності військ до багатонаціональних операцій.
Joint Analysis and Lessons Learned Centre (JALLC)	Збирання, аналізування та поширення уроків з операцій і навчань.	Формування бази знань для удосконалення діяльності Альянсу.
NATO Modelling & Simulation Centre of Excellence (M&S COE)	Освітня та консультативна підтримка; розроблення методологій M&S; проведення курсів.	Сприяння інтеграції M&S у навчальні програми та розвиток експертного потенціалу НАТО.
CA²X² Forum	Платформа для обміну досвідом між військовими, науковими установами та промисловістю.	Розвиток партнерства і пошук інноваційних рішень у сфері M&S.
Інноваційно-технологічний рівень		
Next Generation M&S (NexGen M&S)	Створення інтегрованого багатодоменного синтетичного середовища.	Підвищення реалістичності й масштабності навчань та експериментів.
M&S as a Service (M&SaaS)	Надання імітаційних інструментів через хмарні сервіси.	Забезпечення доступності, масштабованості та економічності використання M&S.

Технічний аспект підходу НАТО полягає в уніфікації стандартів і створенні єдиних тренувальних середовищ. Усі організації дотримуються Генерального плану моделювання та імітації НАТО (NATO M&S Master Plan), який затверджується Північноатлантичною радою, та регламентує обмін даними за загальними протоколами (наприклад, High Level Architecture

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

(HLA) і Distributed Interactive Simulation (DIS)). Новітня концепція – розподілена платформа "імітація як послуга" (MSaaS) передбачає збереження усіх моделей і даних в єдиному синтетичному середовищі з хмарним доступом [7]. Такий підхід дозволяє ефективно поєднувати тренування в різних доменах (сухопутному, повітряному, кіберпросторі) і знижує витрати на підготовку.

Приклади конкретних технічних розробок включають проєкт "Електромагнітний шар" для багатодоменних операцій, у рамках якого створюється віртуальне середовище для відображення електромагнітних ефектів (інфрачервоне / радіовипромінювання) за бойових умов [17]. Це дає змогу навчати персонал оперативно змінювати режими роботи засобів радіоелектронної боротьби та радіолокаційного виявлення, оцінювати їхню ефективність в умовах, що моделюють реальні бойові сценарії. Проводяться експерименти з системами доповненої реальності, розподіленими віртуальними майданчиками та алгоритмами штучного інтелекту для створення різних сценаріїв M&S [18, 19]. Усі ці рішення спрямовано на підвищення достовірності тренувань, зменшення витрат ресурсів і пришвидшення циклів підготовки.

НАТО забезпечує інтеграцію зусиль між згаданими організаціями через спільні програми та стандарти. ACT і M&S CoE регулярно координують напрями роботи, зокрема, керівник центру M&S CoE відзначає тісну роботу з ACT під час розроблення заходів ініціативи "NextGen M&S".

Центр M&S CoE також об'єднує експертні спільноти, його ініціативи забезпечують взаємодію військових, науковців і промисловців на конференціях (що сприяє обміну ідеями та кращими практиками). ACT, зі свого боку, залучає промисловість через NIAG для визначення технічних потреб і тенденцій у сфері M&S [7].

Співпраця прослідковується і на рівні виконання. Наприклад, відзначається, що JWC працює у тісній взаємодії з ACT і ACO для розроблення вправ, які відповідають новим стратегічним пріоритетам НАТО [4]. Усі штаби використовують єдину модель сил НАТО і мережеві ресурси, що підтримуються NCIA, для проведення спільних командно-штабних навчань. Крім того, Дорадча група NMSG на регулярних семінарах і робочих зустрічах створює можливості для обміну інформацією між організаціями та союзниками, забезпечуючи єдність підходів та сумісність імітаційних засобів.

Таким чином, розвиток моделювання та імітації у НАТО забезпечується взаємодією стратегічного планування (NATO M&S Master Plan), науково-дослідної діяльності (STO/NMSG), практичної реалізації (JWC, JFTC, JALLC) та інтеграційних платформ (CA²X² Forum). Ці ініціативи створюють цілісну систему, що дозволяє ефективно проводити підготовку військ до багатодоменних операцій та майбутніх викликів.

У ЗС України розвиток моделювання та імітації до 2022 року відбувався поступово, переважно за підтримки країн – партнерів НАТО, із запозиченням західних підходів до підготовки військ. Перші практичні впровадження імітаційного моделювання в навчання військ розпочалися наприкінці 2000-х років. Зокрема, за підтримки уряду США, в Національному університеті оборони України було встановлено систему JCATS (Joint Conflict and Tactical Simulation), що започаткувало проведення комп'ютерних командно-штабних навчань [28]. Станом на 2019 рік у ЗС України вже функціонували близько 15 центрів імітаційного моделювання у різних видах військ та навчальних установах [29]. Це надало спроможності проводити як тактичні тренування підрозділів, так і командно-штабні (в тому числі міжвидові) навчання від рівня взводу / роти до бригади і вище, у єдиному віртуальному середовищі. Окрім системи JCATS, активно використовуються американська система VBS3 (Virtual Battlespace 3) для віртуального тактичного бою, а також лазерні засоби типу MILES (Multiple Integrated Laser Engagement System) для імітації бойових дій на місцевості. Причому система MILES може об'єднуватися з JCATS – дії підрозділів на полігоні відображаються на

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

екранах штабів у реальному часі [29].

Чинною основою для впровадження систем моделювання та імітації в ЗС України є відомчі документи, зокрема “Концепція розвитку навчальної матеріально-технічної бази Збройних Сил України“, “Концепція розвитку тренажерної бази Збройних Сил України”, “Основні напрямки впровадження навчального програмного забезпечення в підготовку Збройних Сил України”. Вони визначають основні напрями розвитку навчальної матеріально-технічної бази, тренажерів та навчального програмного забезпечення, встановлюють єдині вимоги до тренажерної бази, систематизують використання відповідних засобів у процесі навчання та сприяють взаємній координації розробок різних установ [5, 20]. Але ці концепції не були реалізовані в повному обсязі, переважно через обмежене фінансування, крім того, у процесі їх виконання та формування загальних вимог до навчально-тренувальних засобів недостатньо уваги приділялося специфічним вимогам до тренажерних систем, зокрема аспектам їхньої стандартизації, взаємосумісності та можливості інтеграції в єдине інформаційно-моделювальне середовище [5].

Після початку широкомасштабної війни 2022 року значення систем M&S для ЗС України зросло кардинально. Швидка трансформація збройних сил, переозброєння на західні зразки, розгортання нових бригад потребувало масованої підготовки особового складу в стислі терміни. За таких умов використання імітаторів стало не розкішшю, а необхідністю. Так, за даними Головного управління забезпечення супроводження життєвого циклу озброєння та військової техніки, у 2024 році було кодифіковано та допущено до експлуатації **13 зразків тренажерних засобів вітчизняного виробництва**, тоді як у 2022 – 2023 роках лише один.

Як відповідь на попит, на ринок вийшли як давні виробники, так і нові вітчизняні компанії з виробництва тренувального обладнання. Наприклад, українська компанія Logics7 створила віртуальний тренажер, який повністю імітує роботу мобільних систем ППО і дозволяє відпрацьовувати складні сценарії на кшталт перехоплення крилатих ракет [30]. За даними компанії, її виторг у 2023 році зріс у 10 разів порівняно з довоєнним. Продукція конструкторського бюро “Логіка”, яке спеціалізується на розробленні імітаторів і тренажерів, активно використовується для підготовки мобільних вогневих груп [31]. Окремо слід відзначити приклад української компанії “Skiftech”, яка у 2025 році отримала контракт (у рамках 10-річної програми на 921 млн дол.) від Армії США на розроблення і сервіс своїх лазерних тренажерних систем. Це перший успішний контракт українського підприємства у сфері оборонних технологій зі збройними силами США. Системи Skiftech отримали статус Brave-1 і вже використовуються у навчальних центрах ЗС України, НГУ, ДПСУ та ССО [32].

Паралельно з внутрішніми зусиллями Україна почала отримувати масштабну допомогу від партнерів у сфері підготовки військ. Країни – партнери НАТО розгорнули програми навчання українських солдатів і екіпажів на своїй території, де також широко застосовуються сучасні імітаційні технології. Показовим є приклад навчання українських танкових екіпажів на Leopard 2. У 2023 році в Польщі було проведено 30-денний курс, який поєднував заняття на віртуальних тренажерах з практикою водіння і стрільби на реальних танках [33].

Важливим зразком вітчизняної розробки є створений у Харківському національному університеті Повітряних Сил програмно-математичний комплекс “Віраж-РД”, який є прикладом інтегрованого тренажно-імітаційного синтетичного середовища, призначеного для моделювання оперативно-тактичних дій у повітряному просторі. Система забезпечує імітацію, оброблення та візуалізацію геопросторових і тактичних даних у режимі реального часу, підтримуючи сценарне моделювання з урахуванням тактико-технічних характеристик засобів повітряного нападу, вогневих засобів ППО, радіолокаційних станцій, топографії та логістичних обмежень. Основна методологія застосування “Віраж-РД” передбачає його використання як інструмента дослідницького й прикладного характеру. Шляхом моделювання різних варіантів ведення бойових дій система дозволяє провести порівняльне оцінювання

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

ефективності рішень, оптимізувати розподіл сил і засобів, а також формалізовано обґрунтувати вибір найкращих тактичних сценаріїв.

Варто зазначити, що на національному рівні "Віраж-РД" інтегрований у загальний інформаційний простір підготовки Повітряних Сил. Він використовується сумісно з геоінформаційною системою "Аргумент" (для роботи з цифровими картами, розрахунку оптимальних позицій тощо) та автоматизованою системою збирання й відображення даних про повітряну обстановку "Віраж-Планшет", що забезпечує оброблення та передачу радіолокаційної інформації між підрозділами ППО [34, 35].

Фактично, протягом останнього десятиліття в Україні сформувалася власна школа моделювання та імітації, яка пройшла шлях від локальних навчально-тренувальних розробок до створення інтегрованих середовищ підготовки. Військове керівництво ЗС України, науковці та виробники усвідомлювали та наголошували на необхідності розвитку сучасної тренажерної бази ЗС України. Напередодні широкомасштабної війни було здійснено низку практичних кроків і сформульовано пропозиції щодо прискорення впровадження технологій моделювання та імітації у систему бойової підготовки. Хоча до 2022 року ці ініціативи перебували переважно на стадії концептуальної реалізації, загальна тенденція була очевидною. Фахова українська спільнота усвідомлювала відставання від стандартів НАТО у сфері M&S і поступово розпочала процес його подолання. Отримані результати свідчать, що сформована науково-практична база і накопичений досвід у сфері M&S створюють підґрунтя для подальшої інтеграції українських систем моделювання до європейського та натівського освітньо-тренувального простору.

Аналіз розвитку вітчизняних тренажерних технологій показує, що реалізація більшості проєктів стримувалася низкою об'єктивних чинників. Головними з них були недостатнє фінансування, застаріла матеріально-технічна база, відсутність координаційного центру, який би узгоджував діяльність розробників і користувачів тренажерних систем, а також відсутність єдиних технічних стандартів, узгоджених із вимогами НАТО. Через розпорошення наукових зусиль і дефіцит підготовлених фахівців частина ініціатив не перейшла зі стадії наукових розробок у практичне застосування. Проте закладений теоретичний фундамент дозволив після 2022 року швидко адаптувати вже наявні напрацювання до нових умов підготовки військ, коли технології M&S стали одним із ефективних інструментів навчання.

Подальший розвиток систем M&S в Україні слід орієнтувати на врахування передового досвіду НАТО, де ці системи розглядаються як невід'ємний компонент багатодоменних операцій та колективної підготовки військ. Такі сучасні підходи передбачають, що системи M&S мають не лише забезпечувати якісну підготовку особового складу, а й слугувати аналітичним інструментом для оцінювання прийнятих рішень у процесі планування та ведення операцій. Вони мають відтворювати реалістичну обстановку, забезпечувати налаштування рівнів складності, враховувати часові масштаби бойових дій і мати можливість прив'язки сценаріїв до реальних координат місцевості. Це дає змогу перевіряти ефективність управлінських рішень, оцінювати взаємодію підрозділів та прогнозувати наслідки різних варіантів дій у контрольованому середовищі.

Упровадження автоматизованих процедур збирання, фіксації та аналізу результатів тренувань підвищує об'єктивність оцінювання та створює умови для реалізації повного циклу зворотного зв'язку від навчання до аналітичного опрацювання рішень і подальшого оновлення навчальних сценаріїв. Такий підхід перетворює моделювання на універсальний інструмент підтримки рішень, який поєднує функції підготовки, експериментування й дослідження ефективності бойових дій.

Обговорення (Discussions)

За результатами дослідження виявлено, що ефективність систем M&S визначається

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

рівнем їхньої інтеграції до єдиної методологічної та технічної бази. Аналіз показує, що підходи НАТО до розбудови синтетичних середовищ ґрунтуються на стандартизації, уніфікації протоколів взаємодії та централізованому управлінні розвитком відповідної інфраструктури. У вітчизняній практиці спостерігається поступовий перехід від ізольованих ініціатив до системного підходу, однак залишаються організаційні та методологічні обмеження, зокрема відсутність єдиних критеріїв оцінювання засобів M&S і координаційного центру розробок.

У системі НАТО M&S-системи розглядаються як складова багатодоменних операцій і процесу управління знаннями. Основні принципи їхньої побудови враховуються ще на етапі створення (взаємосумісність, модульність та інтеграція із C4ISR-системами) та забезпечують можливість застосування моделей на стратегічному, оперативному та тактичному рівнях.

Під управлінням знаннями у контексті систем M&S розуміють організований процес накопичення, узагальнення й повторного використання інформації, отриманої в ході навчальних, аналітичних та імітаційних процесів, з метою підвищення ефективності підготовки військ і прийняття рішень. У цьому контексті M&S є інструментом накопичення організаційного досвіду та побудови баз знань для оперативного планування.

Українські системи, попри наявність позитивних прикладів (зокрема програмно-математичний комплекс “Віраж-РД”), характеризуються обмеженою стандартизацією та фрагментарністю інформаційних потоків. Відсутність спільної нормативної бази ускладнює впровадження єдиних підходів до створення та оцінювання якості розроблених продуктів.

Удосконалення національної системи підготовки потребує впровадження єдиної методологічної основи для розроблення, перевірки та валідації засобів M&S. Методологія GM-VV може бути використана як базова для створення національних стандартизованих процедур перевірки достовірності моделей, визначення вимог до документації та критеріїв сумісності. Її адаптація до українських умов сприятиме підвищенню рівня довіри до результатів моделювання і створенню передумов для взаємодії з тренувальними середовищами держав – членів НАТО.

У вітчизняній практиці досить поширеними є терміни “навчальна матеріально-технічна” та “тренажерна” база, що підкреслює навчальне призначення систем. Водночас переважно таке розуміння занижує сприйняття повного функціоналу засобів M&S. Системи моделювання й імітації мають не лише навчальне, а й аналітично-дослідницьке призначення – вони здатні відтворювати складні сценарії, проводити експерименти з варіантами застосування сил і засобів, оцінювати тактико-технічні рішення та формувати кількісні оцінки ефективності. Недостатня увага до цієї ролі обмежує можливості застосування засобів M&S як інструмента підтримки прийняття рішень і наукового дослідження операцій. Усвідомлення і формалізація аналітично-дослідницької функції синтетичних середовищ сприятиме більш ефективному використанню наявних ресурсів і прискоренню розроблення тактичних та оперативних рішень.

Узагальнені результати зіставлення підходів до розроблення, використання та оцінювання засобів M&S у ЗС України та в НАТО наведено у табл. 2.

Таким чином, у вітчизняному підході навчально-тренажерні системи ЗС України розглядаються переважно як інструмент бойової підготовки та навчання. Натомість системи **M&S** у НАТО відіграють роль цілісної системи знань і технологій, що охоплює весь життєвий цикл оборонних рішень від наукових досліджень і розробок до операційного аналізу та підготовки військ.

Розвиток національного сегмента виробництва засобів M&S вимагає поєднання наукового потенціалу університетів із можливостями промислових підприємств. Приклади вітчизняних компаній, які впроваджують власні рішення у сфері віртуальних тренажерів, свідчать про формування бази для технологічного зростання. Доцільним є створення постійно

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

діючого координаційного органу, відповідального за узгодження вимог, сертифікацію систем і узгодження технічних інтерфейсів з міжнародними стандартами.

Таблиця 2. Порівняння ролі систем моделювання й імітації у процесі підготовки та прийняття рішень у ЗС України та НАТО

Критерій	Навчально-тренажерні системи у ЗС України	Modelling and Simulation (M&S) у НАТО
1. Основне призначення	Підготовка особового складу, відпрацювання навичок роботи на конкретних робочих місцях, зразках озброєння чи техніки	Підтримка всього циклу військової діяльності: навчання, аналіз операцій, дослідження, планування, прийняття рішень
2. Рівень інтеграції	Зазвичай автономні системи, орієнтовані на окремі види або роди військ	Інтегровані багаторівневі середовища з об'єднанням різних симуляцій у спільну федерацію
3. Методологічна основа	Переважає практичне тренування; методика спирається на навчальні програми та досвід бойової підготовки	Ґрунтується на єдиній інтегрованій системі M&S (NATO M&S Master Plan) та стандартах SISO, IEEE (HLA, DIS, GM-VV)
4. Типи моделей	Переважно натурні або напівнатурні тренажери (апаратні комплекси з візуалізацією)	Концептуальні, математичні, алгоритмічні та віртуальні моделі, які можуть представляти цілі системи бойових дій, логістики чи управління
5. Мета використання	Формування індивідуальних та колективних навичок управління озброєнням і технікою	Аналіз ефективності систем, відпрацювання сценаріїв операцій, оцінювання ризиків, підтримка рішень командування
6. Організаційний рівень	Переважно тактичний (бойова обслуга, екіпаж, підрозділ, батарея, частина).	Тактичний, оперативний і стратегічний рівні в єдиній архітектурі (наприклад, MSaaS)
7. Технологічна архітектура	Локальні комп'ютерно-тренажерні комплекси, часто без взаємодії з іншими системами	Відкрита, модульна, сумісна за стандартами HLA/FOM, що дозволяє створювати федерації симуляцій (Federated Mission Networking)
8. Управління достовірністю	Оцінка здебільшого емпірична, через результати тренування або експертну перевірку	Використовується формалізована методологія GM-VV для доведення достовірності моделей
9. Рівень автоматизації та інтелектуалізації	Обмежений, сценарії часто задаються вручну	Використовуються когнітивні агенти, автоматичне генерування сценаріїв, адаптивне моделювання
10. Кінцевий результат	Зростання індивідуальної й колективної підготовки персоналу	Підвищення ефективності управління операціями, планування сил і засобів, інтеграція досвіду в цикл навчання та аналізу

Упровадження концепції MSaaS створює умови для розподіленого доступу до тренувальних ресурсів та їх інтеграції у хмарні інфраструктури. Такі рішення можуть забезпечити спільне використання середовищ моделювання, зокрема у системі підготовки Повітряних Сил. До перспективних напрямів розвитку належать використання технологій доповненої реальності, автоматизованих систем оцінювання результатів тренувань та алгоритмів штучного інтелекту для формування адаптивних сценаріїв навчання.

На підставі проведеного аналізу розвитку систем M&S у державах – членах НАТО та оцінки поточного стану їх застосування у ЗС України доцільно запропонувати поетапну систему практичних заходів, спрямованих на формування цілісної національної моделі розвитку M&S-середовища. Заходи структуровано за часовими термінами впровадження – короткостроковим, середньостроковим і довгостроковим.

Короткострокова перспектива (1–2 роки).

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

1) Уніфікація термінології та підходів. Необхідно забезпечити імплементацію єдиної термінологічної бази та класифікації систем M&S НАТО у нормативно-методичних документах ЗС України. Це дозволить досягти єдності розуміння ключових понять, забезпечити узгодженість дій підрозділів та спільність науково-технічного підґрунтя під час створення тренажерно-імітаційних систем.

2) Початкова адаптація стандартів НАТО. Доцільно розпочати поетапне впровадження елементів методології GM-VV для перевірки та валідації наявних тренажерних систем, а також базових архітектурних принципів HLA під час розроблення нових комплексів.

3) Розвиток співпраці з міжнародними структурами. Слід налагодити постійну комунікацію з профільними інституціями НАТО, зокрема ACT, M&S CoE, NMSG та JALLC. Таке співробітництво сприятиме обміну досвідом, спільним семінарам і формуванню навчальних програм для персоналу ЗС України.

4) Створення реєстру національних M&S-засобів. Доцільно провести аудит наявних українських тренажерно-імітаційних систем та створити відкритий каталог (реєстр) для координації розробок, інтеграції нових рішень і запобігання дублюванню зусиль у різних установах та підрозділах.

Середньострокова перспектива (3–5 років).

1) Формування національної концепції розвитку M&S. Необхідно розробити офіційний концептуальний документ, який визначатиме стратегічні цілі, пріоритети, відповідальних виконавців і механізми фінансування розвитку систем моделювання та імітації в Україні. Така концепція має стати підґрунтям для доктринальних і освітніх рішень.

2) Інституціоналізація управління знаннями. Варто створити єдину систему збереження, аналізу та передачі досвіду на основі результатів моделювання, навчань і бойових дій. Центральна база даних сценаріїв, моделей і аналітичних звітів стане основою для розвитку спільного навчального простору та формування доказової бази під час прийняття рішень.

3) Підготовка кадрів і розвиток компетенцій. Рекомендується запровадити навчальні курси у програми військових навчальних закладів за напрямами моделювання та імітації, управління знаннями, аналізу операцій і дослідницьких експериментів. Це забезпечить підготовку фахівців, здатних підтримувати та розвивати національні M&S-платформи.

4) Пілотне впровадження MSaaS. Доцільно розпочати створення хмарної інфраструктури MSaaS, яка надаватиме розподілений доступ до симуляційних ресурсів для навчальних центрів, дослідницьких лабораторій і підрозділів бойової підготовки.

Довгострокова перспектива (понад 5 років).

1) Створення національної інфраструктури M&S. На базі принципів MSaaS необхідно побудувати інтегровану архітектуру M&S-середовища з можливістю взаємодії з аналогічними структурами НАТО та країн-партнерів. Така система стане технологічним каркасом для майбутньої об’єднаної навчально-дослідної мережі оборонного сектору.

2) Заснування координаційного центру M&S. Пропонується створити міжвідомчий центр, відповідальний за координацію наукових, освітніх і промислових ініціатив у сфері моделювання та імітації, а також за стандартизацію, сертифікацію і міжнародну співпрацю. Центр має виконувати функції національного осередку M&S-експертизи.

3) Інтеграція нових технологій. Варто забезпечити системне впровадження технологій доповненої та віртуальної реальності (VR/AR), штучного інтелекту, когнітивного моделювання та автоматизованої аналітики. Це підвищить реалістичність і адаптивність навчальних процесів та ефективність дослідницьких експериментів.

4) Міжнародна участь і обмін досвідом. Необхідно забезпечити участь українських науковців і військових фахівців у спільних дослідженнях та публікаціях у рамках програм NATO STO, SISO, NMSG, що сприятиме інтеграції України до міжнародного наукового простору M&S і підвищить довіру до національних розробок.

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Послідовна реалізація запропонованих рекомендацій дозволить створити в Україні цілісну систему моделювання та імітації, яка відповідатиме принципам НАТО, забезпечить уніфікацію підходів, розвиток кадрового потенціалу і технологічну сумісність національних рішень у межах євроатлантичного оборонного простору.

Висновок (Conclusion)

Таким чином, системи моделювання та імітації (M&S) є ключовим інструментом підтримки бойової підготовки, планування операцій і управління знаннями у сучасних збройних силах. Аналіз показав, що у структурах НАТО M&S розвивається як інтегрована система, яка поєднує навчальні, аналітичні та дослідницькі функції, спираючись на стандартизовані методології (HLA, GM-VV, MSaaS) і мережеві рішення. Цей підхід забезпечує взаємосумісність, ефективність обміну даними та підвищує достовірність симуляцій.

Українська практика свідчить про наявність значного потенціалу у сфері моделювання та імітації, проте він залишається реалізованим лише частково. Наявні системи, такі як програмно-математичний комплекс “Віраж-РД”, демонструють приклади ефективної інтеграції тренажерних і аналітичних функцій, однак на загальнодержавному рівні розвиток таких систем стримується фрагментарністю нормативної бази, відсутністю єдиних стандартів сертифікації та недостатньою координацією між розробниками, навчальними установами та органами військового управління.

Дослідження показало, що для забезпечення сумісності з підходами НАТО Україна потребує переходу від розрізнених ініціатив до побудови цілісної системи M&S, інтегрованої у процеси підготовки, аналізу та прийняття рішень. Упровадження єдиної методологічної основи на базі GM-VV, розвиток інфраструктури типу MSaaS та створення національного координаційного центру з питань M&S сприятимуть підвищенню ефективності системи підготовки та розвитку аналітичних спроможностей сил оборони України.

Рекомендації (Recommendations)

Матеріали статті можуть бути використані під час розроблення програм і рішень у сфері розвитку систем моделювання та імітації в секторі безпеки і оборони України. Результати дослідження становлять практичну цінність для органів військового управління, наукових установ і закладів військової освіти, що займаються інформатизацією процесів підготовки військ, створенням інтегрованих тренажерних комплексів та впровадженням стандартів НАТО у цій галузі.

Подальші дослідження доцільно зосередити на розробленні національної методики верифікації, валідації та акредитації тренажерних систем за моделлю GM-VV, а також на створенні інтегрованих імітаційних середовищ для підвищення ефективності навчання та управлінських рішень.

Конфлікт інтересів (Conflict of Interest)

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

Використані джерела

1. Сирський, О., Лебеденко, А., & Семененко, О. (2025). Україна в умовах “повзучої війни”: зміна парадигми ведення воєнних дій. *Military Science, 3* (2), 6–19. https://doi.org/10.62524/msj.2025.3.2.1.
2. Center for Strategic and International Studies. (2025, May 2). *Lessons from the Ukraine conflict: Modern warfare in the age of autonomy, information, and resilience*. CSIS. https://www.csis.org/analysis/lessons-ukraine-conflict-modern-warfare-age-autonomy-information-and-resilience.

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

3. Гризо, А., Костиря, О., & Трофимов, І. (2025). Російсько-українська війна як каталізатор змін у європейській системі ППО-ПРО: від американської підтримки до стратегічної автономії. *Military Science, 3* (2), 56–77. https://doi.org/10.62524/msj.2025.3.2.5/.
4. Трофимов, І., Худов, Г., Білецький, С., Гризо, А., & Гладіщук, О. (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.
5. Турінський, О. В., Головняк, Д. В., Маліновська, І. Л., & Нос, І. А. (2024). Аналіз стану тренажерної бази Збройних Сил України. *Системи озброєння і військова техніка, 4* (76), 16–21. https://doi.org/10.30748/soivt.2023.76.02.
6. Рудковський, О. М., Баліцький, Н. М., Ванкевич, П. І., Юркевич, Р. М., & Іванік, Є. Г. (2020). Технічні засоби навчання і підготовки військ. Огляд технологій. *Зб. наук. пр. Військової академії (м. Одеса), 2* (14), 214–223. https://doi.org/10.37129/2313-7509.2020.14.2.214-223/.
7. NATO Allied Command Transformation. (2023). *NexGen Modelling and Simulation*. NATO ACT. https://www.act.nato.int/article/nexgen-modelling-and-simulation/.
8. NATO Science and Technology Organization (2012). *NATO Modelling & Simulation Master Plan Version 2.0*. https://www.sto.nato.int/wp-content/uploads/nato-ms-master-plan-web.pdf.
9. NATO Allied Command Transformation. (2023). *NATO Centres of Excellence – Modelling and Simulation*. https://www.act.nato.int/article/nato-centres-of-excellence-modelling-and-simulation/.
10. NATO Allied Command Transformation. (2024*). Advancing NATO's Capabilities Through its Modelling & Simulation Centre of Excellence.* https://www.act.nato.int/article/ms-coe-2024/.
11. NATO Modelling & Simulation Group. (2024). *NMSG overview and challenges* [Briefing paper]. SISO. https://cdn.ymaws.com/www.sisostandards.org/resource/collection/DC589D90-B442-43B4-920E-3A39A227F20D/20240226_NMSG_Overview_and_Challenges_BP_v1.pdf.
12. NATO Joint Force Training Centre. (n.d.). *Mission*. NATO JFTC. https://www.jftc.nato.int/our-work/mission/.
13. NATO Modelling & Simulation Group (NMSG). (2014). *Generic Methodology for Verification and Validation (GM-VV). Vol. 1: Introduction and Overview*. STO-TR-MSG-073-Vol.1. NATO Science and Technology Organization.
14. NATO Modelling & Simulation Group (NMSG). (2015). *Generic Methodology for Verification and Validation (GM-VV). Vol. 2: Implementation Guide*. STO-TR-MSG-073-Vol.2. NATO Science and Technology Organization.
15. NATO Science and Technology Organization. (2024). *Book of Abstracts, Collaborative Programme of Work 2024*.
16. Болкот, П. А., Ванкевич, П. І., & Стратійчук, І. О. (2025). Методологічні принципи оцінювання тренажерних засобів вітчизняних та закордонних розробників. *Збірник наукових праць Національної академії Національної гвардії України, 1* (45), 35–46. https://doi.org/10.33405/2409-7470/2025/1/45/339266.
17. Ventura, P., & De Mattia, S. (2023, Dec. 18). *ELMo – Electromagnetic Layer for Multi-Domain Operations: Developing and testing activities*. NATO Modelling and Simulation Centre of Excellence. https://www.mscoe.org/document/elmo-electromagnetic-layer-for-multi-domain-operations-developing-and-testing-activities/.
18. Naval Technology. (2025, Febr. 12). *DSET 2025: NATO disclose priorities in modelling and simulation*. https://www.naval-technology.com/news/dset-2025-nato-disclose-priorities-in-modelling-and-simulation/.

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

19. NATO Science and Technology Organization. (2023). *AI-augmented immersive simulation in training and DM course of actions analysis (MSG-189 Final Report)*. https://www.sto.nato.int/document/ai-augmented-immersive-simulation-in-training-and-dm-course-of-actions-analysis-2/.
20. Лук'янчук, В. В., Ніколаєв, І. М., Долина, М. П., Донцов, С. М., & Трофименко, Ю. В. (2025). Системно-концептуальні аспекти створення і використання системи навчально-тренажерних засобів для підготовки бойових обслуг зенітних ракетних комплексів (систем). *Наука і техніка Повітряних Сил Збройних Сил України*, *2* (59), 51–58. https://doi.org/10.30748/nitps.2025.59.06.
21. Мельник, Я. В., Кравчук, А. А., Єфімова, Р. Г., & Бобильов, В. Є. (2018). Пропозиції щодо концепції створення тренажерної бази для забезпечення заходів бойової та оперативної підготовки у Збройних Силах України. *Сучасні інформаційні технології у сфері безпеки та оборони, 1* (31), 5–12. https://doi.org/10.33099/2311-7249/2018-31-1-68-72.
22. Simulation Interoperability Standards Organization (SISO). (2006). *Simulation Conceptual Modeling (SCM) Study Group Final Report*. SISO-REF-017-2006.
23. Simulation Interoperability Standards Organization (SISO). (2024). *Final Report for the Electronic Warfare Data Exchange Model (DEM) Study Group*.
24. Заїка, Л. А., Лаврінчук, О. В., & Крайнов, В. О. (2021). Використання можливостей засобів імітаційного моделювання бойових дій у ході практичної підготовки органів військового управління. *Сучасні інформаційні технології у сфері безпеки та оборони*, *3* (42), 89–96. https://doi.org/10.33099/2311-7249/2021-42-3-89-96.
25. Маняков, І. В., & Томків, І. О. (2025). Особливості підготовки командно-штабних навчань із застосуванням системи імітаційного моделювання JCATS в Державній прикордонній службі України. *Національні інтереси України*, *2* (7), 289–299. https://doi.org/10.52058/3041-1793-2025-2(7)-289-299.
26. Popov, O. O., Iatsyshyn, A. V., Iatsyshyn, A. V., et al. (2021). *Immersive technology for training and professional development of nuclear power plants personnel. CEUR Workshop Proceedings, 2898 (1),* 230–254. In *AREdu 2021: 4th International Workshop on Augmented Reality in Education* (May 11, 2021, Kryvyi Rih, Ukraine). http://elibrary.kdpu.edu.ua/bitstream/123456789/4631/1/paper13.pdf.
27. Головань, В. Г., Головань, А. В., Дроздов, М. О., & Нікул, С. О. (2021). Застосування технологій 3D моделювання в підготовці військових фахівців. *Освітні інноваційні технології, 1*, 279–285. https://doi.org/10.18372/2786-5487.1.20276.
28. Укрінформ. (2017, 28 лист.). *Віртуальний вишкіл: військових ЗСУ вчитимуть на симуляторах JCATS*. https://www.ukrinform.ua/rubric-technology/2347114-virtualnij-viskil-vijskovih-zsu-vcitimut-na-simulatorah-jcats.html.
29. АрміяInform. (2019, 11 вер.). *Для навчання військовослужбовців створено вже 15 центрів імітаційного моделювання*. https://armyinform.com.ua/2019/09/11/dlya-navchannya-vijskovosluzhbovcziv-stvoreno-vzhe-15-czentriv-imitaczijnogo-modelyuvannya/.
30. Espreso Global. (2025, 18 лют.). *Як українські тренажери допомагають військовим опанувати нову зброю* [How Ukrainian simulators help troops master new weapons]. Espreso Global. https://global.espreso.tv/russia-ukraine-war-how-ukrainian-simulators-help-troops-master-new-weapons-economichna-pravda.
31. Focus.ua. (2025, 7 жовт.). *Бійців ЗСУ мобільних груп ППО навчають на симуляторах ДШКМ (відео)*. https://focus.ua/uk/voennye-novosti/699229-biyciv-zsu-mobilnih-grup-ppo-navchayut-na-simulyatorah-dshkm-video.
32. AIN.UA. (2025, 13 бер.). *Українська miltech-компанія Skiftech виграла контракт армії США на розробку симулятора*. https://ain.ua/2025/03/13/skiftech-vigrala-kontrakt-armiyi-

ssa-na-rozrobku/.
33. DVIDS. (2023, Febr. 13). *NATO allies train Ukrainian soldiers on Leopard tanks in Poland [Video]*. https://www.dvidshub.net/video/879491/nato-allies-train-ukrainian-soldiers-leopard-tanks-poland-b-roll.
34. Єрмошин, М. О., Кулєшов О. В., Меленті, Д. О., & Шурига М. П. (2022). Моделювання противоповітряного бою зенітного ракетного підрозділу із застосуванням геоінфомаційних систем. *Системи обробки інформації, 2* (169), 42–48. https://doi.org/10.30748/soi.2022.169.05.
35. Центр оперативних стандартів і методики підготовки Збройних Сил України; Командування Повітряних Сил Збройних Сил України. (2019). *ВП 7-09 (12).02: Методичні рекомендації використання спеціалізованого програмного забезпечення "Віраж-Планшет" під час підготовки бойових обслуг підрозділів зенітних ракетних військ Повітряних Сил Збройних Сил України* [Військова навчально-методична публікація]. Затверджено Командувачем Повітряних Сил ЗС України 02 серпня 2019 р. Отримано з https://www.hups.mil.gov.ua/assets/uploads/library/nadhodzhennya/lypen-veresen-2020/pdf/30.pdf.
36. Супрун, К. (2025, 24 жовт.). *Як гра онлайн: НАТО запускає свій віртуальний полігон*. Militarnyi. https://militarnyi.com/uk/articles/yak-merezheva-gra-nato-zapuskaye-svij-virtualnyj-poligon/.

References

1. Syrskyi, O., Lebedenko, A., & Semenenko, O. (2025). Ukraine in a "War of Attrition": The Warfare Paradigm Shift. *Military Science, 3* (2), 6–19. https://doi.org/10.62524/msj.2025.3.2.1.
2. Center for Strategic and International Studies. (2025, May 2). Lessons from the Ukraine conflict: Modern warfare in the age of autonomy, information, and resilience. https://www.csis.org/analysis/lessons-ukraine-conflict-modern-warfare-age-autonomy-information-and-resilience.
3. Hryzo, A., Kostyria, O., & Trofymov, I. (2025). russo-ukrainian war as a catalyst for changes in the european air and missile defense system: from american support to strategic autonomy. *Military Science*, *3* (2), 56–77. https://doi.org/10.62524/msj.2025.3.2.5.
4. Trofymov, I., Khudov, H., Biletskyi, S., Hryzo, A., & Hladishchuk, O. (2024). Peculiarities of the using radio engineering troops of the Air Forces of The Armed Forces of Ukraine during the russian-ukrainian war. *Science and Technology of the Air Force of Ukraine, 2* (55), 76–85. https://doi.org/10.30748/nitps.2024.55.08.
5. Turinskyi, O., Holovniak, D., Malinovska, I., & Nos, I. (2024). Analysis of the trainer base of the Armed Forces of Ukraine. *Systems of Arms and Military Equipment, 4* (76), 16–21. https://doi.org/10.30748/soivt.2023.76.02.
6. Rudkovskyi, O. M., Balitskyi, N. M., Vankevych, P. I., Yurkevych, R. M., & Ivanik, Ye. H. (2020). Technical training and education means for troops: Technology overview. *Collection of Scientific Papers of the Military Academy (Odesa), 2* (14), 214–223. https://doi.org/10.37129/2313-7509.2020.14.2.214-223.
7. NATO Allied Command Transformation. (2023). *NexGen Modelling and Simulation*. https://www.act.nato.int/article/nexgen-modelling-and-simulation/
8. NATO. (2012). *NATO Modelling & Simulation Master Plan Version 2.0*. NATO Science and Technology Organization. https://www.sto.nato.int/wp-content/uploads/nato-ms-master-plan-web.pdf.
9. NATO Allied Command Transformation. (2023). *NATO Centres of Excellence – Modelling*

and Simulation. https://www.act.nato.int/article/nato-centres-of-excellence-modelling-and-simulation/.
10. NATO Allied Command Transformation. (2024). *Advancing NATO's Capabilities Through its Modelling & Simulation Centre of Excellence*. https://www.act.nato.int/article/ms-coe-2024/.
11. NATO Modelling & Simulation Group. (2024). *NMSG overview and challenges* [Briefing paper]. SISO. https://cdn.ymaws.com/www.sisostandards.org/resource/collection/DC589D90-B442-43B4-920E-3A39A227F20D/20240226_NMSG_Overview_and_Challenges_BP_v1.pdf.
12. NATO Joint Force Training Centre. (n.d.). *Mission*. NATO JFTC. https://www.jftc.nato.int/our-work/mission/.
13. NATO Modelling & Simulation Group (NMSG). (2014). *Generic Methodology for Verification and Validation (GM-VV). Vol. 1: Introduction and Overview*. STO-TR-MSG-073-Vol.1. NATO Science and Technology Organization.
14. NATO Modelling & Simulation Group (NMSG). (2015). *Generic Methodology for Verification and Validation (GM-VV). Vol. 2: Implementation Guide*. STO-TR-MSG-073-Vol.2. NATO Science and Technology Organization.
15. NATO Science and Technology Organization. (2024). *Book of Abstracts, Collaborative Programme of Work 2024*.
16. Bolkot, P. A., Vankevych, P. I., & Stratiichuk, I. O. (2025). *Methodological principles for evaluating training devices of domestic and foreign developers. Collection of Scientific Papers of the National Academy of the National Guard of Ukraine*, *1* (45), 35–46. https://doi.org/10.33405/2409-7470/2025/1/45/339266/.
17. Ventura, P., & De Mattia, S. (2023, December 18). *ELMo – Electromagnetic Layer for Multi-Domain Operations: Developing and testing activities.* NATO Modelling and Simulation Centre of Excellence. https://www.mscoe.org/document/elmo-electromagnetic-layer-for-multi-domain-operations-developing-and-testing-activities/.
18. Naval Technology. (2025, Febr. 12). *DSET 2025: NATO disclose priorities in modelling and simulation.* https://www.naval-technology.com/news/dset-2025-nato-disclose-priorities-in-modelling-and-simulation/.
19. NATO Science and Technology Organization. (2023). *AI-augmented immersive simulation in training and DM course of actions analysis (MSG-189 Final Report).* https://www.sto.nato.int/document/ai-augmented-immersive-simulation-in-training-and-dm-course-of-actions-analysis-2/.
20. Lukianchuk, V., Nikolaev, I., Dolyna, M., Dontsov, S., & Trofimenko, Y. (2025). Systemic-conceptual aspects of creating and using a system of training and simulation tools for training combat calculations of antifine missile complexes (systems). *Science and Technology of the Air Force of Ukraine*, *2* (59), 51–58. https://doi.org/10.30748/nitps.2025.59.06.
21. Melnyk, Y. V., Kravchuk, A. A., Yefimova, R. G., & Bobylov, B. Y. (2018). Proposals on the concept of the development of a simulator base for the provision of combat and operational training in the armed forces of Ukraine. *Modern Information Technologies in the Sphere of Security and Defence*, *31* (1), 68–72. https://doi.org/10.33099/2311-7249/2018-31-1-68-72.
22. Simulation Interoperability Standards Organization (SISO). (2006). *Simulation Conceptual Modeling (SCM) Study Group Final Report*. SISO-REF-017-2006.
23. Simulation Interoperability Standards Organization (SISO). (2024). *Final Report for the Electronic Warfare Data Exchange Model (DEM) Study Group.*
24. Zaika, L., Lavrinchuk, O., & Krainov, V. (2021). Use simulation capabilities of combat actions in the training process of military administrative bodies. *Modern Information Technologies in the Sphere of Security and Defence*, *42* (3), 89–96. https://doi.org/10.33099/2311-7249/2021-

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

42-3-89-96.

25. Manyakov, I. V., & Tomkiv, I. O. (2025). Features of conducting command and staff training using the JCATS simulation system in the State *Border Guard Service of Ukraine*. National Interests of Ukraine, *2* (7), 289–299. https://doi.org/10.52058/3041-1793-2025-2(7)-289-299.
26. Popov, O. O., Iatsyshyn, A. V., Iatsyshyn, A. V., *et al.* (2021). *Immersive technology for training and professional development of nuclear power plants personnel. CEUR Workshop Proceedings, 2898* (1), 230–254. In *AREdu 2021: 4th International Workshop on Augmented Reality in Education* (May 11, 2021, Kryvyi Rih, Ukraine). http://elibrary.kdpu.edu.ua/bitstream/123456789/4631/1/paper13.pdf.
27. Golovan , V. H., Golovan , A. V., Drozdov, M. O., & Nikul , S. O. (2025). Application of 3D modeling technologies in the training of military specialists. *Actual Problems in the System of Education: General Secondary Education Institution – Pre-University Training – Higher Education Institution, 1* (5), 279–289. https://doi.org/10.18372/2786-5487.1.20276.
28. Ukrinform. (2017, November 28). *Virtual training: Ukrainian Armed Forces soldiers will be trained on JCATS simulators. Ukrinform.* https://www.ukrinform.ua/rubric-technology/2347114-virtualnij-viskil-vijskovih-zsu-vcitimut-na-simulatorah-jcats.html.
29. ArmiyaInform. (2019, Sept. 11). *Fifteen simulation training centers have already been established for the training of servicemen.* https://armyinform.com.ua/2019/09/11/dlya-navchannya-vijskovosluzhbovcziv-stvoreno-vzhe-15-czentriv-imitaczijnogo-modelyuvannya/.
30. Espreso Global. (2025, Febr. 18). *How Ukrainian simulators help troops master new weapons.* https://global.espreso.tv/russia-ukraine-war-how-ukrainian-simulators-help-troops-master-new-weapons-economichna-pravda.
31. Focus.ua. (2025, Oct. 7). *Air defense mobile group fighters of the Armed Forces of Ukraine are trained on DShKM simulators (video).* https://focus.ua/uk/voennye-novosti/699229-biyciv-zsu-mobilnih-grup-ppo-navchayut-na-simulyatorah-dshkm-video.
32. AIN.UA. (2025, March 13). *Ukrainian miltech company Skiftech won a U.S. Army contract to develop a simulator.* https://ain.ua/2025/03/13/skiftech-vigrala-kontrakt-armiyi-ssa-na-rozrobku/.
33. DVIDS. (2023, Febr. 13). *NATO allies train Ukrainian soldiers on Leopard tanks in Poland [Video]*. https://www.dvidshub.net/video/879491/nato-allies-train-ukrainian-soldiers-leopard-tanks-poland-b-roll.
34. Yermoshin, M., Kuleshov, O., Melenti, D., & Shuriga, M. (2022). Simulation of anti-air fighting of anti-aircraft missile department with the use of geoinformation systems. *Information Processing Systems*, *2* (169), 42–48. https://doi.org/10.30748/soi.2022.169.05.
35. Centre of Operational Standards and Training Methodology of the Armed Forces of Ukraine; Command of the Air Force of the Armed Forces of Ukraine. (2019). *VP 7-09 (12).02: Methodical recommendations for the use of the specialized software "Virazh-Planset" during training of combat crews of air defence missile units of the Air Force of the Armed Forces of Ukraine* [Military training-methodical publication]. Approved by the Commander of the Air Force of the AFU, August 2, 2019. https://www.hups.mil.gov.ua/assets/uploads/library/nadhodzhennya/lypen-veresen-2020/pdf/30.pdf.
36. Suprun, K. (2025, Oct. 24). *Like an online game: NATO launches its virtual training ground*. Militarnyi. https://militarnyi.com/uk/articles/yak-merezheva-gra-nato-zapuskaye-svij-virtualnyj-poligon.

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Analysis of NATO Approaches to Modelling and Simulation Systems and Prospects for Their Adaptation and Implementation in Ukraine

Andrii Hryzo
Candidate of Technical Sciences, Associate Professor
Head of the Scientific 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, Professor
Leading Research Fellow at the Scientific 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
Candidate of 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

Dmytro Nelin
Head of the Scientific Research Division
Ivan Kozhedub Kharkiv National Air Force University
61023, Sumska St. 77/79, Kharkiv, Ukraine
e-mail: nelindima35@gmail.com
ORCID: 0009-0003-9448-392X

Andrii Lukianchykov
Leading Research Fellow at the Scientific Research Division
Ivan Kozhedub Kharkiv National Air Force University
61023, Sumska St. 77/79, Kharkiv, Ukraine
e-mail: laa1968@ukr.net
ORCID: 0000-0002-3584-7901

Abstract. The relevance of the study is determined by the need to transform military training and management systems in the context of new types of threats that emerged during the Russian-Ukrainian war. The widespread use of unmanned systems, high-precision weapons, electronic warfare and cyber-attacks has highlighted the limitations of traditional approaches to military training and operational analysis. In this regard, the role of modelling and simulation systems is growing, which NATO considers a strategic resource for training, planning, research and conducting operations in a multi-domain environment. The aim of this work is to analyze the structure,

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

methodological principles and key areas of development of the modelling and simulation system in NATO, as well as to identify opportunities for adapting these approaches in the Armed Forces of Ukraine. The article reveals the activities of institutional components of the system, approaches to standardization, and technological initiatives. It has been shown that the effectiveness of modelling and simulation systems is determined by the level of integration, standardization and accessibility of synthetic environments. It is justified that in domestic practice, the potential of such systems remains underestimated, and the term “training and simulation base” does not cover the analytical and research function, which is key to supporting decision-making and operations research. The main research methods are systematic and comparative analysis, content analysis of NATO regulatory documents, scientific publications by Ukrainian researchers, and national guidance documents in the field of military training and the development of training and simulation systems. The results of the article can be used in forming a national concept for the development of modelling and simulation systems, developing standards for the validation of simulators and models, and creating a unified information and analytical space for the training of the Armed Forces of Ukraine.

Keywords: modelling and simulation, NATO, simulators, trainers, military training, Armed Forces of Ukraine.

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Received: *December 8, 2025* | **Revisions Requested:** - | **Revision Received:** -
Accepted: *March 1, 2025* | **Published Online:** *April 10, 2026*

Licensed (C) by Creative Commons Attribution International License 4.0 (CC BY-NC-SA)

DOI: 10.62524/msj.2026.4.1.14

Переваги, виклики та застереження застосування роботизованих систем у військовій сфері: комплексний аналіз та рекомендації

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: e-mail: kataza@i.ua
ORCID: 0000-0002-1077-1402

Анотація. Актуальність дослідження зумовлена стрімким зростанням ролі роботизованих та безпілотних систем у сучасних воєнних конфліктах, що супроводжується як розширенням їхніх функціональних можливостей, так і появою нових вразливостей, пов'язаних із фізичною, кібернетичною та енергетичною стійкістю, а також особливостями застосування штучного інтелекту у бойових умовах. В умовах тривалої збройної агресії проти України питання забезпечення ефективного, надійного та безпечного використання роботизованих систем набуває особливого значення для підвищення спроможностей Збройних Сил України. Метою статті є комплексний науковий аналіз переваг, викликів та обмежень застосування роботизованих систем у військовій сфері, оцінювання їх впливу на ефективність виконання бойових завдань, а також обґрунтування підходів до мінімізації ризиків та підвищення стійкості їх функціонування в умовах сучасної війни. Основними результатами дослідження є: систематизація ключових переваг роботизованих систем, зокрема зниження ризиків для особового складу, підвищення точності ураження та розширення розвідувальних можливостей; визначення та класифікація основних груп викликів, серед яких проблеми фізичної та кібербезпеки, енергетичної автономності, стійкості управління та взаємодії "людина–робот"; уточнення змісту поняття "бойовий імунітет" роботизованих систем та оцінювання його впливу на їхню ефективність; розроблення комплексу заходів щодо підвищення живучості, захищеності та надійності функціонування роботизованих платформ у бойових умовах. У статті доведено, що ефективність застосування роботизованих систем визначається не лише їхніми тактико-технічними характеристиками, а передусім рівнем їх інтеграції у єдині контури управління, стійкістю до комплексних впливів противника та здатністю функціонувати в умовах динамічно змінюваного бойового середовища. Обґрунтовано доцільність формування системного підходу до розвитку роботизованих спроможностей, який передбачає поєднання технологічних, організаційних та доктринальних рішень. Матеріали статті можуть бути корисними для органів військового управління, науково-аналітичних установ сектору безпеки і оборони, а також для фахівців у сфері оборонного планування, розвитку безпілотних і роботизованих систем та впровадження інновацій у Збройних Силах України.

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Ключові слова: роботизовані системи, безпілотні системи, бойовий імунітет, кібербезпека, штучний інтелект, взаємодія "людина–робот", енергетична автономність, стійкість функціонування, військові операції, інноваційний розвиток, Збройні Сили України, сучасні воєнні конфлікти, асиметричні спроможності, інтеграція систем.

Вступ (Introduction)

Сучасний стан розвитку збройних конфліктів засвідчує стрімке зростання ролі роботизованих систем у досягненні оперативних і тактичних цілей. Досвід російсько-української війни переконливо підтверджує: безпілотні літальні апарати (БпЛА), наземні роботизовані комплекси (НРК) та морські безпілотні (безекіпажні) системи перетворились із допоміжного засобу на самостійний інструмент збройної боротьби. Роботизовані системи виконують широкий спектр завдань, від ведення розвідки та коригування артилерійського вогню до завдавання ударів і забезпечення логістики в умовах активних бойових дій.

Зростаючий вплив роботизованих систем на перебіг воєнних дій зумовлює необхідність комплексного наукового осмислення переваг, які вони надають, викликів, з якими стикаються збройні сили під час їх впровадження, та застережень щодо можливих негативних наслідків їх застосування. Питання всебічного аналізу цих аспектів залишається на порядку денному оборонної науки, особливо в контексті розвитку Сил безпілотних систем Збройних Сил України (ЗС України) та частин (підрозділів) безпілотних систем (комплексів) інших видів та родів військ.

Метою статті є комплексний аналіз переваг, викликів і застережень застосування роботизованих систем у військовій сфері, а також формування науково обґрунтованих рекомендацій щодо мінімізації ризиків їх використання.

Матеріали та методи (Materials and Methods)

Методологічну основу дослідження складають методи системного аналізу, порівняльного аналізу, класифікації та експертного оцінювання. Інформаційну базу становлять нормативні документи ЗС України, зокрема доктрина "Застосування безпілотних систем у силах оборони України" (2023), Доктрина "Безпілотні системи" (2026), Концепція застосування окремої бригади безпілотних систем (2024), а також результати наукових досліджень за цією тематикою. Для структурування матеріалу застосовано класифікаційний підхід, у межах якого переваги, виклики та застереження систематизовано за тематичними групами з визначенням ступеня пріоритетності та рівня впливу кожної позиції.

Дослідження ґрунтується також на аналізі підходів держав – членів НАТО до забезпечення кібербезпеки та бойового імунітету роботизованих систем, а також на практичному досвіді застосування різних типів роботизованих платформ під час поточного збройного конфлікту.

Результати (Results)

Дослідження переваг, викликів і застережень щодо застосування роботизованих систем у військовій сфері охоплює три взаємопов'язані напрями.

Перший – дослідження переваг, яке полягає в ідентифікації та аналізі позитивних аспектів використання роботизованих систем, включаючи можливості збільшення ефективності операцій, зниження ризиків для особового складу та забезпечення переваги у конкретних бойових ситуаціях.

Другий – дослідження викликів, що зосереджується на ідентифікації та аналізі проблем, що можуть виникати внаслідок використання роботизованих систем, зокрема етичних, правових, технологічних та психологічних питань.

Третій – дослідження застережень, що передбачає аналіз можливих негативних наслідків

The Central Research institute
of the Armed Forces of Ukraine
ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

та ризиків, пов'язаних із застосуванням роботизованих систем.

На рис. 1 представлено схему основних напрямів досліджень при формуванні переваг, викликів і застережень застосування роботизованих систем у військовій сфері.

Аналіз переваг роботизованих систем дозволяє виділити три ключові групи: оперативно-тактичні, розвідувально-інформаційні та системно-функціональні.

Оперативно-тактичні переваги охоплюють зниження ризику для особового складу, бо роботи виконують небезпечні завдання без загрози людському життю, підвищення ефективності та точності операцій, зменшення вразливості до підривних дій, швидкість реакції та гнучкість у складних умовах обстановки.

Розвідувально-інформаційні переваги включають розширення доступу до інформації та зведення даних, покращення розвідки в недоступних для людини районах, підвищення інформаційної свідомості та підтримку динамічного ведення бою у режимі реального часу.

Системно-функціональні переваги визначають довгостроковий потенціал роботизованих систем: підтримка логістики та постачання, здатність до спеціалізації та адаптації, глобальне проєктування сили, можливість масштабованого застосування, а також забезпечення переваги в умовах сучасних технологічних загроз.

На рис. 2 представлено порівняльний аналіз пріоритетності виявлених переваг застосування роботизованих систем. Результати оцінювання засвідчують, що переважна більшість (13 з 15) переваг має високий ступінь пріоритетності, що підтверджує ключову роль роботизованих систем у сучасних операціях.

Під бойовим імунітетом роботизованих систем розуміють їх здатність ефективно функціонувати та виконувати призначені завдання в умовах кіберзагроз та активної протидії противника. Виявлені шість ключових проблем систематизовано та оцінено за рівнем критичності.



Рисунок 1. Напрями досліджень під час формування переваг, викликів і застережень застосування роботизованих систем у військовій сфері

Найвищий рівень загрози (9 балів із 10) становить недостатня кібербезпека, бо слабкий захист дозволяє кіберзловмисникам перехопити контроль над системою, викрасти дані або порушити канали зв'язку. Конструктивні вразливості та атаки типу "відмова в обслуговуванні" оцінено на 8 балів. Для подолання цих загроз застосовуються:

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

криптографічний захист каналів зв'язку, регулярний аудит безпеки, двофакторна автентифікація та системи резервного управління. На рис. 3 представлено результати оцінювання рівня впливу проблем бойового імунітету.

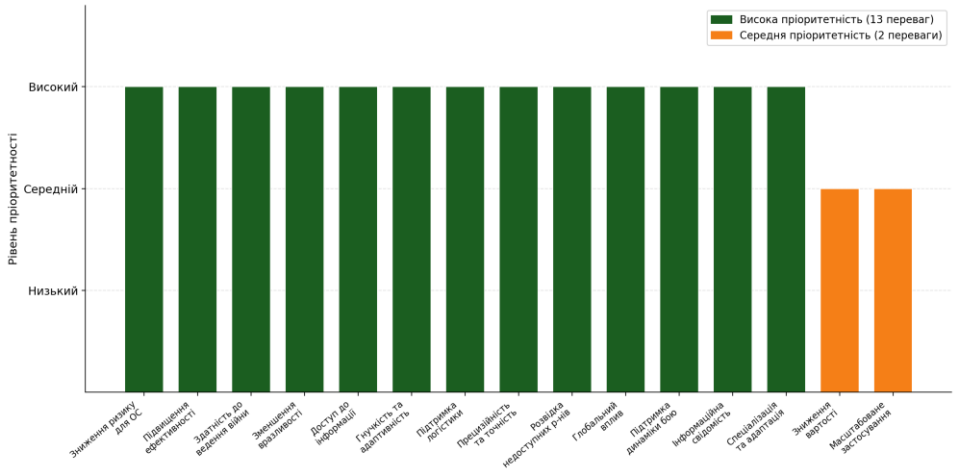


Рисунок 2. Пріоритетність переваг застосування роботизованих систем у військовій сфері

Проблема фізичної та кібербезпеки набуває особливої гостроти в умовах реальних бойових дій. До основних груп проблем належать: фізична безпека (технічні недоліки конструкції, аварії у критичних ситуаціях), кібербезпека (атаки на командні пункти та системи автономного керування), етичні аспекти застосування смертоносних систем без прямого контролю людини, а також реагування на непередбачені ситуації.

Особливо небезпечною є проблема втрати контролю над роботизованою системою. Перехід до самостійного простору ухвалення рішень системами, допущеними до управління зброєю масованого знищення, становить загрозу глобального масштабу. Для нейтралізації ризиків пропонується: розробка міцних кіберзахисних систем, постійне оновлення програмного забезпечення, застосування методів шифрування та автентифікації.

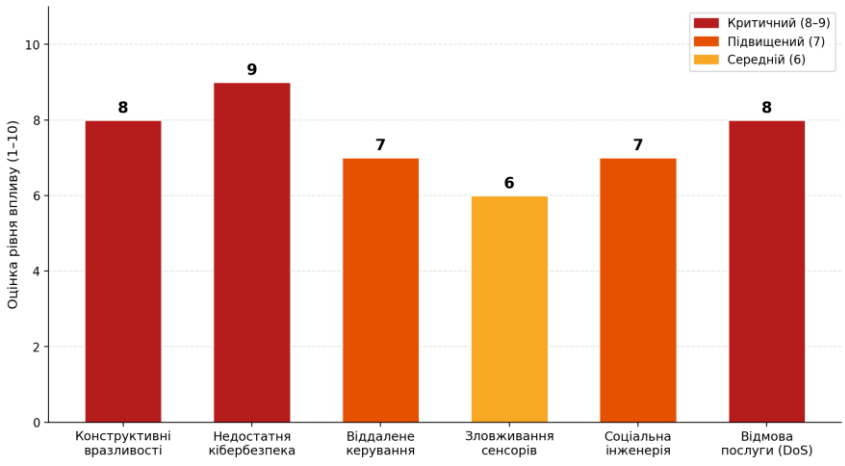


Рисунок 3. Оцінка рівня впливу проблем бойового імунітету роботизованих систем на ефективність їх застосування (за 10-бальною шкалою**)**

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Проблема автономності живлення охоплює десять ключових аспектів: обмежений запас енергії та технічні обмеження акумуляторів; вага та об'єм енергоносіїв; необхідність людського втручання при зарядці; висока енергоємність сенсорів та обчислювального обладнання; вразливість до переривань у постачанні енергії. Особливої уваги потребує розвиток відновлювальних джерел енергії для польового застосування.

Управління роботизованими системами на основі штучного інтелекту породжує широкий спектр проблем: від недостатньої надійності алгоритмів у непередбачуваних ситуаціях до правових питань відповідальності за наслідки автономних дій. Системи ШІ, навчені на обмежених або застарілих даних, виявляють недостатню адаптивність до нових умов бойових дій. Подолання потребує інвестицій у дослідження та впровадження гібридних систем співпраці людей і роботів.

Радарна діаграма (рис. 4) відображає порівняльну оцінку актуальності шести ключових груп викликів застосування роботизованих систем за десятибальною шкалою.

Найвищу актуальність (9 балів) має кібербезпека та бойовий імунітет, що повністю узгоджується з реальним досвідом застосування роботизованих систем під час поточного конфлікту. Правові та етичні аспекти і проблеми автономного управління на основі ШІ отримали оцінку 8 балів, що відображає зростаючу нагальність їх врегулювання.

Взаємодія "людина-робот" у військових системах визначає ефективність і безпеку виконання операцій. Основні проблеми включають: брак довіри до автономних рішень (нерозуміння логіки дій ШІ), низький рівень кібербезпеки підключених систем, етичні дилеми щодо застосування сили без прямого контролю, психологічний вплив на персонал та загроза гонки озброєнь у сфері військової робототехніки.

Ключовим принципом є збереження людського контролю у критичних моментах ухвалення рішень. Роботизовані системи мають розглядатися як доповнення до людських можливостей. Ефективна реалізація цього принципу потребує вдосконалення інтерфейсів взаємодії, психологічної підготовки операторів та розроблення чітких протоколів розподілу відповідальності.

Аналіз запропонованих заходів мінімізації ризиків у розрізі ключових груп викликів демонструє, що найбільш насиченою є сфера управління на основі ШІ – 15 виявлених проблем потребують комбінування технічних, правових та навчальних заходів. Рис. 5 відображає розподіл заходів мінімізації за групами викликів.

Технічні заходи є найчисельнішими у всіх групах. Правові та регуляторні заходи набувають особливого значення у сферах ШІ-управління та взаємодії "людина-робот". Навчання та підготовка персоналу виступає наскрізною компонентою всіх груп, що підкреслює людиноцентричний характер підходу до впровадження роботизованих систем.

Обговорення (Discussion)

Проведений аналіз підтверджує, що застосування роботизованих систем у військовій сфері є складним багатовимірним феноменом, що поєднує значний операційний потенціал з суттєвими ризиками технічного, правового та гуманітарного характеру. Провідні держави світу та блок НАТО сформували системні підходи до забезпечення кібербезпеки роботизованих систем: регуляція і стандартизація вимог, інтенсивне навчання персоналу, масштабні інвестиції у дослідження, широке партнерство з приватним сектором, створення спеціалізованих кіберкоманд.

Для України в умовах війни, що триває, впровадження роботизованих систем має особливе стратегічне значення. Реальні бойові дії є унікальним полігоном для їх апробації, що дозволяє формувати доктрину на основі практичного досвіду. Ключовими пріоритетами є: забезпечення надійного кіберзахисту, підготовка кваліфікованих операторів, розроблення відповідної нормативно-правової бази та забезпечення взаємодії із союзниками. Оптимальна

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

стратегія має забезпечувати баланс між максимізацією бойового ефекту та дотриманням гуманітарних норм, між автономністю та збереженням людського контролю.

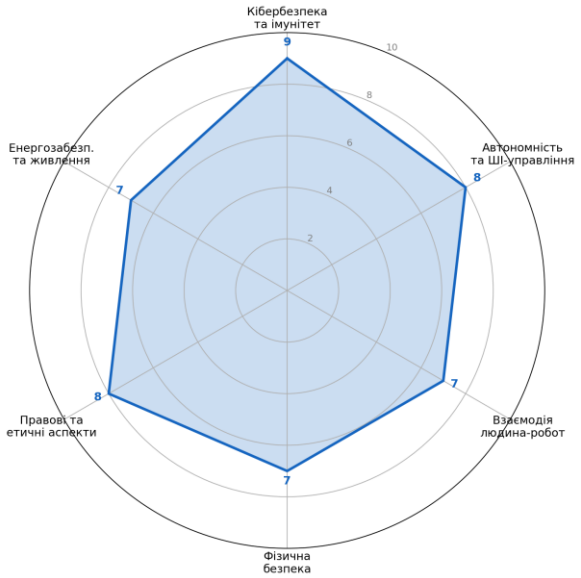


Рисунок 4. Радарна діаграма актуальності ключових напрямів викликів застосування роботизованих систем (бальна оцінка)

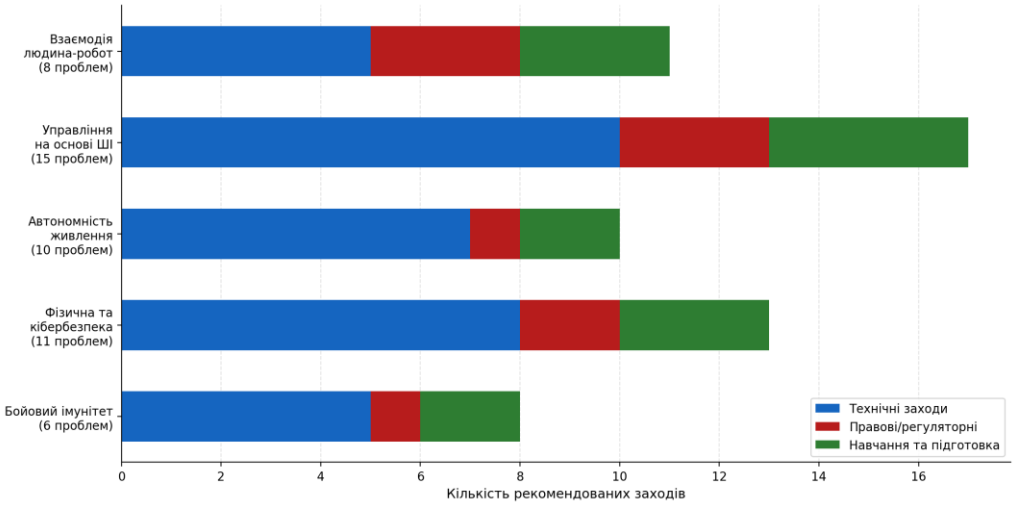


Рисунок 5. Розподіл заходів мінімізації ризиків застосування роботизованих систем за групами викликів

Висновок (Conclusions)

У статті проведено комплексний аналіз переваг, викликів і застережень застосування роботизованих систем у військовій сфері. Отримані результати дозволяють сформулювати такі висновки.

1. Роботизовані системи надають широкий спектр переваг із переважно високим ступенем пріоритетності (13 із 15 переваг). Ключовими є: зниження втрат особового складу, підвищення точності та ефективності операцій, розширення розвідувальних можливостей, гнучкість і масштабованість застосування.

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

2. Серед проблем бойового імунітету найбільш критичним є недостатній рівень кібербезпеки (9 балів із 10). Конструктивні вразливості та атаки типу DoS отримали оцінку 8 балів. Для їх нейтралізації необхідне системне застосування сучасних методів криптографічного захисту та регулярний аудит безпеки.

3. Ключовими групами викликів є кібербезпека та бойовий імунітет (9/10), правові й етичні аспекти та автономне управління на основі ШІ (8/10), взаємодія "людина-робот" та автономність живлення (7/10).

4. Заходи мінімізації ризиків поділяються на три категорії: технічні (переважаючі за кількістю), правові та регуляторні, навчання і підготовка персоналу. Найбільш комплексної уваги потребує сфера управління на основі ШІ – 15 виявлених проблем.

5. Для ЗС України ефективне впровадження роботизованих систем передбачає: системне навчання операторів, формування національної нормативно-правової бази, залучення передових технологій союзників НАТО та максимальне використання досвіду поточних бойових дій для вдосконалення доктрини застосування.

Подальші дослідження доцільно спрямувати на розроблення методичних підходів до кількісного оцінювання бойового імунітету роботизованих систем, вивчення досвіду їх інтеграції у багатодоменні операції, а також формування національних стандартів і вимог кібербезпеки для систем із застосуванням штучного інтелекту.

Конфлікт інтересів (Conflict of Interest)

Автор заявляє про відсутність конкуруючих інтересів за тематикою статті.

Використані джерела

1. Головнокомандувач ЗС України. (2023). *Доктрина "Застосування безпілотних систем у силах оборони України" (ОП 3-0 (46))*.
2. ЦНДІ ЗС України. (2024). *Концепція застосування окремої бригади безпілотних систем (проєкт)*.
3. Fox, A. (2024). *The Russo-Ukrainian War: A strategic assessment two years into the conflict*. Association of the United States Army (AUSA).
4. Semenenko, O., Ostrovskyi, S., Movchan, A., & et al. (2024). Role and place of drone swarms in 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
5. Головнокомандувач ЗС України. (2022). *Тимчасова методика розрахунків бойових потенціалів військових формувань*.
6. Генеральний штаб ЗС України. (2025). *Методика оцінювання ефективності застосування засобів об'єднаної вогневої підтримки з урахуванням протидії засобів РЕБ противника*. ЦНДІ ЗС України.
7. Соболєв, О. М. (Кер.). (2024). *Звіт про НДР "Ієрархія-3" (остат.)*. ЦНДІ ЗС України.
8. Заступник Головнокомандувача ЗС України. (2024). *Методика визначення потреби у безпілотних авіаційних комплексах та боєприпасах до них на операцію*. ЦНДІ ЗС України.
9. Національний університет оборони України. (2017). *Тимчасова єдина загальновійськова методика оперативно-тактичних розрахунків в ході планування вогневого ураження противника* [Навчальний посібник].
10. Городнов, В. П., Дробаха, Г. А., & Єрмошин, М. О. (2004). *Моделювання бойових дій військ (сил) протиповітряної оборони* [Моногр.]. ХВУ.
11. Національна академія оборони України. (2004). *Методика визначення бойових можливостей механізованих (танкових) з'єднань, частин, підрозділів* [Навч. посіб.].
12. АрміяІнформ. (2023, 14 бер.). *Сухопутні війська США зразка 2030 року: вплив досвіду*

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

війни в Україні. https://armyinform.com.ua/2023/03/14/suhoputni-vijska-ssha-zrazka-2030-roku-vplyv-dosvidu-vijny-v-ukrayini/

References

1. Commander-in-Chief of the Armed Forces of Ukraine. (2023). *Doctrine "Employment of Unmanned Systems in the Defense Forces of Ukraine" (OP 3-0 (46))*.
2. Central Research Institute of the Armed Forces of Ukraine. (2024). *Concept for the employment of a separate unmanned systems brigade (draft)*.
3. Fox, A. (2024). *The Russo-Ukrainian War: A strategic assessment two years into the conflict*. Association of the United States Army (AUSA).
4. Semenenko, O., Ostrovskyi, S., & Movchan, A. (2024). Role and place of drone swarms in 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
5. Commander-in-Chief of the Armed Forces of Ukraine. (2022). *Provisional methodology for calculating the combat potentials of military formations*.
6. Chief of the General Staff of the Armed Forces of Ukraine. (2025). *Methodology for evaluating the effectiveness of joint fire support employment, accounting for enemy electronic warfare (EW) countermeasures*. Central Research Institute of the Armed Forces of Ukraine.
7. Soboliev, O. M. (Ed.). (2024). *Report on R&D project "Hierarchy-3" (final)*. Central Research Institute of the Armed Forces of Ukraine.
8. Deputy Commander-in-Chief of the Armed Forces of Ukraine. (2024). *Methodology for determining the requirement for unmanned aerial systems and their munitions for an operation*. Central Research Institute of the Armed Forces of Ukraine.
9. National Defense University of Ukraine (NDUU). (2017). *Provisional unified combined arms methodology for operational-tactical calculations during fire destruction planning* [Training manual].
10. Horodnov, V. P., Drobakha, H. A., & Yermoshyn, M. O. (2004). *Modeling of combat operations of air defense troops (forces)* [Monogr.]. Kharkiv Military University.
11. National Defense Academy of Ukraine. (2004). *Methodology for determining the combat capabilities of mechanized (tank) formations, units, and subunits* [Training manual].
12. ArmyInform. (2023, March 14). *U.S. Army of the 2030 model: The impact of the war experience in Ukraine*. https://armyinform.com.ua/2023/03/14/suhoputni-vijska-ssha-zrazka-2030-roku-vplyv-dosvidu-vijny-v-ukrayini/

Advantages, challenges and caveats of using robotic systems in the military: a comprehensive analysis and recommendations

Yuzef Dobrovolsky
Candidate of Technical Sciences, Associate Professor
Deputy Head of the Department of Military Training
for Academic Work – Head of the Academic Unit
National Aviation University
03048, Medova Street, 1, Kyiv, Ukraine
e-mail: e-mail: kataza@i.ua
ORCID: 0000-0002-1077-1402

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Abstract. The relevance of the study is due to the rapid growth of the role of robotic and unmanned systems in modern military conflicts, which is accompanied by both the expansion of their functional capabilities and the emergence of new vulnerabilities related to physical, cybernetic and energy stability, as well as the features of the application of artificial intelligence in combat conditions. In the context of prolonged armed aggression against Ukraine, the issue of ensuring the effective, reliable and safe use of robotic systems is of particular importance for increasing the capabilities of the Armed Forces of Ukraine. The purpose of the article is a comprehensive scientific analysis of the advantages, challenges and limitations of the use of robotic systems in the military sphere, assessing their impact on the effectiveness of combat missions, as well as substantiating approaches to minimizing risks and increasing the stability of their functioning in conditions of modern war. The main results of the study are: systematization of the key advantages of robotic systems, in particular, reducing risks to personnel, increasing the accuracy of destruction and expanding reconnaissance capabilities; definition and classification of the main groups of challenges, including problems of physical and cyber security, energy autonomy, stability of control and human-robot interaction; clarification of the meaning of the concept of “combat immunity” of robotic systems and assessment of its impact on their effectiveness; development of a set of measures to increase the survivability, security and reliability of the functioning of robotic platforms in combat conditions. The article proves that the effectiveness of the use of robotic systems is determined not only by their tactical and technical characteristics, but primarily by the level of their integration into unified control circuits, resistance to complex enemy influences and the ability to function in a dynamically changing combat environment. The feasibility of forming a systemic approach to the development of robotic capabilities, which involves a combination of technological, organizational and doctrinal solutions, is substantiated. The materials of the article may be useful for military command bodies, scientific and analytical institutions of the security and defense sector, as well as for specialists in the field of defense planning, development of unmanned and robotic systems and implementation of innovations in the Armed Forces of Ukraine.

Keywords: robotic systems, unmanned systems, combat immunity, cybersecurity, artificial intelligence, human-robot interaction, energy autonomy, operational stability, military operations, innovative development, Armed Forces of Ukraine, modern military conflicts, asymmetric capabilities, systems integration.

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Received: *September 14, 2025* | **Revisions Requested: -** | **Revision Received:** -
Accepted: *December 1, 2025* | **Published Online:** *April 10, 2026*

Licensed (C) by Creative Commons Attribution International License 4.0 (CC BY-NC-SA)

DOI: 10.62524/msj.2026.4.1.15

Модель підвищення гнучкості циклу управління оперативно-тактичним угрупованням в умовах множинних невизначеностей обстановки

Вадим Клименко
кандидат військових наук, доцент
докторант науково-організаційного відділу
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: vadymklymenko@ukr.net
ORCID: 0000-0001-9144-2362

Анотація. Актуальність досліджуваної проблеми полягає у необхідності подальшого набуття системою управління угруповання військ (сил) спроможностей у проактивних діях, які демонструють здатність зменшувати вплив невизначеностей обстановки шляхом коригування рішень у реальному часі. Інструментом для налаштування та розвитку цих спроможностей є цикл управління, в межах якого формується логіка побудови стійкого механізму функціонування системи в динамічному середовищі оперативної обстановки. В умовах впливу множинних невизначеностей управлінський цикл залежить від рівня його адаптивності, набуває нелінійного характеру і потребує гнучких підходів до ухвалення рішень. Адаптація системи управління реалізується практичним впровадженням математичних методів аналізу невизначеності та алгоритмів динамічних систем, що дозволяє оцінювати ризики, покращувати точність рішень та адаптивність системи до змінного середовища. Водночас, адаптація – це не лише застосування математичних методів, а й їх інтеграція в алгоритми ухвалення рішень, системи контролю та механізми самонавчання. Метою статті є розроблення моделі, яка підвищує спроможності системи управління та забезпечує: моделювання сценаріїв зміни обстановки в умовах невизначеностей обстановки шляхом мінімізації похибок оцінювання стану системи; стійкість функціонування за рахунок урахування множини випадкових чинників, що впливають на параметри стану системи та, відповідно, на досягнення критеріїв ефективності функціонування; запровадження підсистеми зворотного зв'язку для корекції оцінки ефективності ухвалених рішень на основі моніторингу ключових показників ефективності. Направленість статті полягає у пошуку математичних методів, які сприяють стабільності прогнозу оперативної обстановки, створюють командиру і штабу умови для ухвалення рішень на основі гарантованих оцінок, та забезпечують послідовність у діях в умовах багатьох невизначеностей даних. У статті застосовано наукові підходи, які дозволяють здійснити корекцію плану застосування сил і засобів при зміні оперативної (тактичної) обстановки у реальному часі, передбачають перегляд ризиків і внесення коректив у існуючий план або розроблення нового варіанта дій. На відміну від методу найменших квадратів або методу максимальної правдоподібності, які враховують лише вимірювальну інформацію, що надходить в процесі проведення поточного експерименту, порівняльний аналіз попередніх даних та поточної ситуації найбільш адекватно може бути виконаний методом максимальної апостеріорної ймовірності, який для оцінювання параметрів стану динамічної системи враховує апріорну інформацію про ці параметри. Як

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

відомо, він базується на баєсівському підході й знаходить значення параметру, що максимізує апостеріорну ймовірність, тобто знаходить найімовірніші значення параметрів, беручи до уваги як дані поточної обстановки, так і апріорні знання. Основними результатами статті є підвищення адаптивності циклу управління оперативно-тактичним угрупованням, що передбачає своєчасну корекцію плану застосування військ (сил) у реальному часі. У статті розглянуто характеристики, що визначають спроможності системи управління залежно від її поточного стану, запропоновано модель оптимізації функціонування системи на основі підвищення гнучкості циклу управління в умовах множинних невизначеностей оперативної обстановки. Адаптація моделі до стохастичних змін у даних реалізується завдяки оновленню її параметрів на основі попереднього досвіду з використанням методу максимальної апостеріорної ймовірності. Наведено пропозиції щодо ухвалення компромісних управлінських рішень. Практична значущість отриманих результатів полягає у тому, що використання запропонованої моделі є доцільним для об'єктивної оцінки ймовірності успіху різних сценаріїв на основі доступної розвідувальної інформації. Формування компромісних варіантів рішень передбачає побудову декількох альтернативних планів дій із різним рівнем ризику та ресурсних витрат.

Ключові слова: цикл управління, оцінювання ефективності системи управління, параметри стану системи, метод максимальної апостеріорної ймовірності.

Вступ (Introduction)

Спроможності системи управління у прикладному аналізі – це сукупність властивостей, характеристик та функціональних можливостей, які визначають ефективність, гнучкість та надійність управління у заданих умовах. Виділення їх окремо у самостійні характеристики надає можливість проводити їх вимірювання, оптимізацію, враховувати компроміси між ними тощо. Ефективність управління передбачає ступінь досягнення поставлених цілей при мінімально можливих витратах ресурсів. Надійність – це ймовірність того, що система буде функціонувати безвідмовно у заданих умовах за певний період часу, її стійкість до збоїв зв'язку, помилок оброблення даних, ураження пунктів управління тощо. Гнучкість – здатність системи адаптуватися до змінних вимог без істотного зниження якості управління, швидке перепланування операції після появи нової загрози, тобто критична властивість для виживання та успіху в умовах невизначеності [1].

Для утримання оперативної ініціативи і нарощування можливостей дій на випередження система управління угруповання військ (сил) потребує подальшого набуття спроможностей у проактивних діях, тобто здатності зменшувати вплив невизначеностей обстановки шляхом коригування рішень у реальному часі [2].

Інструментом для налаштування і розвитку цих спроможностей є цикл управління, в межах якого формується логіка побудови стійкого механізму функціонування системи в динамічному середовищі за умов множинних невизначеностей оперативної обстановки.

Цикл управління формує основу для набуття таких спроможностей системи через забезпечення безперервного оновлення ситуаційної обізнаності, прогнозування розвитку подій з метою своєчасного коригування рішень у реальному часі, що дає змогу утримувати ініціативу і діяти на випередження навіть в умовах невизначеностей даних. Чим швидше і гнучкіше працює цикл управління, тим більше система здатна діяти проактивно, а не просто реагувати.

В умовах впливу множинних невизначених чинників оперативної обстановки управлінський цикл залежить від рівня його адаптивності, набуває нелінійного характеру і потребує гнучких підходів до ухвалення рішень. Адаптація системи управління реалізується практичним впровадженням математичних методів аналізу невизначеності та алгоритмів

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

динамічних систем, що дозволяє оцінювати ризики, покращувати точність рішень та адаптивність системи до змінного середовища. Разом з тим, адаптація – це не лише застосування математичних методів, а й їх інтеграція в алгоритми ухвалення рішень, системи контролю та механізми самонавчання [3, 4].

Ефективність, як ступінь досягнення цілей управління, – це прогнозування ситуації зокрема у формі сценарного планування, що передбачає розгляд та оцінку можливих сценаріїв розвитку ситуації ще до її виникнення, розроблення альтернативних варіантів виконання бойових завдань з урахуванням змінної обстановки, попередню розвідку противника і місцевості для визначення найбільш ефективних варіантів дій [5].

Оцінка сценарію розвитку ситуації, яка в контексті циклу управління відповідає ефективності замислу на застосування сил та засобів у конкретній оперативній обстановці, потребує відповідних критеріїв, які характеризують стан системи у визначений період часу, з метою переходу до пропозицій у випередженні противника та економії ресурсів. Критеріями автономних алгоритмів ухвалення рішень, які визначають його доцільність в умовах множинних невизначеностей оперативної обстановки, можуть бути:

бойовий потенціал підрозділу на момент ухвалення рішення, що виражається у математичному очкуванні втрат, які він може завдати противнику;

можливості для виконання маневру силами, засобами та вогнем;

наявність ресурсів (боєкомплекту, запасів, військово-технічного майна);

ступінь бойової готовності підрозділу до виконання завдання;

ступінь протидії противника, що виражається у математичному очкуванні втрат, які він може завдати нашому підрозділу.

Надійність функціонування системи забезпечується шляхом оцінювання власного стану і обстановки без очікування прямої вказівки зверху, тобто система має правильно оцінити власний стан без спотворення даних, реалістично оцінити загрозу та ступінь тиску з боку противника, гарантувати передачу команд на маневр без затримок чи втрат інформації, облік й обмін даними про наявні ресурси, заснований на реальній інформації, стан техніки, людей, комунікацій, що безпосередньо впливає на правильну оцінку готовності до бою, обрати дію з доступних варіантів. По-іншому, надійність – це якість ситуаційної обізнаності для автономного алгоритму ухвалення рішень [6].

Критично важливу роль у досягненні гнучкості динамічної системи управління відіграє оцінювання параметрів її стану, що безпосередньо впливає на гнучкість динамічної системи, визначаючи її здатність адаптуватися, залишатися стабільною та ефективною в умовах невизначеності. Адаптація до стохастичних змін полягає в оновленні параметрів на основі попереднього досвіду, тобто відбувається самонавчання в умовах змін обстановки [7].

Метою статті є розроблення моделі, яка підвищує спроможності системи управління та забезпечує: моделювання сценаріїв зміни обстановки в умовах невизначеності шляхом мінімізації похибок оцінювання стану системи; стійкість функціонування шляхом урахування множини випадкових чинників, що впливають на параметри стану системи та, відповідно, на досягнення критеріїв ефективності функціонування; запровадження підсистеми зворотного зв’язку для корекції оцінки ефективності ухвалення рішень на основі моніторингу ключових показників ефективності.

Матеріали та методи (Materials and Methods)

Корекція плану застосування сил і засобів у реальному часі при зміні оперативної (тактичної) обстановки передбачає перегляд ризиків і внесення коректив у існуючий план або розроблення нового варіанта дій. На відміну від методу найменших квадратів або методу максимальної правдоподібності, які враховують лише вимірювальну інформацію, що надходить в процесі проведення поточного експерименту, порівняльний аналіз попередніх

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

даних та поточної ситуації найбільш адекватно може бути виконаний методом максимальної апостеріорної ймовірності, який для оцінювання параметрів стану динамічної системи враховує апріорну інформацію про ці параметри. Як відомо, він базується на баєсівському підході і знаходить значення параметру, що максимізує апостеріорну ймовірність, тобто знаходить найімовірніші значення параметрів, беручи до уваги як дані поточної обстановки, так і апріорні знання. Однак його ефективність залежить від правильного вибору апріорного розподілу, а також від обчислювальних можливостей для оптимізації складних моделей [8].

Обстановка змінюється нелінійно, невелика зміна положення противника може спричинити радикальні наслідки. Втрата позицій внаслідок вогневого впливу противника може відкрити фланг, створити загрозу прориву, поява нових вогневих засобів у певному районі, навіть тимчасово, може змінити баланс сил і вплинути та темп наступу, дезінформація або відсутність точних даних про противника може призвести до хибного ухвалення рішень.

Таким чином, прагнення до стабільності прогнозу оперативної обстановки обумовлюється тим, що дані, які надходять до органу управління оперативно-тактичним угрупованням, можуть мати фрагментарний або суперечливий характер, змінюватись швидко і непередбачувано, також не всі фактори можливо точно виміряти чи врахувати. Якщо прогноз нестабільний, то навіть незначні зміни вихідних даних будуть приводити до радикально різних прогнозів. Це робить планування дій ненадійним і може призвести до помилок. Стабільний прогноз означає, що командири і штаб будуть ухвалювати рішення на основі гарантованих оцінок, а не постійно переглядати плани, при цьому забезпечується послідовність у діях навіть в умовах невизначеності, менше хаосу при ухваленні рішень [9].

Перевагами методу максимальної апостеріорної ймовірності є можливість урахування багаточисельної кількості невизначених множників оперативної обстановки:

врахування апріорної інформації, попередніх знань, вже відомих статистичних даних, типових сценаріїв розвитку обстановки, ймовірнісних моделей поведінки противника та своїх підрозділів, інтегрування попередніх знань про структуру, функціонування і можливі режими роботи системи, що дозволяє покращити точність оцінювання, тобто забезпечує більш обґрунтоване оцінювання ситуації;

зменшення похибок оцінки та нестабільності, завдяки регуляризації, яка проявляється через урахування апріорної інформації про систему, що “згладжує” оцінки і запобігає їх надмірній залежності від випадкових флуктуацій у даних, оцінка менш чутлива до випадкових або суб’єктивних помилок у вихідних даних, що особливо важливо в умовах, коли дані можуть бути неповними, неточними або суперечливими – як це часто трапляється в реальній бойовій обстановці;

стійкість до переобладнання, оскільки включення апріорних розподілів може запобігти переобладнанню моделі, наприклад, у випадках малої вибірки, коли мала кількість даних, частотні методи часто “перенавчаються” – тобто модель занадто підлаштовується під наявні дані й погано працює на нових (невідомих) даних;

гнучкість, завдяки якій метод може використовуватись для широкого класу задач, включаючи нелінійні системи, де залежності між діями та наслідками складні й не прямі, або нелінійно-гаусові процеси, де шум або невизначеність не підпорядковуються простим нормальним законам.

Урахування великої кількості невизначених множників дозволяє забезпечувати стабільність прогнозу, оскільки він зменшує залежність результату від коливань окремих факторів і в такий спосіб формує узагальнену оцінку стану. Тобто метод не просто “обирає найімовірніший варіант”, а мінімізує чутливість прогнозу до флуктацій в окремих невизначених параметрах. Чим більше множників враховується правильно, тим стійкішим стає результат. Кожен такий фактор може потенційно сильно змінити прогноз, але метод інтегрує інформацію і ймовірнісно “згладжує” вплив окремих нестабільних факторів, завдяки

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

чому прогноз стає стійкішим до змін в окремих даних, досягаються умови його стабільності.

Разом із тим, слід врахувати, що метод є чутливим до вибору апріорного розподілу, неправильний вибір якого може негативно вплинути на точність оцінки, якщо він не відповідає дійсності, отримані оцінки можуть бути зміщеними.

Результати та обговорення (Results and Discussions)

У ряді випадків про вектор оцінюваних параметрів $\bar{X}_0$ ще до проведення поточного експерименту є достатньо визначена апріорна інформація. У нашому випадку вектором оцінюваних параметрів буде набір ключових характеристик обстановки, які потрібно знати та оцінити для ухвалення ефективного рішення: відомості про противника, стан своїх військ, характеристика місцевості, метеообстановка, оцінка інфраструктури і логістики тощо. Цю попередню інформацію необхідно враховувати при обробленні результатів вимірювань, які є носіями апостеріорної інформації.

Коректне врахування апріорної інформації про параметри, що оцінюються, дозволяють компенсувати систематичне зміщення оцінок, що виникає в деяких випадках при використанні методу найменших квадратів або методу максимальної правдоподібності. Це можливо досягти в межах методу максимальної апостеріорної імовірності. Метод зсуває оцінку до найбільш правдоподібного апріорного значення, що зменшує зміщення. Наприклад, з метою досягнення точності координат цілі оцінка буде зміщена до району, який вважається найбільш імовірним на основі розвідданих або ймовірностей, що є важливим в системах управління, де рішення залежать від точності оцінки параметрів [10].

З метою оцінювання параметрів ефективності ухваленого рішення на основі спостережень та з урахуванням невизначеності у вимірюваннях розглянемо апостеріорну щільність розподілу параметрів системи управління оперативно-тактичного угруповання.

Припустимо, маємо систему умовних рівнянь:

$$\bar{Z} = \bar{U}(\bar{X}_0, \bar{\theta}) + \bar{h} \tag{1}$$

із заданим розподілом вектора похибок вимірювань:

$$\bar{h} \in p(\bar{h}). \tag{2}$$

Крім того, нехай маємо щільність розподілу імовірностей вектора $\bar{X}_0$:

$$\bar{X}_0 \in P(\bar{X}_0). \tag{3}$$

Необхідно в умовах задачі (1–3) оптимальним чином визначити оцінку $\hat{\bar{X}}_{\text{об}}$ вектора невідомих параметрів. З цією метою представимо умовну щільність імовірностей $\bar{X}_0$ після отримання вибірки $\bar{Z}$ за формулою Баєса

$$P(\bar{X}_0/\bar{Z}) = kP(\bar{X}_0)f(\bar{Z};\bar{X}_0), \tag{4}$$

де $k = (\int_{(k(\bar{X}_0))} P(\bar{X}_0)f(\bar{Z};\bar{X}_0)d\bar{X}_0)^{-1}$ – нормувальний коефіцієнт, який не залежить від вектора $\bar{X}_0$.

Функція (4) є апостеріорною щільністю розподілу імовірностей (рис. 1), тобто:

$$P_{\text{ac}}(\bar{X}_0) = P\left(\frac{\bar{X}_0}{\bar{Z}}\right).$$

Метод оброблення результатів вимірювань із дотриманням умови

$$P_{\text{ac}}\left(\hat{\bar{X}}_{\text{об}}\right) = max(\bar{X}_0)P_{\text{ac}}(\tilde{\bar{X}}_0) \tag{5}$$

$$\{\tilde{\bar{X}}_0\}$$

є методом максимальної апостеріорної імовірності.

Критерієм якості метода є величина апостеріорної щільності розподілу імовірностей

$$f(\tilde{\bar{X}}_0; \bar{Y}) = P_{\text{ac}}(\tilde{\bar{X}}_0). \tag{6}$$

The Central Research institute
of the Armed Forces of Ukraine
ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Система екстремальних рівнянь для функції (6) з урахуванням рівності (4) записується у вигляді:

$$\left[\frac{dp(\tilde{\bar{X}}_0)}{d\tilde{\bar{X}}_0}\right]^T f(\bar{Z};\tilde{\bar{X}}_0) + P(\tilde{\bar{X}}_0)\left[\frac{df(\bar{Z};\tilde{\bar{X}}_0)}{d\tilde{\bar{X}}_0}\right] = 0 \qquad (7)$$

Завдяки додатковим членам дані рівняння не вироджуються у випадку лінійної залежності часткових похідних від функції правдоподібності за параметрами, що оцінюються. Таким чином, ліквідується невизначена ситуація, яка виникає у такому випадку в методі максимальної правдоподібності.

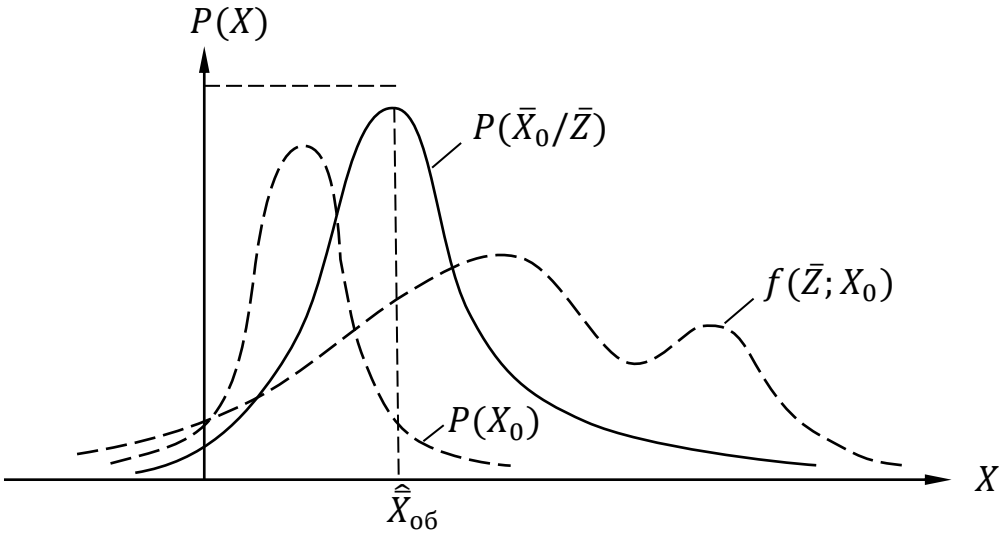


Рисунок 1. Функція апостеріорної щільності розподілу імовірностей

Вектор баєсівських оцінок є випадковим як за рахунок вектора $\bar{Z}$, так і за рахунок вектора $\bar{X}_0$, який належить простору апріорних значень вектора $\bar{X}_0$. У зв'язку з цим оптимальність баєсівських оцінок може розглядатись або на просторі $\sum \bar{Z}$, або на добутку просторів $K(\bar{X}_0)\sum \bar{Z}$. У першому випадку оптимальність оцінок буде умовною або оптимальністю в смислі максимальної правдоподібності. У другому випадку оптимальність оцінок буде безумовною або оптимальністю в середньому.

Апріорна інформація про параметри, що оцінюються, викликає зміщення оцінок відносно дійсних значень параметрів, що оцінюються. Тому баєсівські оцінки в умовному смислі оказуються зміщеними навіть тоді, коли максимально правдоподібні оцінки будуть не зміщеними.

Наявність зміщення у баєсівських оцінок ще не означає зниження їх точності порівняно з оцінками максимальної правдоподібності. Якщо у вимірах є систематична помилка, то зміщення за рахунок апріорної інформації може компенсувати зміщення за рахунок систематичної складової помилки виміру.

Баєсівські оцінки, для яких математичне очікування в безумовному смислі збігається з вектором апріорних математичних очікувань параметрів, що оцінюються, $\bar{m}_{X_0}$, назвемо незміщеними в середньому.

За аналогією з інформаційною матрицею Фішера можливо ввести матрицю для функції $P_{\text{ас}}(\bar{X}_0) = P(\bar{X}_0/\bar{Z})$. Тоді баєсівські оцінки, які мають своєю коваріаційною матрицею матрицю, зворотну до введеної матриці, будуть називатись сумісно ефективними, відповідно, в сенсі максимальної правдоподібності або у середньому.

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Висновок (Conclusion)

У бойовій обстановці рішення залежать від великої кількості змінних: кількості особового складу та його морального стану, темпів просування, погоди, характеру місцевості тощо. Апостеріорний підхід дозволяє об'єднати ці складні фактори в єдину модель ухвалення рішення без необхідності жорсткого спрощення ситуації. Модель дозволяє оновлювати оцінку стану угруповання з урахуванням нових спостережень, правильно поводитись із неповними, шумними та суперечливими даними, адаптивно переоцінювати ймовірності різних варіантів у реальному часі, визначати, де найбільш доцільно посилити оборону чи сконцентрувати резерви.

Під час оцінювання стану підрозділів, ресурсів, ліній зв'язку або активності противника метод апостеріорної ймовірності "довіряє" не лише поточним даним розвідки чи моніторингу, а й враховує попередні знання про типову поведінку противника, відомі особливості місцевості, тактику застосування підрозділів. Якщо розвіддані про розміщення сил противника частково суперечливі, система оцінювання не зробить різких висновків лише на основі нових даних, а "збалансує" їх відповідно до того, що відомо про типові шаблони розміщення сил у подібних ситуаціях. Це зменшує ймовірність помилкової класифікації обстановки або ухвалення ризикованих рішень на основі випадкових чи суб'єктивно спотворених повідомлень.

Досягнення гнучкості реакції циклу управління на множинні невизначені фактори оперативної обстановки передбачає швидку адаптацію, багаторівневий аналіз ризиків, інформаційну перевагу та адаптовані алгоритми управління, що дозволяє мінімізувати втрати, ефективно розподіляти ресурси та зберігати ініціативу в динамічному середовищі бойових дій.

Таким чином, забезпечується гнучкість системи управління оперативно-тактичним угрупованням за рахунок підвищення стійкості оцінок ситуації та надійності ухвалених рішень навіть за умов високої невизначеності й неповноти даних.

Рекомендації (Recommendations)

Використання запропонованої моделі є доцільним для об'єктивної оцінки ймовірності успіху різних сценаріїв на основі доступної розвідувальної інформації. Формування компромісних варіантів рішень передбачає побудову декількох альтернативних планів дій із різним рівнем ризику та ресурсних витрат. Для кожного плану розраховується максимальна апостеріорна ймовірність успіху з урахуванням невизначеностей оперативної обстановки, дій противника, логістики, погодних умов тощо. Матрична оцінка ефективності забезпечує візуалізацію варіантів рішень за критеріями "витрати ресурсів – ймовірність успіху", що дає змогу швидко й об'єктивно виявляти компромісне рішення. Компромісним рішенням є найвища відносна апостеріорна ймовірність успіху за умови допустимих витрат ресурсів.

Запровадження динамічної моделі, яка дозволяє оновлювати вихідні ймовірності у реальному часі та коригувати наміри під час бойових дій, сприятиме швидкій адаптації та автономності в ухваленні рішень, що є важливим для динамічного бойового управління. Ініціативність та автономія командирів стали критичним фактором успіху. В умовах сучасної війни командири низового рівня отримують більше свободи в ухваленні тактичних рішень, це дозволяє швидко впливати на зміни бойової обстановки.

Перехід на адаптивні, матричні та децентралізовані структури управління значно підвищує їх боєздатність, маневреність і стійкість, але потребує модернізації систем зв'язку і управління, а також зміни доктринальних підходів до ведення бойових дій.

Здатність до проактивного управління силами і засобами під час проведення операції передбачає використання автоматизованих систем для оперативного аналізу даних і ухвалення рішень у реальному часі, здійснення маневру на випередження з метою забезпечення кращих позицій або уникнення загроз, оптимальний розподіл ресурсів на основі прогнозованого розвитку подій, використання інтелектуальних систем аналізу для виявлення ранніх ознак змін в обстановці та негайного реагування.

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Результатом адаптивної реакції є мінімізація ефекту “туману війни” за рахунок об’єднання інформації з різних сенсорів, управління не втрачається навіть за умов активної дії засобів РЕБ противника та хаотичних бойових дій.

Конфлікт інтересів (Conflict of Interest)
Автор заявляє, що у нього немає конкуруючих інтересів за тематикою статті.

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. *Зб. наук. пр. Харківського національного ун-ту Повітряних Сил, 4* (62), 53–60. https://doi.org/10.30748/zhups.2019.62.07.
2. 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.
3. 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. *Зб. наук. пр. Харківського національного ун-ту Повітряних Сил.* https://doi:10.30748/ zhups.2019.60.01.
4. 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: 10.30748/soi.2019.158.02.
5. Гавриленко, А. (2024). Ефективність функціонування системи підтримки прийняття рішень органів військового управління на основі сучасних інформаційно-аналітичних технологій (2024). *Науково-технічний журнал Державного науково-дослідного інституту випробувань і сертифікації озброєння та військової техніки*, *2* (4), 40–44.
6. Гриб, Д. А., Демідов, Б. О., Кучеренко, Ю. Ф., Ткачов, А. М., & Шубін, Є. В. (2019). Принципи, методи і технології моделювання і дослідження процесів функціонування складних багатоструктурних систем військового призначення і управління їх структурною динамікою. *Системи обробки інформації, 1* (156), 64–73. https://doi.org/ 10.30748/soi.2019.156.09.
7. Калініна, І. О., Гожий, О. П., Нечахін, В. В., & Шиян, С. І. (2022) Імітаційне моделювання систем зі складним стохастичним процесом обробки даних за допомогою кольорових мереж Петрі. Регіональний міжвузівський збірник наукових праць. *Системні технології, 6* (143), 42–56. https://doi.org/10.34185/1562-9945-6-143-2022-04.
8. Дебела, І. М. (2021). Байєсовський метод оцінки альтернативних рішень. *Таврійський науковий вісник. Серія: Економіка, 8*. https://doi.org/10.32851/2708-0366/2021.8.11.
9. Гудима, О. П. (2021). Удосконалення математичної моделі прогнозування та виявлення кризових ситуацій. *Наука і техніка Повітряних Сил Збройних Сил України, 1* (42), 126–130. https://doi:10.30748/nitps.2021.42.16.
10. Бідюк, П. І., & Гожий, О. П. (2014). *Ймовірнісно-статистичні методи моделювання і прогнозування.*

References

1. Kucherenko, Yu., Nosyk, A., Tkachev, A., & Shubin, S. (2019). Determining the effectiveness of the functioning of the military mission control system taking into account the importance, timeliness and quality of task performance in subsystems. *Collection of scientific papers of the Kharkiv National University of the Air Force, 4* (62), 53–60. https://doi.org/10.30748/

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

zhups.2019.62.07.
2. Kucherenko, Yu., Nosyk, A., Kamak, D., & Voznyi, O. (2024). Network-centric control system and its impact on the combat capabilities of an inter-service group. *Scientific and technical journal of the State Research Institute for Testing and Certification of Armaments and Military Equipment, 1* (3), 52–58.
3. Hryb, D., Demidov, B., Borisenko, M., & Kuznetsova, M. (2019). Informatization of structural dynamics management of complex multi-structural military systems during dynamic changes in the situation in the area of combat operations. *Collection of scientific papers of the Kharkiv National University of the Air Force.* https://doi:10.30748/ zhups.2019.60.01.
4. Hryb D., Demidov B., Khmelevsky S., & Matyushchenko O. (2019). Intelligent technologies in the tasks of controlling the structural dynamics of complex multi-structural systems of military purpose. *Information Processing Systems, 3* (158), 15–26. https://doi:10.30748/ soi.2019.158.02.
5. Gavrylenko, A. (2024). The effectiveness of the functioning of the decision-making support system of military management bodies based on modern information and analytical technologies (2024). *Scientific and technical journal of the State Research Institute for Testing and Certification of Armaments and Military Equipment, 2* (4), 40–44.
6. Hryb, D. A., Demidov, B. O., Kucherenko, Y. F., Tkachev, A. M., & Shubin, E. V. (2019). Principles, methods and technologies of modeling and research of the processes of functioning of complex multi-structured systems of military purpose and control of their structural dynamics. *Information processing systems, 1* (156), 64–73. https://doi.org/10.30748/soi.2019. 156.09.
7. Kalinina, I. O., Gozhyy, O. P., Nechakhin, V. V., & Shiyan, S. I. (2022). Simulation modeling of systems with a complex stochastic data processing process using colored Petri nets. *Regional interuniversity collection of scientific papers. System technologies, 6* (143), 42–56. https://doi.org/10.34185/1562-9945-6-143-2022-04.
8. Debela, I. M. (2021). Bayesian method for evaluating alternative solutions. *Tavria Scientific Bulletin. Series: Economics, 8.* https://doi.org/10.32851/2708-0366/2021.8.11.
9. Hudyma, O. P. (2021). Improving the mathematical model of forecasting and detecting crisis situations. *Science and Technology of the Air Force of the Armed Forces of Ukraine, 1* (42), 126–130. https://doi:10.30748/nitps.2021.42.16.
10. Bidyuk, P. I., & Gozhy, O. P. (2014). *Probabilistic and statistical methods of modeling and forecasting.*

A model for enhancing the flexibility of the command cycle of an operational-tactical formation under conditions of multiple operational uncertainties

Vadym Klymenko
Candidate of Military Sciences, Associate Professor
Doctoral student of the scientific and organizational department
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl avenue, 28 B, Kyiv, Ukraine
e-mail: vadymklymenko@ukr.net
ORCID: 0000-0001-9144-2362

Abstract. The relevance of the researched problem lies in the need for the further development of the command and control system of military groupings, specifically in enhancing its capacity for proactive actions that reduce the impact of situational uncertainties through real-time decision adjustments. The primary mechanism for shaping and improving these capabilities is the command cycle, within which the logic of a resilient functioning mechanism in a dynamic operational

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

environment is formed. Under the influence of multiple uncertainties, the command cycle becomes dependent on its level of adaptability, takes on a nonlinear character, and requires flexible approaches to decision-making. Adaptation of the command and control system is achieved through the practical implementation of mathematical methods for uncertainty analysis and dynamic systems algorithms. This enables risk evaluation, improved decision accuracy, and system adaptability to a changing environment. Adaptation involves not only the use of mathematical tools but also their integration into decision-making algorithms, control systems, and self-learning mechanisms. The objective of this article is to develop a model that enhances the capabilities of the command and control system and ensures the following: scenario modeling of environmental changes under conditions of uncertainty by minimizing errors in the assessment of system state; resilient functioning through the consideration of multiple random factors influencing the system state parameters and the achievement of operational effectiveness criteria; and the introduction of a feedback subsystem to correct the assessment of decisions based on the monitoring of key performance indicators. The article focuses on identifying mathematical methods that contribute to the stability of forecasting the operational environment, provide the commander and staff with the means to make decisions based on reliable estimates, and ensure consistent actions in the presence of extensive data uncertainty. The article employs scientific approaches that allow for real-time adjustment of the plan for deploying forces and assets in response to changes in the operational or tactical situation. These approaches include the re-evaluation of risks and adjustment of the existing plan or development of a new course of action. Unlike the least squares method or the maximum likelihood method, which consider only the measurement data obtained during the ongoing process, a comparative analysis of previous data and the current situation can be most effectively conducted using the method of maximum a posteriori probability. This method estimates the parameters of the state of a dynamic system by incorporating prior knowledge about those parameters. Based on the Bayesian approach, it identifies the parameter values that maximize the posterior probability—thus determining the most likely parameter values by taking into account both real-time data and prior information. The main results of the article include enhancing the adaptability of the command cycle for operational and tactical groupings, which enables timely adjustments of force employment plans in real time. The article outlines the characteristics that determine the capabilities of the command and control system depending on its current state, and proposes a model for optimizing its performance by increasing the flexibility of the command cycle under conditions of multiple operational uncertainties. Adaptation of the model to stochastic changes in data is achieved by updating its parameters based on prior experience using the method of maximum a posteriori probability. Proposals for making balanced and compromise-oriented management decisions are also provided. The practical value of the obtained results lies in the applicability of the proposed model for objectively assessing the probability of success across various scenarios, based on available intelligence information. The formation of compromise decision options involves constructing several alternative courses of action, each with different levels of risk and resource expenditure.

Keywords: command cycle, evaluation of command and control system effectiveness, system state parameters, method of maximum a posteriori probability.

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Received: *January 2, 2026* | **Revisions Requested:** - | **Revision Received:** -
Accepted: *March 2, 2026* | **Published Online:** *April 10, 2026*

Licensed (C) by Creative Commons Attribution International License 4.0 (CC BY-NC-SA)

DOI: 10.62524/msj.2026.4.1.16

Воєнно-економічне прогнозування в системі національної безпеки України: роль, місце та вплив на забезпечення обороноздатності держави

Ірина Чернишова
доктор економічних 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: i-tv@ukr.net
ORCID: 0000-0002-5958-7059

Іван Марко
заслужений економіст України, доктор економічних наук, професор
провідний науковий співробітник
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: marko.df.mo@gmail.com
ORCID: 0000-0002-2590-3623

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

Євген Марко
кандидат економічних наук, старший науковий співробітник
провідний науковий співробітник
Національний університет оборони України
03049, проспект Повітряних Сил, 28, Київ, Україна
e-mail: marko.evgen@gmail.com
ORCID: 0000-0002-9165-8072

Володимир Рахімов
доктор філософії
заступник начальника інституту стратегічних комунікацій
Національний університет оборони України
03049, проспект Повітряних Сил, 28, Київ, Україна
e-mail: rakhimov@edu.nuou.org.ua
ORCID: 0000-0001-9868-986X

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Анотація. Актуальність дослідження зумовлена зростанням ролі економічних чинників у забезпеченні національної безпеки України в умовах широкомасштабної війни та тривалої воєнно-політичної нестабільності. Обмеженість ресурсів, високий рівень невизначеності та динамічність безпекового середовища вимагають науково обґрунтованих підходів до прогнозування економічних можливостей держави у сфері оборони. За цих умов воєнно-економічне прогнозування набуває стратегічного значення як інструмент узгодження оборонних потреб із реальними економічними можливостями та довгостроковими національними інтересами. Метою статті є обґрунтування місця воєнно-економічного прогнозування в системі національної безпеки України та визначення його ролі й впливу на забезпечення обороноздатності держави в умовах воєнно-політичної нестабільності. Для досягнення поставленої мети застосовано системний і структурно-функціональний підходи, методи аналізу та синтезу, а також елементи сценарного й економіко-математичного моделювання. У статті доведено, що воєнно-економічне прогнозування є аналітично-прогнозною підсистемою національної безпеки, яка одночасно функціонує на стратегічному та операційно-стратегічному рівнях. Визначено його ключові функції, обґрунтовано відмінності між прогнозуванням у межах системи національної безпеки та у процесі забезпечення обороноздатності держави, а також систематизовано основні виклики та обмеження його практичного застосування в сучасних умовах. Запропоновано напрями вдосконалення воєнно-економічного прогнозування, зокрема шляхом інституційної інтеграції, впровадження адаптивних сценарних моделей і розроблення єдиної методологічної бази оцінювання воєнно-економічного потенціалу. Практична значущість результатів полягає у можливості їх використання органами державної влади під час стратегічного, оборонного та бюджетного планування з метою підвищення обґрунтованості управлінських рішень і зміцнення обороноздатності України.

Ключові слова: безпекові ризики, бюджетування, воєнна економіка, воєнно-економічне прогнозування, оборонне планування, обороноздатність держави, система національної безпеки, стратегічне планування, управління оборонними ресурсами.

Вступ (Introduction)

Воєнно-економічне прогнозування є одним із ключових елементів стратегічного управління безпекою та обороною держави, особливо важливим це стає у сучасних умовах широкомасштабної війни росії проти України. Український науковий дискурс підкреслює, що здатність держави прогнозувати економічні та ресурсні можливості безпеки є критично важливою для формування адекватної оборонної та економічної політики [1]. Зокрема, оцінювання динаміки воєнно-економічного потенціалу є важливою складовою оборонного планування, оскільки воно визначає можливості держави реагувати на зовнішні виклики та підтримувати тривалі військові операції [2].

Прогнозування, що поєднує економічні, політичні та військові аспекти, має забезпечувати синхронізацію оборонних потреб із економічними можливостями країни. Зазначене особливо важливе в умовах тривалої війни, коли ресурси обмежені, а динаміка зовнішніх загроз нестабільна.

Упродовж останніх років актуальність воєнно-економічного прогнозування суттєво зросла у зв’язку з трансформацією характеру сучасних воєн, підвищенням ролі економічних факторів у забезпеченні стійкості держави та необхідністю довгострокового планування оборонних ресурсів. За цих умов воєнно-економічне прогнозування набуває системного значення як інструмент обґрунтування стратегічних рішень у сфері національної безпеки та оборони.

Отже, мета публікації – надати обґрунтування місця воєнно-економічного

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

прогнозування в системі національної безпеки України та визначити його роль у процесі забезпечення обороноздатності країни в умовах воєнно-політичної нестабільності.

Методологічна основа (Methodological Framework)

Для реалізації мети дослідження використано сукупність загальнонаукових і спеціальних методів пізнання. Зокрема, застосовано системний підхід для визначення місця воєнно-економічного прогнозування в системі національної безпеки України; структурно-функціональний аналіз – для ідентифікації функцій прогнозування на стратегічному та оперативно-стратегічному рівнях; методи аналізу й синтезу – для узагальнення наукових підходів і нормативно-правових засад.

Також використано елементи економіко-математичного та сценарного аналізу, що дозволило оцінити прикладний вплив воєнно-економічного прогнозування на процеси оборонного планування в умовах невизначеності та воєнно-політичної нестабільності.

Результати (Results)

Воєнно-економічне прогнозування за своїм змістом і методологією належить до системи національної безпеки як її аналітично-прогнозна складова, водночас за функціональним призначенням воно безпосередньо спрямоване на забезпечення обороноздатності країни.

Узагалі, воєнно-економічне прогнозування можна розглядати як частину системи національної безпеки. При цьому зазначене прогнозування передбачає виконання низки завдань, а саме: аналіз поточного стану воєнно-економічного потенціалу, оцінювання ресурсних можливостей держави, аналіз траєкторій розвитку економічних та військових показників, а також побудову сценаріїв розвитку подій з урахуванням різноманітних ризиків. Головна мета такого прогнозування полягає у підтримці прийняття рішень на стратегічному рівні держави. Це відповідає загальному підходу, де прогнозування розглядається як інструмент підвищення інформаційної та стратегічної спроможності країни для захисту національних інтересів [3].

Тобто на теоретико-методологічному рівні воєнно-економічне прогнозування є елементом системи національної безпеки, оскільки:

по-перше, охоплює економічну, воєнну, ресурсну та політичну складові безпеки;

по-друге, виконує функцію прогнозування загроз і ризиків, що є базовою функцією системи національної безпеки;

по-третє, забезпечує стратегічне планування у довгостроковому вимірі;

по-четверте, орієнтоване на захист національних інтересів, а не лише збройних сил.

У цьому сенсі воєнно-економічне прогнозування слід розглядати як аналітично-прогнозну підсистему національної безпеки України, що забезпечує науково обґрунтовану підготовку стратегічних рішень у сфері захисту національних інтересів. Разом із тим, з позицій системного підходу, воєнно-економічне прогнозування забезпечує таке:

інтеграцію економічної та воєнної складових національної безпеки;

прогнозування ресурсних, фінансових і виробничих можливостей держави в умовах внутрішніх і зовнішніх загроз;

виявлення економічних обмежень та ризиків, що впливають на здатність держави гарантувати безпеку.

Серед ключових функції, які виконує воєнно-економічне прогнозування у межах системи національної безпеки, можна виділити такі:

інформаційно-аналітична – оскільки воєнно-економічне прогнозування передбачає формування бази даних і аналітичних оцінок;

прогностична – воєнно-економічне прогнозування визначає можливі сценарії розвитку воєнно-економічної ситуації;

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

попереджувальна – завчасно виявляє загрози економічній і воєнній стійкості;

стратегічно-обґрунтувальна – підтримка державної політики у сфері безпеки.

Таким чином, у системі національної безпеки України воєнно-економічне прогнозування є засобом узгодження національних інтересів із реальними економічними можливостями держави. Крім того, у контексті національної безпеки прогнозування має фундаментальний вплив на формування оборонної політики, оскільки дозволяє адаптувати економічну політику до потреб сектору безпеки й оборони, сприяючи довгостроковій стійкості державних фінансів і ресурсної бази. Отже, воєнно-економічне прогнозування може виступати інструментом ресурсного та економічного забезпечення оборонної політики країни або забезпечення її обороноздатності.

Узагалі, обороноздатність держави – це здатність ефективно відбити зовнішню агресію та забезпечити захист національних інтересів. У цьому процесі прогнозування відіграє практичну роль, оскільки визначає бюджетні пріоритети, оцінює потреби в оборонних витратах і ресурси, а також дозволяє оцінювати довгострокові тренди у військово-промисловому комплексі, економічних показниках, інноваціях і соціальних аспектах [4].

Тобто у процесі забезпечення обороноздатності України воєнно-економічне прогнозування має прикладний та функціонально орієнтований характер, оскільки безпосередньо впливає на формування оборонного потенціалу.

На відміну від загальносистемного рівня національної безпеки, воєнно-економічне прогнозування задля забезпечення обороноздатності країни має більш конкретний об’єкт (збройні сили та інші складові сектору оборони), орієнтоване на прийняття практичних управлінських рішень та тісно пов’язане з оборонним плануванням (у тому числі із бюджетним та програмно-цільовим).

Отже, на прикладному рівні воєнно-економічне прогнозування безпосередньо спрямоване на:

обґрунтування обсягів і структури оборонних витрат;

оцінювання можливостей воєнно-промислового комплексу;

прогнозування потреб сектору безпеки і оборони в ресурсах;

визначення економічних меж і стійкості оборонних зусиль у середньо- та довгостроковій перспективі.

Слід зазначити, що сучасні дослідження доводять: економічний потенціал безпосередньо впливає на оборонні витрати та економічну спроможність країни підтримувати тривалі військові дії. Це означає, що прогнозування витрат та їхній взаємозв’язок з економічним зростанням мають враховувати як коротко-, так і довгострокові ефекти на національну економіку, оборонну промисловість та інвестиції в інновації.

Крім того, інструменти економіко-математичного моделювання, включно зі сценарним аналізом, регресійним моделюванням та імітаційними моделями, можуть бути ефективно застосовані для оцінювання динаміки воєнно-економічного потенціалу з урахуванням зовнішніх ризиків і невизначеностей [5].

Отже, воєнно-економічне прогнозування одночасно функціонує на двох взаємопов’язаних рівнях:

стратегічному – у складі системи національної безпеки;

операційно-стратегічному – під час забезпечення обороноздатності держави.

Тобто у системі національної безпеки воєнно-економічне прогнозування формує стратегічне бачення економічних можливостей і ризиків безпеки, тоді як у сфері забезпечення обороноздатності воно трансформується у прикладний інструмент реалізації оборонної політики. Ключові відмінності воєнно-економічного прогнозування за основними критеріями на двох різних рівнях представлено в табл. 1.

Отже, воєнно-економічне прогнозування слід розглядати як ключовий елемент системи

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

національної безпеки України, що забезпечує стратегічну узгодженість між національними інтересами, безпековими загрозами та економічними можливостями країни. Водночас у процесі забезпечення обороноздатності країни воно виконує прикладну функцію економічного та ресурсного забезпечення оборонного потенціалу.

Схематично місце воєнно-економічного прогнозування в системі національної безпеки та його вплив на забезпечення обороноздатності держави представлено на рис. 1.

Таблиця 1. Ключові відмінності воєнно-економічного прогнозування на стратегічному та оперативно-стратегічному рівнях

Критерій	**Характеристика відмінностей**	
Система	Національна безпека	Забезпечення обороноздатності
Рівень	Стратегічний, системний	Операційно-стратегічний, прикладний
Горизонт	Довго- і середньостроковий	Середньо- і короткостроковий
Спрямованість	Національні інтереси	Здатність до оборони
Роль прогнозування	Базова системна функція	Прикладний інструмент

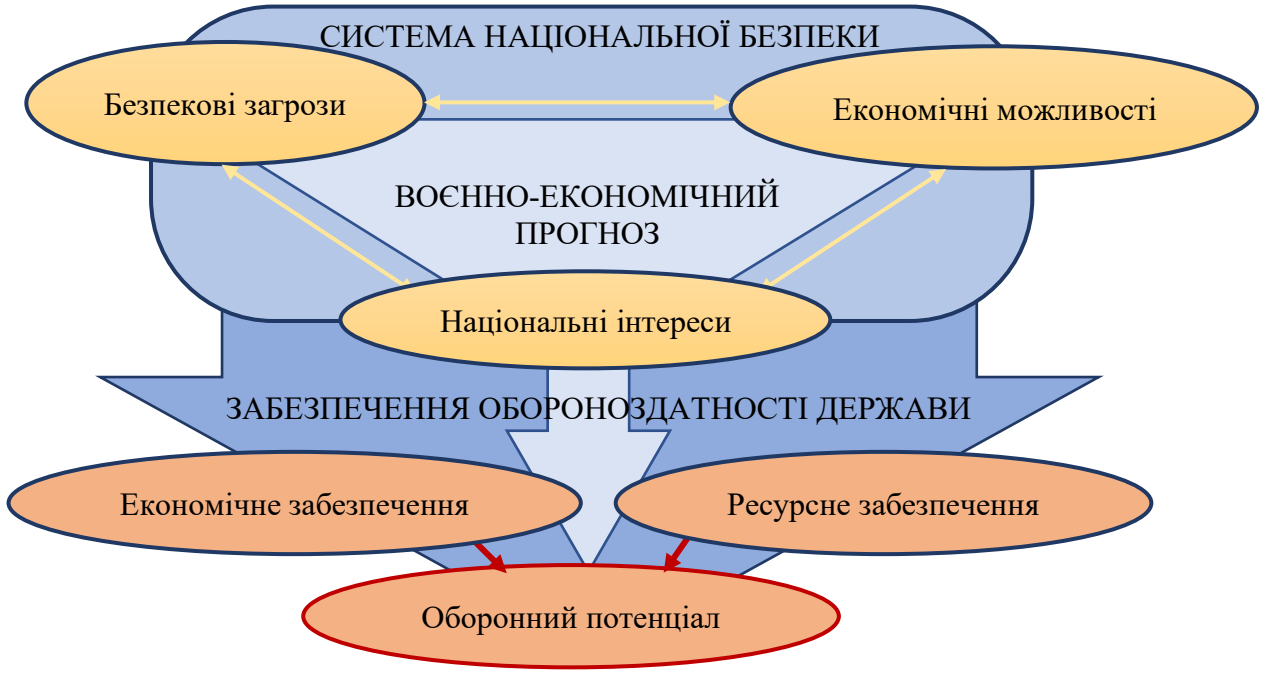


Рисунок 1. Місце воєнно-економічного прогнозування в системі національної безпеки та його вплив на забезпечення обороноздатності держави

Окремо слід зазначити про законодавчі та політичні засади прогнозування в Україні. Так, Україна має низку нормативних документів, які визначають місце воєнно-економічного прогнозування [6–10]. Зокрема, Укази Президента України та рішення Ради національної безпеки і оборони передбачають формування та реалізацію воєнної та економічної політик у взаємозв'язку, що є вирішальним для підготовки країни до оборони та забезпечення ресурсної спроможності збройних сил і сектору безпеки загалом.

Вищезазначене законодавче підґрунтя забезпечує нормативну основу для інтеграції економічних прогнозів у систему стратегічного планування безпеки й оборони, що дозволяє підвищувати узгодженість між економічними рішеннями та оборонними пріоритетами.

Вивчивши нинішню ситуацію, можна визначити певні проблеми та виклики воєнно-

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

економічного прогнозування в умовах нестабільності. Так, одним із ключових викликів є висока невизначеність в оцінюванні траєкторій розвитку воєнно-політичної обстановки. Нинішня війна, економічні санкції, зміни міжнародних економічних умов значно ускладнюють побудову точних прогнозів. Сценарні підходи та імовірнісні моделі стають незамінними у таких умовах. Разом із тим, прогнозування вимагає достовірних даних, що часто важко забезпечити під час кризових ситуацій. Крім того, інформаційна асиметрія у вигляді відсутності оперативних даних про потреби збройних сил у взаємозв'язку зі станом промислового виробництва створюють додаткові ризики невідповідності прогнозів реальності. Координація між різними державними інституціями (економічними, оборонними, фінансовими) є ще одним додатковим викликом. Квінтесенцією усього зазначеного є відсутність єдиної методології оцінювання та прогнозування, що призводить до суперечностей у прийнятті стратегічних рішень.

Отже, на основі аналізу джерел і сучасних практик можна запропонувати низку напрямів удосконалення воєнно-економічного прогнозування, а саме:

1) інституційну інтеграцію підрозділів (організацій, закладів, установ( ) тощо), які відповідають за прогнозування у процесі стратегічного планування. Це забезпечить системність та актуальність аналізу;

2) впровадження адаптивних моделей прогнозування, що враховують сценарну невизначеність;

3) розроблення спільної методологічної бази для секторів економіки і безпеки, що сприятиме узгодженню рішень;

4) підвищення якості даних та інформаційних потоків між установами, що займаються оборонним і економічним аналізом.

Отже, застосування інтегрованих сценарних і кількісно-якісних моделей воєнно-економічного прогнозування створює передумови для підвищення обґрунтованості управлінських рішень у сфері оборонного планування та забезпечення стійкості оборонних зусиль держави.

Обговорення (Discussions)

Результати дослідження підтверджують тезу про те, що воєнно-економічне прогнозування в сучасних умовах виходить за межі суто допоміжного інструменту оборонного планування та набуває статусу самостійного елемента системи національної безпеки. На відміну від традиційних підходів, у яких прогнозування зводиться переважно до оцінювання обсягів оборонних витрат або ресурсного забезпечення збройних сил, у статті обґрунтовано системний характер воєнно-економічного прогнозування як механізму інтеграції економічної, воєнної та безпекової політики держави.

Порівняння отриманих результатів із напрацюваннями вітчизняних і зарубіжних дослідників свідчить про те, що більшість наукових робіт фокусуються на окремих аспектах воєнної економіки – фінансуванні оборони, розвитку воєнно-промислового комплексу або впливі військових витрат на економічне зростання [11–14]. Водночас недостатньо уваги приділяється саме прогнозному компоненту як інструменту управління ризиками та невизначеністю в системі національної безпеки. У цьому контексті запропонований у статті підхід дає можливість розширити наукове уявлення про функціональну роль воєнно-економічного прогнозування та його місце в ієрархії безпекових механізмів держави.

Особливої актуальності зазначені положення набувають в умовах широкомасштабної війни та тривалої воєнно-політичної нестабільності, коли класичні детерміновані моделі прогнозування втрачають ефективність. Як показує аналіз, сучасне воєнно-економічне прогнозування має ґрунтуватися на поєднанні сценарних, імовірнісних та економіко-математичних підходів, що дає змогу враховувати широкий спектр можливих траєкторій

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

розвитку подій. Такий підхід узгоджується з сучасними концепціями стратегічного управління безпекою, які орієнтовані не на точність прогнозу, а на підвищення адаптивності та стійкості державних рішень.

Дискусійним залишається питання інституційного забезпечення воєнно-економічного прогнозування в Україні. З одного боку, наявність нормативно-правових актів та стратегічних документів свідчить про формальне визнання важливості економічної складової національної безпеки. З іншого боку, відсутність єдиного координаційного центру прогнозування, розпорошеність аналітичних функцій між різними органами влади та обмежений обмін даними знижують практичну ефективність прогнозних розрахунків. Це підтверджує необхідність переходу від фрагментарного до системного підходу в організації воєнно-економічного аналізу.

Окремої уваги заслуговує співвідношення стратегічного та прикладного рівнів воєнно-економічного прогнозування. Отримані результати дозволяють стверджувати, що недостатня узгодженість між довгостроковими прогнозами економічного розвитку та середньо- і короткостроковими рішеннями в оборонному плануванні створює ризики нераціонального використання ресурсів і зниження оборонної стійкості держави. У цьому контексті воєнно-економічне прогнозування має виступати не лише інструментом аналізу, а й механізмом зворотного зв'язку між стратегічними цілями національної безпеки та реальними економічними можливостями країни.

Таким чином, результати дослідження відкривають простір для подальших наукових дискусій щодо методологічної уніфікації підходів до воєнно-економічного прогнозування, розроблення інтегрованих моделей оцінювання воєнно-економічного потенціалу та поглиблення міждисциплінарних зв'язків між економікою, безпековими студіями та стратегічним управлінням. У практичному вимірі це створює передумови для підвищення якості стратегічного планування та посилення обороноздатності держави в умовах довготривалих безпекових викликів.

Висновок (Conclusion)

У ході дослідження обґрунтовано, що воєнно-економічне прогнозування є невід'ємним і системотвірним елементом системи національної безпеки України, який забезпечує науково обґрунтоване узгодження між безпековими загрозами, національними інтересами та реальними економічними можливостями держави. Доведено, що його роль не обмежується допоміжною функцією в оборонному плануванні, а полягає у формуванні стратегічного бачення стійкості та ресурсної спроможності держави в умовах воєнно-політичної нестабільності.

Встановлено, що воєнно-економічне прогнозування функціонує на двох взаємопов'язаних рівнях: стратегічному – у складі системи національної безпеки, де воно виконує аналітично-прогнозну та попереджувальну функції, та операційно-стратегічному – у процесі забезпечення обороноздатності держави, де трансформується у прикладний інструмент обґрунтування оборонних витрат, ресурсного забезпечення сектору безпеки і оборони та розвитку воєнно-промислового комплексу.

Обґрунтовано, що ефективність воєнно-економічного прогнозування в сучасних умовах значною мірою залежить від використання інтегрованих методологічних підходів, які поєднують кількісні економіко-математичні моделі зі сценарним та якісним аналізом. Така інтеграція дозволяє підвищити адаптивність стратегічних рішень, враховувати високий рівень невизначеності та своєчасно ідентифікувати критичні ризики для економічної та воєнної стійкості держави.

Виявлено, що ключовими проблемами розвитку воєнно-економічного прогнозування в Україні залишаються фрагментарність інституційного забезпечення, обмежена узгодженість

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

між економічним і оборонним плануванням, а також відсутність єдиної методологічної бази оцінювання воєнно-економічного потенціалу. Подолання цих обмежень є необхідною умовою підвищення ефективності державної політики у сфері національної безпеки та оборони.

Отже, воєнно-економічне прогнозування слід розглядати як ключовий інструмент стратегічного управління безпекою, що забезпечує ресурсну обґрунтованість оборонної політики та сприяє посиленню обороноздатності України в умовах тривалих воєнних загроз. Перспективи подальших досліджень можуть бути пов'язані з розробленням адаптивних прогнозних моделей, удосконаленням інституційних механізмів координації та поглибленням інтеграції воєнно-економічного аналізу в систему стратегічного планування національної безпеки.

Рекомендації (Recommendations)

Доцільним є впровадження воєнно-економічного прогнозування як обов'язкового елемента оборонного та бюджетного планування з чіткою координацією між органами сектору безпеки, економіки та фінансів. Практичне застосування інтегрованих сценарних і економіко-математичних моделей прогнозування дозволить підвищити обґрунтованість розподілу оборонних ресурсів і своєчасно виявляти критичні ризики для обороноздатності держави. Перспективним напрямом є створення єдиної методологічної бази оцінювання воєнно-економічного потенціалу України.

Конфлікт інтересів (Conflict of Interest)

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

Використані джерела

1. Горбулін, В. П., & Качинський, А. Б. (2010). *Стратегічне планування: вирішення проблем національної безпеки.* НІСД.
2. Polovenko, V. (2025). Methodological apparatus for studying the problems of economic support for the armed defense of Ukraine, taking into account the military-economic capabilities of the enemy. *Social Development and Security*, *15* (6), 463–475. https://doi.org/10.33445/sds.2025.15.6.36.
3. Гаврилюк, І. (2025). Основні положення концепції оцінювання та прогнозування рівня воєнно-економічної безпеки держави. *Social Development and Security*, *15* (6), 1–9. https://doi.org/10.33445/sds.2025.15.6.1.
4. *SIPRI Yearbook 2024: Armaments, Disarmament and International Security*. (2024). Oxford University Press. https://www.sipriyearbook.org.
5. Чернишова, І., & Бусель, (2025.) В. Роль методологічних підходів під час оцінювання ефективності воєнно-економічного прогнозування. *Social Development and Security*, *15* (6), 429–439. https://doi.org/10.33445/sds.2025.15.6.33.
6. Про національну безпеку України. Закон України № 2469-VIII (2018, 21 черв.). *Відомості Верховної Ради України*. 2018. № 31. Ст. 241. https://zakon.rada.gov.ua/laws/show/2469-19.
7. Президент України. (2020). *Стратегія національної безпеки України (392/2020).* https://zakon.rada.gov.ua/laws/show/392/2020.
8. Президент України. (2015). *Воєнна доктрина України (555/2015)* (зі змінами). https://zakon.rada.gov.ua/laws/show/555/2015.
9. Президент України. (2021). *Стратегія воєнної безпеки України (121/2021).* https://zakon.rada.gov.ua/laws/show/121/2021.
10. Президент України. (2021). *Стратегія економічної безпеки України на період до 2025 року (347/2021).* https://zakon.rada.gov.ua/laws/show/347/2021.

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

11. Коваль, О. (2023). Вплив видатків Міністерства оборони на економічне зростання України. *Вісник Київського нац. ун-ту ім. Тараса Шевченка. Серія: Військово-спеціальні науки, 4* (56), 26–35. https://doi.org/10.17721/1728-2217.2023.56.26-35.
12. Stavytskyy, A., Kharlamova, G., & Shpyrko, V. (2023). Financing Ukraine's defense expenditures: A new geopolitical paradigm or preservation of sustainable trends? *Bulletin of Taras Shevchenko National University of Kyiv. Series: Economics, 1* (222), 126–140. https://doi.org/10.17721/1728-2667.2023/222-1/16.
13. Chymyshenko, S., & Bolotina, Y. (2023). Роль оборонно-промислового комплексу в економічному розвитку України. *Вісник Київського інституту бізнесу та технологій, 49* (1–2), 87–97. https://doi.org/10.37203/kibit.2023.49.08.
14. Кім, Т., & Українець, Ю. (2022). Військово-промисловий комплекс у сучасній світовій економіці: передумови, фактори, тенденції розвитку. *Економіка та суспільство, 39.* https://doi.org/10.32782/2524-0072/2022-39-33.

References

1. Horbulin, V. P., & Kachynskyi, A. B. (2010). *Strategic planning: Solving national security problems.* National Institute for Strategic Studies.
2. Polovenko, V. (2025). Methodological apparatus for studying the problems of economic support for the armed defense of Ukraine, taking into account the military-economic capabilities of the enemy. *Social Development and Security, 15* (6), 463–475. https://doi.org/10.33445/sds.2025.15.6.36
3. Havryliuk, I. (2025). Basic provisions of the concept for assessing and forecasting the level of the state's military-economic security. *Social Development and Security, 15* (6), 1–9. https://doi.org/10.33445/sds.2025.15.6.1
4. Stockholm International Peace Research Institute. (2024). *SIPRI Yearbook 2024: Armaments, disarmament and international security.* Oxford University Press. https://www.sipriyearbook.org
5. Chernyshova, I., & Busel, V. (2025). The role of methodological approaches in assessing the effectiveness of military-economic forecasting. *Social Development and Security, 15* (6), 429–439. https://doi.org/10.33445/sds.2025.15.6.33
6. On National Security of Ukraine. Law of Ukraine № 2469-VIII (2018, Jun. 21). Vidomosti Verkhovnoi Rady of Ukraine. 2018. № 31. Ст. 241. https://zakon.rada.gov.ua/laws/show/2469-19
7. President of Ukraine. (2020). *National Security Strategy of Ukraine (392/2020).* https://zakon.rada.gov.ua/laws/show/392/2020
8. President of Ukraine. (2015). *Military Doctrine of Ukraine (555/2015).* https://zakon.rada.gov.ua/laws/show/555/2015
9. President of Ukraine. (2021). *Military Security Strategy of Ukraine (121/2021).* https://zakon.rada.gov.ua/laws/show/121/2021
10. President of Ukraine. (2021). *Economic Security Strategy of Ukraine until 2025 (347/2021).* https://zakon.rada.gov.ua/laws/show/347/2021
11. Koval, O. (2023). Ministry of Defence expenditures impact on economic growth of Ukraine. *Bulletin of Taras Shevchenko National University of Kyiv. Series: Military-Special Sciences, 4* (56), 26–35. https://doi.org/10.17721/1728-2217.2023.56.26-35
12. Stavytskyy, A., Kharlamova, G., & Shpyrko, V. (2023). Financing Ukraine's defense expenditures: A new geopolitical paradigm or preservation of sustainable trends? *Bulletin of Taras Shevchenko National University of Kyiv. Series: Economics, 1* (222), 126–140. https://doi.org/10.17721/1728-2667.2023/222-1/16
13. Chymyshenko, S., & Bolotina, Y. (2023). The role of the defense-industrial complex in the

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

economic development of Ukraine. *Bulletin of the Kyiv Institute of Business and Technology, 49* (1–2), 87–97. https://doi.org/10.37203/kibit.2023.49.08

14. Kim, T., & Ukrainets, Y. (2022). Military-industrial complex in the modern world economy: Preconditions, factors, and development trends. *Economy and Society, 39*. https://doi.org/10.32782/2524-0072/2022-39-33

Military-Economic Forecasting in the National Security System of Ukraine: Role, Place and Impact on Strengthening the State's Defence Capability

Iryna Chernyshova
Doctor of Economic Sciences, Senior Researcher
Chief of the Sientific and Ressearch Branch
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl avenue, 28 B, Kyiv, Ukraine
e-mail: i-tv@ukr.net
ORCID: 0000-0002-5958-7059

Ivan Marko
Honored Economist of Ukraine, Doctor of Economics 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: marko.df.mo@gmail.com
ORCID: 0000-0002-2590-3623

Vitalii Busel
Head of the Central Defence Resources Department
General Staff of the Armed Forces of Ukraine
03049, Povitrianykh Syl avenue, 6, Kyiv, Ukraine
e-mail: Busel77vitalii@gmail.com
ORCID: 0009-0004-3043-9695

Yevhen Marko
Candidate of Economic Sciences, Senior Researcher
Leading Research Fellow
National Defence University of Ukraine
03049, Povitrianykh Syl avenue, 28 B, Kyiv, Ukraine
e-mail: marko.evgen@gmail.com
ORCID: 0000-0002-9165-8072

Volodymyr Rakhimov
PhD in Military Sciences
Deputy Head of the Institute of Strategic Communications
National Defence University of Ukraine
03049, Povitrianykh Syl Avenue, 28 B, Kyiv, Ukraine
e-mail: rakhimov@edu.nuou.org.ua
ORCID: 0000-0001-9868-986X

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Abstract. The relevance of this study is determined by the growing role of economic factors in ensuring the national security of Ukraine under conditions of full-scale war and prolonged military-political instability. Limited resources, a high level of uncertainty, and the dynamic nature of the security environment intensify the need for scientifically grounded approaches to forecasting the state's economic capabilities in the defense sector. Under these conditions, military-economic forecasting acquires strategic importance as a tool for aligning defense needs with real economic capacities and long-term national interests. The purpose of the article is to substantiate the place of military-economic forecasting within the national security system of Ukraine and to determine its role and impact on ensuring the state's defense capability under conditions of military-political instability. The methodological framework of the study is based on systemic and structural-functional approaches, methods of analysis and synthesis, as well as elements of scenario-based and economic-mathematical modeling. The article demonstrates that military-economic forecasting constitutes an analytical and forecasting subsystem of national security, functioning simultaneously at the strategic and operational-strategic levels. Its key functions are identified, the differences between forecasting within the national security system and within the process of ensuring defense capability are substantiated, and the main challenges and limitations of its practical application under current conditions are systematized. Directions for improving military-economic forecasting are proposed, including institutional integration, the introduction of adaptive scenario-based models, and the development of a unified methodological framework for assessing military-economic potential. The practical significance of the results lies in their potential use by state authorities in strategic, defense, and budgetary planning to enhance the justification of managerial decisions and strengthen Ukraine's defense capability.

Keywords: security threats, defense budgeting, defense economics, military-economic forecasting, defense planning, force readiness, national security architecture, strategic planning, defense resource management.

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Received: *September 14, 2025* | **Revisions Requested: -** | **Revision Received:** -
Accepted: *December 1, 2025* | **Published Online:** *April 10, 2026*

Licensed (C) by Creative Commons Attribution International License 4.0 (CC BY-NC-SA)

DOI: 10.62524/msj.2026.4.1.17

Рекомендації щодо забезпечення інтероперабельності ситуаційних центрів України

Олексій Соломицький
доктор військових наук, професор
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

Андрій Ігнатьєв
кандидат наук з державного управління
докторант
Національний університет оборони України
03049, проспект Повітряних Сил, 28, Київ, Україна
e-mail: ertya1978@gmail.com
ORCID: 0000-0002-0482-6024

Максим Кудрицький
доктор військових наук
начальник відділу – заступник начальника управління
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: kma_13@ukr.net
ORCID: 0000-0003-1554-4732

Володимир Коваль
кандидат військових наук, старший науковий співробітник
e-mail: vladimerkoval69@gmail.com
ORCID: 0000-0002-6209-6779

Денис Молчанов
науковий співробітник науково-дослідної лабораторії
кафедри військової підготовки
Державний університет “Київський авіаційний інститут”
03048, вулиця Медова, 1, Київ, Україна
e-mail: mdbua2@gmail.com
ORCID: 0009-0007-9268-2764

Анотація. Актуальність дослідження зумовлена зростанням ролі ситуаційних центрів у системі забезпечення національної та воєнної безпеки України, а також необхідністю їх

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

ефективної взаємодії в умовах цифровізації управління та інтеграції до європейського й євроатлантичного безпекового простору. Розгалужена мережа ситуаційних центрів різних органів державної влади та сектору безпеки і оборони потребує узгоджених технологічних, організаційних та правових рішень, які забезпечують можливість обміну інформацією, спільного використання сервісів та однакового розуміння даних. Через наявність значної гетерогенності технічних засобів, програмного забезпечення та інформаційних ресурсів, а також відсутність уніфікованих підходів до оцінювання рівня взаємосумісності таких систем є потреба в розробленні науково обґрунтованих методичних рекомендацій щодо забезпечення інтероперабельності ситуаційних центрів України на національному та міжнародному рівнях. У дослідженні використано комплекс загальнонаукових та спеціальних методів, зокрема системний аналіз, структурно-функціональний підхід, методи наукової абстракції та узагальнення, аналіз нормативно-правових актів і міжнародного досвіду функціонування інформаційно-аналітичних систем моніторингу безпеки, а також експертні методи оцінювання. Методологічною основою дослідження є концепція інтероперабельності інформаційних систем, що передбачає узгодження правового, організаційного, семантичного та технічного рівнів взаємодії між системами моніторингу та ситуаційними центрами. У результаті дослідження обґрунтовано підхід до формування моделі верифікації інтероперабельності ситуаційних центрів України, який передбачає систематизацію вимог щодо взаємосумісності на різних рівнях, експертне оцінювання відповідності ситуаційних центрів цим вимогам та визначення інтегральних показників інтероперабельної придатності і релевантності. Запропоновано послідовність етапів методики оцінювання рівня інтероперабельності, що дозволяє кількісно та якісно визначати ступінь взаємодії ситуаційних центрів між собою, з Головним ситуаційним центром України та з інформаційно-аналітичними системами міжнародних партнерів. Отримані результати створюють передумови для підвищення ефективності функціонування системи моніторингу воєнної безпеки, удосконалення інформаційного забезпечення управлінських рішень та формування єдиного інформаційного простору у сфері безпеки і оборони. Результати дослідження можуть бути корисними для органів державної влади, суб’єктів сектору безпеки і оборони, наукових установ та аналітичних центрів, що займаються питаннями розвитку ситуаційних центрів, цифрової трансформації системи управління безпекою, створення інформаційно-аналітичних систем моніторингу та забезпечення сумісності інформаційних систем у контексті інтеграції України до безпекових структур ЄС і НАТО.

Ключові слова: воєнна безпека, ситуаційні центри, інтероперабельність, інформаційні системи, моніторинг воєнної безпеки, цифрове врядування, інформаційна взаємосумісність, сектор безпеки і оборони, інформаційно-аналітичні системи.

Вступ (Introduction)

У сучасних умовах трансформації безпекового середовища та зростання ролі інформаційно-аналітичних систем у процесах державного управління особливе значення має розвиток ситуаційних центрів як ключових елементів системи моніторингу та реагування на загрози національній безпеці. Ситуаційні центри забезпечують збирання, оброблення, аналізування і поширення інформації щодо стану безпекового середовища, що створює підґрунтя для підготовки та прийняття управлінських рішень на стратегічному, оперативному та тактичному рівнях. У контексті інтеграції України до європейського та євроатлантичного безпекового простору актуальним є питання забезпечення ефективної взаємодії між ситуаційними центрами різних органів державної влади, а також їх сумісності з аналогічними системами міжнародних партнерів.

Водночас функціонування мережі ситуаційних центрів України характеризується

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

значною різнорідністю технічних засобів, програмного забезпечення, інформаційних ресурсів і процедур оброблення даних. Така гетерогенність ускладнює обмін інформацією між системами, знижує ефективність їхньої взаємодії та створює бар'єри для формування єдиного інформаційного простору у сфері безпеки і оборони. У зв'язку із цим особливої ваги набуває проблема забезпечення інтероперабельності ситуаційних центрів, що передбачає досягнення їхньої взаємосумісності на правовому, організаційному, семантичному та технічному рівнях.

Огляд літератури (Literature review)

Проблематика інтероперабельності інформаційних систем, зокрема систем ситуаційних центрів та систем моніторингу безпеки, активно досліджується у наукових працях, присвячених цифровому врядуванню, інформаційним технологіям та управлінню у сфері безпеки. Значна частина досліджень зосереджена на формуванні концептуальних підходів до побудови взаємосумісних інформаційних систем та механізмів їх інтеграції у складні розподілені інформаційно-аналітичні середовища.

Питання інтероперабельності інформаційних систем державного управління та цифрового врядування ґрунтовно розглянуто у працях міжнародних дослідників і міжнародних організацій. Зокрема, у межах Європейської інтероперабельної рамки визначено основні рівні забезпечення взаємосумісності – правовий, організаційний, семантичний і технічний, що створюють основу для інтеграції державних інформаційних систем різних країн та організацій [1]. Подібні підходи застосовуються також у дослідженнях, присвячених архітектурам цифрового врядування та розвитку платформ державного управління, у яких підкреслюється важливість інтеграції інформаційних ресурсів та узгодженості інформаційних процесів між різними органами влади [2].

У наукових працях, присвячених інформаційним системам безпеки, значна увага приділяється ролі інформаційно-аналітичних та ситуаційних центрів у процесах моніторингу, аналізу та підтримки прийняття управлінських рішень. Дослідники зазначають, що ситуаційні центри є інтеграційними елементами систем управління безпекою, оскільки забезпечують об'єднання різнорідних джерел інформації, аналітичних інструментів та механізмів реагування на кризові ситуації [3]. У роботах з проблематики управління надзвичайними ситуаціями також підкреслюється значення інформаційних систем підтримки прийняття рішень, які дозволяють оперативно аналізувати великі обсяги даних та формувати узгоджені управлінські рішення [4].

Окремий напрям досліджень пов'язаний із застосуванням стандартів відкритих систем і архітектурних підходів до забезпечення взаємосумісності інформаційних систем. У працях дослідників розглядаються питання використання сервісно-орієнтованих архітектур, стандартів обміну даними та моделей інтеграції інформаційних ресурсів для створення взаємодіючих інформаційних середовищ [5]. Водночас наголошується, що забезпечення інтероперабельності складних організаційно-технічних систем потребує використання комплексних моделей інтеграції підприємств та інформаційних систем [6]. Подібні підходи застосовуються і в межах спеціалізованих моделей взаємосумісності інформаційних систем, які передбачають багаторівневу структуру взаємодії між системами [7].

У працях українських дослідників увага приділяється питанням стратегічного управління у сфері національної безпеки та розвитку інформаційно-аналітичних систем державного управління. Зокрема, дослідження підкреслюють важливість створення інтегрованих систем моніторингу безпеки та розвитку аналітичних інструментів підтримки прийняття управлінських рішень [8]. Також у наукових роботах розглядаються проблеми забезпечення інформаційної безпеки держави та розвитку інформаційної інфраструктури сектору безпеки і оборони [9].

Таким чином, аналіз наукових джерел свідчить про те, що проблема інтероперабельності

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

інформаційних систем є важливою складовою розвитку сучасних систем управління безпекою та цифрового врядування. Разом із тим питання кількісного та якісного оцінювання рівня інтероперабельності ситуаційних центрів, а також розроблення методичних підходів до її верифікації в умовах функціонування системи моніторингу воєнної безпеки України залишаються недостатньо дослідженими, що зумовлює необхідність подальших наукових досліджень у цьому напрямі.

Методологічна основа (Methodological Framework)

Базовим у дослідженні є системний підхід, який дозволив розглядати ситуаційні центри як складні організаційно-технічні системи, що функціонують у межах єдиної системи забезпечення національної та воєнної безпеки. Застосування цього підходу дало можливість визначити місце ситуаційних центрів у структурі інформаційно-аналітичного забезпечення управління безпекою, встановити взаємозв'язки між їхніми елементами та окреслити основні рівні забезпечення інтероперабельності (правовий, організаційний, семантичний і технічний).

Для аналізу структури та функціонування ситуаційних центрів використано структурно-функціональний метод, що дав змогу дослідити їхні складові елементи, функції та інформаційні зв'язки, а також визначити основні вимоги до взаємосумісності інформаційних систем, які забезпечують моніторинг і оцінювання стану безпекового середовища.

У процесі дослідження також застосовано методи аналізу та синтезу, що дозволили узагальнити наукові підходи до забезпечення інтероперабельності інформаційних систем, проаналізувати міжнародний досвід розвитку систем ситуаційної обізнаності та інтегрованих інформаційно-аналітичних систем, а також сформувати цілісне уявлення про напрями розвитку мережі ситуаційних центрів України.

Крім того, у дослідженні застосовано методи наукової абстракції та узагальнення, що дали змогу сформулювати методичні положення щодо верифікації інтероперабельності ситуаційних центрів, визначити послідовність етапів оцінювання її рівня та сформувати інтегральні показники інтероперабельної придатності й релевантності.

Застосування зазначених методів у сукупності забезпечило наукове обґрунтування запропонованого підходу до оцінювання інтероперабельності ситуаційних центрів України та створило методичну основу для подальшого удосконалення системи інформаційно-аналітичного забезпечення моніторингу воєнної безпеки.

Результати (Results)

Загальна структура системи ситуаційних центрів передбачає, що для оцінювання стану воєнної безпеки та аналізу результатів реалізації національних інтересів службовцями апарату РНБО України інформація має надходити від ситуаційних центрів нижнього рівня, а також аналогічних центрів наших міжнародних партнерів (ЄС/НАТО), з якими функціонують канали зворотного інформаційного зв'язку та постачання. Прикладом аналогічної системи ЄС є система НАТО – CITCEN, EUROSUR (Агентства Європейської прикордонної і берегової охорони (Frontex)), FIEP (Міжнародна асоціація жандармерії та поліції зі статусом військового формування) тощо [10]. Для отримання такої інформації необхідна технічна та операційна сумісність, здатність різних комп'ютерних систем, пристроїв або програм взаємодіяти та обмінюватися даними між собою, використовуючи уніфіковані інтерфейси або протоколи. Ця здатність дозволяє створювати складні системи з неоднорідних, розподілених компонентів, забезпечуючи їхню спільну роботу – інтероперабельність.

Під *інтероперабельністю ситуаційного центру* розуміємо властивість, що характеризує його експлуатаційну сумісність з іншими ситуаційними центрами та надсистемами: Головним ситуаційним центром України та ситуаційними центрами ЄС/НАТО. Під *верифікацією інтероперабельності ситуаційного центру* розуміємо визначення ступеня його відповідності

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

(тобто релевантність) вимогам, що висуваються до інтероперабельності [11]. Забезпечення інтероперабельності здійснюється в інтересах виявлення та усунення бар'єрів взаємосумісності, тобто перешкод щодо обміну інформацією з іншими суб'єктами, спільного використання сервісів або однакового розуміння обмінних інформаційних елементів.

Забезпеченню інтероперабельності систем різного призначення присвячено невелику кількість наукових та навчально-методичних праць, що зумовлює потребу у більш глибокому дослідженні цього аспекту та у формулюванні відповідних методичних рекомендацій для суб'єктів забезпечення воєнної безпеки, на яких покладається функція моніторингу та оцінювання стану воєнної безпеки.

У [12] зроблено висновок про те, що системи цифрового врядування мають бути інтероперабельними, будуватися на основі стандартів обов'язкового використання, які забезпечують суттєве зменшення витрат під час розроблення нових цифрових управлінських стратегій та систем.

Таким чином, для забезпечення інтероперабельності необхідно на абстрактному рівні використати розроблений науково-методичний інструментарій для діагностування її поточного стану, визначення потенціалу розвитку та вимірювання управлінських впливів. Як такий інструментарій запропоновано використовувати модель верифікації інтероперабельності.

Загалом інтероперабельність обладнання, мереж, програмних засобів, інформації та режимів роботи є необхідною умовою нормального функціонування ситуаційних центрів України, адже отримання первинної інформації про стан безпекового середовища (обстановку), своєчасне її постачання до розгалуженої мережі споживачів (до суб'єктів забезпечення безпеки на місцевому, національному, міждержавному та міжнародному рівнях) і подальше її використання для ефективного реагування на загрози (ситуації), а також обмін іншою актуальною інформацією є сутністю призначення самої системи моніторингу і невід'ємним принципом функціонування механізмів забезпечення воєнної та міжнародної безпеки.

Тобто справедливо констатувати, що забезпечення інтероперабельності є однією з головних засад формування, розвитку та інтеграції ситуаційних центрів України (особливо в частині автоматизації та інформатизації моніторингових досліджень).

Високий рівень інтероперабельності може досягатися за рахунок низького рівня гетерогенності систем. Однак за результатами проведеного авторами [11–12] аналізу стану існуючої технічної та технологічної складової моніторингу й оцінювання стану воєнної безпеки України виявлено, що ситуаційні центри характеризуються високим рівнем внутрішньої гетерогенності, яку, зокрема, зумовлено такими чинниками: необхідність забезпечення воєнної безпеки у різних її визначальних сферах, умовах безпекового середовища та порівняно широкого спектру різнорідних загроз; наявність великої кількості як сучасних, так і морально й фізично застарілих вітчизняних та закордонних моніторингових технологій на об'єктах відповідальності; "хронічне" недофінансування затверджених урядом програм та планів щодо створення моніторингової інфраструктури, недостатнє ресурсне забезпечення; спроби побудови локальних моніторингових систем на окремих об'єктах відповідальності суб'єктів забезпечення національної та, зокрема, воєнної безпеки, здебільшого, не досягли очікуваного результату з різних причин (несумісність програмно-апаратних засобів тощо); відсутність загальної концепції (концептуального проєкту) та систематизованих технологічних рішень щодо побудови єдиної централізованої інформаційно-телекомунікаційної системи моніторингу стану воєнної безпеки України; брак досліджень щодо побудови єдиної моніторингової системи.

Закономірно, що такий стан внутрішньої гетерогенності у діяльності ситуаційних центрів України не сприяє належному рівню їхньої взаємодії як між собою, так і з Головним

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

ситуаційним центром України, а також із системами моніторингу регіональної безпеки ЄС/НАТО.

Отже, на початковому етапі побудови моделі верифікації інтероперабельності ситуаційних центрів України адаптуємо до умов їх дослідження базову модель інтероперабельності [1] (рис. 1), а також врахуємо відомий та апробований спосіб послідовного використання принципів відкритих систем і методології функціональної стандартизації, який має широке застосування як для систем промислової автоматизації, так і для створення взаємосумісних систем широкого класу за масштабами та сферами застосування.

Правовий (юридичний) рівень. Кожна державна адміністрація під час реалізації функцій державного управління працює у власній національній правовій системі. Аналогічно, діяльність окремих суб'єктів забезпечення воєнної безпеки регламентується як загальним, так і спеціальним законодавством. Правова взаємосумісність полягає у тому, щоб забезпечити можливість суб'єктів, що працюють у різних правових рамках, політиках та стратегіях, виконувати завдання спільно. Своєю чергою, це зумовлює потребу у чіткому визначенні положень щодо шляхів подолання відмінностей у законодавстві та правових рамках, включаючи можливість ухвалення нових законів та інших нормативно-правових актів.

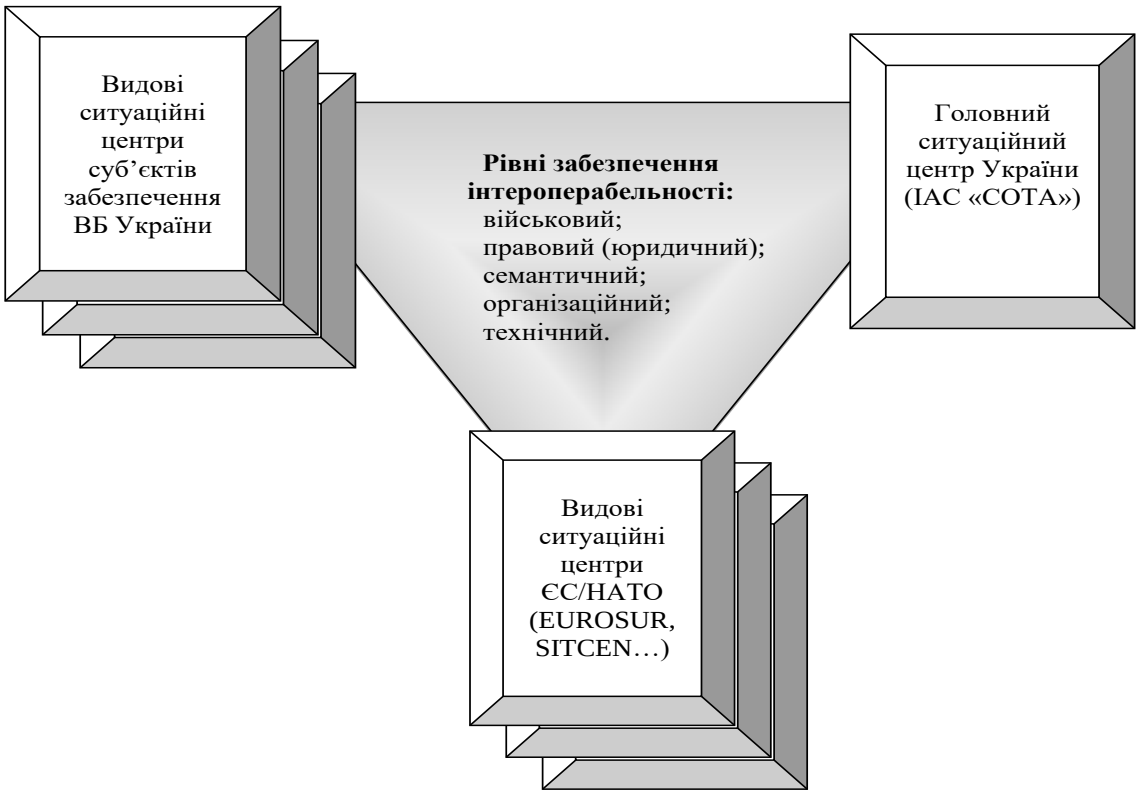


Рисунок 1. Базова модель інтероперабельності ситуаційних центрів України в контексті її європейської та євроатлантичної інтеграції

Першим кроком на шляху до вирішення проблеми правової взаємосумісності є проведення "аудиту сумісності" шляхом аналізу чинного законодавства для виявлення бар'єрів взаємосумісності, таких як галузеві або географічні обмеження у використанні та зберіганні даних, різні та "розмиті" ліцензійні відомості, надмірні обмеження щодо використання конкретних цифрових технологій чи режими їх постачання, суперечливі вимоги

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

до однакових чи подібних процесів (процедур), застарілі вимоги до рівня безпеки та захисту даних тощо.

Тому правову узгодженість в інтересах забезпечення сумісності слід аналізувати перед ухваленням концептуальних (стратегічних) рішень, а також регулярно оцінювати ефективність заходів щодо подальшого наближення стандартів після введення рішень у дію.

Зважаючи на те, що взаємодія державних інформаційних систем, зокрема, забезпечується цифровими каналами та інформаційно-комунікаційними технологіями, питання взаємосумісності на рівні законів та інших нормативно-правових актів слід розглядати якомога раніше, а відповідні документи мають пройти "цифрову перевірку". Зокрема, необхідно: переконатися, що документ відповідає вимогам не лише фізичного, а й цифрового середовища (наприклад, Інтернет); виявити будь-які перешкоди для цифрового обміну; визначити та оцінити вплив документа на інформаційно-комунікаційні технології стейкголдерів.

Це сприятиме взаємодії між державними службами на нижчих рівнях (семантичному, технічному, організаційному), а також збільшить потенціал для повторного використання існуючих рішень в галузі інформаційно-комунікаційних технологій, скоротивши ресурсні витрати та час на впровадження.

У разі зовнішньої взаємодії (з іноземними державами або міжнародними організаціями) юридична цінність будь-якої інформації, якою обмінюються, має зберігатися, має дотримуватися законодавство про захист даних як у державах походження інформації, так і її прийняття. Це може зумовити потребу в укладанні додаткових угод для подолання потенційних розбіжностей у застосуванні чинного законодавства.

Семантичний рівень. Цей рівень описує семантичні аспекти взаємодії, тобто змістовну сторону інформації, якою обмінюються системи. Семантична взаємосумісність – це здатність будь-яких взаємодіючих у процесі комунікації інформаційних систем однаковим чином розуміти сенс інформації, якою вони обмінюються. Тобто семантична взаємосумісність дозволяє системам комбінувати отриману інформацію з іншими інформаційними ресурсами і обробляти її смисловий зміст. Семантичної взаємосумісності може бути досягнуто, якщо застосувати стандарти розширюваної мови розмітки типу XML (зокрема XSLT, XAML, XUL, RSS, MathML, GraphML, XHTML, SVG, XML Schema).

Організаційний рівень фокусує увагу на прагматичних аспектах горизонтальної та вертикальної взаємодії ситуаційних центрів. На цьому рівні узгоджуються стратегічні цілі і досягаються угоди (меморандуми) про співпрацю між адміністративними органами, які мусять (або мають намір) обмінюватися інформацією, хоча мають різні внутрішню структуру і процеси. Організаційна взаємосумісність має на меті задовольнити вимоги спільноти користувачів: служби мають бути доступними, легко ідентифікуватися і бути орієнтованими на користувача. Організаційна взаємосумісність досягається шляхом застосування нормативно-правових документів (угод, конвенцій, договорів (меморандумів, протоколів) про співпрацю, стратегій тощо). Тобто організаційна взаємосумісність – це здатність брати участь у досягненні спільних цілей на рівні процесів (процедур).

Технічний рівень. Технічна взаємосумісність – здатність до обміну даними між системами, що беруть участь в обміні. Технічний рівень описує синтаксис або формати переданої інформації, фокусуючи увагу на тому, яким чином представлено інформацію в комунікаційному середовищі. Технічний рівень включає *такі ключові аспекти*, як відкриті інтерфейси, служби зв'язку, інтеграція даних і проміжний шар програмного забезпечення (Middleware), уявлення та обмін даними, служби доступу та захисту інформації. Технічна взаємосумісність досягається, головним чином, завдяки використанню стандартних протоколів зв'язку типу TCP/IP.

Основні етапи удосконаленого підходу забезпечення взаємосумісності відображено на

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

рис. 2. Сутність удосконалення існуючого підходу, задекларованого у документі ЄС [1], полягає у включенні після кожного етапу забезпечення взаємосумісності обов'язкових опитувань ключових стейкголдерів (замовників, постачальників, розробників, споживачів, персоналу, що супроводжує інформаційні системи і використовує програмне забезпечення та відповідні послуги), з метою виявлення та усунення проблемних питань, а також уможливлення впливу на результати попередніх етапів для їх покращення.

Послідовна реалізація етапів має привести до створення інтероперабельної мережі ситуаційних центрів.

Проте означений підхід не дозволяє кількісно оцінити стан інтероперабельності. Розуміння рівня інтероперабельності не відображається бінарними варіантами на зразок "так" або "ні" через багатоаспектність цього явища. Оскільки інтероперабельність не є фізичною величиною, її критерії (показники) мають визначатися на основі експертного оцінювання. Водночас найбільш дієвими виявляються шкали порядку або інтервалів, а також нечіткі шкали. Для зручності оцінювання рівня інтероперабельності прийнято п'ять рівнів оцінювання, які наведено в табл. 1 [1].

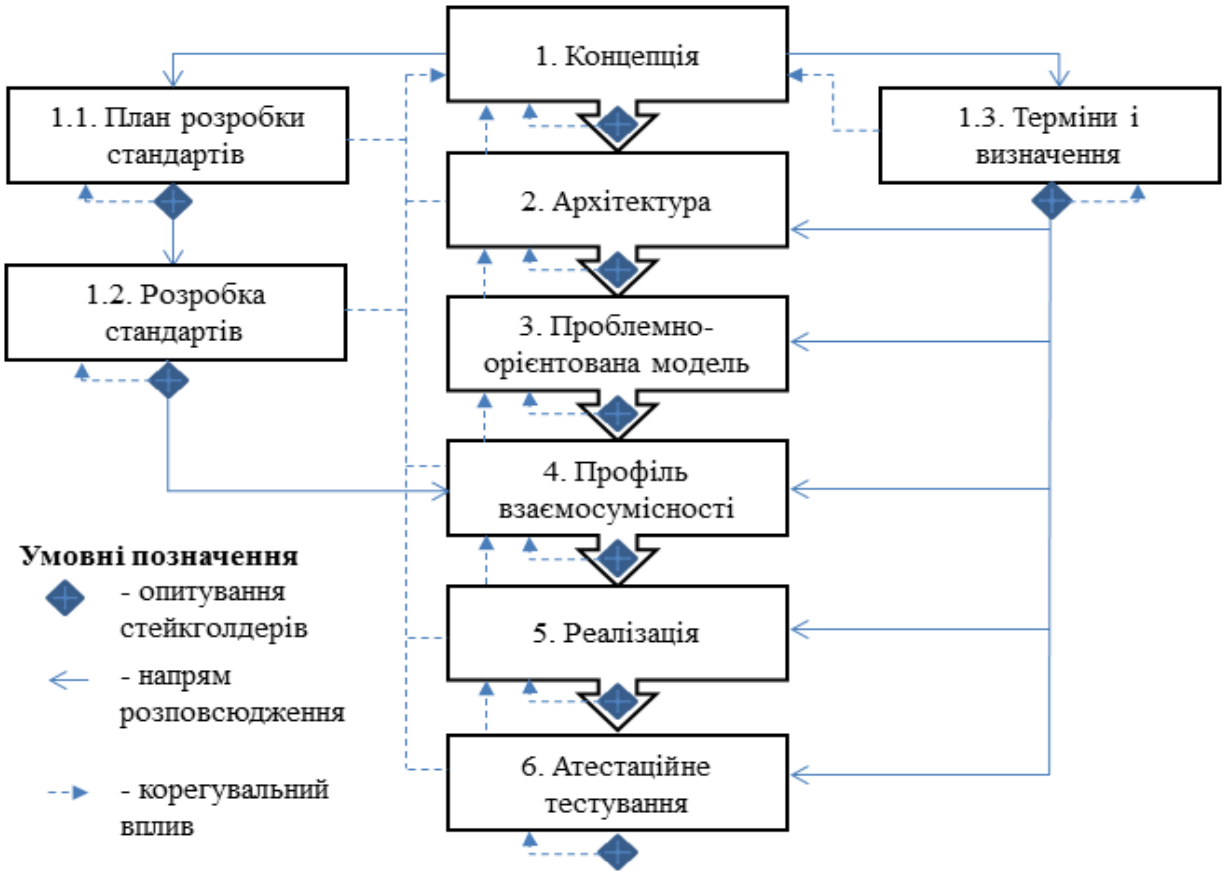


Рисунок 2. Основні етапи забезпечення інтероперабельності ситуаційних центрів України

Загалом забезпечення та верифікація інтероперабельності ситуаційного центру слід здійснювати щодо всіх компонентів (підсистем та елементів) надсистем, що мають зовнішні зв'язки із цими системами на правовому, організаційному, семантичному та технічному рівнях.

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Таблиця 1. Рівні оцінювання інтероперабельності

№ рівня	Рівні сумісності	Опис
1	Відсутній	Взаємодія відсутня. Інтероперабельність неможлива та не планується.
2	Мінімальний	Кожна із систем має індивідуальну архітектуру. Інтероперабельність реалізується через специфічні процедури або за тимчасовою схемою.
3	Помірний	Заходів щодо поліпшення сумісності було вжито, але залишається значний потенціал для подальшого удосконалення інтероперабельності.
4	Кваліфікований	Зв'язки інтероперабельні. Відсутні лише деякі чинники повної сумісності.
5	Повна сумісність	Досягнуто максимального рівня інтероперабельності.

Висновок (Conclusion)

У статті досліджено проблематику забезпечення інтероперабельності ситуаційних центрів України як важливої передумови ефективного функціонування системи моніторингу та оцінювання стану воєнної безпеки. Проведений аналіз показав, що ситуаційні центри відіграють ключову роль у формуванні інформаційно-аналітичної підтримки процесів прийняття управлінських рішень у сфері національної безпеки, забезпечуючи збирання, оброблення, аналізування і поширення інформації про стан безпекового середовища. Водночас встановлено, що існуюча мережа ситуаційних центрів характеризується значною технічною, програмною та організаційною гетерогенністю, що ускладнює обмін інформацією між системами та знижує ефективність їхньої взаємодії.

У ході дослідження узагальнено теоретичні підходи до розуміння інтероперабельності інформаційних систем та обґрунтовано доцільність використання багаторівневої моделі забезпечення взаємосумісності, яка охоплює правовий, організаційний, семантичний і технічний рівні взаємодії. Визначено основні чинники, що впливають на рівень інтероперабельності ситуаційних центрів, зокрема відмінності у нормативно-правовому регулюванні, різнорідність інформаційно-комунікаційних технологій, відсутність уніфікованих стандартів обміну даними та недостатню координацію інформаційних процесів між суб'єктами сектору безпеки і оборони.

Обґрунтовано методичний підхід до верифікації інтероперабельності ситуаційних центрів України, який передбачає визначення вимог до взаємосумісності на різних рівнях функціонування систем, експертне оцінювання ступеня їх виконання та розрахунок показників інтероперабельної придатності й релевантності. Запропонована послідовність етапів оцінювання дозволяє визначати рівень інтероперабельності ситуаційного центру, встановлювати потенціал його взаємодії з іншими інформаційними системами та визначати напрями подальшого розвитку.

Рекомендації (Recommendations)

Отримані результати можуть бути використані під час формування та розвитку мережі ситуаційних центрів України, удосконалення системи інформаційно-аналітичного забезпечення державного управління у сфері безпеки і оборони, а також у процесі інтеграції національних інформаційних систем моніторингу безпеки з відповідними системами Європейського Союзу та НАТО. Реалізація запропонованих підходів сприятиме підвищенню ефективності обміну інформацією, покращенню координації між суб'єктами сектору безпеки і оборони та розвитку інтегрованої системи ситуаційної обізнаності держави.

Конфлікт інтересів (Conflict of Interest)

Одним із авторів статті є член редакційної колегії. Для уникнення конфлікту інтересів редакційний процес здійснював Олег Семененко.

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Використані джерела

1. European Commission. (2017). *New European interoperability framework: Promoting seamless services and data flows for European public administrations*. Publications Office of the European Union.
2. Janssen, M., & Estevez, E. (2013). Lean government and platform-based governance: Doing more with less. *Government Information Quarterly, 30*, S1–S8.
3. Turoff, M., Chumer, M., Van de Walle, B., & Yao, X. (2004). The design of a dynamic emergency response management information system. *Journal of Information Technology Theory and Application, 5* (4), 1–36.
4. Bui, T., & Sankaran, S. (2001). Decision support systems for situation management. *Communications of the ACM, 44* (1), 84–90.
5. Chen, D., Doumeingts, G., & Vernadat, F. (2008). Architectures for enterprise integration and interoperability: Past, present and future. *Computers in Industry, 59* (7), 647–659.
6. Vernadat, F. (2010). *Enterprise modeling and integration: Principles and applications*. Chapman & Hall.
7. Peristeras, V., & Tarabanis, K. (2004). *The connection, communication, consolidation, collaboration interoperability framework (C4IF) for information systems interoperability*. In Interoperability of Enterprise Software and Applications (pp. 61–72).
8. Горбулін, В., & Качинський, А. (2010). *Стратегічне планування: вирішення проблем національної безпеки*. НІСД.
9. Даник, Ю., Катеринчук, І., & Пічугін, М. (2016). *Інформаційна безпека держави: теорія та практика*. ЖНАЕУ.
10. *Нацгвардія України стала повноправним членом Асоціації FIEP*. https://nangu.edu.ua/news/38987-nacgvardiya-ukraini-stala-povnopravnim-chlenom-asociacii-fiep.
11. Ігнатьєв, А. М., & Купрієнко, Д. А. (2021). *Модель і методика верифікації інтероперабельності системи моніторингу прикордонної безпеки у контексті євроінтеграції України. Сучасні аспекти науки (с. 19–34)*. Т. IV. колективної моногр. (За ред. Є. О. Романенка, І. В. Жукової). ФОП КАНДИБА Т. П.
12. Осьмак, А. С. (2020). *Механізми забезпечення інтероперабельності сервісної діяльності органів публічної влади*. [Дис. докт. філософії, Національна академія державного управління при Президентові України].

References

1. European Commission. (2017). *New European interoperability framework: Promoting seamless services and data flows for European public administrations.* Publications Office of the European Union.
2. Janssen, M., & Estevez, E. (2013). Lean government and platform-based governance: Doing more with less. *Government Information Quarterly, 30*, S1–S8.
3. Turoff, M., Chumer, M., Van de Walle, B., & Yao, X. (2004). The design of a dynamic emergency response management information system. *Journal of Information Technology Theory and Application, 5* (4), 1–36.
4. Bui, T., & Sankaran, S. (2001). Decision support systems for situation management. *Communications of the ACM, 44* (1), 84–90.
5. Chen, D., Doumeingts, G., & Vernadat, F. (2008). Architectures for enterprise integration and interoperability: Past, present and future. *Computers in Industry, 59* (7), 647–659.
6. Vernadat, F. (2010). *Enterprise modeling and integration: Principles and applications.* Chapman & Hall.
7. Peristeras, V., & Tarabanis, K. (2004). *The connection, communication, consolidation,*

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

collaboration interoperability framework (C4IF) for information systems interoperability. In Interoperability of Enterprise Software and Applications (pp. 61–72).
8. Horbulin, V., & Kachynskyi, A. (2010). *Stratehichne planuvannia: vyrishennia problem natsionalnoi bezpeky.* NISD.
9. Danyk, Yu., Katerynchuk, I., & Pichuhin, M. (2016). *Informatsiina bezpeka derzhavy: teoriia ta praktyka.* ZhNAEU.
10. *Natshvardiia Ukrainy stala povnopravnym chlenom Asotsiatsii FIEP*. https://nangu.edu.ua/news/38987-nacgvardiya-ukraini-stala-povnopravnim-chlenom-asociacii-fiep.
11. Ihnatiev, A. M., & Kupriienko, D. A. (2021). *Model i metodyka veryfikatsii interoperabelnosti systemy monitorynhu prykordonnoi bezpeky u konteksti yevrointehratsii Ukrainy. Suchasni aspekty nauky (s. 19–34).* T. IV kolektyvnoi monohr. (Za red. Ye. O. Romanenka, I. V. Zhukovoi). FOP KANDYBA T. P.
12. Osmak, A. S. (2020). *Mekhanizmy zabezpechennia interoperabelnosti servisnoi diialnosti orhaniv publichnoi vlady*. [Dys. d-ra filosofii, Natsionalna akademiia derzhavnoho upravlinnia pry Prezydentovi Ukrainy].

Recommendations for Ensuring the Interoperability of Ukraine's Situation Centers

Oleksii Solomitskyi
Doctor Of Military Sciences, Profesor
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

Andrii Ignatiev
Candidate of Technical Sciences in Public Administration, Doctoral Student
National University of Defense of Ukraine
03049, Povitryanykh Sil Avenue, 28, Kyiv, Ukraine
e-mail: ertya1978@gmail.com
ORCID: 0000-0002-0482-6024

Maksym Kudrytskyi
Doctor Of Military Sciences
Head Of Research Department
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl avenue, 28 B, Kyiv, Ukraine
e-mail: kma_13@ukr.net
ORCID: 0000-0003-1554-4732

Volodymyr Koval
Candidate of Military Sciences, Senior Researcher
e-mail: vladimerkoval69@gmail.com
ORCID: 0000-0002-6209-6779

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Denis Molchanov
Researcher
Research Laboratory
Department of Military Training
State University "Kyiv Aviation Institute"
03048, Medova Street, 1, Kyiv, Ukraine
e-mail: mdbua2@gmail.com
ORCID: 0009-0007-9268-2764

Abstract. The relevance of the study is обусловлена by the growing role of situation centers in the system of ensuring Ukraine's national and military security, as well as by the need for their effective interaction in the context of governance digitalization and integration into the European and Euro-Atlantic security space. The extensive network of situation centers operating within various state authorities and the security and defense sector requires coordinated technological, organizational, and legal solutions that enable information exchange, shared use of services, and a common understanding of data. The presence of significant heterogeneity in technical equipment, software, and information resources, as well as the absence of unified approaches to assessing the interoperability level of such systems, necessitates the development of scientifically grounded methodological recommendations for ensuring the interoperability of Ukraine's situation centers at both national and international levels. The study employs a set of general scientific and specialized methods, including system analysis, the structural and functional approach, methods of scientific abstraction and generalization, analysis of regulatory and legal acts and international experience in the functioning of security monitoring information and analytical systems, as well as expert evaluation methods. The methodological basis of the research is the concept of information systems interoperability, which involves the coordination of legal, organizational, semantic, and technical levels of interaction between monitoring systems and situation centers. As a result of the study, an approach to developing a verification model for the interoperability of Ukraine's situation centers has been substantiated. This approach involves the systematization of interoperability requirements at different levels, expert assessment of the compliance of situation centers with these requirements, and the determination of integral indicators of interoperability capability and relevance. A sequence of stages of the methodology for assessing the level of interoperability has been proposed, which makes it possible to quantitatively and qualitatively determine the degree of interaction among situation centers, with the Main Situation Center of Ukraine, and with the information and analytical systems of international partners. The obtained results create the prerequisites for improving the efficiency of the military security monitoring system, enhancing the information support of managerial decision-making, and forming a unified information space in the field of security and defense. The results of the research may be useful for public authorities, entities of the security and defense sector, research institutions, and analytical centers engaged in the development of situation centers, the digital transformation of the security governance system, the creation of security monitoring information and analytical systems, and the interoperability of information systems in the context of Ukraine's integration into the security structures of the EU and NATO.

Keywords: military security, situation centers, interoperability, information systems, military security monitoring, digital governance, information interoperability, security and defense sector, information and analytical systems.

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Received: *January 20, 2026* | **Revisions Requested:** - | **Revision Received:** -
Accepted: *March 5, 2026* | **Published Online:** *April 10, 2026*

Licensed (C) by Creative Commons Attribution International License 4.0 (CC BY-NC-SA)

DOI: 10.62524/msj.2026.4.1.18

Понятійна невизначеність штурмових дій та методичні наслідки для оцінювання ефективності їх ведення

Олександр Колесник
начальник кафедри Управління діями підрозділів
десантно-штурмових військ та морської піхоти
Військова академія (Одеса)
65009, вул. Фонтанська дорога, 10, Одеса, Україна
e-mail: oleks1612@gmail.com
ORCID: 0000-0002-9461-3304

Анотація. Актуальність статті визначається наявністю стійкої термінологічної невпорядкованості у воєнно-наукових працях, бойових статутах і навчально-методичних матеріалах щодо застосування понять “наступ”, “атака”, “штурм” і “штурмові дії”. Унаслідок цього штурмові дії нерідко інтерпретуються через логіку наступу, а “штурм” ототожнюється з повним циклом дій. За сучасних умов насиченості поля бою безпілотними системами, засобами радіоелектронної боротьби, інженерними загородженнями та високоточною зброєю така термінологічна нечіткість безпосередньо впливає на якість планування, організацію взаємодії та обґрунтованість оцінювання результатів дій підрозділів. Метою цієї статті є впорядкування понятійного апарату через науково коректне розмежування “штурму” і “штурмових дій” у співвідношенні з “наступом” і “атакою” та визначенні методичних наслідків термінологічної підміни під час оцінювання ефективності ведення штурмових дій підрозділами та частинами. Методологічну основу становлять порівняльно-логічний аналіз та контент-аналіз національних доктринальних та навчально-методичних документів у зіставленні з доктринальною термінологією Північноатлантичного альянсу, а також сформовано концептуальну структуру штурмових дій для подальшого обґрунтування критеріїв оцінювання. У результатах показано, що наступ доцільно трактувати як ширшу форму ведення бойових дій, у межах якої атака виступає етапом, а штурм – тактично обмеженою фазою безпосереднього оволодіння об’єктом. Автор пропонує розглядати штурмові дії як багатофазовий і компонентний комплекс узгоджених тактичних дій, що охоплює підготовку, дії безпосередньо на об’єкті, закріплення та утримання досягнутого результату. Виявлено механізми підміни понять та показано, що перенесення просторово-часових показників наступу на штурмові дії породжує методичну помилку оцінювання ефективності. Запропоновано коло базових критеріїв ефективності штурмових дій, орієнтованих на досягнутий ефект, ізоляцію об’єкта, управління, збереження боєздатності, синхронізацію вогню та маневру, інженерне й логістичне забезпечення у поєднанні з інформаційною протидією спостереженню противника. Отримані результати формують цілісне методичне підґрунтя для подальшого розвитку інструментарію оцінювання штурмових дій у сучасних умовах бойових дій, при цьому їх практична значущість полягає у можливості використання уточненого понятійного апарату, структурно-фазового подання штурмових дій та обґрунтованих критеріїв ефективності під час розроблення навчально-

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

методичних матеріалів, аналізу бойового досвіду й удосконалення підготовки органів управління та підрозділів.

Ключові слова: штурмові дії, штурм, ефективність, критерії оцінювання, понятійний апарат.

Вступ (Introduction)

Сучасні умови ведення бойових дій характеризуються високою інтенсивністю, динамічністю та значною технологічною насиченістю поля бою, зокрема широким застосуванням безпілотних літальних апаратів, засобів радіоелектронної боротьби, інженерних загороджень і високоточної зброї. За таких умов істотно зростає роль якості управління діями підрозділів, а також коректності понятійного апарату, який визначає логіку планування, зміст підготовки, організацію взаємодії та підхід до оцінювання ефективності бойових дій.

Водночас у наукових працях, бойових статутах і навчально-методичних матеріалах простежується стійка термінологічна невпорядкованість у використанні понять “наступ”, “атака”, “штурм” і “штурмові дії”. Зазначені терміни нерідко подаються як взаємозамінні або розмежовуються непослідовно за рівнем управління, масштабом, часово-просторовими межами та цільовою спрямованістю. Якщо поняття “наступ” і “атака” здебільшого мають відносно усталене трактування, то співвідношення понять “штурм” і “штурмові дії” залишається дискусійним і методично нечітким.

Наслідком такої невизначеності є часткова підміна понять, за якої штурмові дії (ШД) описуються ознаками, притаманними наступу, а штурм помилково ототожнюється із самодостатньою системою дій. Водночас за своєю сутністю штурм є лише окремою фазою у складі ширшого комплексу ШД, що охоплює підготовку, вогневе ураження, маневр, інженерне, логістичне та морально-психологічне забезпечення з подальшим закріпленням досягнутого результату. Додатково підміна понять посилюється тим, що в окремих нормативних визначеннях термін “штурмові дії” подається в дужках як “штурм” або штурм ототожнюється з атакою, що закріплює плутанину вже на рівні дефініцій.

Понятійна невизначеність має не лише теоретичний, а й прикладний характер, оскільки унеможливлює формування обґрунтованої системи оцінювання ефективності штурмових дій. На практиці це проявляється перенесенням непридатних показників із контексту наступу, зокрема темпу або глибини просування, на оцінювання дій штурмових загонів (груп). У результаті виникає суперечність між потребою в точному оцінюванні ефективності штурмових дій та нечіткістю їх понятійного визначення, що зумовлює необхідність науково обґрунтованого розмежування понять “штурм” і “штурмові дії” у співвідношенні з наступом та атакою.

Аналіз національних доктринальних і навчально-методичних джерел свідчить про наявність тенденції до зближення, а подекуди й ототожнення понять “штурм” і “штурмові дії” з категоріями наступального бою, що формує підґрунтя для подальшої термінологічної плутанини під час оцінювання результатів бойових дій. Так, у бойовому статуті ДшБП 3-03.58(59) частина IV, рівень взвод–відділення, ШД подаються як “штурмові дії (штурм)” та визначаються через прорив переднього краю, стрімке просування вперед і захоплення укріпленого пункту або об’єкта, що фактично накладає на ШД логіку наступу й орієнтує оцінювання на показники темпу та просування [1, 2]. Аналогічний підхід простежується і в бойовому статуті ДшБП 3-03.56 частина II, рівень батальйон, де ШД описуються як узгоджені дії штурмового загону (групи), спрямовані на прорив і захоплення об’єктів або населених пунктів у поєднанні з вогневою підтримкою [3].

Структура навчально-методичних матеріалів додатково підсилює зазначену підміну

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

понять. У тактичних публікаціях, присвячених підготовці та веденню ШД, відповідні розділи безпосередньо поєднуються з варіантами ведення наступу в урбанізованій місцевості, що вбудовує штурмові дії у рамки наступального бою та не фіксує межі між етапом (атака, штурм) і комплексом дій (штурмові дії) [4]. Водночас прикладні матеріали з підготовки штурмових груп демонструють фазовий характер практики їх застосування, де після захоплення або зачистки об'єкта підрозділи здійснюють закріплення, організовують оборону та можуть продовжувати ШД на інших об'єктах, передаючи зайняті позиції групам закріплення [5]. Це підтверджує ширший зміст ШД порівняно з одноактним етапом штурму в розрізі їх ведення.

У науково-прикладних джерелах, присвячених сучасним бойовим діям, акцентується увага на організації та підготовці штурмових підрозділів з урахуванням реального бойового досвіду, зокрема набутого Силами безпеки та оборони України під час ведення бойових дій. У цих роботах ШД розглядаються як послідовність взаємопов'язаних фаз, що включають підготовку, ізоляцію об'єкта, безпосереднє захоплення та подальше закріплення результату [6, 7, 8]. Такий підхід узгоджується з фазовою концепцією ШД і корелює з аналітичними матеріалами, сумісними з доктринальними підходами НАТО та США, де "Assault" трактується як кульмінаційна фаза ширшого офензивного процесу, а не як самодостатня форма бойових дій [11, 12].

Подібні висновки містяться й у науково-прикладних дослідженнях. Зокрема у публікації [10], присвяченій веденню бойових дій у міських умовах, штурм розглядається як складова розгорнутого циклу дій, що включає захоплення ключових пунктів, перегрупування, зачистку та формування зовнішнього периметра, а не як самодостатня дія [10]. Наукові публікації щодо застосування штурмових груп у структурі складових Сил безпеки та оборони України також вказують на відсутність розвиненого методичного апарату оцінювання ефективності ШД та визначають перспективним напрямом розроблення методики [8].

Зіставлення національних підходів із доктринальними документами НАТО додатково актуалізує проблему. У термінології НАТО поняття "Assault" у межах дослідження розглядається як кульмінаційна фаза атаки, тоді як "Attack" розглядається як форма наступальних дій, що підтверджує фазовий характер штурму та недоцільність його ототожнення з повним циклом бойових дій [11, 12].

Методологічна основа (Methodological Framework)

Методологічну основу дослідження становить сукупність загальнонаукових і спеціальних методів. Термінологічний і контент-аналіз застосовано для виявлення особливостей трактування понять "наступ", "атака", "штурм" і "штурмові дії" у наукових, нормативних і навчально-методичних джерелах. Порівняльно-логічний аналіз використано для розмежування зазначених категорій за рівнем управління, масштабом, часовими, просторовими межами та цільовою спрямованістю. Метод узагальнення дозволив сформувати методичні висновки щодо наслідків понятійної невизначеності для оцінювання ефективності ШД та обґрунтувати необхідність уточнення їх понятійного апарату.

Результати (Results)

Встановлено, що у воєнно-науковому та доктринальному розумінні наступ є формою бойових дій ширшого рівня, яка охоплює сукупність різнорівневих і різнотипних дій, об'єднаних єдиною тактичною, а переважно – оперативною метою. Його зміст у межах дослідження розглядається не окремою тактичною дією, а загальною логікою досягнення переваги над противником шляхом розгрому його угруповання, захоплення або утримання території та створення умов для подальшого розвитку успіху. Такий підхід закріплений у бойових статутах, зокрема в ДшБП 3-03.56, де наступ розглядається як рамкове поняття, у межах якого організовуються дії підрозділів і частин різного рівня [3].

The Central Research institute
of the Armed Forces of Ukraine
ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Характерними ознаками наступу є просторове розширення, поетапність виконання завдань і залучення значних сил і засобів, що зумовлює відповідний рівень управління та планування. У нормативних документах наступ описується через визначення смуг і рубежів, темпу просування та організації взаємодії між частинами та підрозділами, що безпосередньо пов'язує його з оперативно-тактичним рівнем управління [2, 3, 4]. Відповідно, ключовими показниками ефективності наступу виступають темп і глибина просування, стійкість до протидії противника, а також співвідношення сил і засобів, що є методично обґрунтованим саме для аналізу цього рівня бойових дій.

Обґрунтовано, що у межах наступу можуть застосовуватися різні способи дій, зокрема атака, маневр, обхід, охоплення, а також ШД як інструмент досягнення локального та критичного для противника ефекту. При цьому ШД не є синонімом наступу і не замінюють його, а реалізуються в заданому наступом контексті з метою захоплення або знищення конкретних об'єктів, подолання вузлів опору чи прориву підготовленої ділянки оборони противника [5]. Перенесення ознак і критеріїв оцінювання наступу безпосередньо на ШД ігнорує відмінність між логікою наступу та системою узгоджених тактичних дій, що зумовлює методичні помилки під час аналізу ефективності ШД.

У бойових статутах поняття "атака" визначається як етап наступального бою, який полягає у стрімкому просуванні підрозділів у бойовому порядку в поєднанні з вогнем усіх наявних вогневих засобів з метою знищення противника [1, 2]. Таке трактування чітко фіксує атаку як фазу наступальних дій, а не як самостійну систему бойових дій.

Встановлено, що атака має чітко окреслені часові та просторові межі й реалізується лише після створення відповідних умов. У нормативних документах наголошується, що її успіх залежить від ефективності вогневої підготовки, організації взаємодії, стійкості управління та здатності підрозділів підтримувати заданий темп під вогнем противника [2, 3]. Водночас вона не охоплює повного спектру заходів, пов'язаних із підготовкою району, ізоляцією противника та закріпленням досягнутого результату.

У контексті ШД, атака може розглядатися лише як один із елементів їх структури, призначений для безпосереднього зближення з противником і ураження визначеного об'єкта. Тактичні публікації підкреслюють, що під час дій у населених пунктах або на підготовлених позиціях, атака, як правило, поєднується зі штурмом і не може бути ефективною без попередньої розвідки, вогневого ураження, інженерного забезпечення та подальшого закріплення результату [4]. Ототожнення понять "атака" і "штурм" або використання атаки як універсального критерію оцінювання ефективності дій штурмових підрозділів є методично некоректним.

Встановлено, що у національних нормативних документах і доктринальних підходах НАТО "штурм" розглядається як тактично обмежена дія з чітко визначеними часовими та просторовими межами, спрямована на безпосереднє захоплення або знищення конкретного об'єкта противника. У бойових статутах "штурм" пов'язується з вирішальною фазою зближення з противником, під час якої основні зусилля зосереджуються на прориві підготовленої оборони, захопленні позиції, будівлі або вузла опору [1]. Аналогічний підхід закріплений у доктринальних документах НАТО, де "Assault" розглядається як кульмінація атаки, тобто завершальна фаза безпосереднього оволодіння об'єктом [11].

З'ясовано, що штурм не є самодостатньою формою бойових дій і реалізується лише за умови попереднього створення сприятливих умов. Національні бойові статути й публікації наголошують на необхідності розвідки, вогневого подавлення противника, організації взаємодії та забезпечення зближення, без яких штурм втрачає ефективність [2, 3]. Подібна логіка простежується і в доктринальних документах НАТО, де "штурм" розглядається як завершальна фаза послідовності офензивних дій, обмежена у часі та просторі [11, 12].

Отже, ефективність ШД безпосередньо залежить від рівня підготовки та послідовної

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

організації штурмових груп, що забезпечує досягнення локального тактичного ефекту на визначеному об'єкті. Цей висновок узгоджується з результатами сучасних науково-прикладних досліджень, у яких підкреслюється роль спеціалізованої підготовки, злагодженості дій та укомплектованості штурмових підрозділів для виконання завдань у складних умовах сучасного бою [7, 8, 9].

Обґрунтовано, що в межах ШД штурм є лише однією з фаз і не охоплює повного цикла тактичних заходів. Тактичні публікації та навчально-методичні матеріали з підготовки штурмових груп демонструють, що після завершення штурму необхідним є закріплення, організація оборони, відбиття контратак і відновлення боєздатності підрозділів, а в окремих випадках – підготовка до проведення подальших ШД у межах того ж району [5].

Автором запропоновано розглядати ШД як комплекс узгоджених тактичних дій частин і підрозділів, спрямованих на досягнення локального та критичного для противника ефекту шляхом захоплення або знищення його ключових об'єктів, дезорганізації системи управління та створення умов для подальшого розвитку наступу. На відміну від одноактного штурму, ШД охоплюють повний цикл заходів і характеризуються багатофазністю, що охоплює повний цикл дій – від створення умов до стабілізації результату [1, 4, 5].

Компонентність ШД полягає у необхідності синхронізованого застосування розвідки, вогневого ураження, маневреності, інженерного, логістичного та морально-психологічного забезпечення, а також стійкого управління. У бойових статутах ДШВ Збройних Сил України наголошується, що ефективність штурмових дій визначається не лише застосуванням штурмових груп, а узгодженістю всіх компонентів у обмеженому просторі й часі [2, 3]. Подібний комплексний підхід закладений і в доктринальних документах НАТО [11].

Оцінювання ШД за результатами окремої фази, зокрема штурму або атаки, є методично некоректним [6]. Навчально-методичні матеріали з підготовки штурмових груп свідчать, що після захоплення об'єкта вирішального значення набувають дії – закріплення, відбиття контратак резервів, відновлення боєздатності та підтримання управління [5]. Доктринальні підходи НАТО, своєю чергою, також орієнтують оцінювання офензивних дій на досягнутий ефект і стійкість результату, а не лише на факт захоплення об'єкта або темп просування [11].

Підміна понять у наукових і навчально-методичних джерелах найчастіше проявляється через дефініційне зближення термінів, структурну підміну та методичну інерцію. У національних бойових публікаціях штурмові дії нерідко визначаються через ознаки наступу або ототожнюються зі штурмом, що формує методичну помилку вже на рівні понятійного апарату [1, 3]. Унаслідок цього багатофазовий характер ШД (підготовка–штурм–закріплення–утримання) залишається поза фокусом аналізу. Таким чином, автор пропонує уточнені наукові визначення базових понять.

Штурм – це обмежені в часі та просторі тактичні дії підрозділів, спрямовані на безпосереднє захоплення або знищення визначеного об'єкта противника в умовах попередньо створених сприятливих умов із рішучим застосуванням вогню, маневру та узгоджених дій елементів бойового порядку.

Штурмові дії – це сукупність узгоджених тактичних дій частин і підрозділів, що проводяться у визначеному районі з метою виявлення, дезорганізації та ураження противника, захоплення або знищення його ключових об'єктів із подальшим закріпленням і утриманням досягнутого результату, створенням сприятливих умов для розвитку наступу.

Для узагальнення викладеного та наочного відображення логіки взаємозв'язку між фазами ШД, місцем атаки та штурму в їх структурі доцільно розглянути узагальнену схему структури ШД, яку представлено на рис. 1

У методологіях оцінювання ефективності бойових дій, зокрема в підходах MoE (Measures of Effectiveness – міри ефективності) та MoP (Measures of Performance – міри виконання), ключового значення набуває коректне формулювання мети дій і очікуваного

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

результату. За інтерпретації ШД у логіці наступу показники MoE зводяться до параметрів просторового розширення (глибина, темп, ширина смуги), тоді як MoP – до процесних характеристик темпу просування [4, 8]. Натомість для оцінювання ШД підрозділів релевантними є інші характеристики, пов'язані з досягненням локального критичного ефекту, ефективністю управління, узгодженістю дій штурмових груп і підрозділів забезпечення, збереженням боєздатності та стійкістю закріплення результату [4, 5, 9].

Для наочного зіставлення відмінностей у підходах до оцінювання ефективності наступу та ШД доцільним є порівняння їх ключових критеріїв і типових методичних помилок, що подано в табл. 1.



Рисунок 1. Структура штурмових дій

Застосування показників, відповідних для наступу, під час аналізу ШД призводить до виникнення метричної помилки, за якої оцінюються не досягнутий ефект і стійкість результату, а окремі характеристики загального процесу. Подібний підхід формує хибні управлінські та навчально-методичні висновки, оскільки ігнорує багатофазовий і компонентний характер ШД, на що вказують як національні доктринальні документи, так і підходи НАТО [3, 5, 11].

Коректне трактування ШД як комплексу узгоджених тактичних дій створює методичну основу для формування системи критеріїв ефективності та їх подальшої формалізації, зокрема із застосуванням AHP (Analytic Hierarchy Process – метод аналізу ієрархій). Застосування AHP є методично доцільним з огляду на потребу ієрархізації критеріїв та врахування чинників сучасного бойового середовища, зокрема динаміки обстановки, стійкості управління, міжвидової взаємодії, обмеженості ресурсів, часових факторів, ризиків, втрат і адаптивності командирів частин та підрозділів.

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Таблиця 1. Порівняння підходів до оцінювання ефективності наступу та штурмових дій (MoE/MoP) і типових метричних помилок

Ознака	Наступ	Штурмові дії
Мета дій	Просторове розширення, розгром противника, захоплення рубежів, районів	Досягнення локального критичного ефекту шляхом захоплення або знищення ключового об'єкта, дезорганізація противника
MoE / MoP	MoE – темп наступу, глибина просування, ширина смуги; MoP – своєчасність просування підрозділів, дотримання часових показників зайняття визначених рубежів, послідовність і безперервність розвитку наступальних дій	MoE – досягнення локального критичного ефекту та створення умов для подальших дій; MoP – своєчасність і узгодженість виконання фаз ШД, ефективність управління, застосування вогневих засобів та інженерного забезпечення, збереження боєздатності під час штурмових дій
Типова метрична помилка	-	Застосування критеріїв наступу (темп, дотримання часових показників зайняття визначених рубежів) для оцінювання штурмових дій

Примітка: показники ефективності подано з урахуванням відмінностей між логікою наступу та багатофазовим характером штурмових дій. MoE (Measures of Effectiveness) відображають досягнення запланованого ефекту, MoP (Measures of Performance) – якість і спосіб ведення дій. Використання показників, характерних для наступу, для оцінювання штурмових дій розглядається як методична помилка.

З урахуванням виявлених методичних обмежень і з метою уникнення перенесення критеріїв, характерних для наступу, на думку автора, доцільним є окреслення кола базових критеріїв, які відображають специфіку ШД як багатофазового та компонентного комплексу тактичних дій. Формування цих критеріїв ґрунтується не на просторових показниках, а на досягнутому ефекті, стійкості управління та узгодженості дій частин і підрозділів у складних умовах бойової обстановки.

До ключових критеріїв ефективності ШД належать: досягнення локального критичного ефекту на об'єкті штурму, ізоляція об'єкта та недопущення підходу резервів, збереження боєздатності штурмових загонів (груп), а також стійкість управління під час ведення ШД. Зазначені критерії безпосередньо відображають здатність підрозділів не лише виконати завдання на визначеному об'єкті, а й зберегти спроможність для подальших дій у складі військової частини.

Важливими складовими ефективності ШД, крім того, виступають синхронізація вогню та маневру, ефективність інженерного забезпечення в умовах інженерних загороджень і фортифікаційного обладнання об'єктів противника, інформаційна перевага та протидія засобам спостереження противника, а також логістичне й медичне забезпечення як чинники стійкості ШД. Сукупність окреслених критеріїв відображає інтегрований характер ШД і взаємозумовленість їх складових у межах єдиного тактичного задуму, створюючи методичну основу для подальшої ієрархізації та формалізації оцінювання ефективності із застосуванням методів багатокритеріального аналізу, зокрема AHP (Analytic Hierarchy Process), що дає змогу враховувати різну вагомість критеріїв залежно від умов обстановки, характеру об'єкта штурму та рівня управління.

Обговорення (Discussion)

Отримані результати підтверджують, що в національних нормативно-доктринальних документах і навчально-методичних матеріалах зберігається тенденція до розмиття меж між поняттями "наступ", "атака", "штурм" і "штурмові дії", що безпосередньо впливає на процес

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

оцінювання результатів бойових дій частин і підрозділів. Зокрема, у бойових статутах ШД часто описуються через ознаки, характерні для наступу, такі як прорив, стрімке просування та захоплення району, що методично орієнтує аналіз ефективності на просторово-часові показники, а не на досягнутий тактичний ефект і стійкість результату. Водночас отримані у дослідженні висновки свідчать, що такий підхід є коректним лише для оцінювання наступу як форми бойових дій, але не відповідає природі ШД як багатофазового комплексу тактичних заходів.

Зіставлення результатів дослідження з доктринальними підходами НАТО підтверджує доцільність авторського розмежування понять. У термінології НАТО чітко розрізняються "*Attack"* як форма офензивних дій і "*Assault"* як її кульмінаційна фаза, обмежена в часі та просторі. Такий підхід концептуально унеможливлює ототожнення штурму з повним циклом дій і не допускає перенесення критеріїв оцінювання наступальних операцій на аналіз ефективності окремої фази або локального бою. Отримані в роботі результати узгоджуються з цією логікою та демонструють, що ШД доцільно розглядати як комплекс взаємопов'язаних фаз і компонентів, а не як варіант або "зменшену копію" наступу.

Встановлено, що ефективність штурмових дій безпосередньо залежить від рівня підготовки та послідовної організації штурмових загонів (груп), що забезпечує досягнення локального тактичного ефекту на визначеному об'єкті. Цей висновок узгоджується з результатами сучасних науково-прикладних досліджень, у яких підкреслюється роль спеціальної підготовки, злагодженості дій та укомплектованості штурмових підрозділів для виконання завдань у складних умовах сучасного бою [7, 8, 9].

Обґрунтований у статті перелік критеріїв ефективності ШД принципово відрізняється від традиційних показників наступу і методично відповідає сучасному характеру бойових дій. На відміну від підходів, орієнтованих на темп і глибину просування, запропоновані критерії акцентують увагу на досягненні локального критичного ефекту, управлінні, збереженні боєздатності та стійкості закріпленого результату. Такий підхід узгоджується з практикою застосування штурмових груп у складних умовах урбанізованої місцевості та підготовленої оборони противника [16], де вирішальним є не швидкість просування, а здатність підрозділу утримати досягнутий результат і продовжити дії в інтересах задуму вищого рівня [14, 15, 17].

З методичної точки зору авторська позиція є більш коректною, оскільки чітко визначає об'єкт оцінювання – саме ШД, як комплекс узгоджених тактичних дій, а не окрему фазу (штурм або атаку). Це дозволяє уникнути так званої метричної помилки, коли для аналізу застосовуються показники, що не відображають реальної ефективності дій у сучасному бойовому середовищі. Крім того, запропонований підхід створює передумови для формалізації оцінювання ефективності ШД із використанням методів багатокритеріального аналізу, зокрема АНР, що відповідає доктринальним вимогам НАТО щодо комплексної оцінки бойових спроможностей.

Таким чином, результати дослідження та їх обговорення свідчать, що уточнення понятійного апарату штурмових дій і методично коректне розмежування їх із наступом, атакою та штурмом не є суто теоретичним завданням, а мають безпосереднє прикладне значення для підготовки командирів, аналізу бойового досвіду та побудови систем оцінювання ефективності дій частин та підрозділів складових Сил безпеки та оборони України.

Висновок (Conclusion)

Отримані результати та їх зіставлення з національними доктринальними положеннями і підходами НАТО свідчать, що проблема співвідношення понять "штурм" і "штурмові дії" з категоріями "наступ" та "атака" має системний характер і виходить за межі суто термінологічної дискусії. Вона безпосередньо впливає на логіку планування бойових дій, аналіз бойового досвіду та формування методик оцінювання ефективності дій підрозділів.

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Узагальнення матеріалів дослідження дозволяє розглядати наступ як форму бойових дій ширшого рівня, у межах якої атака – функція етапу наступальних дій, а штурм – тактично обмежена фаза безпосереднього оволодіння об'єктом. ШД при цьому доцільно інтерпретувати як самостійний комплекс узгоджених тактичних дій багатофазового та компонентного характеру, що охоплює підготовку, штурм, закріплення й утримання досягнутого результату та не зводиться до одноактного захоплення об'єкта.

Ключовим методичним наслідком такого розмежування є усунення підстав для перенесення на ШД критеріїв, релевантних для оцінювання наступу. Ототожнення зазначених понять призводить до метричної помилки, коли ефективність дій оцінюється за показниками темпу або просторового просування, що не відображають реального тактичного ефекту, стійкості результату та боєздатності підрозділів у сучасних умовах бою.

Таким чином, чітке понятійне розмежування штурму і штурмових дій створює необхідне методичне підґрунтя для формування адекватної системи показників ефективності та виконання (MoE/MoP) і забезпечує логічну основу для подальшого розроблення формалізованої методики оцінювання ефективності штурмових дій підрозділів з урахуванням сучасного характеру бойових дій.

Рекомендації (Recommendations)

З урахуванням отриманих результатів перспективним напрямом подальших досліджень може стати розроблення методики оцінювання ефективності ШД частин і підрозділів, що ґрунтується на чіткому й узгодженому понятійному апараті та враховує їх багатофазовий і компонентний характер. Така методика має передбачати формування системи показників MoE та MoP, орієнтованих не на просторово-часові параметри, а на досягнутий тактичний ефект, стійкість результату, ефективність управління та збереження боєздатності підрозділів у процесі виконання завдання та після його завершення.

Методично обґрунтованим є застосування ієрархічних методів підтримки ухвалення рішень для визначення пріоритетності критеріїв і розрахунку їх вагових коефіцієнтів з урахуванням умов обстановки, характеру об'єкта штурму та рівня управління. Подальша апробація запропонованого підходу в навчально-методичних матеріалах, системах підготовки командирів і під час аналізу бойового досвіду створить передумови для підвищення обґрунтованості управлінських рішень та удосконалення практики оцінювання ефективності штурмових дій частин і підрозділів у сучасних умовах бойових дій, а також сприятиме уніфікації підходів до оцінювання ефективності дій штурмових загонів (груп) на різних рівнях управління.

Конфлікт інтересів (Conflict of Interest)

Автор заявляє, що у нього немає конфлікту інтересів.

Використані джерела

1. Командування Десантно-штурмових військ ЗС України спільно з Військовою академією (м. Одеса). (2024). Бойовий статут Десантно-штурмових військ Збройних сил України (частина IV: взвод, відділення)*: ДшБП 3-03.58(59).*
2. Командування Десантно-штурмових військ ЗС України спільно з Військовою академією (м. Одеса). (2024). Бойовий статут Десантно-штурмових військ Збройних сил України (частина III: рота, ротна тактична група)*: ДшБП 3-03.57.*
3. Командування Десантно-штурмових військ ЗС України спільно з Військовою академією (м. Одеса). (2024). Бойовий статут Десантно-штурмових військ Збройних сил України (частина II: батальйон, загін спеціального призначення, батальйонна тактична група)*: ДшБП 3-03.56.*

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

4. Командування Десантно-штурмових військ ЗС України спільно з Національним університетом оборони України (м. Київ). (2024). Бойовий статут Десантно-штурмових військ Збройних сил України (частина І: бригада, полк)*: ДшБП 3-03.55*.
5. Командування підготовки Командування Сухопутних військ ЗС України. (2023). Штурмові дії*: СТКП 7-00(113).01(11).* Тактична публікація.
6. Центр оперативних стандартів і методики підготовки ЗС України спільно з Головним управлінням доктрин та підготовки Генерального штабу ЗС України. (2023). Підготовка штурмових груп (взвод, відділення) до ведення штурмових дій*: методичні матеріали*.
7. Рибчук, О. (2021). Сучасні методики підготовки штурмових підрозділів до виконання бойових завдань. *Зб. наук. пр. Військового інституту Київського нац. ун-ту ім. Тараса Шевченка*. https://znp-vo.nuou.org.ua/article/view/249973
8. Сич, С., & Овчаренко, В. (2023). Рекомендації щодо застосування штурмових груп підрозділів швидкого реагування для виконання завдань за призначенням. *Зб. наук. пр. Національної академії Державної прикордонної служби України. Серія: Військові та технічні науки*, *4* (89). 10.32453/3.v89i4.1282.
9. Kolesnyk, O., & Nashyvochnikov, O. (2024). Training of units of a separate airborne assault brigade for assault operations: problematic issues and ways to solve them. *Military Science Journal*, *2* (3). https://doi.org/10.62524/msj.2024.2.3.09.
10. Шульман, О. (2020). Особливості дій штурмових груп у населених пунктах: досвід воєнних конфліктів на Близькому Сході. *АрміяInform*. https://armyinform.com.ua/2020/12/16/osoblyvosti-dij-shturmovyh-grup-u-naselenyh-punktah-dosvid-voyennyh-konfliktiv-na-blyzkomu-shodi/
11. NATO Standardization Office. (2020). *NATO Glossary of Terms and Definitions (AAP-06).*
12. Department of the Army (USA). (2017). *FM 3-0 Operations*.
13. Лобода, Ю., & Богайчук, В. (2022). Аналіз праць західних військових теоретиків про підготовку та ведення штурмових дій у місті малими підрозділами сухопутних військ. *Вісник Національного ун-ту оборони України, 66* (2), 64–70. https://doi.org/10.33099/2617-6858-2022-66-2-64-70
14. Anderson, M. M. (2023). *Decided among the cities*. Modern War Institute. https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MJ-23/Decided-among-the-Cities/Anderson-Decide-among-the-Cities-UA.pdf
15. Fiore, N. (2020). *A case study of urban battle during large-scale combat operations*. Military Review. https://mwi.westpoint.edu/urban-warfare-case-study-7-second-battle-of-fallujah/
16. RAND Corporation. (2005). *Urban operations training strategy for America's joint force*. https://www.rand.org/content/dam/rand/pubs/monographs/2006/RAND_MG439.pdf
17. U.S. Army University Press. (1999). *Sharp corners: Urban operations at century's end*. https://www.armyupress.army.mil/Portals/7/combat-studies-institute/csi-books/SharpCorners.pdf

References

1. Air Assault Forces Command of the Armed Forces of Ukraine. (2024). *Combat regulations of the Air Assault Forces of the Armed Forces of Ukraine (Part IV: Platoon, squad), DShBP 3-03.58(59).* Air Assault Forces Command of the Armed Forces of Ukraine in cooperation with the Military Academy (Odesa).
2. Air Assault Forces Command of the Armed Forces of Ukraine. (2024). *Combat regulations of the Air Assault Forces of the Armed Forces of Ukraine (Part III: Company, company tactical group), DShBP 3-03.57.* Air Assault Forces Command of the Armed Forces of Ukraine in cooperation with the Military Academy (Odesa).

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

3. Air Assault Forces Command of the Armed Forces of Ukraine. (2024). *Combat regulations of the Air Assault Forces of the Armed Forces of Ukraine (Part II: Battalion, special task detachment, battalion tactical group), DShBP 3-03.56.* Air Assault Forces Command of the Armed Forces of Ukraine in cooperation with the Military Academy (Odesa).
4. Air Assault Forces Command of the Armed Forces of Ukraine. (2024). *Combat regulations of the Air Assault Forces of the Armed Forces of Ukraine (Part I: Brigade, regiment), DShBP 3-03.55.* Air Assault Forces Command of the Armed Forces of Ukraine in cooperation with the National Defence University of Ukraine (Kyiv).
5. Training Command of the Ground Forces of the Armed Forces of Ukraine. (2023). *Tactical publication: Assault actions, STKP 7-00(113).01(11).* Training Command of the Ground Forces of the Armed Forces of Ukraine.
6. Center for Operational Standards and Training Methodology of the Armed Forces of Ukraine. (2023). *Preparation of assault groups (platoon, squad) for conducting assault actions: Methodological materials.* Center for Operational Standards and Training Methodology of the Armed Forces of Ukraine in cooperation with the Main Directorate of Doctrines and Training of the General Staff of the Armed Forces of Ukraine.
7. Rybchuk, O. (2021). Modern methods of training assault units for the execution of combat tasks. *Collection of Scientific Papers of the Military Institute of Taras Shevchenko National University of Kyiv.* https://znp-vo.nuou.org.ua/article/view/249973
8. Sych, S., & Ovcharenko, V. (2023). Recommendations on the use of assault groups of rapid response units for mission execution. *Collection of Scientific Papers of the National Academy of the State Border Guard Service of Ukraine: Military and Technical Sciences*, *4* (89). https://doi.org/10.32453/3.v89i4.1282
9. Kolesnyk, O., & Nashyvochnikov, O. (2024). Training of units of a separate airborne assault brigade for assault operations: Problematic issues and ways to solve them. *Military Science Journal*, *2* (3). https://doi.org/10.62524/msj.2024.2.3.09
10. Shulman, O. (2020). Peculiarities of assault group actions in populated areas: Experience of armed conflicts in the Middle East. *ArmiiaInform.* https://armyinform.com.ua/2020/12/16/osoblyvosti-dij-shturmovyh-grup-u-naselenyh-punktah-dosvid-voyennyh-konfliktiv-na-blyzkomu-shodi/
11. NATO Standardization Office. (2020). *NATO glossary of terms and definitions (AAP-06).*
12. Department of the Army. (2017). *FM 3-0: Operations.*
13. Loboda, Y., & Bohaichuk, V. (2022). Analysis of works by Western military theorists on the preparation and conduct of assault actions in urban areas by small land forces units. *Bulletin of the National Defence University of Ukraine*, *66* (2), 64–70. https://doi.org/10.33099/2617-6858-2022-66-2-64-70
14. Anderson, M. M. (2023). *Decided among the cities. Military Review.* https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MJ-23/Decided-among-the-Cities/Anderson-Decide-among-the-Cities-UA.pdf
15. Fiore, N. (2020). *A case study of urban battle during large-scale combat operations. Military Review.* https://mwi.westpoint.edu/urban-warfare-case-study-7-second-battle-of-fallujah/
16. RAND Corporation. (2005). *Urban operations training strategy for America's joint force.* https://www.rand.org/content/dam/rand/pubs/monographs/2006/RAND_MG439.pdf
17. U.S. Army University Press. (1999). *Sharp corners: Urban operations at century's end.* https://www.armyupress.army.mil/Portals/7/combat-studies-institute/csi-books/SharpCorners.pdf

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Conceptual uncertainty of assault actions and methodological implications for assessing their effectiveness

Oleksandr Kolesnyk
Head of the Department
Military Academy (Odesa)
65009, Fontanska Road, 10, Odesa, Ukraine
e-mail: oleks1612@gmail.com
ORCID: 0000-0002-9461-3304

Abstract. The relevance of this article stems from the persistent terminological inconsistency present in military-scientific research, combat manuals, and training and methodological materials regarding the use of the term's *offensive, attack, assault,* and *assault actions*. As a consequence, assault actions are frequently interpreted through the logic of an offensive, while *assault* is erroneously equated with the complete cycle of actions. Under contemporary conditions-characterized by a battlefield saturated with unmanned systems, electronic warfare assets, engineer obstacles, and precision-guided weapons-such terminological ambiguity directly affects the quality of planning, the organization of coordination, and the soundness of assessing the results of unit actions. The purpose of this article is to systematize the conceptual framework through a scientifically sound differentiation between assault and assault actions in relation to offensive and attack, as well as to identify the methodological consequences of terminological substitution in the assessment of the effectiveness of conducting assault actions by units and formations. The methodological framework is based on comparative-logical analysis and content analysis of national doctrinal and training-methodological documents in comparison with the doctrinal terminology of the North Atlantic Alliance. In addition, a conceptual structure of assault actions is developed to further substantiate the criteria for evaluating their effectiveness. The results demonstrate that an offensive should be interpreted as a broader form of conducting combat actions, within which an attack functions as a stage, while assault constitutes a tactically limited phase of the direct seizure of an objective. The author proposes to consider assault actions as a multi-phase and component-based complex of coordinated tactical actions encompassing preparation, actions directly at the objective, consolidation, and retention of the achieved result. Mechanisms of terminological substitution are identified, and it is shown that transferring spatial and temporal indicators of an offensive to assault actions generates a methodological error in effectiveness assessment. A set of core criteria for assessing the effectiveness of assault actions is proposed, oriented toward the achieved effect, isolation of the objective, command and control, preservation of combat capability, synchronization of fire and maneuver, engineer and logistical support, combined with information countermeasures against enemy surveillance. The obtained results form an integrated methodological basis for the further development of tools for assessing assault actions under contemporary combat conditions. Their practical significance lies in the applicability of the refined conceptual framework, the structural-phase representation of assault actions, and the substantiated effectiveness criteria in the development of training and methodological materials, the analysis of combat experience, and the improvement of the training of command-and-control elements and subordinate units.

Keywords: assault actions, assault, effectiveness, evaluation criteria, conceptual framework.

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Received: *September 11, 2025* | **Revisions Requested:** - | **Revision Received:** -
Accepted: *December 1, 2025* | **Published Online:** *April 10, 2026*

Licensed (C) by Creative Commons Attribution International License 4.0 (CC BY-NC-SA)

DOI: 10.62524/msj.2026.4.1.19

Проблемні питання оборонного менеджменту: організаційно-правовий аспект

Володимир Дідіченко
кандидат військових наук, 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

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

Ярослав Янковий
ад'юнкт кафедри інформаційної боротьби
Інститут стратегічних комунікацій
Національний університет оборони України
03049, проспект Повітряних Сил, 28, Київ, Україна
e-mail: ya.yankovyi@gmail.com
ORCID: 0009-0007-1718-3607

Дмитро Рибак
старший викладач кафедри територіальної оборони
Інститут державного військового управління
Національний університет оборони України
03049, проспект Повітряних Сил, 28, Київ, Україна
e-mail: rybak.dima@ukr.net
ORCID: 0009-0005-4239-2131

Денис Череп
молодший науковий співробітник
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: dcherep03@gmail.com
ORCID: 0009-0005-9327-1022

Анотація. Актуальність статті зумовлена потребою у всебічному аналізі проблем і протиріч організаційно-правового аспекту оборонного менеджменту України, що набули

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

особливого значення в умовах широкомасштабної агресії. Ефективність управління оборонними ресурсами, прозорість планування і підзвітності, а також узгодженість дій органів сектору безпеки і оборони визначають стійкість держави. Метою статті є визначення ключових проблем організаційно-правового забезпечення оборонного менеджменту, аналіз їхнього впливу на функціонування сектору безпеки і оборони та окреслення шляхів удосконалення відповідно до міжнародних стандартів. Методологічна основа ґрунтується на поєднанні історико-правового, інституційного, системного та порівняльного аналізу. Результати дослідження засвідчили, що, попри сформовані базові механізми, війна виявила низку проблем: складність міжвідомчої координації, прогалини у законодавстві, дисбаланс між прозорістю та секретністю, кадрові й організаційні труднощі, слабкість оборонно-промислового комплексу. Водночас, воєнний досвід став каталізатором трансформацій – реформування оборонних закупівель, цифровізації управління, розширення парламентського і громадського контролю. Установлено, що підвищення ефективності оборонного менеджменту потребує завершення інституціоналізації реформ за стандартами НАТО, посилення цивільного контролю, удосконалення законодавства з урахуванням уроків війни, модернізації мобілізаційної системи та розвитку кадрового потенціалу. Практичне значення результатів полягає у можливості їх використання Міністерством оборони, Генеральним штабом Збройних Сил України та іншими структурами сектору безпеки і оборони, а також у підготовці фахівців у сфері оборонного менеджменту. Перспективними напрямами подальших досліджень є оцінювання ролі організаційно-правових механізмів у післявоєнному відновленні та інтеграції України до євроатлантичного простору.

Ключові слова: оборонний менеджмент, організаційно-правове забезпечення, демократичний цивільний контроль, сектор безпеки і оборони, управління ресурсами, обороноздатність, національна безпека.

Вступ (Introduction)

Оборонний менеджмент є важливим елементом національної безпеки держави, забезпечення її обороноздатності [1]. Особливо актуальними стають питання його організаційно-правового забезпечення для України з огляду на необхідність збереження територіальної цілісності та суверенітету держави в умовах широкомасштабної агресії з боку російської федерації.

Оборонний менеджмент полягає в застосуванні сучасних методів менеджменту (планування, організації, керівництва і контролю) для досягнення цілей оборони ефективним і економічним способом [2]. Він розглядає оборону як “суспільне благо”, яке держава має забезпечувати максимально результативно. Звідси виникає потреба у запровадженні найкращих управлінських практик у діяльність оборонних інституцій, щоб підвищити їхню ефективність та підзвітність суспільству [3]. Отже, організаційно-правовий аспект оборонного менеджменту – це сфера, у якій управлінські рішення в обороні спираються на чітко визначену систему органів та належну нормативно-правову базу і відображають, яким чином за допомогою законів і структур влади держава організовує керівництво обороною.

Методологічна основа (Methodological Framework)

Методологічна основа дослідження оборонного менеджменту України ґрунтується на комплексному підході, що поєднує інституційно-правовий, системний та порівняльний аналіз. У статті використано методи історико-правового аналізу для вивчення еволюції нормативної бази оборонного управління, а також інституційний підхід, що дозволяє розкрити роль державних органів у процесі ухвалення рішень у секторі безпеки й оборони.

Важливим елементом методології є застосування системного аналізу, який дає

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

можливість розглядати оборонний менеджмент як багаторівневу систему, що функціонує на стратегічному, оперативному та тактичному рівнях (Букур-Марку, Г., Флурі, Ф., & Тагарєв, Т.). При цьому оборонний менеджмент трактується не лише як управлінська діяльність у військовій сфері, а й як частина державного управління, підпорядкована принципам належного врядування, прозорості та демократичного цивільного контролю (Закон України "Про національну безпеку України", 2018).

Для обґрунтування організаційно-правових механізмів використано нормативно-правовий аналіз положень Конституції України, базових законів ("Про оборону України", "Про мобілізаційну підготовку та мобілізацію", "Про правовий режим воєнного стану", "Про основи національного спротиву"), а також підзаконних актів та доктринальних документів, що визначають архітектуру сектору безпеки та оборони. Такий підхід дає змогу простежити взаємозв'язок між законодавчими нормами і практичною реалізацією оборонної політики (Буртянський, П., 2018; Ivanova, V., & Rudolph, J., 2025).

Методологічний інструментарій також включає порівняльний аналіз досвіду країн – членів НАТО щодо впровадження системи оборонного планування, програмування, бюджетування та виконання (ППБВ), що нині імплементується в Україні (Гайдер, С., 2024). Це дозволяє визначити відповідність українських реформ міжнародним стандартам та окреслити напрями їх подальшої інституціоналізації.

Крім того, у дослідженні застосовано структурно-функціональний підхід, який дає змогу оцінити ефективність взаємодії органів управління обороною та виявити існуючі організаційно-правові протиріччя ("Судово-юридична газета", 2025). Застосування цього підходу уможливлює розроблення практичних рекомендацій щодо усунення прогалин у нормативній базі, посилення координації між суб'єктами сектору безпеки й оборони, підвищення прозорості та підзвітності процесів.

Отже, методологія дослідження інтегрує історико-правовий, системний, інституційний, порівняльний та структурно-функціональний підходи. Їх поєднання забезпечує всебічність аналізу та дозволяє сформулювати науково обґрунтовані висновки і практичні рекомендації, спрямовані на вдосконалення організаційно-правових механізмів оборонного менеджменту України.

Результати і обговорення (Results and Discussions)

Оборонний менеджмент є спеціальною сферою державного управління, що полягає в реалізації оборонної політики на практиці шляхом ефективної організації сил і засобів для забезпечення воєнної безпеки держави. У науковій літературі немає єдиного загальноприйнятого визначення цього поняття. Як зазначають західні дослідники, оборонний менеджмент "інкапсулює ідею про те, що оборонним організаціям необхідно втілювати оборонну політику в життя, розробляючи для цього адекватні та стійкі механізми планування, системи забезпечення та інфраструктуру" [1]. Тобто оборонний менеджмент можна розуміти як науку і практику управління оборонною сферою, що охоплює функції планування, організації, керівництва (командування) та контролю в рамках сектору безпеки і оборони України (СБіО України).

Важливою особливістю сучасного розуміння оборонного менеджменту є його зв'язок із принципами демократичного цивільного контролю та належного врядування у СБіО України. Ефективне управління обороною має здійснюватися під демократичним наглядом суспільства і обраних інституцій. Згідно з національними концепціями ефективний менеджмент у сфері оборони базується на засадах демократичного цивільного контролю, інших євроатлантичних принципах і стандартах, інноваційних рішеннях та сучасних підходах [2]. Отже, **теоретичною основою** оборонного менеджменту є поєднання принципів військового керівництва з принципами публічного управління та права: забезпечення обороноздатності держави має

відбуватися інституційно впорядкованими методами, підзвітно та відповідно до закону.

Оборонний менеджмент охоплює стратегічний, оперативний і тактичний рівні управління СБіО України. На стратегічному рівні йдеться про формування оборонної політики, планування розвитку сил оборони та ресурсне забезпечення цієї політики. На цьому рівні керівництво здійснюють вищі державні органи (керівництво держави, уряду, сектору оборони). На оперативному і тактичному рівнях управління реалізується безпосередньо у діяльності військового командування – у плануванні й проведенні воєнних операцій, керівництві військами, забезпеченні їх необхідними ресурсами та координації дій підрозділів. Оборонний менеджмент, таким чином, є багаторівневою системою, де організаційно-правові механізми відіграють ключову роль у тому, щоб усі рівні – від стратегічного планування до роботи конкретних військових частин – діяли узгоджено і результативно.

Організаційно-правовий аспект оборонного менеджменту об'єднує дві нерозривно пов'язані складові: організаційну (інституційну) та правову (нормативну) (рис. 1).



Рисунок 1. Складові організаційно-правового аспекту оборонного менеджменту

Організаційна компонента оборонного менеджменту охоплює структуру та механізми функціонування системи оборонного управління. До неї належать:

• ***Суб'єкти управління обороною*** – органи державної влади та військового керівництва, наділені відповідними функціями (Президент України, Рада національної безпеки і оборони України, Міністерство оборони України, Генеральний штаб ЗС України, командування видів військ, інші складові сил оборони, органи сектору безпеки тощо) [2, 3].

• ***Організаційна структура*** – ієрархія підпорядкованості та взаємодії між цими суб'єктами, розподіл задач між рівнями стратегічного, оперативного і тактичного керівництва.

• ***Процеси та процедури управління*** – системи оборонного планування, бюджетування, управління ресурсами, кадрового менеджменту, системи зв'язку і координації між суб'єктами тощо.

Правова компонента – сукупність норм і правил, що встановлюють рамки діяльності згаданих організаційних структур. Вона містить:

• ***Конституційні норми.***

• ***Законодавчі акти парламенту, які регулюють основи національної безпеки і оборони.***

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

• ***Підзаконні акти та доктринальні документи.***

• ***Внутрішні нормативні акти військового управління***, що регламентують повсякденне управління військовими організаціями.

Отже, організаційна компонента визначає: хто і як керує обороною, а правова – на підставі яких норм і правил здійснюється це керівництво (рис. 2).

Система управління обороною України має складну багатокомпонентну структуру, закріплену в законодавстві та розподілі повноважень між різними органами влади. Повноваження, функції та завдання суб'єктів управління обороною України визначаються Конституцією України та відповідними законами України [2, 3].

Організаційна компонента	Правова компонента
Система органів управління обороною (державні органи, військові структури)	Система нормативно-правових актів (закони, укази, накази, стандарти)
Структура підпорядкованості, горизонтальні та вертикальні зв'язки	Розподіл повноважень і завдань, закріплений законодавчо
Кадровий склад органів, посадові інститути (міністр, начальник Генштабу)	Правовий статус посадових осіб та органів (компетенція, відповідальність)
Процеси планування, координації, контролю (механізми управління)	Процедури та порядки, затверджені нормативно (плани, інструкції, стандарти)
Матеріальні та людські ресурси управлінського апарату	Фінансово-правові основи забезпечення управління (бюджет, закупівлі за законом)

Рисунок 2. Схематичне порівняння двох компонент організаційно-правового аспекту оборонного менеджменту

До складу сил оборони України, крім ЗС України, входять інші військові формування та правоохоронні органи, зокрема Національна гвардія України (НГ України), Державна прикордонна служба (ДПС України), Служба безпеки України (СБ України), Державна служба спеціального зв'язку та захисту інформації (ДССЗтаЗІ України) тощо. У мирний час ці відомства виконують притаманні їм функції окремо. В особливий період (під час воєнного стану, війни) для стратегічного керівництва всіма силами оборони може створюватися особливий орган – Ставка Верховного Головнокомандувача [3].

З метою територіальної оборони держави та залучення громадян до захисту країни( ) в Україні запроваджено нові організаційно-правові інститути. З 1 січня 2022 року набув чинності Закон України "Про основи національного спротиву", який створив систему територіальної оборони та руху національного спротиву [4]. У межах ЗС України було сформовано Сили територіальної оборони (СТрО) – окремий рід військ, розгорнутий у кожній області, що комплектується резервістами і добровольцями для охорони та оборони визначених територій. Крім того, законом передбачено можливість утворення добровольчих формувань територіальних громад із числа цивільних громадян для участі в територіальній обороні. Організаційно СТрО підпорядковані безпосередньо командуванню ЗС України, тобто входять до єдиної вертикалі військового управління, хоча тісно взаємодіють з місцевими військовими адміністраціями. Такий правовий механізм дозволив легалізувати та впорядкувати участь добровольців у обороні, уникнути хаотичного формування загонів поза державною підпорядкованістю, як це частково було у 2014 році.

Система оборонного планування і ресурсного забезпечення в Україні також закріплена законодавчо та поступово реформується відповідно до натовських стандартів. Важливим прогресом

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

стало впровадження системи планування, програмування, бюджетування та виконання (ППБВ), яка використовується в країнах НАТО. Із 2020 року в Міністерстві оборони за підтримки іноземних радників запущено проєкт трансформації оборонного менеджменту, який має на меті перейти до багаторічного оборонного планування з обґрунтуванням бюджетних запитів за програмами і результатами [6]. Це означає, що Україна організаційно і нормативно переходить на стандарти оборонного планування, прийняті в НАТО, що забезпечить більш прозоре й ефективне використання ресурсів та взаємосумісність планових документів.

Нормативно-правову базу функціонування оборонного сектору України складає ціла система законів та підзаконних актів. Ключовими законами є: Закон "Про оборону України" (1991, із численними змінами), який визначає основи оборони держави, структуру воєнного командування, правовий режим воєнного стану і повноваження органів влади; Закон "Про національну безпеку України" (2018), що встановлює архітектуру сектору безпеки і оборони та механізми демократичного цивільного контролю; Закон "Про мобілізаційну підготовку та мобілізацію" (1993, нова редакція 2005) – регулює питання мобілізації людських і матеріальних ресурсів; Закон "Про правовий режим воєнного стану" (2015) – визначає порядок запровадження воєнного стану та особливі повноваження в його умовах; Закон "Про основи національного спротиву" (2021) – про територіальну оборону та підготовку населення до оборони; Закон "Про державні закупівлі" і спеціальний Закон "Про оборонні закупівлі" (2020) – регулюють порядок закупівель товарів і послуг для оборони (державне оборонне замовлення) тощо.

Отже, в Україні сформовано базові організаційно-правові механізми оборонного менеджменту. Однак під час практичної реалізації цих механізмів у ході широкомасштабної російсько-української війни виявлено низку проблем і протиріч організаційно-правового характеру. До основних з них належать (рис. 3):

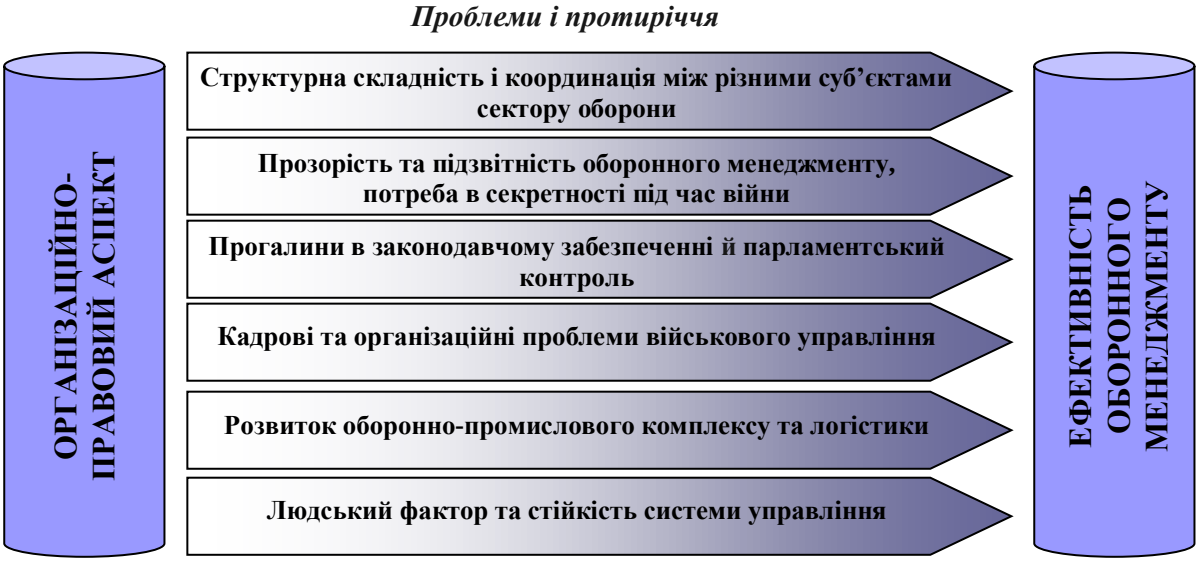


Рисунок 3. Проблеми і протиріччя організаційно-правового характеру оборонного менеджменту в Україні

1. Структурна складність і координація між різними суб'єктами сектору оборони. Сектор безпеки і оборони охоплює багато відомств (ЗС України, Нацгвардія, прикордонники, СБУ, МВС тощо), і хоча закон визначає їхню загальну взаємодію, на практиці узгодженість дій іноді ускладнена. Історично склалося, що кожне силове відомство мало власну вертикаль підпорядкування, і під час бойових дій 2014–2015 рр. це призводило до проблем. Це вказало на системну проблему: відсутність єдиного керівництва всіма силами оборони під час

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

спільних операцій. Для усунення цієї прогалини законодавчо запроваджено посаду Командувача об'єднаних сил та механізм підпорядкування йому підрозділів інших відомств у особливий період [6].

На початку широкомасштабної війни у лютому 2022 р. знову постало завдання негайно об'єднати під єдиним командуванням ЗС України, НГ України, Національну поліцію (НП), ДПС України, СТрО та інші структури для оборони Києва, Харкова, інших напрямків. Хоч це завдання вдалося виконати завдяки створенню Ставки ВГК і регіональних військових адміністрацій, але певні розбіжності та конкуренція повноважень між відомствами в перші дні війни мали місце.

Отже, проблема міжвідомчої координації залишається актуальною: навіть за наявності правових норм( ) необхідні підзаконні акти, узгоджені плани взаємодії, спільні штаби тощо, аби структура управління реально стала цілісною.

Ще один аспект структурної проблематики – розмежування повноважень та відповідальності всередині самого військового керівництва.

Щодо ролі МО України в оперативному плануванні: за законом МО України формально не займається веденням операцій, але в умовах війни Міністр оборони України активно комунікує із союзниками, координує постачання озброєнь, що безпосередньо впливає на операції. Це потребує чіткої координації між політичним керівництвом і ГШ ЗС України. Отже, потрібне подальше вдосконалення нормативного регулювання взаємодії між МО України та ГШ ЗС України, аби уникнути як дублювання функцій, так і виникнення "сірих зон" відповідальності.

2. Прозорість та підзвітність оборонного менеджменту, потреба в секретності під час війни. Одна з головних суперечностей організаційно-правового характеру – баланс між відкритістю, демократичним контролем в обороні та військовою таємницею, оперативною доцільністю. Оборонна сфера тривалий час залишалася менш прозорою: існувала практика, коли посилання на секретність закупівель або операцій слугувало приводом звільнити МО України від загальних правил прозорості та підзвітності [7].

Широкомасштабна війна загострила цю проблему. З одного боку, величезні обсяги коштів спрямовуються на армію, що вимагає контролю їх використання. З іншого – війна об'єктивно потребує секретності в закупівлях озброєнь, оперативних переміщеннях військ, планах тощо.

3. Прогалини в законодавчому забезпеченні й парламентський контроль. Хоч більшість необхідних законів у сфері оборони ухвалено, деякі напрями досі не мають достатнього правового регулювання або потребують оновлення. Зокрема, критики Закону "Про національну безпеку України" (2018 р.) зазначали, що він залишив чинною стару систему органів безпеки без суттєвої реорганізації [6].

Є сфери (наприклад, волонтерська діяльність, приватні ініціативи в обороні, цифровізація оборони), що швидко еволюціонували під час війни і потребують юридичного закріплення постфактум.

Парламентський контроль над оборонним сектором під час воєнного стану також обмежений об'єктивно (діє цензура, деякі засідання профільного комітету проводяться в закритому режимі).

Для посилення демократичного контролю після війни доведеться наздоганяти згаяне: зокрема, переглянути діяльність тимчасових слідчих комісій ВР України з питань оборони, активізувати Рахункову палату щодо аудитів оборонних закупівель, можливо, створити окремий незалежний орган парламентського контролю за сектором безпеки (на зразок комісій з оборони в США чи комітетів з контролю за розвідкою).

4. Кадрові та організаційні проблеми військового управління. Війна виявила як сильні сторони українського військово-стратегічного управління, так і проблемні місця,

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

пов'язані з людським фактором та організацією роботи штабів. Із позитивного – українське військове керівництво виявило гнучкість і креативність, що дозволило виграти битву за Київ та успішно проводити операції на Харківщині й Херсонщині у 2022 році. Із негативного – з'ясувалось, що система територіальних центрів комплектування та соціальної підтримки (ТЦК та СП), яка відповідає за мобілізацію, була пронизана корупцією й не готова до мобілізації сотень тисяч резервістів.

Для сталого вирішення проблеми необхідно реформувати інституційно цю ланку: перевести ТЦК та СП на нові рейки: наповнити їх якісно новими людьми, частково замінити військових на цивільних менеджерів HR-напряму, впровадити цифровий реєстр військовозобов'язаних для мінімізації контакту людини з чиновником, підвищити зарплати й відповідальність персоналу ТЦК та СП.

5. Розвиток оборонно-промислового комплексу та логістики. Організаційно-правові питання менеджменту оборони передбачають не лише безпосереднє управління військами, а й управління тиловим забезпеченням, оборонною промисловістю. У цій сфері також є проблемні моменти.

Проблеми оборонно-промислового комплексу (ОПК) полягають не лише у формі управління, а й в інтеграції в загальну систему оборонного менеджменту. Війна 2022 р. показала, що українська армія критично залежна від постачання зброї із Заходу, а власне виробництво не покриває потреб. Причини об'єктивні (обмеженість технологій, знищення частини заводів обстрілами), але також і організаційні: довоєнна відсутність достатніх інвестицій в ОПК, повільність прийняття на озброєння нових зразків, бюрократичні перепони для приватних виробників.

Логістика і складське господарство ЗС України – ще один виклик. Тут виникає організаційно-правовий аспект: необхідно врегулювати нормативно нові процеси, внести зміни до положень про облік військового майна, про порядок планування, навчити персонал працювати з новими системами.

6. Людський фактор та стійкість системи управління. Війна – це випробування не тільки законів і структур, а й людей, які ними керують. Українська система оборонного менеджменту показала загалом високу стійкість: ні військово-політичне керівництво, ні органи управління не дезорганізувалися під ударом агресора. Але були й негативні моменти, особливо на початку широкомасштабного вторгнення. Це свідчить про необхідність ще прискіпливішого добору кадрів на керівні посади, перевірки на доброчесність та лояльність. Організаційно слід удосконалити систему кадрового резерву: потрібні дієві механізми ротації, підготовки наступників, щоб критичні посади не залишалися вакантними або зайнятими випадковими особами.

Підсумовуючи, основні проблемні питання оборонного менеджменту України в організаційно-правовому вимірі можна звести до наступного:

- ✧ злагодженість між різними складовими сектору оборони;
- ✧ чіткість і неконфліктність розподілу повноважень;
- ✧ забезпечення прозорості та підзвітності без шкоди боєздатності;
- ✧ своєчасне оновлення нормативної бази відповідно до викликів;
- ✧ боротьба з корупцією та інерцією бюрократії;
- ✧ розвиток спроможностей (кадрових, технічних, промислових) управлінської системи.

Багато з цих проблем стали особливо помітними під час війни, але саме воєнний час і дав поштовх до їхнього розв'язання.

З огляду на виявлені проблеми та набутий досвід, можна запропонувати конкретні кроки для підвищення ефективності оборонного менеджменту України в організаційно-правовій площині (рис. 4).

Ці рекомендації спрямовані на зміцнення як інституційної спроможності системи, так і

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

її підзвітності та гнучкості.

1. Завершення та інституціоналізація реформ управління і планування. Необхідно повністю імплементувати стандарти NATO у структурі військового управління. Зокрема, слід впровадити нову модель оборонного планування ППБВ на постійній основі у всіх структурах МО України та ЗС України (не лише пілотно в окремих видах військ). Це вимагатиме затвердження на рівні закону або постанови Кабінету Міністрів України єдиної методики планування оборонних програм, щоб кожен витрачений бюджетний ресурс був прив'язаний до конкретної програми та очікуваних спроможностей.

2. Посилення демократичного контролю та антикорупційних механізмів. Необхідно мати реальні важелі контролю за оборонним сектором навіть під час дії воєнного стану. Доцільно уже зараз створити при Комітеті ВР України з питань національної безпеки, оборони та розвідки підкомітет з парламентського нагляду, який би в закритому режимі, але регулярно( ) заслуховував звіти МО України. На виконання норми Закону України [2] потрібно ухвалити закон про парламентський контроль над спецслужбами, а також розглянути можливість запровадження інституту омбудсмена з питань оборони – уповноваженого, який опікувався б правами військовослужбовців і питаннями прозорості.



Рисунок 4. Шляхи підвищення ефективності оборонного менеджменту України

3. Удосконалення законодавства з урахуванням уроків війни. Необхідно провести ревізію всіх профільних законів та внести зміни, продиктовані практикою 2022–2025 років. Приміром, Закони України: "Про оборону України" (щодо особливостей функціонування Ставки Верховного Головнокомандувача та її складу), "Про правовий режим воєнного стану" (щодо діяльності військово-цивільних адміністрацій, розмежування їхніх компетенцій з органами місцевого самоврядування), "Про основи національного спротиву" (щодо врегулювання статусу добровольчих формувань після деокупації територій). Слід законодавчо врегулювати волонтерську діяльність в обороні: визначити правовий статус волонтерів, пільги для них, можливості взаємодії з військовими частинами.

4. Реформа системи мобілізації і військового обліку. Потрібно закріпити на

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

законодавчому рівні створення Єдиного державного реєстру військовозобов'язаних, з інтеграцією з Реєстром виборців, демографічним реєстром тощо; оновити Положення про ТЦК та СП, передбачивши там цивільні посади фахівців з рекрутингу, соціальної роботи – тобто фактично трансформувати ТЦК та СП у сучасні HR-агенції для війська.

5. Розвиток кадрового потенціалу і військової освіти. Ефективний оборонний менеджмент потребує висококваліфікованих кадрів – менеджерів, як військових, так і цивільних. Тому слід реформувати систему військової освіти відповідно до стандартів НАТО: запровадити навчальні програми з оборонного менеджменту, логістики, спільного (інтегрованого) командування для офіцерів та державних службовців.

6. Підготовка до післявоєнного переходу. Організаційно-правова система має бути готовою до повоєнної трансформації. Потрібно буде перевести економіку з воєнних рейок, оптимізувати чисельність війська, реінтегрувати ветеранів. Уже зараз слід закладати правові механізми для демобілізації: розробити критерії, черговість звільнення військовослужбовців, систему соціального захисту для них.

7. Підвищення стійкості системи управління до нових загроз. У сучасному світі не лише традиційні військові загрози актуальні. Менеджмент оборони має враховувати кібербезпеку, інформаційні операції, можливі диверсії проти командних пунктів. Тому потрібно розвивати розподілену систему командування (запасні командні пункти, автоматизовані системи управління військами тощо).

8. Залучення громадянського суспільства до розбудови оборонного менеджменту. Українське громадянське суспільство вже продемонструвало високу мотивацію допомагати армії – волонтери, фонди, ініціативи типу "Армія дронів" (спільний проєкт Мінцифри та волонтерів) тощо. Цей потенціал треба інтегрувати в офіційні рамки. Пропонується створити при МО України постійно діючі громадські ради або робочі групи за напрямами (волонтери, IT-спільнота, ветерани, правозахисники), які б безпосередньо комунікували з керівництвом щодо болючих питань.

Насамкінець, варто зазначити, що вдосконалення організаційно-правових аспектів оборонного менеджменту має відбуватися безперервно, у відповідь на динаміку безпекового середовища. Україна фактично проходить пришвидшений шлях трансформації свого сектору оборони – те, на що інші держави витрачали десятиліття, здійснюється за роки чи навіть місяці. Це великий виклик і водночас шанс створити сучасну, ефективну, підзвітну систему оборонного управління, спроможну захистити державу від нинішніх та майбутніх загроз.

Висновок (Conclusion)

Організаційно-правовий аспект оборонного менеджменту України зазнав суттєвих змін протягом останніх років та особливо був випробуваний у період широкомасштабної війни 2022–2025 рр. Теоретичні засади оборонного управління, засновані на демократичному цивільному контролі та системному підході до планування оборони, поступово втілюються в практичні механізми. Україна створила необхідну правову базу для ефективного оборонного менеджменту: визначено ролі та повноваження ключових суб'єктів, запроваджено нові структури, узгоджено процеси планування і ресурсного забезпечення із західними стандартами. У ході війни ця система довела свою життєздатність – військово-політичне керівництво змогло організувати відсіч агресії, мобілізувати всі наявні ресурси та адаптуватися до зовнішніх змін.

Водночас аналіз показує, що є низка проблемних питань та протиріч в організаційно-правовому забезпеченні оборонного менеджменту, які знижують його результативність. Серед них – складність координації різних компонентів сил оборони, необхідність досягнення балансу між секретністю і прозорістю, подолання корупційних ризиків, усунення бюрократичної неефективності в окремих процесах, незавершеність окремих реформ, кадрові

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

виклики. Багато з цих проблем стали особливо очевидними під час війни.

Практичний досвід широкомасштабної війни дав потужний імпульс до змін. Уже здійснено низку невідкладних заходів: реформовано систему оборонних закупівель, розпочато цифровізацію управління, проведено чистку і ротацію кадрів там, де були зловживання. Але для системного вирішення наявних питань потрібні подальші, глибші перетворення – як нормативні, так і організаційні.

Запропоновані шляхи вдосконалення передбачають як заходи негайного характеру (законодавчі зміни, підсилення контролю, доукомплектування структур), так і стратегічні напрями розвитку (розвиток людського потенціалу, післявоєнна трансформація). Реалізувавши ці рекомендації, можна підвищити ефективність, прозорість і гнучкість оборонного менеджменту України.

Україна фактично формує новітній підхід до оборонного менеджменту, який поєднує бойовий досвід та кращі світові стандарти управління. В умовах екзистенційної загрози це надзвичайно складне завдання, але водночас саме війна стала каталізатором для прориву в розвитку сектору оборони. Організаційно-правові зміни, що наразі впроваджуються, закладають фундамент для сильної оборонної інституції, здатної діяти ефективно як у воєнний, так і в мирний час. Удосконалений оборонний менеджмент гарантуватиме високий рівень обороноздатності України у довгостроковій перспективі, слугуватиме стабільності й миру в усьому регіоні.

Рекомендації (Recommendations)

Матеріали статті може бути використано під час планування заходів розвитку Збройних Сил України у повоєнний період. Стаття також може бути корисна науковцям, які займаються проблематикою оборонного менеджменту та воєнної політики, та фахівцям, які причетні до впровадження оборонного менеджменту у Міністерстві оборони України та Збройних Силах України.

Перспективними напрямами подальших досліджень є оцінювання ролі організаційно-правових механізмів у післявоєнному відновленні та інтеграції України до євроатлантичного простору.

Конфлікт інтересів (Conflict of Interest)

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

Використані джерела

1. Букур-Марку, Г., Флурі, Ф., & Тагарєв, Т. (2010). Оборонний менеджмент: ознайомлення. *Женевський центр демократичного контролю над збройними силами (ДКЗС). Geneva Centre for the Democratic Control of Armed Forces. Серія: Менеджмент безпеки та оборони, 1.* https://www.dcaf.ch/sites/default/files/publications/documents/Book_Defense_ukr_final.pdf
2. Верховна Рада України. (2018). Закон України "Про національну безпеку України" № 2469-VIII. *Відомості Верховної Ради України, 31.* https://zakon.rada.gov.ua/laws/show/2469-19#Text
3. Верховна Рада України. (1991). Закон України "Про оборону України" № 1932-XII. *Відомості Верховної Ради України, 9.* https://zakon.rada.gov.ua/laws/show/1932-12#Text
4. Верховна Рада України. (2021). Закон України "Про основи національного спротиву" № 1702-IX. *Відомості Верховної Ради України, 41.* https://zakon.rada.gov.ua/laws/show/1702-20#Text
5. Верховна Рада України. (1993). Закон України *"Про мобілізаційну підготовку та мобілізацію"* № 3543-XII (ред. 2005). https://zakon.rada.gov.ua/laws/show/3543-12

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

6. Буртянський, П. (2018). За лекалами НАТО: що може змінити закон "Про національну безпеку України". *Громадський простір*. https://www.prostir.ua/?blogs=za-lekalamy-nato-scho-mozhe-zminyty-zakon-pro-natsionalnu-bezpeku-ukrajiny
7. Ivanova, V., & Rudolph, J. (2025). Ukraine's Defense Ministry Needs Protection – From Itself. *German Marshall Fund*. https://www.gmfus.org/news/ukraines-defense-ministry-needs-protection-itself
8. Гейдер, С. (2024). *Міноборони і Генштаб ЗС України розпочали новий етап реформи системи оборонного менеджменту.* Міністерство оборони України. https://mod.gov.ua/news/minoboroni-i-genshtab-zs-ukraini-rozpochali-novij-etap-reformi-sistemi-oboronnogo-menedzhmentu
9. Міноборони впроваджує військову версію SAP за стандартами НАТО. (2025). *Судово-юридична газета в Україні*. https://sud.ua/uk/news/ukraine/328943-minoborony-vnedryaet-voennuyu-versiyu-sap-po-standartam-nato

References

1. Bukur-Marcu, G., Fluri, P., & Tagarev, T. (2010). Defense Management: An Introduction. *Geneva Centre for the Democratic Control of Armed Forces (DCAF). Series: Security and Defense Management, 1*. https://www.dcaf.ch/sites/default/files/publications/documents/Book_Defense_ukr_final.pdf
2. Verkhovna Rada of Ukraine. (2018). Law of Ukraine "On National Security of Ukraine" No. 2469-VIII. *Vidomosti of the Verkhovna Rada of Ukraine, 31*. https://zakon.rada.gov.ua/laws/show/2469-19#Text
3. Verkhovna Rada of Ukraine. (1991). Law of Ukraine "On Defense of Ukraine" No. 1932-XII. *Vidomosti of the Verkhovna Rada of Ukraine, 9.* https://zakon.rada.gov.ua/laws/show/1932-12#Text
4. Verkhovna Rada of Ukraine. (2021). Law of Ukraine "On the Fundamentals of National Resistance" No. 1702-IX. *Vidomosti of the Verkhovna Rada of Ukraine, 41*. https://zakon.rada.gov.ua/laws/show/1702-20#Text
5. Verkhovna Rada of Ukraine. (1993). Law of Ukraine *"On Mobilization Preparation and Mobilization"* No. 3543-XII (as amended in 2005). https://zakon.rada.gov.ua/laws/show/3543-12
6. Burtianskyi, P. (2018). According to NATO Templates: What the Law "On National Security of Ukraine" Can Change. *Hromadskyi Prostir.* https://www.prostir.ua/?blogs=za-lekalamy-nato-scho-mozhe-zminyty-zakon-pro-natsionalnu-bezpeku-ukrajiny
7. Ivanova, V., & Rudolph, J. (2025). Ukraine's Defense Ministry Needs Protection – From Itself. *German Marshall Fund.* https://www.gmfus.org/news/ukraines-defense-ministry-needs-protection-itself
8. Haider, S. (2024). *The Ministry of Defense and the General Staff of the Armed Forces of Ukraine Launched a New Stage of Reform of the Defense Management System*. Ministry of Defense of Ukraine. https://mod.gov.ua/news/minoboroni-i-genshtab-zs-ukraini-rozpochali-novij-etap-reformi-sistemi-oboronnogo-menedzhmentu
9. The Ministry of Defense Introduces the Military Version of SAP According to NATO Standards. (2025). *Sudovo-Yurydychna Hazeta v Ukrayini.* https://sud.ua/uk/news/ukraine/328943-minoborony-vnedryaet-voennuyu-versiyu-sap-po-standartam-nato

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Problematic Issues of Defense Management: Organizational and Legal Aspect

Volodymyr Didichenko
Candidate of Military Sciences (PhD in Military Science), 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: DVP1951@ukr.net
ORCID: 0000-0002-0440-2299

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

Yaroslav Yankovyi
Adjunct of the Department of Information Warfare
Institute of Strategic Communications
National Defense University of Ukraine
03049, Povitrianykh Syl Avenue, 28 B, Kyiv, Ukraine
e-mail: ya.yankovyi@gmail.com
ORCID: 0009-0007-1718-3607

Dmytro Rybak
Senior teacher of the Department of Territorial Defense
Institute of State Military Management
National Defence University of Ukraine
03049, Povitroflotskyi Avenue, 28, Kyiv, Ukraine
e-mail: rybak.dima@ukr.net
ORCID: 0009-0005-4239-2131

Denys Cherep
Junior Research Fellow
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl avenue, 28 B, Kyiv, Ukraine
e-mail: dcherep03@gmail.com
ORCID: 0009-0005-9327-1022

Abstract. The relevance of the article is determined by the need for a comprehensive analysis of the problems and contradictions of the organizational and legal aspects of Ukraine's defense management, which have gained particular significance under the conditions of large-scale aggression. The effectiveness of defense resource management, the transparency of planning and accountability, as well as the coherence of actions of the security and defense sector bodies determine the resilience of the state. The purpose of the article is to identify the key problems of the organizational and legal framework of defense management, analyze their impact on the functioning of the security and defense sector, and outline ways for their improvement in accordance with international standards. The methodological basis is grounded in the combination of historical-legal,

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

institutional, systemic, and comparative analyses. The research results indicate that despite the existence of basic mechanisms, the war has revealed a number of issues: the complexity of interagency coordination, legislative gaps, the imbalance between transparency and secrecy, personnel and organizational difficulties, and the weakness of the defense-industrial complex. At the same time, wartime experience has become a catalyst for transformations — the reform of defense procurement, the digitalization of management, and the expansion of parliamentary and public oversight. It has been established that improving the effectiveness of defense management requires the completion of the institutionalization of reforms according to NATO standards, the strengthening of civilian control, the improvement of legislation based on wartime lessons, the modernization of the mobilization system, and the development of human resources. The practical significance of the results lies in their potential use by the Ministry of Defense, the General Staff of the Armed Forces of Ukraine, and other structures of the security and defense sector, as well as in the training of specialists in the field of defense management. Promising directions for further research include assessing the role of organizational and legal mechanisms in post-war recovery and Ukraine's integration into the Euro-Atlantic space.

Keywords: defense management, organizational and legal support, democratic civilian control, security and defense sector, resource management, defense capability, national security.

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Received: *January 12, 2026* | **Revisions Requested:** - | **Revision Received:** -
Accepted: *March 2, 2026* | **Published Online:** *April 10, 2026*

Licensed (C) by Creative Commons Attribution International License 4.0 (CC BY-NC-SA)

DOI: 10.62524/msj.2026.4.1.20

Аналіз впливу хімічної та радіаційної дифузії на організм людини

Артем Карпусь
ад'юнкт
кафедра радіаційного, хімічного, біологічного захисту та цивільної безпеки
Інститут логістики та підтримки військ (сил)
Національний університет оборони України
03049, проспект Повітряних Сил, 28, Київ, Україна
e-mail: karpusark@gmail.com
ORCID: 0009-0003-2406-1924

Алі Кенгерлі
ад'юнкт
кафедра радіаційного, хімічного, біологічного захисту та цивільної безпеки
Інститут логістики та підтримки військ (сил)
Національний університет оборони України
03049, проспект Повітряних Сил, 28, Київ, Україна
e-mail: alikenherli@gmail.com
ORCID: 0009-0005-5794-6221

"Природа діє невидимими частинками".
(*Лукрецій)*

Анотація. Статтю присвячено комплексному дослідженню механізмів хімічної та радіаційної дифузії як ключових чинників ураження людини в умовах сучасних військових конфліктів і техногенних катастроф. Розкрито фізико-математичну сутність дифузійних процесів, що базуються на законах Фіка, й обґрунтовано трансформацію локальних джерел зараження в об'ємні зони контамінації. Метою публікації є детальне дослідження того, як хімічні сполуки та радіоактивні елементи поширюються у навколишньому середовищі та проникають в організм людини, стаючи критичними чинниками ураження під час сучасних військових конфліктів та аварій техногенного характеру. Автори зробили спробу пояснити, як за допомогою математичних законів Фіка визначити фізичну суть того, як невелика хмара газу або локальне місце вибуху перетворюється на масштабну зону зараження. У роботі ставиться завдання проаналізувати реальні приклади застосування іритантів та токсичних речовин, таких як хлор і аміак, що використовуються під час російської агресії проти України для дезорієнтації та витіснення військовослужбовців Збройних Сил України із укріплень. Важливою частиною мети є виявлення слабких місць у сучасному захисному спорядженні, зокрема дослідження того, як молекули отруйних речовин мають змогу проходити крізь фільтри або навіть саму гуму масок протигазів. Детально проаналізовано тактику застосування іритантів (CS, хлоропікрин) та сильнодіючих отруйних речовин (хлор, аміак), що використовуються для дезорієнтації та витіснення особового складу Збройних Сил України із фортифікованих позицій. Особливу увагу приділено фізіологічним аспектам, а саме:

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

трансдермальному проникненню токсинів та хімічним опікам дихальних шляхів. Важливим практичним аспектом дослідження є аналіз критичних недоліків засобів індивідуального захисту, зокрема явища "дифузійного проскоку" крізь фільтри та проникності полімерних матеріалів масок для молекул отруйних речовин. Радіаційний блок дослідження зосереджується на процесах внутрішнього опромінення через інгаляційні та пероральні шляхи. Автор розкриває механізм селективної дифузії радіонуклідів, де ізотопи (Стронцій-90, Йод-131, Цезій-137) заміщують стабільні хімічні елементи в органах-мішенях, спричиняючи радіоліз клітинної води та пошкодження ДНК. Висвітлено як негайні прояви променевої хвороби, так і довгострокові стохастичні наслідки (онкогенез, мутації). Висновки роботи підкреслюють стратегічну значущість моніторингу дифузійних процесів для розроблення сучасних систем захисту. Стаття базується на актуальних даних щодо застосування хімічних сполук під час російської агресії проти України, що робить її критично важливою для фахівців з радіаційного, хімічного та біологічного захисту, військової медицини та цивільної безпеки.

Ключові слова: хімічна та радіаційна дифузія, радіаційне ураження, закони Фіка, іританти, сильнодіючі отруйні речовини.

Вступ (Introduction)

У сучасних геополітичних умовах питання захисту від впливу хімічних і радіаційних чинників набуває критичного значення для глобальної безпеки [7]. Світова спільнота стикається з викликами, де межа між випадковими промисловими аваріями та навмисним використанням небезпечних речовин стає дедалі тоншою [5, 12]. Процеси хімічної та радіаційної дифузії є фундаментальними фізико-хімічними явищами, що визначають динаміку формування зон ураження та тривалість контамінації об'єктів [1, 4].

Аналіз наукових джерел за останні роки свідчить про глибокий інтерес до механізмів поширення хімічних сполук. Дослідження організації із заборони хімічної зброї (ОЗХЗ) та праці провідних фахівців акцентують увагу на токсикологічних ефектах іритантів та промислових сполук, таких як хлор і аміак, підкреслюючи їхню здатність уражати глибокі відділи дихальної системи [12, 13]. Питання радіаційної безпеки та внутрішнього опромінення детально розглядаються в стандартах МАГАТЕ та роботах з моделювання радіаційно-індукованої сегрегації [8, 4]. Водночас, практичні звіти вказують на систематичне застосування спецзасобів типу К-51 та РГ-ВО в зоні бойових дій, що потребує негайного перегляду існуючих протоколів захисту [3]. У науковій літературі також порушується проблема ефективності сорбційних матеріалів та їхньої здатності протистояти дифузійному проникненню отруйних речовин у критичних умовах [9, 11].

Попри значну кількість фундаментальних досліджень, у більшості робіт розглянуто хімічну та радіаційну дифузію як ізольовані процеси. Наукова новизна цього дослідження полягає у комплексному підході до аналізу цих явищ як єдиного дифузійного детермінанта ураження організму людини [14]. Уперше в межах однієї роботи поєднується математичне обґрунтування за законами Фіка [1, 2] із аналізом уразливості полімерних матеріалів засобів індивідуального захисту до "дифузійного проскоку" [11]. На основі аналізу досвіду відсічі збройній агресії проти України у статті пропонується оновлена концепція оцінювання ризиків, що враховує селективну дифузію радіонуклідів та трансдермальний вплив сучасних бойових токсичних хімічних речовин (БТХР) [6, 15].

Матеріали та методи (Materials and Methods)

В основу роботи покладено комплексний аналіз процесів масоперенесення та іонізуючого випромінювання. Теоретичним підґрунтям для аналізу хімічної дифузії стали фундаментальні закони Фіка, що дозволяють кількісно описати рух молекул у газовому

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

середовищі та біологічних тканинах [1]. Для оцінювання кінетики дифузійних процесів у багатокомпонентних системах використано методи термодинаміки, зокрема рівняння Даркена, що описує взаємозв'язок між коефіцієнтами дифузії та хімічним потенціалом компонентів [2].

У процесі підготовки статті було застосовано наступні методи:

математичне моделювання: використання диференціальних рівнянь у частинних похідних для опису поширення хмар отруйних речовин від локального джерела до формування об'ємної зони ураження [1, 4];

компаративний аналіз: зіставлення токсикологічних характеристик іритантів (CS, хлоропікрин) та сильнодіючих отруйних речовин (СДОР) (хлор, аміак) на основі даних ОЗХЗ та галузевих стандартів GHS [7, 12];

системний підхід: вивчення механізмів внутрішнього опромінення крізь призму селективної дифузії радіонуклідів, що базується на моделях радіаційно-індукованої сегрегації [4, 8].

Інформаційною базою роботи були:

нормативно-правові акти та методичні рекомендації МОЗ та ДСНС України щодо надання допомоги при хімічних та радіаційних ураженнях [6, 15];

наукові періодичні видання, що висвітлюють досвід медичного забезпечення військ та цивільного захисту в умовах збройної агресії [3, 13];

стандарти та звіти міжнародних організацій (МАГАТЕ, ВООЗ, ОЗХЗ), які визначають глобальні протоколи безпеки та класифікації небезпечних речовин [5, 8, 12];

технічна документація щодо характеристик фільтрувально-поглинальних систем та засобів індивідуального захисту органів дихання [11, 14].

Об'єктом дослідження є процеси дифузійного проникнення небезпечних агентів у навколишнє середовище та організм людини. Предметом дослідження є закономірності впливу цих процесів на біологічні структури та ефективність існуючих засобів захисту в умовах екстремальних концентрацій і радіаційного фону [9, 14].

Результати та обговорення (Results and Discussions)

Хімічна дифузія

Хімічна дифузія – це процес масоперенесення, зумовлений хаотичним тепловим рухом молекул, що призводить до вирівнювання концентрацій речовини в просторі.

Для військової діяльності дифузія є основним механізмом перетворення локального джерела хімічного зараження (наприклад, місця розриву снаряда) в об'ємну зону ураження, або подальше розповсюдження зараження шляхом контакту із чинником [4] (чи результатом) зараження, що утворює перехресне зараження.

Існує математична модель, що пояснює процес перемішування речовини із зони високої концентрації в зону низької концентрації та визначена першим законом Фіка [1]. Для опису поширення отруйних речовин застосовується перший закон Фіка, що має наступний вигляд:

$$J = -D\frac{dC}{dx}, \quad (1)$$

де: J – дифузійний потік (кількість речовин, що проходять через одиницю площі за одиницю часу), одиниця вимірювання моль/м^2*с;

D – коефіцієнт дифузії (характеризує швидкість проникнення речовини в конкретне середовище), одиниця вимірювання м^2/с;

c – концентрація речовини, одиниця вимірювання моль/м^2;

x – координата вздовж напрямку дифузії (м);

dC/dx – градієнт" концентрації (зміна концентрації на одиницю довжини).

"-" – вказує на те, що потік речовини спрямований протилежно до вектора градієнта

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

концентрації. Тобто речовина рухається від більшої концентрації до меншої.

Для нестаціонарних процесів (коли концентрація змінюється не лише у просторі, а й із часом, що характерно для газового інциденту) використовується другий закон Фіка [1]. Цей закон пояснює, як швидко змінюється концентрація в конкретному місці, та має наступний математичний вигляд:

$$\frac{dc}{dt} = D\frac{d^2c}{dx^2}, \quad (2)$$

де: dc/dt – швидкість зміни концентрації в часі в певній точці (просторі);
dc – нескінченно мала;
dt – нескінченно малий проміжок часу;
D – коефіцієнт дифузії;
d^2c/dx^2 – друга похідна концентрації за координатою.

Другий закон Фіка дозволяє розрахувати час [3], через який небезпечна концентрація небезпечних хімічних речовин (НХР) / СДОР / БТХР досягне позицій військовослужбовців на певній відстані від епіцентру джерела забруднення (місця вибуху).

Застосування нелетальної хімічної зброї

Застосування нелетальної хімічної зброї (іритантів) та СДОР у військових конфліктах набуває поширення, попри систематичні спроби міжнародної спільноти заборонити це. Одним із документів, що регламентує заборону використання СДОР, є “Конвенція про заборону хімічної зброї (КЗХЗ)” [9].

СДОР – це промислові хімічні речовини (хлор, аміак та інші), які виробляються у величезних кількостях для мирних цілей, але можуть бути зброєю у разі навмисного витоку, обстрілу підприємств або терористичних інцидентів.

До іритантів (НХР) належать такі гази, як CS або хлоропікрин. Зазначені іританти дозволені для поліцейських операцій (розгін натовпу). КЗХЗ суворо заборонено використовувати іританти як засіб ведення війни [9].

Використання СДОР та НХР у бою або на етапах підготовки до нього дуже часто є засобом деморалізації та демонстрації переваги. Також їх можуть використовувати для “попередження” до використання більш небезпечної зброї. Головна небезпека іритантів / СДОР у замкненому просторі (бліндажі) полягає в тому, що вони викликають паніку [6] та неможливість чинити опір, що призводить до швидкої загибелі підрозділу від звичайної зброї (табл. 1).

Таблиця 1. Симптоми негативної дії СДОР / НХР на організм людини

Речовина	Тип дії	Шлях дифузії	Основні симптоми	Стан у міжнародному праві
CS / Хлоропі-крин	Сльозогінний (іритант)	Слизові оболонки, пори шкіри	Різь в очах, кашель, нудота	Заборонено в бою
Хлор Cl_2	Задушливий (СДОР)	Альвеолярні мембрани легень	Опік дихальних шляхів, набряк легень	Повна заборона як зброї
Аміак NH_3	Подразнювальний / задушливий	Глибока тканинна дифузія	Опіки слизової, зупинка дихання	Повна заборона як зброї

Процес дифузії для СДОР та іритантів

Явище дифузії у контексті СДОР та іритантів (CN, CS) є ключовим фактором, що визначає ефективність хімічної атаки [2] або інциденту / теракту. У військовій справі дифузія – це не просто фізичне змішування, а процес “доставлення” отруйних речовин безпосередньо в тканини організму крізь захисні бар’єри [3].

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Механізми дифузії іритантів (CN та CS).

Речовини CN (хлорацетофенон) та CS (динітрил о-хлорбензильмалонової кислоти) зззвичай використовуються у вигляді аерозолів. Більшість військовослужбовців сприймає ці аерозолі як "гази" [2], але насправді це дрібнодисперсні тверді частки, які дифундують у вологому середовищі.

Дифузія в слизові оболонки людини. Молекули CS надзвичайно гігроскопічні. Потрапляючи на очі або в носоглотку, вони миттєво дифундують у слізну рідину [6] та слиз, що викликає лавиноподібне подразнення нервових закінчень (рис. 1).

Дифузія крізь одяг / спорядження виникає через те, що молекули іритантів мають малий розмір, це дозволяє їм дифундувати крізь пори звичайної бавовняної форми [10].

Під час війни у В'єтнамі американський підрозділ "тунельні щури" використовував CS для викурювання партизанів. Через дифузію аерозолю в замкненому просторі та його затримку в тканинах одягу [6] солдати часто отримували вторинні (перехресні) опіки шкіри (особливо в місцях потовиділення), оскільки піт (завдяки своїм фізико-хімічним властивостям) прискорював дифузію молекул CS усередину епідермісу.

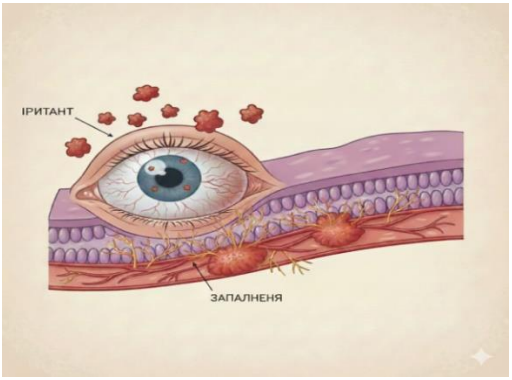


Рисунок 1. Дія іритантів у слизовій оболонці людини

СДОР у ході ведення бойових дій

До СДОР належать хлор, аміак, азотна кислота – речовини, які часто стають інструментом "хімічного тероризму" [10], який важко довести у міжнародній правовій базі. З огляду на те, що Україна – аграрна країна з розгалуженим сільськогосподарським сектором, запаси аміако- та хлоровмісних сполук вражають своїми масштабами.

Хлор (Cl_2). У разі терористичного акту в замкненому просторі хлор швидко витісняє кисень. Його дифузія крізь мембрани альвеол призводить до утворення соляної кислоти безпосередньо в тканинах. В Іраку (у 2006–2007 рр.) військовослужбовці зазнавали уражень навіть у бронетехніці, оскільки хлор дифундував крізь системи вентиляції без спеціальних фільтрів [6].

Аміак (NH_3). На відміну від кислот, аміак дифундує вглиб тканин, розчиняючи білки (коліквaційний некроз). На сході України військовослужбовці сил оборони України мали випадки, коли аміак миттєво дифундував у слизову очей, викликаючи повну сліпоту за секунди (табл. 2).

Небезпека у застосуванні СДОР проти особового складу полягає в тому, що загальна кількість СДОР сягає цифри більше 6000 сполук. Зважаючи на те, що в ході бойових дій особовий склад підрозділів виконує завдання на території очисних споруд, підприємств легкої та важкої промисловості, які "насичені" СДОР через специфіку виробничих процесів та цільового призначення, він наражається на небезпеку ураження саме СДОР. Для захисту від СДОР потрібні спеціальні фільтрувально-поглинальні елементи (ФПК), які стримуватимуть

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

певний СДОР. Саме через відсутність індикаторних засобів та фільтрувальних елементів від певних СДОР з'являються ризики ураження особового складу.

Таблиця 2. Наслідки дифузійного впливу на організм людини

Речовина	Тип дифузії	Основний ефект	Уразливість військових
CN (Хлораце-тофенон)	Швидка дифузія в рогівку	Сльозотеча, печіння	Втрата візуального контакту, обмежена дієздатність
CS (Газ "Терен")	Дифузія в дихальні шляхи	Паніка, кашель, спазм	Неможливість віддавати команди, деморалізуючий фактор
Хлор / аміак	Глибока тканинна дифузія	Набряк легень, опіки	Тимчасова недієздатність, залучення додаткових сил та засобів для евакуації або смерть
VX / "Зарин"	Трансдермальна дифузія	Параліч нервової системи, перелам кісток у результаті судомних скорочень	Потреба у повній ізоляції тіла, перехресне зараження, поточна паніка, деморалізація особового складу

Наступим ризиком є процес накопичення у ФПК та процес "дифузійного проскоку". Під час інтенсивного використання фільтрувальних елементів виникає явище "дифузійного проскоку", а саме:

насичення (забивання) фільтра: якщо концентрація СДОР дуже висока, молекули дифундують крізь шари сорбенту швидше, ніж він встигає їх зв'язати [5]. У цьому випадку негативним явищем є погодні умови (волога), яка "зв'язує" сорбент, створивши міжпрошаркові щілини, крізь які проникає СДОР [6];

дифузія крізь гуму: молекули (БТХР) іприту або VX-газів можуть дифундувати безпосередньо крізь гумову маску протигаза, особливо в старих зразках (ГП-5, ПМГ, ПМК, ПФЛ, ПБФ та ін.), де гума втратила щільність [7];

"дифузійний проскок" є найбільшою небезпекою для екіпажів, що діють всередині техніки: якщо концентрація СДОР біля машини занадто висока, то молекули газу дифундують крізь фільтри вентиляції швидше, ніж сорбент встигає їх поглинути. Також старі гумові ущільнювачі та шолом-маски протигазів можуть пропускати гази через втрату гумою щільності (дифузія крізь пори) [8] (рис. 2).

Сучасна російська агресія супроводжується систематичним використанням хімічних речовин як інструменту "тихого" терору.

На рис. 3 наведено приклад появи "проскоку" за звичайних умов (штрих-пунктир) та умов підвищеної вологи (зелена крива) за однаковою концентрацією (пряма лінія).

Історичні факти застосування СДОР та іритантів

У часи Першої світової війни під час битви при Іпрі (1915 р.) Німеччина використала рідкий хлор із балонів. Хлор важчий за повітря, тому він заповнював траншеї, викликаючи хімічні опіки легень та задуху.

Зафіксовано випадки застосування під час війни у В'єтнамі, коли армія США масово використовувала газ CS для "викурювання" бійців В'єтконгу з підземних тунелів. Це дозволяло або вигнати противника на поверхню під вогонь артилерії, або тимчасово вивести його з ладу в замкненому просторі.

У Сирії (у 2014–2018 рр.) під час облоги міст (Дума або Хан-Шейхун) неодноразово фіксувалися скидання бочок із хлором. Оскільки хлор є промисловим товаром, його використання легше "замаскувати" під промислову аварію, ніж використання нервово-паралітичних речовин на кшталт "Зарину", що в подальшому буде доведено, а винуватців притягнуть до відповідальності.

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

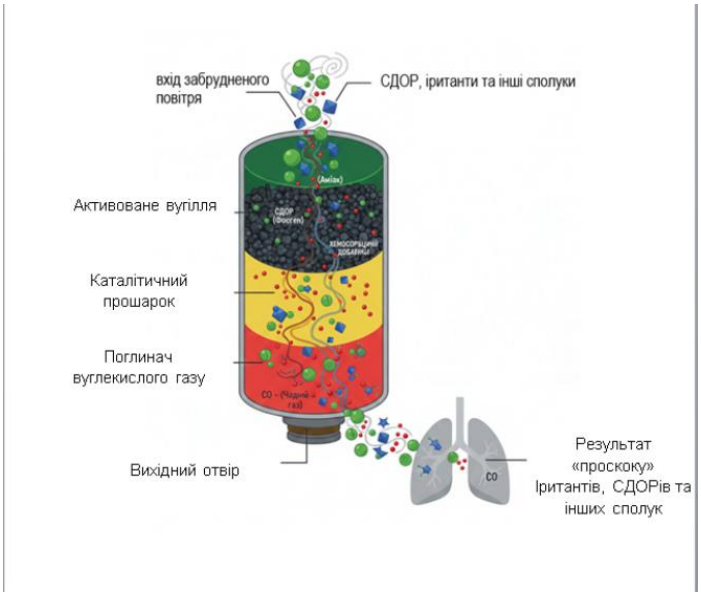


Рисунок 2. Результат “дифузійного проскоку” крізь фільтрувально-поглинальний елемент

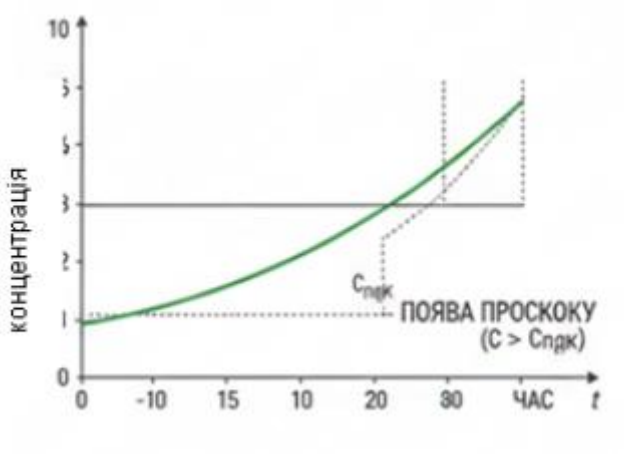


Рисунок 3. Результат “дифузійного проскоку” у графічному вигляді

У ході російсько-української війни росія використовує тактику “гібридного” застосування СДОР та іритантів, намагаючись маскувати воєнні злочини під промислові аварії або поліцейські заходи, щоб уникнути посилення міжнародних санкцій, які впливають на економічну стабільність країни. росія не цурається використовувати промислові / техногенні інциденти як метод війни. Під час боїв за промислові зони (наприклад, Сєвєродонецький “Азот”) обстріли складів з аміаком або азотною кислотою створювали зони смертельного зараження, що фактично працювало як хімічна зброя. У районі населеного пункту Рубіжне російські війська цілеспрямовано обстрілювали цистерни з азотною кислотою (HNO_3) та аміаком (NH_3) [6]. Це також створило зони смертельної контамінації, які фактично виконували роль хімічної зброї в населеному пункті та на рубежах оборони Збройних Сил України (ЗС України), але подавалося російською пропагандою як випадкові влучання та “наслідки бойових дій”.

Унаслідок обстрілу підприємства “Сумихімпром” (березень 2022 р.) було пошкоджено

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

резервуар з аміаком. Хмара поширилася на кілька кілометрів, що змусило жителів населеного пункту Новоселиці терміново вживати заходів захисту та евакуюватися. Це, своєю чергою, призвело до створення несприятливих умов оборони для ЗС України та спричинило додатковий психологічний тиск на населення.

Підрозділи рф неодноразово пошкоджували аміакопровід "Тольятті-Одеса" – трубопровід у Харківській та Донецькій областях (жовтень 2025 року, населений пункт Дружківка). Це призводило до необхідності використання засобів захисту та обмеження у веденні бойових дій через швидку насиченість фільтрувальних елементів та перехресне зараження через епітелій та піт військовослужбовців.

У серпні 2024 року на Тернопільщині після нічної атаки на промисловий об'єкт виникла пожежа, що спричинила викид хлору та соляної кислоти в повітря мирного міста. Гранично-допустиму концентрацію було перевищено у 4–10 разів.

Під час штурму Маріуполя (2022 р.) підрозділи рф використовували CS. Застосування CS в умовах обмеженої вентиляції створювало концентрацію, що призводила до швидкого насичення вугільних фільтрів протигазів особового складу та до його подальшого ураження.

Більшого поширення набуває застосування скидів НХР із дронів. Станом на листопад 2025 року офіційно зафіксовано понад 9 000 випадків застосування хімічних речовин, переважно шляхом скидання гранат К-51 та РГ-ВО із БпЛА [6]. Ці гранати містять речовину CS та хлоропікрин, що суворо заборонено КЗХЗ як засіб ведення війни [9]. Наступне, чого намагаються досягти росіяни, – психологічний тиск на особовий склад ЗС України та його дезорієнтація. Метою таких атак є не лише фізичне ураження, а й витіснення бійців ЗС України з фортифікаційних споруд під вогонь артилерії [6].

Радіаційна дифузія

Радіаційна дифузія в організмі людини стосується процесів кінетики радіонуклідів – їх надходження, переміщення (транспортування) та перерозподілу між тканинами, рідкими середовищами в організмі людини та її органами [2]. Цей процес регулюється законами дифузії, осмосу та активного біологічного транспорту. На відміну від зовнішнього опромінення [2], внутрішня дифузія ізотопів створює пролонговане радіаційне навантаження на критичні органи.

Радіонукліди потрапляють до внутрішнього середовища організму людини трьома основними шляхами, а саме:

1. Інгаляційний шлях. Газоподібні сполуки та аерозолі дифундують через альвеолярно-капілярну мембрану. Швидкість дифузії залежить від дисперсності часток. Частки розміром $d < 0.5$ мкм проникають безпосередньо в кров, оминаючи захисні бар'єри верхніх дихальних шляхів.

2. Пероральний шлях. Найбільш масовий шлях у постійних умовах забруднення. Дифузія відбувається через слизову оболонку шлунково-кишкового тракту (ШКТ). Інтенсивність залежить від хімічної валентності елемента та його розчинності.

3. Перкутанний шлях. Дифузія через непошкоджену шкіру є обмеженою, проте для тритію (^{3}H) та деяких органічних сполук вона є значущим фактором ризику [1], що має суттєвий вплив на організм людини.

Після потрапляння в системний кровотік починається етап селективної дифузії [2]. Організм людини часто не розрізняє радіоактивні ізотопи [1] та їхні стабільні хімічні аналоги, через що відбувається помилкове вбудовування радіонуклідів у метаболічні цикли, а саме:

Остеотропна група. Такі елементи, як Стронцій-90 (^{90}Sr) та Радій-226 (^{226}Ra) дифундують у кісткову тканину, заміщуючи Кальцій. Це призводить до опромінення гемопоетичної (кровотворної) системи.

Тиреотропна група. Ізотопи Йоду (^{131}I) концентруються у щитоподібній залозі за допомогою активного транспорту, де рівень концентрації може у тисячі разів перевищувати

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

рівень у крові [12].

Гепатотропна та рівномірна дифузія

Цезій-137 (^{137}Cs), виступаючи аналогом Калію, дифундує рівномірно по м'яких тканинах (м'язи, печінка) [2], створюючи загальний гамма-фон усередині тіла.

Дифузія радіонуклідів усередину клітини призводить до іонізації її структур. У науці виділяють два ключових механізми деструкції – пряма дія випромінювання та непряма дія з радіолізом води.

Дія опромінення поділяється на пряму та непряму [13].

Пряма дія випромінювання – це процес, коли іонізуюча частинка безпосередньо взаємодіє з макромолекулами. Найкритичнішим є пошкодження ДНК:

одинарні та подвійні розриви ланцюгів;

виникнення зшивок "білок-ДНК" [2];

порушення генетичного коду, що веде до мутагенезу або апоптозу клітини.

Непрямою дією та радіолізом води є те, що клітина складається з води на 70–80%, основна енергія випромінювання поглинається нею. Процес радіолізу описується рівнянням (3):

$$H_2O \xrightarrow{\alpha,\beta,\gamma} H_2O^+ + e^- \rightarrow \cdot OH + H\cdot \quad (3)$$

Утворення вільних радикалів (зокрема гідроксильного радикалу ·OH) запускає ланцюгові реакції перекисного окиснення ліпідів, що руйнує клітинні мембрани [2].

Соматичні та стохастичні наслідки радіаційної дифузії для організму

Наслідки дифузійного накопичення радіації поділяються на детерміновані та стохастичні (імовірності) ефекти.

Детерміновані ефекти виникають у разі перевищення певного порогу дози (променева хвороба, променеві опіки, стерильність). Характеризуються прямою залежністю важкості стану від отриманої дози.

Стохастичні (імовірнісні) ефекти не мають порогу. Навіть одинична дифузія ізотопу в ДНК-структуру може призвести до раку або генетичних відхилень у майбутніх поколінь. До них належать лейкози, солідні пухлини та спадкові хвороби.

Безпосередній ризик подальших наслідків радіаційної дифузії залежить від впливу на організм людини отриманої еквівалентної дози (вимірюється в Зівертах, Зв):

малі дози (до 0,1 Зв): прямих симптомів немає, але зростає ризик онкологічних захворювань та генетичних мутацій, які можуть проявитися через десятиліття або у нащадків;

середні дози (1–2 Зв): розвивається легка форма гострої променевої хвороби (нудота, слабкість, зміна складу крові);

високі дози (понад 6 Зв): тяжка форма променевої хвороби, що без термінової допомоги зазвичай призводить до смерті через руйнування кісткового мозку та ШКТ.

Історичні приклади радіаційної дифузії

Чорнобильська катастрофа стала головним джерелом даних про **біологічну тропність** (вибірковість) радіонуклідів (дифузія Йоду-131 та Цезію-137) [13].

Йод-131 та щитоподібна залоза. У перші тижні після аварії основним чинником ураження був ^{131}I. Через вживання забрудненого молока радіоактивний йод потрапляв у ШКТ, звідки дифундував у кров і вибірково накопичувався в щитоподібній залозі. Це призвело до різкого зростання випадків раку щитоподібної залози серед дітей (понад 6000 випадків за наступні 20 років), оскільки дитячий орган має інтенсивніший метаболізм.

Цезій-137 та м'язові тканини. ^{137}Cs став довгостроковим фактором. Як аналог Калію він дифундує по всьому тілу, але найбільше концентрується в м'язах. Дослідження дітей у Гомельській області (Білорусь) у 1990-х роках виявили пряму залежність між рівнем накопиченого Цезію в м'яких тканинах і частотою патологій серцево-судинної системи та нирок.

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Аварія на АЕС “Фукусіма-1” (2011 р.). Морська дифузія та харчові ланцюги. Японська аварія продемонструвала шлях дифузії через морські екосистеми [11].

Величезну кількість радіоактивної води було скинуто в океан. Радіонукліди дифундували у тканини морських організмів (риба, молюски). Хоча японська влада запровадила суворий контроль, випадки виявлення ^{134}Cs та ^{137}Cs у рибі поблизу узбережжя підтвердили механізм передачі радіації людині через трофічні ланцюги.

На відміну від Чорнобиля, де був тепловий вибух [12], у “Фукусімі” відбулися вибухи водню [11]. Це призвело до утворення дрібнодисперсних аерозолів, які при вдиханні дифундували через легені безпосередньо в кровотік ліквідаторів.

Прямий контакт та внутрішня дифузія, що сталися під час інциденту в Гоянії, Бразилія (1987 р.). Ця подія пов’язана з крадіжкою джерела Цезію-137 із залишеної лікарні. Порошок хлориду цезію мав яскраво-блакитне світіння, що привабило людей. Вони торкалися його руками та випадково споживали з їжею. У постраждалих спостерігалася швидка дифузія цезію в усі органи. Лікарі використовували берлінську лазурит (фероціанід заліза) – препарат, який “перехоплює” Цезій під час його дифузії в кишковик, запобігаючи повторному всмоктуванню в кров. Це врятувало життя багатьом пацієнтам, прискоривши виведення радіації.

Випробування ядерної зброї (1950–60-ті рр.) спричинили глобальну дифузію Стронцію-90 на полігонах та в місцях проведення цих випробувань [11]. Під час атмосферних ядерних випробувань Стронцій-90 розповсюджувався глобально. “Кістковий шукач”: ^{90}Sr хімічно подібний до Кальцію. Він дифундує в кісткову матрицю, де залишається на десятиліття (період напіврозпаду – 29 років). Масові дослідження молочних зубів дітей у США у 1950-х роках (“Baby Tooth Survey”) показали значне зростання вмісту Стронцію, що стало одним із вагомих аргументів для заборони ядерних випробувань в атмосфері (табл. 3).

Таблиця 3. Приклади радіаційної дифузії на історичних подіях

Подія	Ключовий радіоактивний елемент	Орган, що уражено у більшості	Основний шлях потрапляння в організм
Чорнобиль	Йод-131	Щитоподібна залоза	Харчовий
Фукусіма	Цезій-137	М’язи, серце	Вода, морепродукти
Гоянія	Цезій-137 (порошок)	Весь організм	Контактний / Пероральний
Ядерні тести	Стронцій-90	Кістки, зуби	Опади →трава, кущі, дерева→тварини→їжа (як наслідок усього ланцюга)

Висновок (Conclusion)

Аналіз процесів хімічної та радіаційної дифузії у військових конфліктах та техногенних інцидентів демонструє, що дифузія є не просто фізичним явищем змішування речовин, а критичним чинником доставлення токсичних та радіоактивних агентів безпосередньо в тканини організму крізь захисні бар’єри. Хімічна дифузія, що описується законами Фіка, забезпечує перетворення локального джерела зараження в об’ємну зону ураження, де іританти (CS, хлоропікрин) та СДОР (хлор, аміак) спричиняють швидку дезорієнтацію, паніку та незворотні ураження дихальної системи й слизових оболонок. Особливу небезпеку становить явище “дифузійного проскоку”, коли через високу концентрацію речовин або підвищену вологість сучасні засоби захисту (ФПК) [15] втрачають ефективність, а застарілі гумові маски стають проникними для молекул отрути.

Водночас, радіаційна дифузія створює пролонговане внутрішнє навантаження на організм через механізм селективної дифузії. Організм помилково вбудовує радіонукліди у метаболічні цикли, заміщуючи життєво важливі елементи, такі як Стронцій-90, що накопичується в кістках як аналог Кальцію. Йод-131 концентрується в щитоподібній залозі, а

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Цезій-137 рівномірно дифундує по м'яких тканинах [14], створюючи постійний внутрішній гамма-фон. На клітинному рівні цей процес супроводжується радіолізом води та утворенням вільних радикалів, що руйнує ДНК і призводить як до негайних детермінованих ефектів (променева хвороба), так і до віддалених стохастичних наслідків, таких як рак або генетичні мутації.

У сучасних умовах агресії використання СДОР і радіоактивних ізотопів перетворюється на інструмент "гібридного" тиску та тероризму, де цілеспрямовані обстріли хімічних підприємств або використання іритантів маскуються під промислові аварії чи поліцейські заходи. Це створює зони смертельної контамінації для комбатантів та некомбатантів, які мають на меті не лише фізичне знищення особового складу, а й глибоку деморалізацію та психологічний тиск на населення. Це потребує впровадження високоточних засобів моніторингу та сучасних стандартів індивідуального захисту учасників збройного конфлікту на всіх рівнях [15].

Рекомендації (Recommendations)

Дослідження становить значну цінність для широкого кола фахівців, діяльність яких пов'язана з безпекою, медициною та стратегічним плануванням у сфері РХБ / ХБР захисту. Першочергово матеріал є критично важливим для офіцерів та експертів служб РХБ / ХБР захисту, оскільки наукове обґрунтування явища "дифузійного проскоку" та математичне моделювання зон ураження за законами Фіка дозволяють переглянути терміни експлуатації фільтрувально-поглинальних елементів, систем і тактику розгортання сил у зонах контамінації.

Для військових і тактичних медиків стаття слугує змістовним посібником з ідентифікації симптомів ураження іритантами та СДОР, такими як хлор чи аміак, а також розкриває механізм селективної дифузії радіонуклідів, що є ключовим для призначення специфічної антидотної терапії та проведення йодної профілактики. Одночасно із цим, викладена інформація є цінною для фахівців ДСНС та цивільного захисту, адже може допомогти вдосконалювати протоколи евакуації населення та заходи з дезактивації територій з урахуванням глибини проникнення хімічних сполук у матеріали.

Наукова новизна щодо проникності полімерів та гуми під дією хімічних сполук створює надійну базу для розробників засобів індивідуального захисту, стимулюючи перехід до нових композитних матеріалів. Крім того, теоретичні викладки та аналіз реального бойового досвіду застосування хімічних речовин у сучасних конфліктах роблять цей матеріал незамінним для викладачів і курсантів військових ВНЗ, а також для командирів підрозділів, надаючи їм аргументовану базу для ухвалення рішень щодо захисту особового складу та вибору надійного екіпірування в умовах екстремальних концентрацій отруйних речовин.

Конфлікт інтересів (Conflict of Interest)

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

Використані джерела

1. Фік, А. (1855). Дифузія. *Annalen der Physik,170* (1), 59–86.
2. Даркен, Л. С. (1948). Дифузія, рухливість та їх зв'язок із вільною енергією утворення вакансій. *Transactions of the Metallurgical Society of AIME, 175*, 184–201.
3. Ельзенбаумер, Р., Фат, Б., & Єгер, Б. (н. д.). *Інтерметалічні сполуки в електронній упаковці*.
4. ASM International. (н. д.). Аналіз руйнувань та запобігання. У *Довідник ASM* (Т. 11). ASM International.
5. Каллістер, В. Д., мол., & Ретвіш, Д. Г. (2018). *Матеріалознавство та інженерія: Вступ*

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

(10-те вид.). John Wiley & Sons.
6. Центр національного спротиву. (2024). *Звіти щодо застосування російськими окупаційними військами гранат К-51 та РГ-ВО на лінії бойового зіткнення*. Міністерство оборони України.
7. Настар, М., & Суассон, Ф. (2012). Моделювання радіаційно-індукованої сегрегації. *Comprehensive Nuclear Materials, 1*, 447–485.
8. Даркен, Л. С. (1948). Дифузія, рухливість та їх зв'язок між собою. *Transactions of the AIME, 175*, 184–201.
9. Всесвітня організація охорони здоров'я. (2020). *Заходи громадської охорони здоров'я у відповідь на загрозу застосування хімічної або біологічної зброї* (2-ге вид.). ВООЗ.
10. Міністерство охорони здоров'я України. (2022). *Надання медичної допомоги постраждалим внаслідок дії хімічних агентів у ході ведення бойових дій: Методичні рекомендації*. МОЗ.
11. Організація із заборони хімічної зброї (ОЗХЗ). (2023). *Довідник щодо властивостей іритантів та токсичних промислових хімікатів (Хлор, Аміак)*. OPCW Technical Secretariat.
12. Копилова, С. О., & Ткаченко, І. М. (2023). *Вплив хімічних чинників на дихальну систему військовослужбовців в умовах сучасної війни*. Журнал військової медицини України, *4* (2), 56–64.
13. Шматков, П. Д. (2021). *Військова токсикологія, радіологія та медичний захист: Підручник*. Військово-медична академія України.
14. Організація Об'єднаних Націй. (2023). *Узгоджена на глобальному рівні система класифікації та маркування хімічних речовин (GHS)*. (10-те перегл. вид.). ООН.
15. Міжнародне агентство з атомної енергії (МАГАТЕ). (2018). *Захист населення у разі ядерної або радіологічної аварійної ситуації*. (Серія норм безпеки № GSG-11). IAEA.
16. Трахтенберг, І. С., & Коршун, М. М. (2021). *Гігієна праці та виробнича санітарія: Навчальний посібник для ВНЗ*. Медицина. (Розділ про токсикологію СДОР та методи сорбційного захисту).
17. Коттон, Ф. А., & Вілкінсон, Дж. (2015). *Сучасна неорганічна хімія*. Wiley-Interscience. (Механізми взаємодії галогенів та аміаку з біологічними структурами).
18. Державна служба України з надзвичайних ситуацій (ДСНС). (2022). *Методичні рекомендації щодо організації радіаційного та хімічного спостереження в умовах воєнного стану*. ДСНС України.

References

1. Fick, A. (1855). On liquid diffusion. *Annalen der Physik, 170*(1), 59–86.
2. Darken, L. S. (1948). Diffusion, mobility and their interrelation through free energy in binary metallic systems. *Transactions of the Metallurgical Society of AIME, 175*, 184–201.
3. Elsenbaumer, R., Fath, B., & Jäger, B. (n.d.). *Intermetallic compounds in electronic packaging*.
4. ASM International. (n.d.). Failure analysis and prevention. In *ASM Handbook* (Vol. 11). ASM International.
5. Callister, W. D., Jr., & Rethwisch, D. G. (2018). *Materials science and engineering: An introduction* (10th ed.). John Wiley & Sons.
6. National Resistance Center. (2024). *Reports on the use of K-51 and RG-VO grenades by Russian occupation forces on the line of active combat*. Ministry of Defense of Ukraine.
7. Nastar, M., & Soisson, F. (2012). Radiation-induced segregation modeling. *Comprehensive Nuclear Materials, 1*, 447–485.
8. Darken, L. S. (1948). Diffusion, mobility and their interrelation. *Transactions of the AIME, 175*, 184–201.

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

9. World Health Organization (WHO). (2020). *Public health response to biological and chemical weapons: WHO guidance* (2nd ed.). WHO.
10. Ministry of Health of Ukraine. (2022). *Provision of medical care to victims of chemical agents during combat operations: Methodological recommendations*. MOH.
11. Organisation for the Prohibition of Chemical Weapons (OPCW). (2023). *Handbook on the properties of irritants and toxic industrial chemicals (Chlorine, Ammonia)*. OPCW Technical Secretariat.
12. Kopylova, S. O., & Tkachenko, I. M. (2023). Impact of chemical factors on the respiratory system of military personnel in modern warfare. *Journal of Military Medicine of Ukraine, 4*(2), 56–64.
13. Shmatkov, P. D. (2021). *Military toxicology, radiology, and medical protection: Textbook*. Ukrainian Military Medical Academy.
14. United Nations. (2023). *Globally Harmonized System of Classification and Labelling of Chemicals (GHS)* (10th revised ed.). UN.
15. International Atomic Energy Agency (IAEA). (2018). *Arrangements for the protection of the public in a nuclear or radiological emergency* (Safety Standards Series No. GSG-11). IAEA.
16. Trachtenberg, I. S., & Korshun, M. M. (2021). *Occupational hygiene and industrial sanitation: Textbook for higher education institutions (Section on toxicology of hazardous substances and sorption protection methods)*. Medytsyna.
17. Cotton, F. A., & Wilkinson, G. (2015). *Advanced inorganic chemistry*. Wiley-Interscience. (Mechanisms of interaction of halogens and ammonia with biological structures).
18. State Emergency Service of Ukraine (SESU). (2022). *Methodological recommendations for the organization of radiation and chemical observation under martial law*. SESU Ukraine.

Analysis of the impact of chemical and radiation diffusion on the human body

Artem Karpus
Adjunct
Department of Radiological, Chemical, Biological Defense
and Civil Safety Institute of Force Support and Information Technologies
National Defense University of Ukraine
03049, Povitrianykh Syl Ave, 28, Kyiv, Ukraine
e-mail: karpusark@gmail.com
ORCID: 0009-0003-2406-1924

Ali Kenherli
Adjunct
Department of Radiological, Chemical, Biological Defense
and Civil Safety Institute of Force Support and Information Technologies
National Defense University of Ukraine
03049, Povitrianykh Syl Ave, 28, Kyiv, Ukraine
e-mail: alikenherli@gmail.com
ORCID: 0009-0005-5794-6221

“Nature works by unseen bodies”
(Lucretius)

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Abstract. This scientific article is devoted to a comprehensive study of the mechanisms of chemical and radiation diffusion as key factors in human injury during modern military conflicts and man-made disasters. The article reveals the physical and mathematical essence of diffusion processes based on Fick's laws, justifying the transformation of local sources of infection into volumetric contamination zones. The aim of this article is a detailed study of how chemical compounds and radioactive elements spread in the environment and penetrate the human body, becoming critical factors of injury during modern military conflicts and industrial accidents. The paper seeks to explain how Fick's mathematical laws can define the physical essence of how a small gas cloud or a local explosion site transforms into a large-scale contamination zone. The task is to analyze real-world examples of the use of irritants and toxic substances, such as chlorine and ammonia, which are used during the russian aggression against Ukraine to disorient and displace servicemen of the Armed Forces of Ukraine from the fortifications. A vital part of this objective is identifying vulnerabilities in modern protective equipment, specifically investigating how toxic molecules can pass through filters or even the rubber of gas masks. The article provides a detailed analysis of the tactics of using irritants (CS, chloropicrin) and TIMs (chlorine, ammonia) used to disorient and displace personnel of the Armed Forces of Ukraine from fortified positions. Particular attention is paid to physiological aspects, namely: transdermal penetration of toxins and chemical burns of the respiratory tract. A significant practical aspect of the study is the analysis of critical flaws in personal protective equipment (PPE), specifically the phenomenon of "diffusion breakthrough" through filters and the permeability of mask polymer materials to toxic molecules. The radiation block of the study focuses on internal exposure processes via inhalation and oral pathways. The author reveals the mechanism of selective diffusion of radionuclides, where isotopes (Strontium-90, Iodine-131, Cesium-137) substitute stable chemical elements in target organs, causing radiolysis of cellular water and DNA damage. Both immediate manifestations of radiation sickness and long-term stochastic consequences (oncogenesis, mutations) are highlighted. The findings of the work emphasize the strategic importance of monitoring diffusion processes for the development of modern protection systems. The article is based on current data regarding the use of chemical compounds during the Russian aggression against Ukraine, making it critically important for specialists in CBRN (NBC) specialization, military medicine, and civil security.

Keywords: chemical and radiation diffusion, radiation injury, Fick's laws, irritants, toxic industrial materials/chemicals (TIMs/TICs).

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Received: *October 22, 2025* | **Revisions Requested:** - | **Revision Received:** -
Accepted: *January 21, 2026* | **Published Online:** *April 10, 2026*

Licensed (C) by Creative Commons Attribution International License 4.0 (CC BY-NC-SA)

DOI: 10.62524/msj.2026.4.1.21

Literature Survey on Warfighter Information Network-Tactical

Muhanned AL-Rawi
Bandung Institute of Technology
Indonesia
e-mail: muhrawi@yahoo.com
ORCID: 0000-0003-1407-6519

Abstract. Under the conditions of conducting combat operations, information superiority is becoming one of the key factors of operational success. Increasing requirements for the speed, security and volume of data transmission, as well as the need to integrate heterogeneous command, control, communications and intelligence (C4I) systems, necessitate the development of fundamentally new tactical networks. The article is devoted to the analysis of the Warfighter Information Network-Tactical (WIN-T), which forms the basis for the implementation of the Force XXI concept and ensures dominance in the information domain. The aim of the study is to describe the architecture, principles of operation and mechanisms for ensuring the information security of WIN-T, as well as to generalise the results of previous research in this field. A separate objective is to demonstrate the military applications of the network for enhancing mobility, survivability and the effectiveness of command and control of troops. The study is based on a system analysis of open architectural specifications of WIN-T, including its division into the upper and lower levels of the Tactical Internet. Network topologies (LAN-A, LAN-B, WAN) are considered using switches, routers, ATM and HSMUX technologies, as well as radio communication systems (NTDR, SINCGARS, EPLRS). To ensure security, the concept of "defence-in-depth" is applied. The methodology also includes a literature review analysing QoS solutions, cryptographic methods, cognitive radio systems and Deep Reinforcement Learning technologies. The article provides a detailed description of the WIN-T architecture, which integrates the US Army Battle Command System (ABCS) and ensures connectivity from brigade level down to individual vehicles. It is shown that WIN-T establishes a unified IP-based transport network (Everything over IP), combining satellite communications (Ku/Ka bands), radio relay links and fibre-optic channels. Measurement-Based Admission Control (MBAC) mechanisms are implemented to prioritise traffic (voice, video, data). In the security domain, a multi-layered intrusion detection and response system is employed. A separate result is the presentation of the Named Data Networking (NDN) concept as an alternative to traditional IP-based networks for improving efficiency under complex conditions. WIN-T enables commanders to receive updated topographic maps, real-time video streams from the battlefield and intelligence data directly while on the move. The network supports the operation of critical systems such as the Advanced Field Artillery Tactical Data System (AFATDS) and the Command Post of the Future (CPOF). Field test results confirmed throughput exceeding 1 Mbps in the Ka band at movement speeds above 25 miles per hour. The proposed solutions for power optimisation and resource allocation based on Multi-Agent Deep Reinforcement Learning (MADRL) significantly enhance resistance to signal interception, which is critical for the survivability of elements on the battlefield.

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Keywords: WIN-T, architecture, security, military applications.

Introduction

By offering network security and interoperability support to the army battle command system (ABCS) and its battlefield functional areas (BFAs), the WIN-T helps to improve maneuver force mobility. As operations in the present and the future place increasing demands on tactical voice, data, and multimedia signal support systems, this idea of communication services will give the warfighter a force multiplier.

In order to give warfighters the information they need to make decisions, the different information systems must be combined into a single, cohesive "system-of-systems" that supports joint operations and spans the strategic, operational, and tactical levels.

Methodological Framework

The methodological framework of this study is based on a comprehensive system analysis of the architecture, protocols, and security mechanisms of the Warfighter Information Network-Tactical (WIN-T), utilizing approaches inherent to military telecommunications engineering and network management.

First, the research is founded on a structural-functional analysis of the WIN-T architecture. It examines the integration of the Army Battle Command System (ABCS) with its key subsystems: Force XXI Battle Command Brigade (FBCB2), Army Tactical Command and Control System (ATCCS), and Global Command and Control System-Army (GCCS-A). The topology of command post networks is analyzed, particularly the division into LAN-A (intra-vehicle or edge network) and LAN-B (inter-vehicle or core network), as well as the role of the Tactical Packet Network (TPN), which consists of NC, LEN, SEN nodes and the System Control Center (SCC).

Second, the methodology includes a comparative analysis of networking technologies. The study investigates local area network implementation methods: router-based architectures, where routing decisions are made between local and remote command posts, and switch-based architectures, where switches provide local data delivery within a single segment. The application of ATM, HSMUX, HCLOS, HCTR technologies, satellite systems, and radio networks (NTDR, SINCGARS, EPLRS) for bandwidth management and quality of service is also analyzed.

Third, the defense-in-depth concept is applied to assess information security. This approach involves creating multiple sequential barriers against external and internal threats, each integrating detection, protection, and response functions. The study relies on cryptographic principles (public and secret key cryptography) as well as real-time intrusion detection methods.

Fourth, the work employs modeling and experimental verification. It mentions the use of the OPNET Modeler environment for developing and testing Quality of Service (QoS) solutions, specifically the Measurement-Based Admission Control (MBAC) algorithm, which prioritizes different traffic types (voice, video, data) based on computed end-to-end congestion levels. Additionally, field test results of SOTM terminals in Ku and Ka bands are presented, measuring throughput at the application layer.

Fifth, the article uses a literature review as a method of knowledge synthesis. Previous works are analyzed in the following areas: replacement of legacy MSE/TRI-TAC systems, WIN-T vulnerabilities and cryptographic countermeasures, QoS for encrypted tactical networks, integration of WIN-T with GIG and JTRS, application of Named Data Networking (NDN) as an alternative to IP-based networks, and the use of Multi-Agent Deep Reinforcement Learning (MADRL) for optimizing power allocation and spreading factor assignment to ensure Low Probability of Interception (LPI).

Thus, the methodological framework of this work is multi-layered and combines architectural analysis, network modeling, cryptographic methods, experimental testing, and a review of

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

contemporary research, providing a comprehensive understanding of the operation, protection, and development prospects of WIN-T.

Results and Discussion

1.1 Wit-t architecture

Through an integrated digital information network that offers automated C2 and SA information through a smooth data architecture of both planned and existing C2 systems, the ABCS assists planners and leaders at the tactical to strategic level. The Force XXI battle command-brigade (FBCB2), Army tactical command and control system (ATCCS), and global command and control system-Army (GCCS-A) are all part of the ABCS.

At each echelon, the information flow requirements dictate the physical layout of command posts, the communications equipment that supports them, and the ABCS LAN infrastructure. The basis for networking and communication in each Force XXI tactical operations center (TOC) is largely the same, despite these differences. The ATCCS, which aim to offer a collection of common services, facilitate the integration of C2 functions. A client-server architectural environment is in place to integrate and enable interactive information processing in order to fulfill this shared setting. The service is requested by the client computer and related software, and it is delivered by the server and related software. A local area network (LAN) or wide area network (WAN) is used to carry out this data information media exchange process.

Several BFACS sharing a single LAN at a CP make up an ABCS LAN. The WAN that links the different ABCS LANs throughout the battlefield is connected by the tactical packet network (TPN), also referred to as the MSE packet switch network or MPN (See Fig. 1). The system control center (SCC), small extension nodes (SEN), large extension nodes (LEN), and the node center (NC) are the main resources utilized for TPN communications. The tactical network that connects the ATCCS LANs is anchored by these resources. High speed multiplexer circuit cards (HSMUX), asynchronous transfer mode (ATM) switching, satellites, range extension terminals, near-term data radio (NTDR), high capacity line-of-sight (HCLOS) and high capacity trunk radios (HCTR), and other technologies have been introduced to help manage bandwidth and improve quality of service.

Two segments typically make up a TOC LAN, as shown in referred to as LAN-A (intra-vehicle LAN or edge component) and LAN-B (inter-vehicle LAN or core component). The FSE can extend the AFATDS workstation into the TOC SICPS using a third LAN-C. All peripherals, including workstations and printers, are connected by the LAN-A. that can be found in a single car, tent, or uniform integrated command post system. All TOC LAN-A segments can be connected to the LAN-B to enable information sharing throughout the TOC.

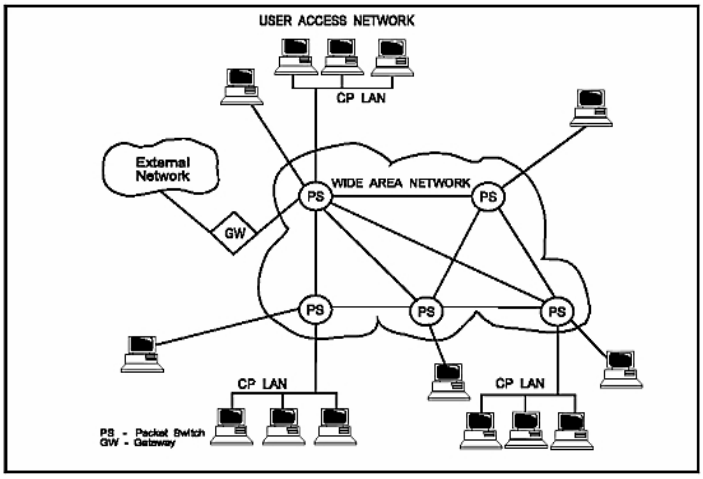


Fig. 1 Simplified TPN Architecture

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

A typical twisted pair connection, ethernet hubs, or routers/switches are used to implement the LAN-A. A router makes it easier to manage IP addresses and make decisions about internet work forwarding when LAN-A components connect to LAN-B. Additionally, this improves a LAN's effective use of its available bandwidth. Whether a message is sent to the local TOC or to another TOC is decided by a router.

Each vehicle in an ABCS BN TOC has either a standalone router or a router integrated into an Ethernet switch (a router-switch). Every vehicle at brigade and division TOCs has an Ethernet switch or router-switch. The router-switch integrates the capabilities of a switch and a router. Local forwarding decisions to LAN devices are made by Ethernet switches (see Figs. 2 and 3).

A multi-star network configuration is created by digital TOCs using at least two core routers integrated into a central ethernet switch that is connected in a star pattern to one of the core routers. Because this configuration uses less router, it simplifies the initial setup and enhances performance.

Like a LAN, a WAN is able to communicate with higher, lower, and adjacent units over a greater distance. It is a network of networks made up of several local area networks (LANs) linked to radio networks like CNR or MSE as well as to one another. Due to the limitations of a coaxial cable network, a wide area network (WAN) combines radio networks and MPNs to distribute data throughout the system as needed.

Both the physical communications network that serves as the general-purpose data backbone and the general idea of an integrated battlespace automated infrastructure are referred to as the tactical internet (TI). The "tactical internet" gets its name from its extensive and deliberate resemblance to the commercial internet.

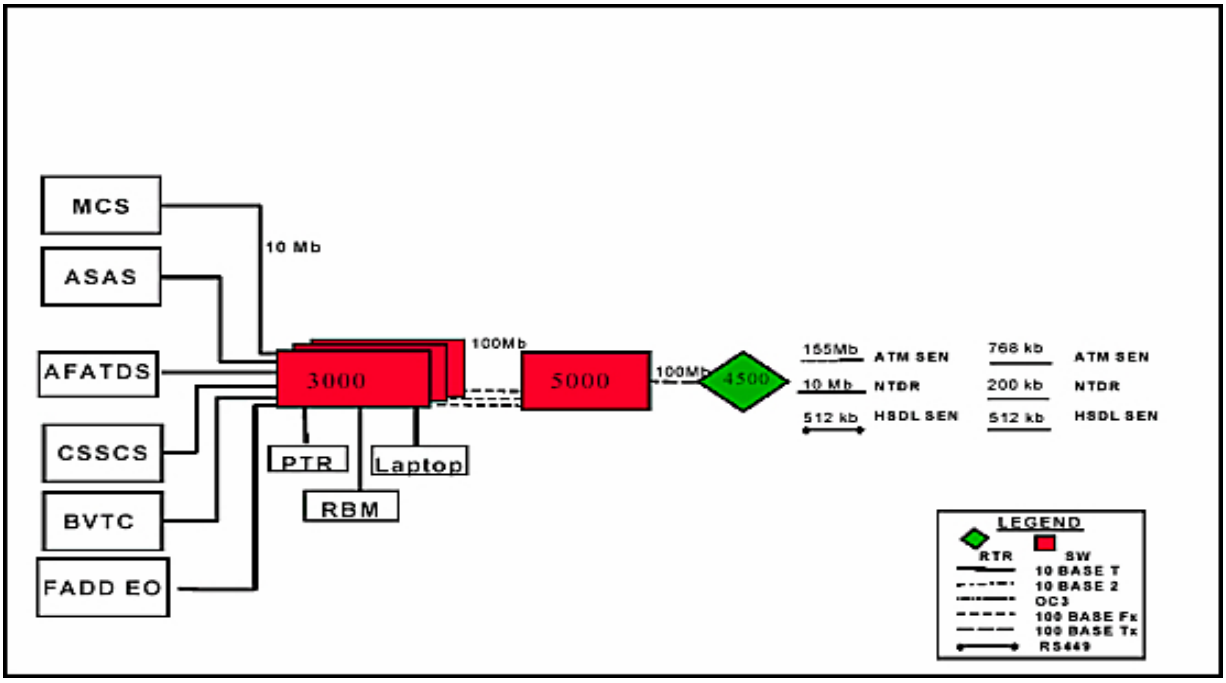


Fig. 2. Switched-based TOC Architecture

Two separate information exchange layers are formed by the TI, as shown in Fig.4 are known as the upper and lower TI. Other WIN-T systems, multi-channel satellite systems, and MSE make up the upper TI layer. For units at brigade and lower, the lower TI serves as the communications support system. It is made up of the FBCB2 computers and software, EPLRS, and SINCGARS SIP radios, which are connected via routers and both commercial and military protocols.

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

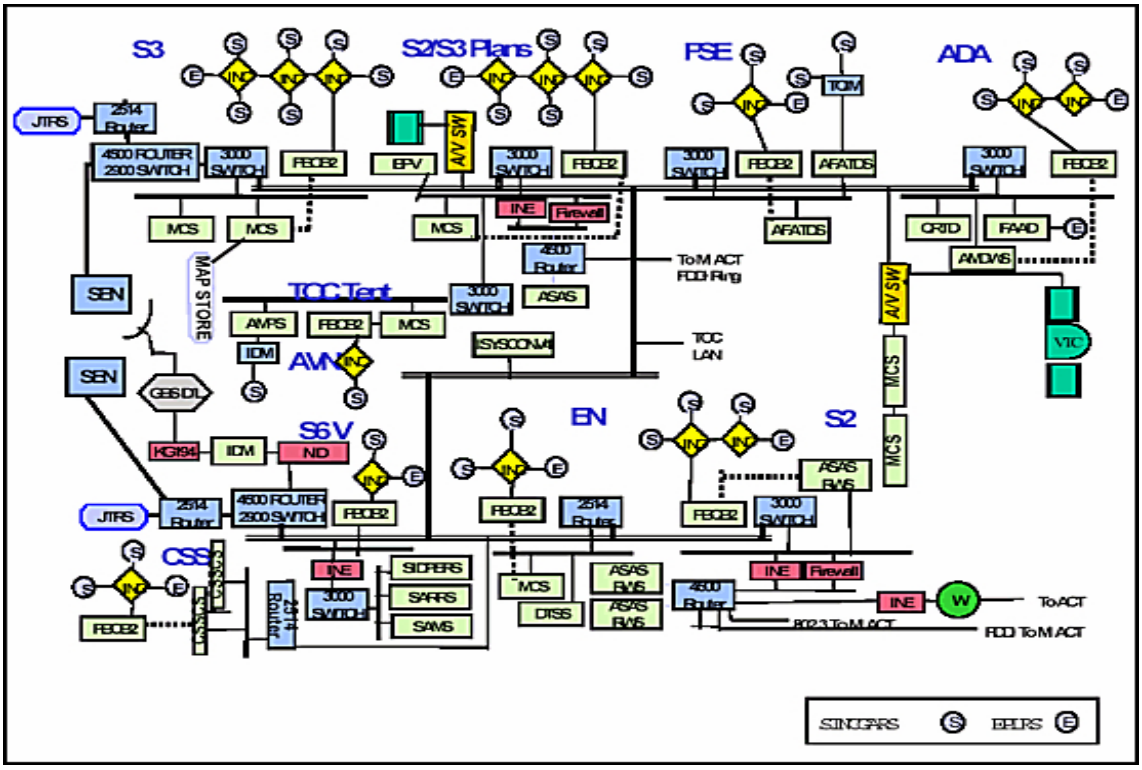


Fig. 3. Brigade TOC LAN

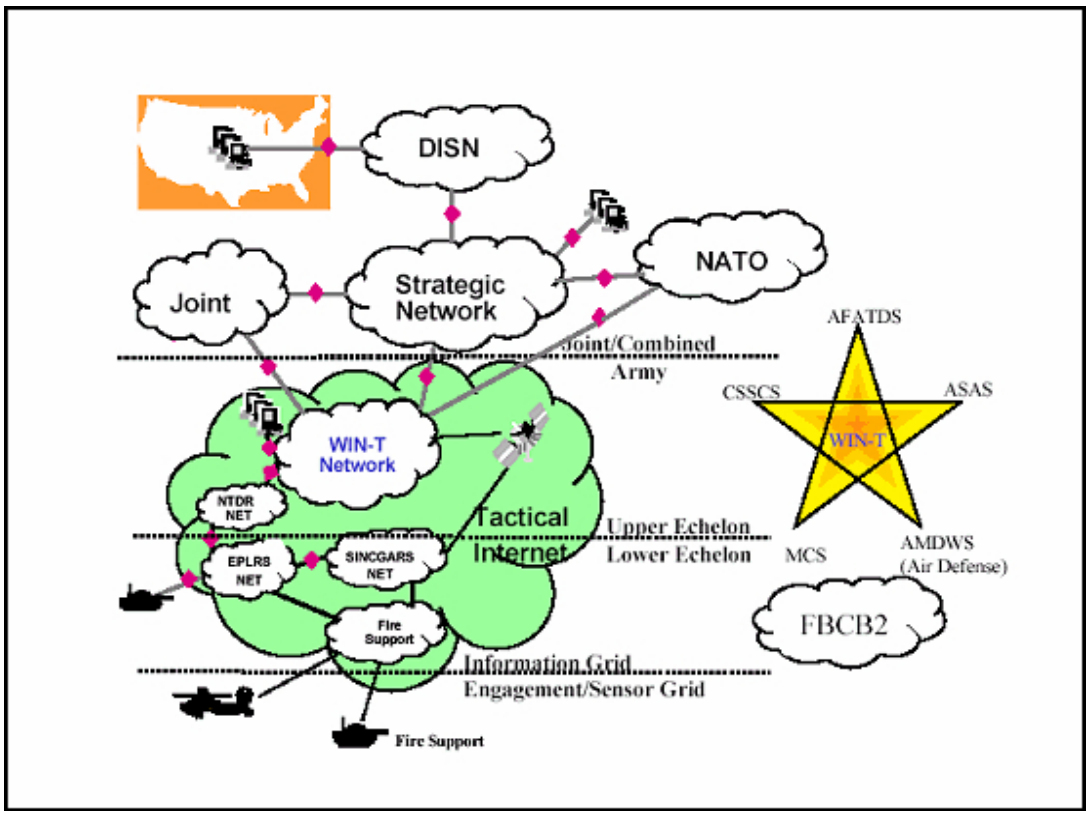


Fig. 4. WIN-T Conceptualization

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Network management and careful planning are necessary for the TI. When fully operational, the integrated system control (ISYSCON) hardware and software suite serves as the TI's management platform and interface for the FBCB2-equipped task force. The brigade task force also uses other systems, such as FBCB2, network control station-EPLRS (NCS-E), or commercial computers set up for network management, to plan and oversee the TI.

The TI contains a variety of digital systems that are intended to supply information to the commander, soldiers, and lower C2 and SA personnel from every unit in the brigade task force. The digital tools necessary for efficient C2 and battlefield SA, adapted to the operational needs and specific function of the unit's platforms, will make up each task force tier.

1.2 Information and network security

With the help of a universal TCP/IP data network, the Army's digitization efforts aim to field a variety of embedded and standalone end-user computers. That network will be made up of diverse radio networks with data capabilities (e.g. EPLRS, NTDR, MSE, SINCGARS), and wire communication links (e.g. local area networks), and a network infrastructure of specialized computers will connect and support these links (e.g. name servers, security servers, switches, and routers). The Army is unable to field a "bullet-proof" network, despite the fact that manufacturers create systems with security in mind and highly qualified personnel adhere to the proper protocols. As a result, it is essential to continue being able to perform real-time security management and intrusion detection as part of regular operations and to respond appropriately when issues arise. Real-time security management is envisioned by ABCS's information systems protection concept as an element of network and system management. Information and network security are implemented using a variety of security tools.

As shown in Fig.5, the "defense-in-depth" concept is the foundation of network protection. The defense-in-depth strategy aims to create several obstacles against an outsider, a hostile insider, etc. Every barrier integrates features for detection, protection, and response.

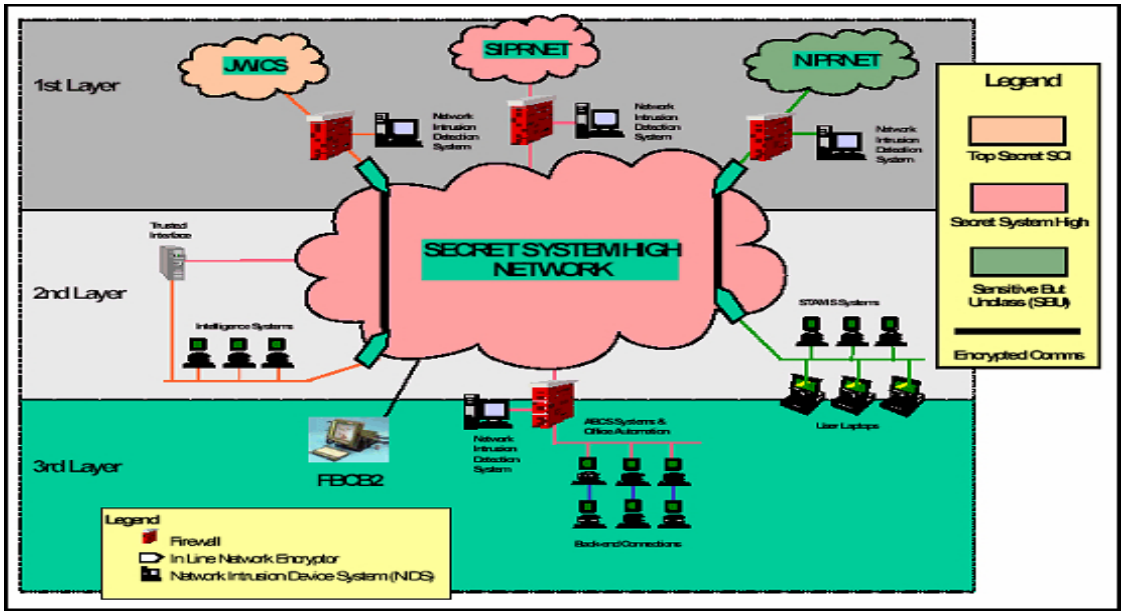


Fig. 5. Concept of Defense-in-Depth Network Protection

1.3 Military applications

The military uses of WIN-T are centered on giving the U. S. Army with a robust, mobile, and secure backbone for data, voice, and video tactical communications. It supports expeditionary

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

operations by connecting forces across long, non-linear battlefields using both line-of-sight and satellite communications, facilitating mission command for commanders from command posts to moving vehicles, and enabling real-time situational awareness through applications like live video streams and digital force maps. The following is a summary of the applications.

a) With WIN-T, commanders can view real-time topographical maps of friendly forces, access mission command applications from any location on the battlefield, and get intelligence updates to help them make prompt, well-informed decisions.

b) Voice calls, video conferences, and data transfers are all made possible by WIN-T's high-speed, high-capacity, and secure communications, which are crucial for sharing vital information and organizing operations.

c) By giving combat vehicles mobile network capabilities, WIN-T Increment 2 enables constant command and control while forces move across the battlefield.

d) Through the use of satellite and terrestrial transportation, the network provides a scalable, reliable network infrastructure that facilitates expeditionary operations and links forces in remote areas.

e) The Advanced Field Artillery Tactical Data System and Command Post of the Future are just two examples of the mission-critical systems that WIN-T supports by acting as the data pipe that gives them the connectivity they need to function properly.

f) To improve unit effectiveness and survivability, soldiers can use WIN-T to stream live video, digitally call for artillery support, and send requests for medical assistance.

2. Literature survey

The Warfighter Information Network Tactical (WIN-T), the US Army's intended replacement for the mobile subscriber equipment (MSE) and the antiquated tri-service tactical communications (TRI-TAC) system, are described in[1]. These systems are now approaching the end of their intended life cycle and are collectively referred to as the area common user system (ACUS). In place of them, WIN-T offers a cutting-edge, seamless multimedia transport system that links and supports all Army levels. It has been a mobile, secure, and resilient network with a large capacity. The current systems and how WIN-T offers an operational substitute are discussed in the paper. The cost as an independent variable (CAIV) acquisition method, which the Army has employed to acquire the new system, is also covered in the paper.

The paper in [2] looks at the different kinds of enemies, the dangers they present, and the weaknesses that the Army's Warfighter Information Network (WIN) is probably targeting. An outline of the potential applications of cryptographic techniques to address WIN vulnerabilities is given. A review of public key and secret key cryptography techniques, along with an analysis of their relative benefits and drawbacks, is included. The authors list several security-related concerns that need more thought in their conclusion.

A QoS solution for the Army's warfighter information network tactical (WIN-T) was created by general dynamics C4S in [3]. This solution is also being applied to other QoS applications in tactical networks. When using an encryption device, the encryptor prevents any information exchange between the WAN, where traffic shaping is done, and the LAN, where call admission control (CAC) decisions are made. OPNET Modeler was used to develop and test this solution. An algorithm of the measurement based admission control (MBAC) type forms the basis of this solution. Based on a calculated end-to-end congestion level, this MBAC algorithm controls the flow of diverse traffic entering a tactical wireless ad hoc network. Different types of traffic, including voice, video, and data, can have varying real-time requirements and varying levels of importance (survivability). Based on the QoS characteristics of each class of service and the state of the path to the destination node, the algorithm ranks the admission of calls or sessions (at a source node) in order of priority.

A QoS solution for tactical networks with security considerations is presented in the paper in [4]. A partitioned QoS approach is proposed since encryption stops the cipher text side and the plain text side from exchanging QoS information. The plain text side QoS solution includes

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

measurement-based admission control (MBAC), according to the authors. Based on a calculated end-to-end congestion level, MBAC uses real-time measurements to control the flow of traffic entering a tactical core network. The advantages of employing MBAC are examined in this essay, along with any potential drawbacks. The study demonstrates how a Markov chain expressing the degree of path congestion can be constructed using the measurements. A few simulation results from applying MBAC to an OPNET model of the warfighter information network-tactical (WIN-T) network are also presented in the paper.

In [5], the architecture framework that is suggested in this paper fills in the gaps in communication capacity and offers vital transport capabilities that will revolutionize battlefield communications to come. A thorough testing and evaluation process is in progress to guarantee the smooth, end-to-end integration of wireless services with the GIG resources for sending C4ISR data to the edge. Upon deployment, the WSDN will have the capability to expand DISN services to theaters with either fixed or mobile installations. The warfighter information network-tactical (WIN-T) users will have more mobility and the joint tactical radio system (JTRS) will have more interoperable capabilities.

The design, test methodology, and measured performance of the Ku- and Ka-band SOTM terminals are covered in [6]. These terminals are used to assess how the Army warfighter can be provided with dependable voice over IP (VoIP), video, and data communications while they are on the move. In order to evaluate the performance of the design in a networked and operationally relevant environment as well as the maturity of key technologies, the WIN-T DT/OT, and more especially the SOTM tests, were utilized. Antenna aperture, pedestal station keeping, and throughput performance are some of the more important design factors. The formal DT/OT testing process was successful in meeting the throughput requirement of 256 kbps at the application layer (layer 3). During SOTM testing, vehicles operating at speeds exceeding 25 mph were evaluated for throughput capability of roughly 770 kbps at Ku-band over the Americom AMC-9 satellite and Ka-band (using a satellite emulator) of 1 Mbps and higher.

According to [7], the L-3 Linkabit multi frequency-time division multiple access (MF-TDMA) demand-assigned multiple access (DAMA) Network Centric Waveform (NCW) has been chosen by the Warfighter Information Network-Tactical (WIN-T) community as the networking standard for fullmesh IP over SHF satellite communications. Large-aperture strategic terminals and small-aperture tactical/mobile terminals using satellite communications on the move (S-COTM) are just two examples of the diverse network of terminals that the NCW supports. By using an advanced network scheduler, it makes nearly optimal use of satellite and terminal resources to maximize network data throughput and terminal population. In this paper, the main characteristics of the waveform MAC and Physical Layers are described.

The study in [8] offers a methodology for evaluating and analyzing tactical communications networks to ascertain whether or not they adhere to DoD recommendations for network-centric warfare. The process is a component of the national security system (NSS) and information technology (IT) interoperability process of the Department of Defense (DoD), which is capability-focused and effects-based. The paper focuses on this process's evaluation and analysis stage. As an example, the methodology is demonstrated using the Warfighter Information Network-Tactical (WIN-T). Army tactical Global Information Grid (GIG) design, development, production, and fielding are accomplished through a single integrating net-centric framework established by the WIN-T program. In order to conduct tactical communications in a Net-Centric Environment (NCE), WIN-T had to overcome certain obstacles, which are explained and their solutions are provided. An integrated Operational, Systems, Technical, and All Views architecture that sufficiently handles all internal and external system information exchanges is said to be necessary in order to support the net-centric warfare concept. Using and updating this architecture is crucial for all stages of system development and improvement.

The paper in [9] offers a method for enabling DSA functionality on existing military radios

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

without requiring any changes to their firmware or hardware. In contrast to embedded sensors that have sophisticated feature-based sensing algorithms, application-level messaging, and a cognitive engine written in a high-level language that is located outside the radios, external sensors enable DSA functionality in radios. A network of three Warfighter Information Network-Tactical (WIN-T) Local Area Waveform (LAW) nodes in friendly and unfriendly interference was used in a real-time over-the-air demonstration for such a cognitive radio test-bed at the US Army CERDEC's Ft.Dix facility. The system, test-bed operation, and some field demonstration results are briefly described in this paper.

In [10], a plan for bringing four different networks together under the Internet Protocol (IP) umbrella is proposed. WIN-T, the Army Warfighter Information Network-Tactical area common user system, is the first network. Using the Mobile Ad Hoc Interoperability Networking Gateway (MAINGATE) system, the second network extends to the local common user system. Third is the wireless access network based on Worldwide Interoperability for Microwave Access (WiMax), and fourth is the 802.11 WiFi network. At the tactical level of the battlefield, this paper aims to present a basic wireless strategy that will establish "Everything over IEEE" ("EoIEEE") and everything over IP (EoIP) standards.

Unlike Internet Protocol (IP) network systems, Named Data Networking is a novel idea that adopts a fundamentally different approach in [11]. IP-type networks use locations, represented by IP addresses, to direct data transmission messages to their intended recipients. On the other hand, Named Data Networks (NDNs) give more attention to the data itself than to the specific locations of the data. In an NDN, the actual data being sent or requested—rather than the assumed locations of the data content—determines the forwarding decisions. To enable IP message delivery, NDNs name the data itself rather than network locations. By avoiding many of the issues and inefficiencies that plague IP networks, this novel method enables NDN nodes to more readily utilize the broadcast capabilities present in many modern networking devices. It is worthwhile to look into the advantages that NDN might be able to offer military communication systems, as many of these systems rely on IP mechanisms to provide networking functionality. Particular aspects of the NDN architecture's design offer an effective substitute for IP-based systems, especially for those functioning in challenging environments. Thus, an emulation analysis of military communication networks aided by NDN is presented in this paper. The authors also give a brief overview of the NDN architecture and how it can be integrated into different military communication networks, including the Army's Warfighter Information Network-Tactical (WIN-T) and the Navy's Automated Digital Networking System (ADNS). Initial findings indicate that applying the NDN architecture to these military communication networks results in significant performance improvements.

The study in[12] presents the theory of operation for the Warfighter Information Network-Tactical (WIN-T), the Army's future communications network. From theater-level to the commander at the company level, the WIN-T is the Army's first fully integrated data network, supporting most tactical Warfighters in the tactical theater. The future force will be widely distributed, and WIN-T will eventually provide a variety of communications tiers, such as satellite communications (SATCOM), airborne relay, and ground-based Line-Of-Sight (LOS). The WIN-T architecture was created in four stages. The Increment 2 and Increment 3 stages of the WINT program are the main topics of this study. From company level units to theater level echelon, the Army warfighter can utilize WIN-T, a common user system, which offers Everything over IP (EoIP) capabilities. With every increment, the tactical warfighter gains new capabilities and improved technologies.

Ground combat vehicles (GCVs) in Warfighter Information Network-Tactical (WIN-T) systems are autonomous and highly networked in [13,14]. In a dynamic environment, it can be difficult to safeguard numerous wireless communication links from enemy interception. GCV mobility makes it easy to breach the Low Probability of Interception (LPI) capacity, especially when using multiple interception techniques at once. The issue of maintaining LPI capability under both conventional optimization and Deep Reinforcement Learning (DRL) techniques is examined by the

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

authors in this work. In contrast to earlier research, the authors suggest an anti-interception approach that counters both correlation-based and energy-based interceptor techniques. The strategy jointly optimizes power allocation (PA) and spreading factor assignment (SA) of the WIN-T to avoid these interceptors. The authors used sophisticated techniques like decomposition and difference of convex functions (DC) to solve the problem because it is mathematically formulated as a non-convex optimization model. The authors developed a Multi-Agent Deep Reinforcement Learning (MADRL) approach to get the optimal solution almost instantly. The suggested MADRL strategy's performance is near the optimal solution, according to the numerical results, which makes it suitable for real-world systems.

Conclusion

This paper focused on warfighter information network-tactical, one of the most significant technologies in the field of military telecommunication networks. The paper described the operation of this technology and its military applications. Additionally, the paper included a brief description of some earlier technological works.

Recommendations

Based on the conducted analysis of WIN-T architecture, literature review, and identified problematic aspects (particularly regarding security, quality of service, and integration of heterogeneous networks), the following recommendations are formulated for further development, implementation, and operation of the Warfighter Information Network-Tactical.

1. Network Architecture Improvement

1.1. Fault tolerance enhancement. The current multi-star topology with core routers creates potential single points of failure. It is recommended to implement redundant core configurations (redundant core routers) with automatic failover protocols (e.g., VRRP or HSRP) at brigade and division Tactical Operations Centers (TOCs).

1.2. LAN-A/LAN-B segmentation optimization. To improve throughput, it is recommended to implement dynamic QoS marking at the LAN-A/LAN-B boundary, taking into account priorities of different traffic types (voice, video, intelligence data). This will prevent queuing at edge switches.

1.3. NDN integration. Given the promising research results of Named Data Networking (NDN) [11], it is recommended to conduct experimental implementation of NDN at the lower tactical internet (lower TI) level as an alternative or overlay to IP. This is particularly relevant for environments with limited bandwidth and frequent communication disruptions, where priority is delivery of named data (e.g., "friendly commander's position") rather than connections between specific IP addresses.

2. Information Security Assurance

2.1. Expansion of the defense-in-depth concept. It is recommended to add a separate "AI-based adaptive response" layer to the existing defense-in-depth model. Using the results from [13,14] on MADRL, it is proposed to implement machine learning agents that reconfigure in real time power allocation parameters and spreading factor assignments to counter correlation-based and energy-based interception techniques.

2.2. Elimination of the QoS gap between plaintext and ciphertext traffic. Since encryptors block information exchange between WAN and LAN [3,4], it is recommended to develop a low-overhead signaling protocol that transmits aggregated congestion metrics (e.g., delay or packet loss levels) in encrypted form. This will allow coordination of MBAC operation on both sides of the encryptor.

2.3. LPI/LPD enhancement for moving vehicles. For Ground Combat Vehicles (GCVs), it is recommended to apply a hybrid approach: combining traditional optimization methods (DC function methods and decomposition) with MADRL to ensure Low Probability of Interception (LPI) even at speeds exceeding 25 mph. This should account for the possibility of simultaneous application of multiple interception techniques.

3. Quality of Service (QoS) Management

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

3.1. MBAC adaptation to electronic warfare conditions. The Measurement-Based Admission Control (MBAC) algorithm should be supplemented with a jamming detection mechanism. In case of jamming detection, it is recommended to switch to more conservative admission thresholds and activate routing mechanisms bypassing affected areas.

3.2. Mission-based traffic prioritization. Instead of rigid service class divisions (voice, video, data), it is recommended to implement dynamic prioritization based on mission metadata (e.g., a fire support request should have higher priority than video broadcast from a general situational awareness channel).

4. Experimental Verification and Testing

4.1. Expansion of test scenarios. In addition to controlled conditions using satellite emulators [6], it is recommended to conduct WIN-T testing in more realistic conditions: with active electronic warfare jamming, multipath fading, and dynamically changing interference spectra.

4.2. MADRL field validation. Deep Reinforcement Learning algorithms [13,14] should be verified on actual WIN-T hardware using tactical radios (SINCGARS, EPLRS, NTDR) in multi-agent group configurations.

5. Integration with Joint Forces and Systems

5.1. Interoperability expansion with GIG and JTRS. It is recommended to accelerate the development of gateways for seamless data exchange between WIN-T and the Joint Tactical Radio System (JTRS), as well as with the Global Information Grid (GIG). Particular attention should be paid to ensuring operation in multinational coalition operations.

5.2. Support for expeditionary operations. To provide communications in remote areas without ground infrastructure, it is recommended to more widely use a combination of satellite channels (SOTM) and aerial relays (HALE, MALE UAVs), which will maintain communications in undeployed theaters of operations.

6. Future Research Directions

The following priority directions for further research are identified:

Development of cognitive spectrum management algorithms capable of operating within encrypted tactical networks without revealing signaling information.

Quantitative comparison of NDN and IP-based protocols in WIN-T in terms of latency, overhead, and packet loss resilience.

Investigation of defense-in-depth impact on MBAC performance and development of methods for coordinating security and QoS policies.

Creation of a realistic benchmark testbed for WIN-T testing under electronic warfare conditions with the ability to reproduce active jamming and interception scenarios.

This "Recommendations" section logically concludes the article and provides concrete steps for researchers, developers, and military professionals.

Conflict of Interest

The author declares that he has no competing interests related to the subject of the article.

References

1. Sharret, P. (1999). WIN-T—the Army's new tactical intranet. *In MILCOM 1999. IEEE Military Communications Conference Proceedings* (Vol. 2, pp. 1383–1387). IEEE. https://doi.org/10.1109/MILCOM.1999.821430
2. Jacobs, S. (1999). Tactical network security. *In MILCOM 1999. IEEE Military Communications Conference Proceedings* (Vol. 1, pp. 651–655). IEEE. https://doi.org/10.1109/MILCOM.1999.822764
3. McCann, C. J., Elmasry, G. F., Russell, B., & Welsh, B. (2004). A measurement-based approach for multilevel admission of heterogeneous traffic in wireless ad-hoc networks. *In IEEE MILCOM 2004. Military Communications Conference* (Vol. 3, pp. 1562–1565). IEEE.

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

https://doi.org/10.1109/MILCOM.2004.1495171
4. Elmasry, G. F., & McCann, C. J. (2005). Partitioned QoS solution for tactical networks—addressing the impact of encryption. *In MILCOM 2005—IEEE Military Communications Conference* (Vol. 1, pp. 1–6). IEEE. https://doi.org/10.1109/MILCOM.2005.1605653
5. Shah, S. A. (2005). DISN advanced wireless mobile services (DAWMS) in global net-centric environment for the warfighter. *In MILCOM 2005—IEEE Military Communications Conference* (Vol. 4, pp. 2590–2595). IEEE. https://doi.org/10.1109/MILCOM.2005.1606057
6. Wexler, R. S., Hoffmann, R., Collins, M. R., & Moran, P. (2006). Successful development and test of SATCOM On-The-Move (OTM) Ku-band Ka-band systems for the Army's Warfighter Information Network-Tactical (WIN-T). *In MILCOM 2006—IEEE Military Communications Conference* (pp. 1–7). IEEE. https://doi.org/10.1109/MILCOM.2006.302343
7. Wiss, & Gupta, R. (2007). The WIN-T MF-TDMA mesh network centric waveform. *In MILCOM 2007—IEEE Military Communications Conference* (pp. 1–6). IEEE. https://doi.org/10.1109/MILCOM.2007.4454797
8. Hermelee, & Turczyn, S. (2007). Assessment and analysis of tactical communications in a net-centric environment. *In MILCOM 2007—IEEE Military Communications Conference* (pp. 1–6). IEEE. https://doi.org/10.1109/MILCOM.2007.4455070
9. Mody, N., et al. (2010). On making the current military radios cognitive without hardware or firmware modifications. *In MILCOM 2010—IEEE Military Communications Conference* (pp. 2327–2332). IEEE. https://doi.org/10.1109/MILCOM.2010.5680354
10. Carlson, F. R. (2011). Strategy for tactical cellular connectivity. *Proceedings of SPIE, 8062*, 80620N. https://doi.org/10.1117/12.881205
11. Etefia, M., Gerla, M., & Zhang, L. (2012). Supporting military communications with Named Data Networking: An emulation analysis. *In MILCOM 2012—IEEE Military Communications Conference* (pp. 1–6). IEEE. https://doi.org/10.1109/MILCOM.2012.6415685
12. Ali, S. R., & Wexler, R. S. (2013). Army Warfighter Network–Tactical (WIN-T) theory of operation. *In MILCOM 2013—IEEE Military Communications Conference* (pp. 1453–1461). IEEE. https://doi.org/10.1109/MILCOM.2013.246
13. Le, V. H., Nguyen, T. T., Nguyen, K. K., & Singh, S. (2022). Joint energy and correlation based anti-intercepts for ground combat vehicles. *In MILCOM 2022—IEEE Military Communications Conference* (pp. 867–872). IEEE. https://doi.org/10.1109/MILCOM55135.2022.10017791
14. Le, V. H., Nguyen, T. T., & Nguyen, K. K. (2023). Dual wireless anti-interception for ground combat vehicles. *IEEE Transactions on Vehicular Technology, 72*(12), 16236–16248. https://doi.org/10.1109/TVT.2023.3298514

Огляд літератури щодо питань військової тактичної інформаційно-комунікаційної мережі WIN-T

Муханнад Аль-Раві
Бандунзький технологічний інститут
Індонезія
e-mail: muhrawi@yahoo.com
ORCID: 0000-0003-1407-6519

Анотація. У сучасних умовах ведення бойових дій інформаційна перевага стає одним із ключових факторів успіху операцій. Зростаючі вимоги до швидкості, безпеки та обсягів передачі даних, а також необхідність інтеграції різнорідних систем управління, зв'язку, комп'ютеризації та розвідки (C4I) вимагають створення принципово нових тактичних мереж. Стаття присвячена аналізу тактичної інформаційної мережі бійця (Warfighter Information

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Network-Tactical, WIN-T), яка є основою для реалізації концепції Force XXI та забезпечення домінування в інформаційному просторі. Метою роботи є опис архітектури, принципів функціонування та механізмів забезпечення інформаційної безпеки WIN-T, а також узагальнення результатів попередніх досліджень у цій галузі. Окремим завданням є демонстрація військових застосувань мережі для підвищення мобільності, живучості та ефективності управління військами. Дослідження базується на системному аналізі відкритих архітектурних специфікацій WIN-T, зокрема її поділу на верхній і нижній рівні тактичного інтернету (Tactical Internet). Розглядаються мережеві топології (LAN-A, LAN-B, WAN) із використанням комутаторів, маршрутизаторів, технологій ATM, HSMUX, а також засобів радіозв'язку (NTDR, SINCGARS, EPLRS). Для забезпечення безпеки застосовано концепцію «ешелонованого захисту» (defense-in-depth). Методологія також включає огляд літератури, де аналізуються рішення QoS, методи криптографії, когнітивні радіосистеми та технології Deep Reinforcement Learning. У статті детально описано архітектуру WIN-T, яка інтегрує систему управління боєм армії США (ABCS) та забезпечує зв'язок від рівня бригади до окремого транспортного засобу. Показано, що WIN-T створює єдину транспортну мережу з підтримкою IP (Everything over IP), що поєднує супутниковий зв'язок (Ku/Ka-діапазони), радіорелейні лінії та волоконно-оптичні канали. Упроваджено механізми адаптивного управління доступом на основі вимірювань (MBAC) для пріоритезації трафіку (голос, відео, дані). У сфері безпеки реалізовано багаторівневу систему виявлення вторгнень та реагування. Окремим результатом є представлення концепції Named Data Networking (NDN) як альтернативи традиційним IP-мережам для підвищення ефективності в складних умовах. WIN-T забезпечує командирів можливістю отримувати оновлені топографічні карти, відеопотоки з поля бою та дані розвідки в реальному часі безпосередньо під час руху (on-the-move). Мережа підтримує роботу критичних систем, таких як Advanced Field Artillery Tactical Data System (AFATDS) та Command Post of the Future (CPOF). Результати польових випробувань підтвердили пропускну здатність понад 1 Мбіт/с у Ka-діапазоні при швидкості руху понад 25 миль/год. Запропоновані рішення з оптимізації потужності та розподілу ресурсів на основі MADRL значно підвищують стійкість до перехоплення сигналу, що має вирішальне значення для живучості підрозділів на полі бою.

Ключові слова: WIN-T, архітектура, безпека, військові застосування.

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., Шнукало А.

Формат 70x100/16
Папір офсетний. Друк цифровий.
Ум. друк. арк. 23,83.
Наклад 200 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