УДК [351.743+351.746.1+355/359](477)(05)

ISSN 2786–6920 (Print),
ISSN 2786–880X (Online)

КИЇВСЬКИЙ ІНСТИТУТ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ

НАУКОВИЙ ВІСНИК КИЇВСЬКОГО ІНСТИТУТУ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ

№ 2 (7) 2025

Scientific Bulletin of the Kyiv Institute of the National Guard of Ukraine

Засновник: Київський інститут Національної гвардії України.
Видається з грудня 2022 року. *Періодичність:* двічі на рік.
Свідоцтво про державну реєстрацію друкованого засобу інформації
КВ № 25202-15142 Р від 03.08.2022 р.

Наукове видання внесено до Реєстру суб'єктів у сфері медіа. Ідентифікатор медіа у Реєстрі R30-01116 (рішення Національної ради України з питань телебачення та радіомовлення № 53 від 01.09.2023 р.).

Видання входить до категорії «Б» Переліку наукових фахових видань України зі спеціальностей: К1 – Державна безпека, К6 – Забезпечення військ (сил), D8 – Право (наказ МОН від 20.06.2023 р. № 768); К5 – Військове управління (за видами збройних сил) (наказ МОН від 25.10.2023 р. № 1309).

Рекомендовано до друку та розміщення у мережі Інтернет вченою радою КІ НГУ, протокол № 7 від 29.11.2025 р.

Науковий вісник Київського інституту Національної гвардії України. Київ : КІ НГУ, 2025. № 2 (7). 180 с.

Проблематика: актуальні питання розвитку складових сектору безпеки і оборони України; службово-бойова діяльність НГУ: безпековий та оборонний аспекти; забезпечення громадської, державної та воєнної безпеки; розвиток спроможностей складових сектору безпеки і оборони України та впровадження передових технологій; нормативно-правове забезпечення й актуальні проблеми діяльності складових сектору безпеки і оборони України.

«Науковий вісник Київського інституту Національної гвардії України» є рецензованим виданням, що підтримує політику відкритого доступу до наукових публікацій.

Електронні копії видання зберігаються у базі даних «Наукова періодика України» Національної бібліотеки України імені В. І. Вернадського https://surl.li/zjvams.

Думка редакційної колегії може не збігатися з поглядами авторів матеріалів. За достовірність фактів, цитат, власних назв, посилань на використані джерела та інших відомостей відповідають автори наукових статей. У разі цитування посилання на журнал є обов'язковим.

Контакти редакції: вул. Оборони Києва, 7, м. Київ, 03179, Україна, +380660578940
Вебсайт видання: kingu-visnyk.kyiv.ua, email: visnyk_kingu@ukr.net

UDC [351.743+351.746.1+355/359](477)(05)

ISSN 2786–6920 (Print),
ISSN 2786–880X (Online)

KYIV INSTITUTE OF THE NATIONAL GUARD OF UKRAINE

SCIENTIFIC BULLETIN

OF THE KYIV INSTITUTE

OF THE NATIONAL GUARD OF UKRAINE

No. 2 (7) 2025

Науковий вісник Київського інституту Національної гвардії України

It was founded by: Kyiv Institute of the National Guard of Ukraine.
It is published since December 2022. Frequency: twice a year.
Certificate of state registration of the printed media
KB No. 25202-15142 P dated 03.08.2022.

Amendments to the register of media entities – registrants No. 53 dated 09.01.2023 of the National Council of Ukraine on Television and Radio Broadcasting Register ID – R30-01116.

The publication is included in category "B" of the List of Scientific Professional Publications of Ukraine in the following specialties: K1 – State Security, K6 – Provision of Troops (Force), D8 – Law (Order of the Ministry of Education and Science of Ukraine dated 20.06.2023 No. 768); K5 – Military Administration (by types of armed forces) (Order of the Ministry of Education and Science of Ukraine dated 25.10.2023 No. 1309).

Recommended for publication and posting on the Internet
by the Academic Council of the KI NGU, protocol No. 7 of 29.11.2025.

Scientific Bulletin of the Kyiv Institute of the National Guard of Ukraine. Kyiv : KI NGU, 2025. No. 2 (7). 180 p.

Topics: current issues of development of the security and defence sector of Ukraine; service and combat activities of the NGU: security and defence aspects; ensuring public, state and military security; development of capabilities of the security and defence sector of Ukraine and introduction of advanced technologies; regulatory and legal support and current issues of the security and defence sector of Ukraine.

The "Scientific Bulletin of the Kyiv Institute of the National Guard of Ukraine" is a peer-reviewed publication that supports the policy of open access to scientific publications.

Electronic copies of the Scientific Bulletin are stored in the "Scientific Periodicals of Ukraine" database of the Vernadsky National Library of Ukraine https://surl.li/zjvams.

The editorial board's opinion may not coincide with the authors' views of the materials. The authors of scientific articles are responsible for accurate facts, quotations, proper names, references to sources and other information. When quoting, reference to the Scientific Bulletin is mandatory.

Contacts of the editorial board: 7 Oborony Kyieva Str., Kyiv, 03179, Ukraine, +380660578940.
Website: kingu-visnyk.kyiv.ua, email: visnyk_kingu@ukr.net

РЕДАКЦІЙНА КОЛЕГІЯ

EDITORIAL BOARD

ЗМІСТ

CONTENTS

UDC 534.2:531.19 DOI 10.59226/2786-6920.2.2025.7-15

ABRAMOV SERHII
Candidate of Technical Sciences, Associate Professor,
Senior Researcher of the Research Laboratory for Training Troops,
Kyiv Institute of the National Guard of Ukraine
https://orcid.org/0000-0003-0675-4850

TYTARENKO OLEKSII
Doctor of Juridical Sciences, Associate Professor,
Head of the Research Laboratory for Training Troops,
Kyiv Institute of the National Guard of Ukraine
https://orcid.org/0000-0002-3271-9402

USE OF DIMENSIONAL AND DIMENSIONALLESS COMPLEXES TO DESCRIBE AN EXPLOSION

The paper considers the development and verification of a system of dimensional and dimensionless complexes that adequately describe the physics of electrical conductor explosions (ECEs) in a wide range of modes, providing the possibility of predictive scaling and process control. In conditions where the source parameters (capacitance of the capacitor bank C, inductance of the discharge circuit L, initial voltage U_0) and conductor geometry can vary widely, the ECEs process acts as a flexible technical tool. The influence of the main parameters of the power source - capacitor bank capacity (C), discharge circuit inductance (L) and initial voltage (U_0) - as well as the geometry of the conductor on the kinetics of energy transformations during ECEs is considered. It is shown that changing these parameters allows varying the rate of energy release, the temporal evolution of current and voltage, the temperature and volume of plasma, which directly determines the intensity of mechanical (shock wave, pressure) and electro-optical (luminescence, radiation spectrum) effects. For each group, the physical content, limits of applicability, and its effect on the peak excess pressure, duration of the positive phase, impulse, as well as the radiation characteristics and dimensional-energy distribution of particles in the case of nanomaterial synthesis are determined. The methodology combines analytical calculations, scaled experimental studies of discharge series with variations in C, L, U_0, conductor geometry, and medium properties. The expected results are universal empirical and semi-automated correlations that will allow controlling the characteristics of the ECEs for specific applications: a pulsed light source with a controlled spectrum and duration, a controlled shock wave generator for research and industrial needs, and adaptive pulse current interrupters. The results obtained can be used to develop pulsed light sources with a controlled spectrum, shock wave generators and adaptive switching systems in high-voltage technology, as well as in the development of a device for detecting and clearing mines on water logistics routes for operational units of the National Guard of Ukraine in the conditions of performing combat missions.

Keywords: *explosion; parameter; installation; current; impact; conductor.*

Statement of the problem. The ability to vary the characteristics of electrical conductor explosions (ECEs) over a wide range by adjusting the electrical parameters of the power source, modifying the conductor geometry, or changing the properties of the surrounding medium makes ECEs

a readily tunable "tool" that significantly broadens their range of applications [1–3]. Varying the capacitance of the capacitor bank, the inductance of the discharge circuit L, or the initial voltage U_0 can substantially affect both the rate of energy release during the explosion and the total energy released in an ECE. This enables the use of an exploding conductor as a pulsed light source, a source of **shock waves (SWs)**, an interrupter of pulsed currents, and a tool for producing nanomaterials with controllable particle sizes [4], among other applications.

Analysis of recent research and publications. In this context, the task of finding wire and circuit parameters for achieving a specific technological effect becomes relevant; this concerns the classification of explosions and the tools for determining the necessary parameters [5]. The first work devoted to the classification of different types of **electrical conductor explosions (ECEs)** based on a range of different characteristics is presented in this publication [6]. The question of which parameters and sets of metrics can most comprehensively characterize the results obtained in explosion experiments was also addressed in earlier studies. For example, in [7, 8], when investigating the electrical and optical characteristics of conductor explosions up to the moment of explosion, dependencies of the volumetric energy density W/V for conductors of various materials (in later works the energy density W/m was used) on the current density were constructed. These studies were the first to propose using an additional variable quantity—the so-called "action integral":

$$S_i = \int_0^t I^2 dt, \qquad (1)$$

where: *I* is the current in the discharge channel.
These approaches to the classification and analysis of experimental results are actively used at present as well [9, 10].

Another approach to the problem is also used, based on the application of dimensional and similarity methods to the study of **electrical conductor explosions (ECEs)** (see [11]). In the works of several authors, it has been shown that identical oscillograms – characterized by the same decay phase, its depth, and the magnitude of the secondary discharge current pulse – can be obtained with different combinations of exploding conductor parameters. The presence of identical electrical characteristics allowed for the assumption of the phenomenon's similarity. As a result of analyzing arrays of experimental data and physical processes occurring at various stages of the explosion, these authors obtained certain dimensionless sets – similarity criteria – whereby the electrical characteristics of the explosion for these stages coincided when the criteria were preserved. The advantages of this approach include the clear analytical form of the resulting expressions and the possibility, based on them, to predict the type of electrical characteristics in ECEs under different conditions.

The purpose of the article is to clarify how these two approaches – based on the analysis of dimensional and dimensionless sets describing the explosion – relate to each other and to what extent they can be used to predict the parameters of currents arising during an **electrical conductor explosion (ECE)**, and particularly the **shock waves (SWs)**.

Presentation of the main material. To determine the influence of various factors and parameters of an ECE – both "primary" ones, such as current, voltage, conductor length, etc., and composite ones (stored energy, similarity criteria, etc.) – on the amplitude of the shock wave generated by the explosion, we use the widely known experimental data presented in [11] to analyze the impact of changes in dimensionless similarity criteria on the electrical characteristics of ECEs. The criteria obtained in this work include, in addition to combinations of the discharge circuit parameters and a set of values characterizing the properties of the conductor material, also the geometric parameters of the conductors. For example, the **P_2 criterion** includes the conductor diameter d_w:

$$P_2 = \frac{1}{S^2 \gamma_0 \sigma_0 (\lambda_m + \lambda_b)} \cdot \frac{C^{3/2} U_0^2}{L^{1/2}}, \qquad (2)$$

and the P_3 criterion – its length *l_w*:

$$P_3 = \frac{Al^2}{U_0^2\sqrt{LC}}. \quad (3)$$

Here, γ_0 is the density, σ_0 is the electrical conductivity, and λ_m and λ_b are the specific heats of melting and vaporization of the conductor material, which characterize the individual properties of the conductor metal. In (2), *S* is the cross-sectional area of the conductor, $S = \pi d^2/4$, and in (3), $A = 10^4$ *(V²·s)/m²* is the spark constant, which does not depend on the conductor material.

To illustrate the effect of changing these parameters on the nature of the explosion, [11] presents dimensionless current oscillograms for the electrical explosion of copper conductors**,** showing the change in the sharp decay phase of the current when varying P_2 by changing the conductor diameter *d_w* (P_3 and the conductor length *l_w* remain unchanged). From the presented current oscillograms, it follows that as the diameter of the exploding conductor increases, the first current peak rises, as does the time to explosion. At the same time, the initial rising sections of the current coincide with the short-circuit current and with each other. To illustrate the effect of changing P_3 (varying *l_w*, *d_w* unchanged) on the nature of the explosion, another set of current oscillograms is presented. It is shown that changing the conductor length has little influence on the explosion phase.
A third set of oscillograms is provided to demonstrate the actual similarity of the electrical characteristics of the explosion under different conditions when both $\mathbf{P_2}$ and $\mathbf{P_3}$ are kept equal. At the same time, practically all dimensional parameters characterizing the explosion regime can vary quite significantly.

The main electrical parameters and the parameters of the exploding conductors for these three cases are presented in Table 1. In the first group (I), numbers 1 to 3 show the parameter values with constant $\mathbf{P_3}$ and *l_w*, while in the second group (II), numbers 4 to 9 correspond to unchanged $\mathbf{P_2}$ and *d_w*. The parameter set labeled III in Table 1 (numbers 10 to 13) corresponds to the situation where the presented discharge current curves are similar (practically coinciding) for different regimes in which $\mathbf{P_2}$ and $\mathbf{P_3}$ are the same.

Table 1. Main electrical parameters and parameters of exploding conductors

		U_0, 10^3 В	C, 10^{-6} Ф	L, 10^{-6} Г	Imax, 10^3 А	l_w, 10^{-3} А	d_w, 10^{-3} м	W_0/m, 10^6 Дж/м	Π_2, 10^{-1}	Π_3, 10^{-2}	Π_2/Π_3
I	1	14	99,0	3	80,4	100	0,40	86,46	36,10	2,960	122,00
	2	»	»	»	»	»	0,50	55,33	14,80	»	50,00
	3	»	»	»	»	»	0,68	29,92	4,33	»	14,60
II	4	»	»	10	44,0	20	0,50	276,70	8,10	0,065	10^3
	5	»	»	»	»	40	»	138,30	»	0,259	312,00
	6	»	»	»	»	100	»	55,33	»	1,620	50,00
	7	»	»	»	»	140	»	39,52	»	3,180	25,50
	8	»	»	»	»	180	»	30,74	»	5,250	15,40
	9	»	»	»	»	260	»	21,28	»	11,000	7,39
III	10	40	3,0	2,26	46,1	116	0,30	32,78	5,66	3,230	17,50
	11	18	34,6	2,53	66,6	100	0,51	30,73	5,08	3,300	15,40
	12	14	99,0	3,00	80,4	100	0,66	31,76	4,87	2,960	16,50
	13	8	48,0	10,60	17,0	67	0,33	30,02	4,57	3,110	14,70

In Table 1: U_0 – initial voltage of the capacitor bank, C – capacitance of the capacitor bank, L – inductance of the discharge circuit, $I_{max} = U_0 / \sqrt{(L/C)}$ – maximum current, l_w, d_w – length and diameter of the conductor, W_0/m – ratio of stored energy to conductor mass, P_2 and P_3 – similarity criteria.

The mathematical model describing the currents arising during an *UEE* includes a number of relations that characterize the complex nonlinear process of conductor destruction under the action of high current pulses, Joule heating, plasma expansion in the discharge channel, and so on, including a system of hyperbolic-type equations to describe the behavior of gas-dynamic parameters in space. Such systems of equations do not admit analytical solutions, so the problems were solved numerically.

For the mathematical description of *ECEs*, the thermal explosion model proposed in [12] was used. The adiabatic heating of the conductor in the model is described by a system of equations with dimensionless variables:

$$\begin{cases} i'' + R_0 C\omega (ir)' + i = 0; \\ \theta' = \left(I_m^2 R_0 \Big/ c_p m_w T_C \omega \right) i^2 r; \\ r = (1-\theta)^{-n}, \end{cases} \qquad (4)$$

which includes the equations of the RLC discharge circuit (***R*** – resistance, Ω), the heat balance equation, and the equation relating the conductor's resistance to temperature.

Here, $i = I/I_{max}$, where I is the discharge current in the circuit; $r = R/R_0$; $\theta = T/T_c$, U_0 is the initial voltage; R_0 is the resistance at the initial temperature T_0, °C; T_c is the critical temperature; c_p, m_w are the heat capacity ([c_p] = J/(kg·K)) and mass of the conductor ([m_w] = kg). A prime denotes the derivative with respect to $\tau=\omega t$ (t – time, $\omega = (LC)^{-1/2}$). From system (4), it is straightforward to eliminate the temperature. By combining the second and third equations of the system, one can write: $\theta' = (I_m^2 R_0/cmT_c\omega) i^2 (1-\theta)^{-n}$.

Integrating the above equation under zero initial conditions ($\tau = 0$, $\theta(0) = \theta_0$), we obtain the dependence of the resistance on the "action integral" S_i in the form [13]:

$$r = \left(1 - P_2 \int_0^\tau i^2 \, d\tau\right)^{-\frac{n}{n+1}} \qquad (5)$$

where $n \approx 3.5$ is the exponent.

The combined solution of the current equation from system (4) and relation (5) gives the dependence of the conductor's resistance on the current at any phase of the conductor explosion. The initial conditions for solving system (4) are "zero":

$$r(0) = 1,\ i(0) = 0,\ \theta(0) = \theta_0. \qquad (6)$$

To "individualize" the fluid flow, it is necessary to link the solution of the conductor explosion problem with the flow problem by determining the conditions at the contact break. For this purpose, we use an equation describing the displacement of the conductor surface due to thermal expansion.The radial thermal expansion of the conductor depends linearly on temperature, $a = a_0(1 + \alpha T)$, so the expansion velocity (for α = const, where α is the linear thermal expansion coefficient, and a is the conductor radius) is given by:

$$a' = P_a i^2 r, \qquad (7)$$

where $P_a = \alpha I_m^2 R_0 / C_p m\omega$. Here, we used the energy balance from system (4) to eliminate the temperature. Solving system (4) in the form modified by (7), and in the presence of (6), provides the law of thermal expansion of the conductor, which is necessary to detail the flow in an underwater electrical explosion of conductors **.**

The plasma (arc) stage of an *underwater electrical explosion (UEE)* can be described within the framework of the model developed in [14]. The energy balance for the discharge channel is written as [15]:

$$(\gamma_a - 1)^{-1} \left(\tilde{P}F\right)' + \tilde{P}F' = 2\Pi_1 i^2 r/\pi, \qquad (8)$$

where P, F, i, r are the dimensionless pressure, cross-section, current, and resistance of the discharge channel, respectively:

$$F = S/S_{ef},\ \tilde{P} = P/P_{ef},\ S = \pi a^2;\ S_{ef} = \pi U_0^2 (C/\omega^2 \gamma_0 l)^{1/2};\ P_{ef} = \gamma_0 S_{ef} \omega^2 / 2\pi.$$

To determine the electrical resistance of the discharge channel, an empirically established relation is used [11].

$$r = \frac{Al(\gamma_a - 1)}{R_0 P_{ef} S_{ef}} \left(\tilde{P}\right) F^{-1}. \qquad (9)$$

Equations (8) and (9), together with the current equation (4), form a system of equations for determining the boundary conditions used to solve the boundary-value problem. The initial conditions are chosen as "natural" – the radius of the discharge channel, as well as the pressure and velocity fields in the calculation region, are known at the moment of the conductor-to-discharge-channel "switching."

The system of unsteady gas-dynamic equations with one spatial variable in differential form (in Eulerian variables) is written as [16]:

$$\begin{cases} \frac{\partial}{\partial t}(x^v \gamma) + \frac{\partial}{\partial x}(x^v \gamma u) = 0; \\ \frac{\partial}{\partial t}(x^v \gamma u) + \frac{\partial}{\partial x}\left(x^v (p + \gamma u^2)\right) = v x^{v-1} p; \\ \frac{\partial}{\partial t}\left[x^v \gamma \left(\varepsilon + \frac{u^2}{2}\right)\right] + \frac{\partial}{\partial x}\left[x^v \lambda u \left(\varepsilon + \frac{u^2}{2}\right)\right] = 0, \end{cases} \qquad (10)$$

where **x, t** are Eulerian coordinates; **γ** – density; **ε** – specific internal energy of the gas; **p** – pressure; the exponent **ν = 0** for planar, **ν = 1** for cylindrical, and **ν = 2** for spherical flow symmetry.

The flows arising during an *underwater electrical explosion of conductors (UEE)* generally have cylindrical symmetry; therefore, we will assume **ν = 1** hereafter. For an unambiguous description of the flow, system (10) is supplemented with the equation of state of the fluid in the Tait form:

$$P = G\left(\frac{\gamma}{\gamma_0}\right)^x - B, \qquad (11)$$

where *G, χ, B* are constants. The initial conditions for system (10) were: $P(0, x) = P\infty$, $u(0, x) = 0$, $a_0 < x < x\_b$, where *xb* is the radius of the cylinder (calculation region). At the conductor (channel) surface and at the boundary of the calculation region, no-flow boundary conditions were applied. The conductor was positioned coaxially within a rigid cylindrical shell with a diameter of 11 mm.

To solve system (4), a correction formula for the one-dimensional case was used in combination with the Runge–Kutta method, applying direct iterations at each step. The integration of the system equations over a small time interval $\Delta\tau$ was carried out using artificial correction formulas derived from interpolation relations. Considering the smallness of Δτ, the trapezoidal rule was used for integrating the functions, while the products of functions were integrated using the artificial formulas.

The system of equations (10)–(11) with the initial and boundary conditions was solved using the standard finite-difference method of S. K. Godunov [16]. The model was tested by comparing the calculation results with experimental data [17].

Some results of the calculation of conductor explosions in water for the circuit and conductor parameters given in Table 1 are presented in Table 2. The row numbering and parameter groups correspond to those in Table 1 – for example, row 1 shows the results of the UEE calculation with the parameters listed in row 1 of Table 1.

Table 2. Results of conductor explosion calculations in water

		P_a, 10^9 Па	N_{max}, 10^9 Вт	N_{max}/l_w, 10^9 Вт/м	I_{ex}, 10^3 А	I_{ex}/I_{max}	S_i, 10^3 А^{2}с	t_{ex}, 10^{-6} с	$\frac{t_{ex}}{\pi\sqrt{LC}}$	W_{ex}, Дж	W_{ex}/m, 10^6 Дж/кг
I	1	0,260	5,89	58,9	40,00	0,498	6,05	9,89	0,183	672	5,990
	2	0,298	6,29	62,9	52,60	0,654	14,80	13,50	0,250	1047	5,969
	3	0,339	6,13	61,3	71,30	0,886	50,50	21,70	0,400	1945	5,997
II	4	0,240	0,57	28,4	35,70	0,810	14,80	30,20	0,305	210	5,995
	5	0,237	1,16	28,9	35,40	0,804	14,80	30,30	0,306	421	6,015
	6	0,227	2,54	25,4	34,50	0,784	14,80	30,60	0,310	1050	5,989
	7	0,221	3,80	27,1	33,93	0,770	14,80	30,90	0,312	1479	6,026
	8	0,225	4,45	24,7	33,40	0,758	14,80	31,10	0,315	1898	6,012
	9	0,202	5,90	22,7	38,10	0,729	14,80	31,60	0,320	2737	6,003
III	10	0,218	10,30	88,6	38,60	0,838	1,91	2,94	0,359	438	5,979
	11	0,301	6,98	69,8	57,00	0,857	16,00	11,00	0,375	1095	6,004
	12	0,337	6,27	62,7	69,70	0,867	44,80	20,60	0,381	1835	6,008
	13	0,133	7,70	11,5	14,90	0,867	28,00	27,70	0,392	307	6,008

Here, P_a – pressure on the wall at the moment the shock wave arrives, N_{max} – maximum power, N_{max}/l_w – maximum power per unit length of the channel, I_{ex} – current value at the moment of explosion, I_{ex}/I_{max} – relative ("normalized") current at the moment of explosion, S_i – "action integral", t_{ex} – explosion time, $t_{ex} / (\pi\sqrt{LC})$ – "normalized" explosion time, W_{ex} – energy released in the conductor at the moment of explosion, W_{ex}/m – ratio of the energy released in the conductor at the moment of explosion to the conductor mass.

By comparing the results of the conductor explosion calculations presented in Table 2 with the initial electrical parameters and the parameters of the exploding conductors (Table 1), one can note both agreement in some cases and complete discrepancy in others. Let us first examine how this manifests for individual parameter groups.

Group I. With unchanged circuit parameters and P_3 (which corresponds to the arc stage of the discharge [11]), the P_2 criterion is reduced by increasing the conductor diameter. At the same time, W_0/m and P_2/P_3 also decrease. The pressure P_a rises, as do the other measured parameters presented in Table 2. One might conclude that the primary cause of this is the increase in conductor diameter, provided we do not assume that changes in the parameters recorded in this experiment could lead to different results.

Group II. Here, P_3 is increased by increasing the conductor length, while all other parameters are fixed. Again, W_0/m and P_2/P_3 decrease synchronously. The pressure generally decreases across the parameter group as the conductor length increases, with regime №8 being the only exception to this trend. It is noteworthy that increasing the conductor length by 13 times reduces the pressure by no more than 16%. The maximum power increases with the conductor length, while the power per unit length of the conductor slightly decreases overall. All other measured parameters either increase slightly or remain unchanged. It should also be noted that in this group, conductor 7 has geometric parameters identical to №2 (Group I), differing electrically only in the circuit inductance. The calculated pressure for the conductor from the first group ($L = 3 \cdot 10^{-6}$ *H*) is significantly higher than that for the conductor from the second group ($L = 10^{-5}$ *H*), indicating the influence of the temporal factor on the pressure magnitude during an underwater electrical explosion of conductors (UEE).

Group III. This is the group of parameters for which the current characteristics of the *UEE* are similar despite large differences in both the geometric parameters of the conductors and the circuit parameters [11]. Here, a wide scatter in pressure behavior can also be noted – from No 10 to No 12, an increase (up to 35 %), and significantly lower values (1.6–2.5 times less) for No 13. At the same time, N_{max} values for these parameters are close, while N_{max}/l_w is significantly lower specifically for №13. For this regime, the explosion time is the longest in the group, and the energy released in the conductor at the moment of explosion is the lowest. These explosion features may be associated with the fact that, in this regime, the initial voltage is minimal, while capacitance and inductance are relatively large – that is, several factors "act" simultaneously. In any case, the inability to identify a primary factor or group of factors responsible for such pressure behavior in Group III when all parameters change indicates that the phenomenon is truly multifactorial, and it is currently impossible to combine all these factors into a single explanation.

Overall, among the calculated parameters in Table 1 and the measured values, N_{max}, N_{max}/l_w, the similarity criteria P_2, P_3, their ratio P_2/P_3, and W_0/m correlate relatively well with the pressure on the chamber wall. These parameters have long been used for preliminary assessments of explosion characteristics; moreover, as noted, some of them serve as similarity criteria. The only question concerns the validity of using the W_0/m ratio. It is known [18] that for optimal electrical explosion regimes, the ratio $(W_0/m)_{opt}$ depends on the properties of the conductor metal, i.e., it is invariant with respect to the discharge circuit parameters and conductor dimensions:

$$\left(W_0/_m\right)_{opt} = \sqrt{10^2 A} \cdot \left[\frac{\sigma_0 \cdot (\lambda_m + \lambda_b)}{8\pi^2 \gamma_0}\right]^{1/2}. \quad (12)$$

Let us consider the expression for the experimentally determined similarity criteria related to the electrical characteristics of conductor explosions (2). If we take the ratio of the second similarity criterion P_2 (2), which directly characterizes the explosion phase, to P_3 (3), which is more related to the arc stage of the discharge, it is easy to obtain the expression:

$$\frac{\mathrm{P}_2}{\mathrm{P}_3} = \frac{4}{A}\left(\frac{W_0}{m}\right)^2 \cdot \frac{\gamma_0}{\sigma_0(\lambda_m + \lambda_b)}. \quad (13)$$

Using formula (12), we obtain:

$$\frac{W_0}{m} = \frac{\pi\sqrt{2}}{10}\left(\frac{W_0}{m}\right)_{opt}\left(\frac{\mathrm{P}_2}{\mathrm{P}_3}\right)^{\frac{1}{2}}. \quad (14)$$

the dependence of W_0/m for an arbitrary conductor explosion regime, which includes the ratio of similarity criteria and the metal-specific constant $(W_0/m)_{opt}$. From formula (13), it follows that the ratio of stored energy to the conductor mass for any *UEE* regime, despite being a dimensional quantity, can be regarded as a similarity criterion of the electrical characteristics of a conductor explosion, since it includes the ratio of established similarity criteria and the quantity $(W_0/m)_{opt}$, which depends only on the properties of the conductor material.

Conclusions and prospects for further research. Various approaches to classifying types of conductor electrical explosions in a liquid have been examined, and it has been established that all the approaches considered in this study are applicable. For classifying conductor explosion types, it has been shown that, for describing the electrical characteristics of the explosion, these approaches are approximately equivalent. The use of the approach based on similarity criteria for predicting the nature of the explosion, in our view, is more “technologically convenient,” since the criteria are expressed in an explicit analytical form. Our evaluations have shown that the classification approach based on specific energy is also justified. We have confirmed that the ratio W_0/m also serves as a similarity criterion, expressed in dimensional form. For the specific stored energy in an arbitrary regime, an analytical expression has been obtained, the form of which supports the hypothesis that it also constitutes a similarity criterion. The influence of various factors on the gas dynamics of the explosion has been investigated. For individual cases, the parameters whose impact on the amplitude of the pressure wave is most significant have been identified.

The application of the considered approaches to predicting the gas-dynamic characteristics of an explosion is limited in nature. The results of this study show that such prediction is possible only in certain cases, when a single parameter is varied while all other parameters are kept fixed. In general, it may be assumed that the parameters whose variation leads to pronounced changes in the electrical characteristics are those that have a significant effect on the gas-dynamic characteristics of the explosion. The obtained results can be used in further developments related to remote demining in operational units of the National Guard of Ukraine under combat mission conditions.

References

1. Baranov M. I. (2017). *Rozrakhunkova otsinka osnovnykh fizyko-tekhnichnykh harakterystyk plazmy v lokalnii zoni povitrianoho elektrychnoho vybukhu metalevoho provodnika pid vplyvom velykoho impulsnoho strumu* [Estimated evaluation of the main physical and technical characteristics of plasma in the local zone of air electric explosion of a metallic conductor under a large pulsed current]. *Visnyk Natsionalnoho tekhnichnoho universytetu "KhPI".* Kharkiv, vol. 38 (1260), pp. 5–9 [in Ukrainian].

2. Baranov M. I. (2017). *Pryblyznyi rozrakhunok aktyvnoho oporu plazmennoho kanala iskrovoho rozriada u vysokovoltnomu sylnotochnomu povitrianomu kommutatori atmosfernoho tysku* [Approximate calculation of the active resistance of the plasma channel of a spark discharge in a high-voltage high-current air switch at atmospheric pressure]. *Visnyk Natsionalnoho tekhnichnoho universytetu "KhPI". Seriia: tekhnika ta elektrofizyka vysokykh napruh*. Kharkiv, vol. 15 (1237), pp. 5–11 [in Ukrainian].

3. Khainatskyi S. A. (2017). *Do pytannia pro klasyfikatsiiu elektrychnoho vybukhu providnykiv u ridyni* [On the classification of electrical explosion of conductors in liquid]. *Visnyk Natsionalnoho tekhnichnoho universytetu "KhPI". Seriia: tekhnika ta elektrofizyka vysokykh napruh*. Kharkiv, vol. 15 (1237), pp. 92–97 [in Ukrainian].

4. Baklar V. Yu., Kuskova N. I., Chelpanov D. I. (2016). *Fazovi traektorii vuhletsiu u protsesi vysokoenerhetychnykh rezhymiv elektrovybukhu hrafitovoho providnyka* [Phase trajectories of carbon in the process of high-energy modes of electric explosion of a graphite conductor]. *Visnyk Natsionalnoho tekhnichnoho universytetu "KhPI". Seriia: tekhnika ta elektrofizyka vysokykh napruh.* Kharkiv, vol. 36 (1208), pp. 5–9 [in Ukrainian].

5. Baranov M. I. (2003). *Sproshchena matematychna model elektrychnoho vybukhu providnukiv pid vplyvom velykykh impulsnykh strumiv* [Simplified mathematical model of the electric explosion of conductors under the influence of large pulsed currents]. *Visnyk Natsionalnoho tekhnichnoho universytetu "KhPI". Seriia:* elektrotekhnika i elektromekhanika. Kharkiv, vol. 3, pp. 59–64 [in Ukrainian].

6. Khainatskyi S. A. (2009). *Doslidzhennia optymalnoho rezhymu elektrychnoho vybukhu providnykiv u vodi i povitri* [Studies of the optimal mode of electric explosion of conductors in water

and air]. *Elektronna obrobka materialiv*, no. 5, pp. 57–64 [in Ukrainian].

7. Baranov, M. I., Koliushko, G. M., Kravchenko, V. I., Nedzel'skii, O. S., & Dnyshchenko, V. N. (2008). A current generator of the artificial lightning for full-scale tests of engineering objects. *Instruments and Experimental Techniques*, no. 3 (51), pp. 401–405. DOI: https://doi.org/10.1134/S0020441208030123 [in English].

8. Baranov M. I., Buriakovskyi S. H. (2024). *Elektrotekhnichne obladnannia dlia heneruvannia i vymiriuvannia povnoho impulsnoho strumu shtuchnoi blyskavky v umovah vysokovoltnoi elektrofizychnoi laboratorii* [Electrical engineering equipment for generating and measuring of complete pulse current of artificial lightning in the conditions of high-voltage electrophysics laboratory]. *Electrotekhnika i elektromekhanika,* no. 3, pp. 55–65. DOI: https://doi.org/10.20998/2074-272X.2024.3.08 [in Ukrainian].

9. Khainatskiy, S. A. (2009). Investigations on optimal mode of electric explosion of conductors in water and air. *Surface Engineering and Applied Electrochemistry*, no. 45 (5), pp. 397–403 [in English].

10. Kryvytskyi Ye. V. (1986). *Dynamika elektrovybukhu v ridyni* [Dynamics of electric explosion in liquid]. Kyiv : Naukova dumka [in Ukrainian].

11. Kryvytskyi Ye. V., Khainatskyi S. A. (1982). *Pro mekhanizm elektrychnoho vybukhu providnykiv* [On the mechanism of electric explosion of conductors]. *Tekhnichna elektrodynamika,* no. 4, pp. 22–28 [in Ukrainian].

12. Khainatskyi S. A. (1983). *Doslidzhennia zalezhnosti oporu providnyka, shcho vybukhaie, vid "intehrala dii" v riznykh modeliakh elektrovybukhu.* [Investigation of the dependence of the resistance of an exploding conductor on the "action integral" in various models of electric explosion]. *Fizychni osnovy elektrychnoho vybukhu.* Kyiv : Naukova dumka, pp. 65–73 [in Ukrainian].

13. Fedorovych O. A., Voitenko L. M. (2008). *Pro koeffitsiienty rozpadu neidealnoi plazmy impulsnykh rozriadiv u vodi pry kontsentratsiiakh elektroniv* $2\times10^{20} \geq Ne \geq 2\times10^{17}$ sm^{-3} [On the decay coefficients of non-ideal plasma of pulsed discharges in water at electron concentrations $2\times10^{20} \geq Ne \geq 2\times10^{17}$ cm^{-3}]. *Pytannia atomnoi nauky i tekhniky. Seriia: plazmenna elektronika i novi metody pryskorennia,* no. 4, pp. 288–293 [in Ukrainian].

14. Fedorovych O. A., Voitenko L. M. (2008). *Eksperymentalni doslidzhennia koefitsiienta rozpadu neidealnoi plazmy impulsnykh rozriadiv u vodi* [Experimental studies of the decay coefficient of non-ideal plasma of pulsed discharges in water]. *Ukrainskyi fizychnyi zhurnal,* no. 5, pp. 451–457 [in Ukrainian].

15. Beskaravainyi N. M., Pozdieiev V. A. (1980). *Khvylovi zadachi pro rozshyrennia porozhnyny v ridyni z urakhuvanniam kinechnosti peremishchennia mezh* [Wave problems on the expansion of a cavity in a liquid considering the finiteness of boundary displacements]. *Fizyko-mekhanichni protsessy pry vysokovoltnomu rozriadi u ridyni.* Kyiv : Naukova dumka, pp. 88–97 [in Ukrainian].

16. Tsarenko P. I., Rizun A. R., Zhyrnov M. V., Ivanov V. V. (1984). *Hidrodynamika i teplofizychni kharakterystyky potuzhnykh pidvodnykh iskrovykh rozriadiv* [Hydrodynamics and thermophysical characteristics of powerful underwater spark discharges]. Kyiv : Naukova dumka [in Ukrainian].

Received / Стаття надійшла до редакції: 17.09.2025
Revised / Прорецензовано: 30.09.2025
Accepted / Схвалено до друку: 06.10.2025

ABRAMOV SERHII
Candidate of Technical Sciences, Associate Professor,
Senior Researcher of the Research Laboratory for Training Troops,
Kyiv Institute of the National Guard of Ukraine
https://orcid.org/0000-0003-0675-4850

TYTARENKO OLEKSII
Doctor of Juridical Sciences, Associate Professor,
Head of the Research Laboratory for Training Troops,
Kyiv Institute of the National Guard of Ukraine
https://orcid.org/0000-0002-3271-9402

ВИКОРИСТАННЯ РОЗМІРНИХ І БЕЗРОЗМІРНИХ КОМПЛЕКСІВ, ЩО ОПИСУЮТЬ ВИБУХ

Досліджено процеси розроблення та верифікації системи розмірних і безрозмірних комплексів, які адекватно описують фізику електричного вибуху провідників у широкому діапазоні режимів, уможливлюючи прогнозне масштабування і керування процесом.

В умовах, коли параметри джерела і геометрія провідника можуть змінюватись у широких межах, процес електричного вибуху провідників є гнучким технічним інструментом. Розглянуто вплив основних параметрів джерела живлення – ємності конденсаторної батареї (C), індуктивності розрядного контуру (L) і початкової напруги (U_0), – а також геометрії провідника на кінетику енергетичних перетворень під час електричного вибуху провідників. Показано, що зміна цих параметрів дає змогу варіювати швидкість виділення енергії, часову еволюцію струму й напруги, температуру та об'єм плазми, що безпосередньо визначає інтенсивність механічних (ударна хвиля, тиск) і електрооптичних (світіння, спектр випромінювання) ефектів. Для кожної групи визначено фізичний зміст, межі застосовності та її вплив на пік надлишкового тиску, тривалість позитивної фази, імпульс, а також характеристики випромінювання й розмірно-енергетичний розподіл частинок у випадку синтезу наноматеріалів.

Методологія поєднує аналітичні розрахунки, масштабоване експериментальне дослідження серій розрядів із варіюванням C, L, U_0, геометрії провідника і властивостей середовища. Очікуваними результатами є універсальні емпіричні та напівавтоматизовані кореляції, що дають змогу керувати характеристиками електричного вибуху провідників для конкретних застосувань: імпульсне джерело світла з контрольованим спектром і тривалістю, керований генератор ударних хвиль для дослідницьких і промислових потреб, адаптивні переривники імпульсних струмів.

Отримані результати можливо використовувати для розроблення імпульсних джерел світла з контрольованим спектром, генераторів ударних хвиль і адаптивних комутаційних систем у високовольтній техніці, а також для розроблення установки з виявлення й розмінування водних логістичних маршрутів для підрозділів оперативного призначення Національної гвардії України в умовах виконання бойових завдань.

Ключові слова: *вибух; параметр; установка; струм; вплив; провідник.*

UDC 355

DOI 10.59226/2786-6920.2.2025.16-27

ARCHAKOVA OLEKSANDRA
Candidate of Technical Sciences,
Associate Professor at the Department of Tactics,
Kyiv Institute of the National Guard of Ukraine
https://orcid.org/0009-0000-2260-4751

DEVELOPMENT OF INFORMATION TECHNOLOGIES AND THEIR IMPACT ON THE TRANSFORMATION OF MILITARY UNMANNED AVIATION

The article provides a comprehensive systemic analysis of the interrelationship between the development of information technologies and the transformation of military unmanned aerial vehicles (UAVs). It is demonstrated that modern warfare, particularly the full-scale aggression against Ukraine, has evidenced the shift of UAVs from an auxiliary means to a leading instrument for reconnaissance, fire adjustment, strike operations, and more.

The significance of this research lies in its uncovering of the key role of information technologies in modern warfare, identifying and analyzing the critical technologies that provide a strategic and tactical advantage.

The study covers the historical evolution of UAVs and details the synergistic impact of five key IT innovations on their functionality: Artificial Intelligence (AI), sensor fusion, cloud and edge computing, the Internet of Things (IoT), and network architectures for swarms.

The following research methods (at the theoretical level) were utilized in the article: analysis of scientific literature, systemic analysis, and comparative analysis.

***Keywords**: unmanned aviation; UAVs; drones; artificial intelligence; sensor fusion; cloud and edge computing; Internet of Things; swarm network architectures.*

Statement of the problem. The tactics of conducting combat operations in modern military engagements, particularly during the full-scale aggression against Ukraine, have undergone fundamental changes, as unmanned aerial systems have assumed a leading role as an indispensable tool for reconnaissance, fire adjustment, strike operations, and the attainment of information superiority [1]. Recognition of the critical role of unmanned aviation on the battlefield has led to the establishment of the Unmanned Systems Forces within the structure of the Armed Forces of Ukraine as a separate branch of the armed forces [2].

It should be noted that the development of military unmanned aviation is based on the integration of advanced technological solutions with accumulated combat experience. However, at present, there is no comprehensive understanding of which cutting-edge technologies most significantly affect the quality and effectiveness of UAV employment and ensure their operational advantage during the execution of combat missions.

The formulated problem necessitates research aimed at identifying, analyzing, and structuring the mechanisms of influence of each technology in order to determine how these technological solutions provide new combat capabilities for unmanned aviation and transform the role of the human operator in modern armed conflict.

Analysis of recent research and publications. The role of unmanned aerial vehicles (UAVs) in modern military conflicts has been examined by a number of Ukrainian scholars, including Yu. F. Kucherenko, M. V. Naumenko, M. Yu. Kuznietsova, V. A. Lupandin, H. V. Mehelbei, O. Y. Matsko, T. L. Kurtseitov, and P. O. Mironenko [4, 5], who emphasize their

importance for achieving and maintaining information superiority in military operations. The authors consider unmanned lethal aviation as an element of the air component, analyze the role of UAVs in contemporary armed conflicts, and highlight their significance in gaining and sustaining information dominance within network-centric operations. These studies constitute an important starting point that outlines future directions for the development of unmanned aviation; however, the technological prerequisites for UAV development, as well as their consequences and emerging challenges, are not addressed by the researchers.

Certain aspects of technical development and its implications are discussed in the works of V. P. Horbulin and S. P. Mosov [6–8]. The authors emphasize that the transformation of UAVs is a multidimensional process encompassing not only technical aspects, but also profound ethical, legal, and doctrinal changes that require continuous investigation. Nevertheless, the issue of a comprehensive and systematic analysis of the interrelationship between modern information technologies and their synergistic impact on the evolution of military UAVs remains insufficiently explored.

I. O. Tonkonoh analyzes the evolution and impact of unmanned aerial vehicles in contemporary armed conflicts [9]. The author traces the growth of UAV employment from the mid-2000s to the present, including the current experience of UAV use in the Russian–Ukrainian war, where unmanned lethal systems have demonstrated their ability to influence the course of hostilities. However, the study does not delve into specific IT innovations, their architectures, outcomes, or other aspects of integrating advanced information technologies into military UAVs.

Foreign researchers [10, 11] analyze certain modern information technologies; however, they do not provide a comprehensive examination of other key information technologies. Moreover, their research primarily focuses on general principles of information technologies rather than on specific military challenges and corresponding solutions.

Thus, at present, the issue of the co-evolution of information technologies and military unmanned aviation remains insufficiently addressed and requires further research.

The scientific novelty of this study lies in the development of a basic architecture describing the interrelationship between modern technological solutions and the functional capabilities of military unmanned aerial vehicles. This architecture integrates contemporary information technologies while taking into account the specific characteristics of military unmanned aviation, thereby enabling the optimization of available computational, financial, and human resources.

The results of the study can be used to optimize resource allocation for the development of advanced unmanned systems, as well as for the training of military specialists, including engineers and UAV operators.

The purpose of the article is to: provide a comprehensive overview of the current state and future prospects of the development of military unmanned aviation under the influence of information technologies; systematize and analyze key information technologies and their transformative impact on the functional capabilities of military UAVs.

Presentation of the main material. The idea of employing unmanned aerial vehicles for military purposes emerged in the early twentieth century. The first prototypes, such as the “flying torpedoes” of the First World War (for example, the Kettering Bug developed in the United States), represented early attempts to create remotely controlled aircraft-projectiles [12]. Their reliability and accuracy were low; nevertheless, they laid the foundation for subsequent developments of the “unmanned aircraft” concept, capable of reaching a target without the direct involvement of a pilot.

During the Second World War, Germany made extensive use of V-1 cruise missiles, which in essence were early unmanned aerial weapons designed to strike targets without a pilot on board [13]. The Allied forces also experimented with radio-controlled target aircraft (such as the American OQ-2 Radioplane target drone) for air defense training purposes [14]. This period marked an important step in the advancement of remote control and autopilot technologies.

A significant impetus for the development of military UAVs was provided by the Vietnam War.

The United States extensively employed reconnaissance UAVs, in particular the Ryan AQM-34 Firebee, to collect intelligence over enemy territory saturated with air defense systems [15]. These platforms enabled the acquisition of critically important data on enemy positions, movements, and infrastructure under conditions of high risk for manned aviation, while at the same time minimizing losses among flight personnel.

During the Yom Kippur War (1973), the Israeli military actively used reconnaissance UAVs such as the Firebee and the Tadiran Mastiff to monitor Egyptian and Syrian positions. UAVs also played a crucial role in Operation "Artzav 19" in Lebanon in 1982 by providing intelligence under conditions of a high air defense threat and minimizing risks to manned aircraft, particularly through their use in detecting and suppressing enemy surface-to-air missile systems. This underscored the strategic advantage provided by unmanned systems in reconnaissance operations and in breaching integrated air defense systems [16].

The "zero-attrition doctrine," which began to take shape in the 1970s, further stimulated the development and deployment of unmanned systems, as they made it possible to accomplish missions without endangering the lives of military personnel, which became a key argument for their continued advancement. This period was also characterized by technological breakthroughs in avionics, control systems, and navigation. More advanced autopilot systems emerged, enabling UAVs to perform increasingly complex maneuvers and missions with greater precision. The development and integration of inertial navigation systems and the first GPS-based solutions (albeit with limited availability) significantly increased flight autonomy and accuracy [17].

The late twentieth and early twenty-first centuries were marked by rapid technological progress that drove the development of unmanned aviation, its integration into a wide range of military operations, and a qualitative transformation of its roles and missions.

During Operation Desert Storm (the Gulf War, 1990–1991), U.S. Navy UAVs such as the RQ-2 Pioneer were actively used for intelligence, surveillance, and reconnaissance and targeting (ISR/T), particularly for detecting Iraqi artillery positions and adjusting fire. These systems transmitted imagery and video in near real time, providing commanders with a high level of situational awareness on the battlefield [18].

Similarly, during Operation Iraqi Freedom (2003), UAVs such as the reconnaissance Predator and its later armed variants were widely employed for intelligence gathering, monitoring the movement of Iraqi forces, target designation for manned aircraft, and even for direct strikes against enemy assets. Their ability to operate under persistent surveillance conditions significantly increased the effectiveness of ground operations and enabled faster achievement of operational objectives [19].

The most revolutionary step was the development and large-scale employment of armed UAVs. Following the terrorist attacks of September 11, 2001, the United States began extensive use of the MQ-1 Predator (after its modification to carry weapons) and later the MQ-9 Reaper for counterterrorism operations. Armed UAVs equipped with air-to-ground missiles (e.g., AGM-114 Hellfire) became a primary instrument for delivering high-precision, "surgical" strikes against leaders and militants of terrorist organizations in Afghanistan, Pakistan, Yemen, and Somalia. These operations made it possible to strike targets while minimizing risks to one's own personnel and reducing collateral damage among civilian populations [20]. This fundamentally transformed the concept of "remote" warfare and counterterrorism operations.

The military aggression of Russia against Ukraine has opened a new chapter in the history of warfare, in which unmanned systems play a decisive role due to their mass employment. UAVs have evolved from narrowly specialized strike platforms to systems performing a wide range of tactical and strategic tasks. In particular, the use of modern UAVs by Ukraine's security and defense forces has significantly altered the course of the russian–ukrainian war [21].

The rapid development of information technologies has become the driving force behind the evolution of military UAVs, which have been integrated into warfare tactics and security measures, enabling real-time exchange of intelligence data. As a result, the current stage of UAV development is characterized by the rapid integration of advanced digital solutions and the expansion of combat capabilities, allowing one to speak of a genuine "UAV revolution" in the military domain. The stages of development of military unmanned aviation are presented in Table 1.

Table 1 – Stages of Development of Military Unmanned Aviation

Evolution Stage	Time Period	Key Features	Primary UAV Functions	Examples of UAV Applications
Early Concepts	early 20th century – 1960s	Low reliability, limited accuracy, experimental nature	Target drones, remotely controlled projectile prototypes	Kettering Bug, V-1, Target Drone OQ-2 Radioplane
Cold War and Vietnam Era	1960s–1980s	Growing importance of reconnaissance without risk to pilots; improved control systems	Reconnaissance, surveillance	Ryan AQM-34 Firebee, Tadiran Mastiff (Yom Kippur War, 1973)
Emergence of Strike UAVs	1990s – 2000s	Integration of UAVs into a wide range of military operations; emergence of strike capabilities	Reconnaissance, surveillance, target designation, direct strikes	RQ-2 Pioneer (Operation Desert Storm 1990–1991) MQ-1 Predator, MQ-9 Reaper (Afghanistan, Iraq)
Modern Information Technologies	2010s – present	High degree of autonomy, mass deployment, and industrial-scale integration of information technologies	Reconnaissance, strike operations, logistics support, electronic warfare countermeasures, swarm attacks	Bayraktar TB2, Akıncı (Syria, Libya, Nagorno-Karabakh) Leleka-100, Punisher, R18 , Baba Yaga, PD-2 and Raybird-3 (Ukraine, 2022-2025).

Let us consider several modern technologies that have influenced the transformation of military unmanned aviation: artificial intelligence, cloud/edge computing, the Internet of Things, sensor fusion, and network architectures of drone swarms.

Artificial Intelligence. Artificial intelligence (AI) is a central element in the transformation of military UAVs, providing them with unprecedented levels of autonomy and operational efficiency [22]. Owing to AI, drones are becoming capable of executing complex missions without direct human supervision, which significantly alters the dynamics of combat operations.

In intelligence, surveillance, and target designation, AI is used for image analysis, target labeling, and real-time video stream processing. Integrated machine vision systems enable UAVs to identify objects and classify them as hostile, thereby substantially enhancing situational awareness. Modern UAVs, including the Ukrainian *Shark*, are equipped with automatic tracking of selected targets and autonomous determination of their coordinates, ensuring high accuracy for artillery target designation.

One of the key capabilities enabled by artificial intelligence is autonomous flight execution. Through AI-driven algorithms, UAVs can operate independently, reducing the need for continuous operator control. By utilizing data from onboard sensors, such platforms analyze the operational environment in real time, adapt to changing conditions, and effectively avoid obstacles, which increases both flight safety and mission effectiveness.

Artificial intelligence is particularly critical in swarm missions, as it enables drones to function as a coordinated system, synchronizing actions to accomplish complex operations. Publicly available footage demonstrates how the Third Assault Brigade in the Kharkiv region conducted an unprecedented operation to seize enemy fortifications exclusively using drones and ground robotic platforms, without the involvement of infantry and without personnel losses [23]. This example clearly illustrates how AI-based solutions fundamentally transform modern warfare tactics and enhance defensive capabilities.

A representative example of the application of AI in military UAVs is the Turkish STM Kargu-2 drone. This quadcopter demonstrated enhanced autonomy, the ability to operate in swarms, GPS-denied navigation, and the use of facial recognition and machine-learning algorithms for target identification and engagement. It was employed in Libya in 2020, which marked one of the first documented cases of autonomous target engagement in combat operations [24].

Another example is the U.S. MQ-9 Reaper, which is equipped with the *Agile Condor* module and is capable of autonomous navigation, detection of ground anomalies, and flight-path correction based on an evolving situational understanding. However, in accordance with U.S. policy, decisions regarding the use of lethal force require human oversight.

It is also important to note the developments by Israeli researchers in the field of AI-enabled loitering munitions, such as Harpy and Harop, which are capable of fully autonomous detection and engagement of radar systems, operating on the principle of kamikaze drones. These systems were employed, among other instances, during the escalation of hostilities in Nagorno-Karabakh in 2020.

The rapid advancement of AI in military unmanned aviation has led to a significant transformation of the human operator's role. Today, AI enables drones to operate autonomously, reducing the need for continuous human intervention. Consequently, the operator's role is evolving from direct piloting and real-time control toward supervision, strategic mission planning, and the management of exceptional or unforeseen situations.

Cloud and Edge Computing. The essence of cloud and edge computing technologies lies in local data processing—conducted as close as possible to the point of data generation—rather than exclusively within centralized cloud infrastructures. This approach enables autonomous data analysis directly on devices such as intelligent sensors or UAVs, eliminating the need to transmit the entire data stream to remote processing centers. As a result, systems operate faster, more reliably, and more efficiently, as their dependence on continuous Internet connectivity is reduced.

The application of cloud and edge computing significantly expands the computational capabilities of military UAVs, overcoming their physical limitations and ensuring rapid data processing, which is critical for the effectiveness of tactical operations.

Cloud computing provides rapid access to remote computational resources via network connectivity. Its use in unmanned aviation enhances UAV capabilities by compensating for limited onboard processing power and size constraints. The implementation of tactical cloud solutions contributes to increased operational efficiency and improved situational awareness at the command level.

The essence of edge computing lies in the decentralization of the traditional cloud: data is processed and stored locally rather than on remote servers. This is achieved by deploying computational resources as close as possible to end users and devices. In military operations, this capability for real-time data processing is critical, providing commanders with a decisive advantage for rapid and effective decision-making.

Modern military UAVs can generate a substantial volume of data – often terabytes per single flight. AI-driven solutions, combined with cloud and edge computing, enable the analysis of large datasets in real time, enhancing situational awareness, mission planning, the generation of operational scenarios, and forecasting enemy actions.

Advanced UAVs, such as the MQ-9B SkyGuardian, utilize onboard AI capabilities for data processing directly on the aircraft. As a result, they can operate fully autonomously – from target recognition and navigation in complex environments to dynamic in-mission task adjustments without commands from the ground [25].

Despite their significant advantages, the integration of cloud and edge computing into unmanned aviation faces several challenges, including bandwidth limitations in combat conditions and ensuring the physical security of network infrastructure. These challenges highlight the need to achieve an optimal balance between centralization (cloud) and decentralization (edge) to maximize both operational efficiency and system resilience.

Internet of Things. The Internet of Things (IoT) is a network concept that connects physical objects ("things") equipped with embedded sensors, software, and communication capabilities. In simple terms, it represents a network in which unmanned aerial vehicles – from small reconnaissance drones to large strategic platforms – are connected to the Internet or to a unified network, enabling them to collect and exchange data as well as to interact with one another and with human operators.

IoT significantly expands the capabilities of military UAVs by transforming them into interconnected "flying nodes" for data collection and exchange, which is critically important for modern warfare.

The interaction and networked data-exchange capabilities provided by IoT are key enablers for the development of unmanned aviation systems. In

the UAV context, this technology supports real-time sensor data collection and monitoring, fundamentally improving situational awareness. By encompassing monitoring across multiple domains (air, land, and maritime), IoT directly contributes to increased operational accuracy and to the reduction of risks to personnel.

To ensure enhanced situational awareness and the creation of a shared operational picture, IoT-enabled drones can effectively interact with other IoT components, including cloud platforms, analytical systems, and AI-based solutions. Through IoT technologies, systems acquire the capability for fully automated and timely threat neutralization while maintaining a high degree of precision in target engagement.

The primary challenges facing the application of IoT in military UAVs include security, reliability, interoperability, energy consumption, and network limitations. The growing number of devices connected to open or semi-open networks increases the risks of identification and cybersecurity threats. Moreover, centralized cloud-based approaches – where raw data is transmitted to the cloud for analysis – are not viable in tactical environments due to time constraints and limited communication and computational resources.

The integration of the Internet of Things transforms military UAVs from individual, remotely controlled assets into integral, interconnected nodes within a vast "Internet of Military Things." They become real-time data collectors and transmitters, contributing to a unified and comprehensive battlefield picture. This evolution aligns with the paradigm of network-centric warfare, in which seamless information exchange among all elements of a military operation enhances overall combat effectiveness. Within this framework, air, land, and maritime assets – including other IoT-enabled systems – continuously and transparently share data, thereby increasing coordination, responsiveness, and operational superiority.

Sensor Fusion. Sensor fusion is the process of combining (integrating) data obtained from multiple different sensors or sources in order to create a unified, more complete, accurate, and reliable representation of the environment or the system state than can be achieved by any individual sensor alone. The primary objective of sensor fusion is to exploit the strengths of each sensor while compensating for their respective limitations.

For example, an autonomous UAV may employ the following sensors:

- a camera, which provides detailed information on color, textures, and visual features, but performs poorly in fog or low-light conditions;
- a laser rangefinder (LiDAR), which generates an accurate 3D representation of objects and distances, but is sensitive to snow and rain;
- a radar, which delivers data on range and velocity and performs well in adverse weather, but has relatively low spatial resolution;
- an inertial measurement unit (IMU), which measures angular velocity, acceleration, and orientation, but accumulates errors over time due to drift.

The integration of data from these heterogeneous sensors enables:

- improved accuracy of the derived information, resulting in more reliable estimates of key parameters (e.g., precise object positioning);
- increased robustness and redundancy in data acquisition, allowing the system to continue functioning even if one sensor fails or is degraded (for instance, if a camera is blinded by sunlight, radar and LiDAR data can still be used);
- expanded informational coverage, providing insights that no single sensor can deliver independently (e.g., combining LiDAR-generated 3D point clouds with color data from optical cameras).

Sensor fusion is a key enabler of enhanced situational awareness provided by military UAVs, as it integrates data from diverse sensor modalities to generate a coherent and comprehensive battlefield picture. Through such integration, unmanned platforms can not only detect and identify objects, but also assess their dynamics, evaluate threat levels, and formulate optimal response options.

For instance, a UAV may use radar to detect vehicle movement through cloud cover, electro-optical/infrared (EO/IR) sensors for visual confirmation of the target, and electronic intelligence systems to determine whether the object is emitting hostile signals. The fusion and

processing of all these data streams ensure higher reliability and a deeper understanding of the operational environment.

Technological advances in the field of microelectromechanical systems (MEMS) and low-power electronics have enabled significant sensor miniaturization. This has made it possible to develop high-precision sensors with reduced resource consumption, which in turn has facilitated their deployment on small tactical drones [26]. Such compactness supports distributed sensing and rapid data collection for military units.

Multisensor fusion becomes critically important in combat environments where the adversary employs sophisticated camouflage techniques or operates within mixed civilian settings. The integration of heterogeneous sensor data helps reduce uncertainty and, consequently, minimize the risk of losses. Accumulated sensor information enables the prediction of enemy maneuvers and the identification of persistent behavioral patterns, thereby accelerating the operational decision-making cycle and reducing the cognitive burden on commanders in combat conditions.

Network Architectures of Drone Swarms. A drone swarm is generally understood as a group of unmanned aerial vehicles that operate together as a single, coordinated, and autonomous system to accomplish a shared mission. Swarms of drones acting in coordination offer significant advantages over individual UAVs in terms of coverage, redundancy, and overall effectiveness.

Network architectures are fundamental to the efficient coordination and operation of UAV swarms, enabling them to function as an integrated whole.

In the military context, drone swarms possess considerable potential, as they can:

- saturate air defense systems: a large number of drones attacking simultaneously can overwhelm or exceed the interception capacity of an adversary's air defense systems;
- conduct reconnaissance and strike operations: unmanned platforms provide rapid and comprehensive area surveillance, target identification, and coordinated engagement;
- operate under electronic warfare (EW) conditions: owing to autonomy and local inter-drone interaction, a swarm can continue its mission even in the event of lost communication with a human operator.

However, these advantages are accompanied by increased system complexity, particularly with respect to ensuring secure and reliable communication among drones. Coordinated cyber or kinetic attacks, as well as network disruptions, can compromise the entire swarm, making security a primary concern for such systems [27]. The implementation of secure network architectures for drone swarms is therefore critical for their successful deployment in combat environments.

Classical network architectures for swarms (such as star or point-to-point topologies), which may be suitable for individual UAVs, are characterized by single points of failure, limited operational range, and low resilience under adversarial conditions, rendering them unreliable in contested environments. A partial mitigation approach involves direct peer-to-peer connectivity among UAVs combined with decentralized decision-making. Nevertheless, such implementations face constraints related to the size, weight, and power of onboard communication modules, as well as technical challenges associated with dynamic routing reconfiguration, which can lead to communication breakdowns and information loss.

As a solution to enhance swarm reliability – addressing limitations inherent in classical architectures – a mesh network topology can be employed. Its decentralized nature allows each drone to maintain multiple communication links, thereby increasing system resilience. Built-in dynamic routing and self-healing capabilities enable automatic rerouting of operational data in the event of the combat loss of individual drones or electronic jamming, ensuring continuity of operations. Moreover, mesh architectures facilitate rapid scaling of swarm size without complex reconfiguration.

The development of diverse and robust swarm network architectures is therefore critical for improving the operational effectiveness, resilience, and flexibility of military unmanned systems.

The evolution of new UAV capabilities enabled by modern information technologies is summarized in Table 2.

Table 2 – Basic Architecture of the Interrelationship Between Information Technologies and the Functional Capabilities of Military Unmanned Aerial Vehicles

Information Technology	New UAV Capabilities	Key Challenges
Artificial Intelligence (AI)	Image decoding, target designation, real-time video processing; autonomous operation, reducing human intervention; adaptation to changing conditions, obstacle detection and avoidance; swarm coordination for complex tasks; FPV drone guidance; automatic target tracking and coordinate determination.	Algorithm development complexity; cognitive load on operators; ethical and legal dilemmas of autonomous decision-making.
Cloud and Edge Computing	Rapid access to information; expanded computational capabilities for UAVs; improved decision-making quality and situational awareness; real-time big data processing; reduced latency and bandwidth requirements (edge computing).	Physical security of network infrastructure; bandwidth limitations in tactical environments; potential lack of redundancy; dependence on future network standards (5G/6G); complexity of scaling at the tactical level.
Internet of Things (IoT)	Interaction and data exchange between drones; real-time sensor data collection and monitoring; enhanced situational awareness; real-time transmission of data and command signals.	Security, reliability, compatibility, energy consumption, network limitations; increased risks of identification and cybersecurity breaches; underdeveloped cybersecurity solutions; centralized cloud approaches are impractical in tactical scenarios.
Sensor Fusion	Integration of heterogeneous sensor data; creation of a comprehensive battlefield picture; target detection and identification, behavior analysis, threat reporting; uncertainty reduction and minimization of losses.	Further miniaturization and efficiency improvements of sensors; integration with broader networks; development of specialized sensors.
Drone Swarm Network Architectures	Decentralized structure eliminating single points of failure; dynamic routing and self-healing; scalability and addition of new drones without reconfiguration.	Regulatory approval for cellular network use; achieving true swarm autonomy; limitations of traditional architectures.

Thus, the transformation of military unmanned aviation has been driven by the development of artificial intelligence, the Internet of Things, sensor fusion, edge computing, and network solutions for drone swarms.

Conclusions and prospects for further research. The conducted study provides a comprehensive analysis of the current state of military unmanned aviation under the influence of information technologies. The widespread

implementation of UAVs has fundamentally changed the tactics of combat operations, making high-precision strike and reconnaissance capabilities accessible at the tactical level. This shift has led to a reevaluation of military doctrines, force structures, and training systems, as operational effectiveness increasingly depends on technological superiority and rapid adaptability.

The article examined the stages of development of military UAVs, from primitive projectile prototypes (e.g., Kettering Bug, V-1) to integrated, highly autonomous systems, which provide a decisive strategic advantage. It has been established that the evolution of UAVs has been driven by the ongoing aim to minimize personnel losses (the "zero-attrition" doctrine) and the need for reliable intelligence and precision strikes in combat zones.

Thus, the modern transformation of military UAVs is directly linked to the evolution of contemporary information technologies, which is based on the integration of five key digital technologies:

- Artificial intelligence (AI): transforms UAVs into autonomous combat systems capable of independently executing complex missions, including target recognition, automatic tracking, and engagement in GPS-denied environments. AI shifts the role of the operator from direct piloting to strategic supervision and mission oversight;
- Sensor fusion: integrates data from miniaturized sensors to create a coherent, reliable, and accurate battlefield picture, which is critical for reducing uncertainty and minimizing collateral damage under complex operational conditions;
- Cloud and edge computing: overcome the physical constraints of UAV platforms by enabling local, real-time processing of terabytes of data at the edge, thereby accelerating tactical decision-making and ensuring autonomous operation even in the absence of stable communications;
- Internet of Things (IoT): transforms drones into interconnected network nodes that exchange data in real time with other military assets, forming a unified operational picture;
- Network architectures for drone swarms: ensure survivability, resilience, and scalability of swarm systems in contested environments.

The convergence of AI, IoT, sensor fusion, and mesh-based network architectures leads to a "UAV revolution," positioning unmanned aviation as a core, integrated, and highly intelligent element of modern military strategy. This technological synergy, combined with enhanced system survivability, becomes a decisive factor that fundamentally reshapes the tactics and strategy of contemporary warfare.

Despite these significant advances, substantial challenges remain. These include ensuring robust cybersecurity in dynamically evolving threat environments, increasing resilience against increasingly sophisticated electronic warfare capabilities, developing algorithms that enable true swarm autonomy, and addressing profound ethical and legal issues related to accountability for decisions made by autonomous systems.

Based on the conducted analysis, several key directions for further research have been identified, arising from the need to overcome existing technological challenges and to achieve maximum autonomy and resilience of systems in complex combat environments:

- the development of hybrid drone swarm architectures that combine the advantages of multiple communication technologies to ensure maximum resilience, including the integration of AI, swarm intelligence, and self-learning algorithms;
- the design of AI algorithms capable of explaining their decisions in order to ensure meaningful human control, that is, to optimally integrate human judgment into autonomous systems without reducing their operational effectiveness;
- the development and implementation of advanced cryptographic methods for securing data transmission channels to ensure the integrity, accuracy, and timeliness of information exchange.

References

1. Zaluzhnyi V. *Nova pryroda viiny zminyla sutnist osnov hlobalnoi bezpeky: ukrainskyi dosvid i maibutnii svitovyi poriadok* [The new nature of crime has changed the essence of global security: the Ukrainian experience and the future world order]. Retrieved from: https://surl.lu/yskfcc (accessed 25 July 2025) [in Ukrainian].

2. *Ukaz Prezydenta Ukrainy Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 25 chervnia 2024 roku "Pro stvorennia u strukturi Zbroinykh Syl Ukrainy Syl bezpilotnykh system yak okremoho rodu syl" № 382/2024* [Decree of the President of Ukraine on the Resolution of the National Security and Defense Council of Ukraine dated June 25, 2024 "On the Creation of Unmanned Aerial Systems as a Separate Type of Force in the Structure of the Armed Forces of Ukraine" activity no. 382/2024]. (2024, June 25). Retrieved from: https://surl.lt/hphpvs (accessed 20 July 2025) [in Ukrainian].

3. Natsionalnyi instytut stratehichnykh doslidzhen (2017). *Avtonomni voienni robototekhnichni systemy* [Autonomous military robotic systems]. Retrieved from: https://surl.lu/bsxbih (accessed 25 July 2025) [in Ukrainian].

4. Kucherenko Yu. F., Naumenko M. V., Kuznietsova M. Yu. (2018). *Analiz dosvidu zastosuvannia bezpilotnykh litalnykh aparativ ta vyznachennia napriamku yikh podalshoho rozvytku pry vedenni merezhetsentrychnykh operatsii* [Analysis of the experience of using unmanned aerial vehicles and identification of the direction of their further development when conducting network-centric operations]. *Systemy ozbroiennia i viiskova tekhnika*, no. 1 (53), pp. 25–30 [in Ukrainian].

5. Lupandin V. A., Mehelbei H. V., Matsko O. Yu., Kurtseitov T. L., Mironenko P. O. (2019). *Osnovni tendentsii stvorennia ta zastosuvannia hrup bezpilotnykh litalnykh aparativ* [The main trends in the creation and use of drones]. *Nauka i tekhnika Povitrianykh Syl Zbroinykh Syl Ukrainy,* no. 2, pp. 88–96 [in Ukrainian].

6. Mosov S. P. (2024). *Roinnia droniv viiskovoho pryznachennia: realii ta perspektyvy.* [The development of military drones: realities and perspectives]. *Zbirnyk naukovykh prats Tsentru voienno-stratehichnykh doslidzhen Natsionalnoho universytetu oborony Ukrainy*, no. 1 (80), pp. 77–86 [in Ukrainian].

7. Horbulin V. P., Mosov S. P. (2024). *Roi droniv – kulminatsiia dronizatsii voien* [Drone swarms are the culmination of drone warfare]. *Visnyk Natsionalnoi akademii nauk Ukrainy,* no. 3, pp. 3–11 [in Ukrainian].

8. Horbulin V., Mosov S. (2022). *Smertelna avtonomna zbroia* [Lethal autonomous weapons]. *Oboronnyi visnyk*, no. 3–4, pp. 18–24 [in Ukrainian].

9. Tonkonoh I. O. (2024). *Deiaki aspekty vykorystannia BPLA* [Some aspects of using BPLA]. Proceedings of the All-Ukrainian scientificand practical conference *"Operatyvno-boiova diialnist syl sektoru bezpeky i oborony v umovakh voiennoho stanu"* (Kyiv, October 24, 2024). Kyiv : NA SBU, vol. 1, pp. 316– 319 [in Ukrainian].

10. Yongkun Zhou , Bin Rao, And Wei Wang (2020). UAV Swarm Intelligence: Recent Advances and Future Trends. IEEE Access: Multidisciplinary rapid review. *Open Access Journal*, no. 8, pp. 183856 – 183878 [in English].

11. Yahao Ding, Zhaohui Yang, Quoc-Viet Pham, Zhaoyang Zhang, Mohammad Shikh-Bahaei (2023). Distributed Machine Learning for UAV Swarms: Computing, Sensing, and Semantics. Retrieved from: http://arxiv.org/abs/2301.00912v1 (accessed 1 August 2025) [in English].

12. Jimmy Stamp. Unmanned Drones Have Been Around Since World War I. Retrieved from: https://surl.li/vkfypn (accessed 1 August 2025) [in English].

13. Thomas A. Hughes, John Graham Royde-Smith. V-1 missile military technology. Retrieved from: https://surli.cc/vuswjg (accessed 1 August 2025) [in English].

14. National Museum of the United States Air Force. Radioplane OQ-2A. Retrieved from:

https://surl.li/iuggai (accessed 1 August 2025) [in English].

15. Foundation Museum of Aviation. Ryan. AQM-34N Firebee. Retrieved from: https://surl.li/xasyis (accessed 1 August 2025) [in English].

16. Eitan, Y. (2005). The Role of UAVs in the Yom Kippur War. *Journal of Military History,* no. 69 (3), pp. 789–805 [in English].

17. Goff, P. (2012). Evolution of UAV Technology in Military Applications. *Air & Space Power Journal*, no. 26 (3), pp. 69–79 [in English].

18. GlobalSecurity.org (2011). Pioneer Short Range (SR) UAV. Retrieved from: https://surl.li/gcdygp (accessed 1 August 2025) [in English].

19. Peter Faber and Carlo Masala (2024). Operation Iraqi Freedom: Lessons Learned, Ways Ahead, and Open Questions. *RESEARCH PAPER Academic Research Branch – NATO Defense College*, no. 9, pp. 2–7 [in English].

20. Alan W. Dowd (2013). Drone Wars: Risks and Warnings. Retrieved from: https://surl.lu/jyqqvs (accessed 14 August 2025) [in English].

21. Dignitas. Fund (2025). *Ukrainski brendy BPLA u suchasnii viini droniv* [Ukrainian brands BPLA in modern drones]. Retrieved from: https://surl.li/hktcsn (accessed 5 August 2025) [in Ukrainian].

22. Daniel Caballero-Martin, Jose Manuel Lopez-Guede, Julian Estevez, Manuel Graña (2024). Artificial Intelligence Applied to Drone Control: A State of the Art. Retrieved from: https://surl.li/xctyvf (accessed 15 August 2025) [in English].

23. Texty.org.ua (2025). *Bezpretsedentna operatsiia: Tretia shturmova atakuvala vykliuchno nazemnymy ta FPV-dronamy i zakhopyla polonenykh* [Unprecedented operation: The third assault group attacked exclusively with ground and FPV drones and buried the prisoners]. Retrieved from: https://surl.li/qblxrj (accessed 1 September 2025) [in Ukrainian].

24. Grace Sheehan (2025). Cheap Drones, Expensive Lessons: Ethics, Innovation, and Regulation of Autonomous Weapon Systems. Retrieved from: https://surl.li/ehyrno (accessed 5 September 2025) [in English].

25. Namber Analytics (2025). Enhancing Military Strategies With Edge Computing in Aerospace Defense Technology. Retrieved from: https://surl.li/xugkhs (accessed 10 September 2025) [in English].

26. Army.mil (2020). Army researchers develop breakthrough sensors for small drones. Retrieved from: https://surli.cc/gvlxsc (accessed 10 September 2025) [in English].

27. Jacobsen, R. H., Matlekovic, L., Shi, L., Malle, N., Ayoub, N., Hageman, K., et al. (2023). Design of an Autonomous Cooperative Drone Swarm for Inspections of Safety Critical Infrastructure. *Applied Sciences,* no. 13, art. 1256. DOI: https://doi.org/10.3390/app13031256 [in English].

Received / Стаття надійшла до редакції: 06.10.2025
Revised / Прорецензовано: 17.10.2025
Accepted / Схвалено до друку: 26.10.2025

АРЧАКОВА ОЛЕКСАНДРА ВІКТОРІВНА
кандидат технічних наук, доцент кафедри тактики,
Київський інститут Національної гвардії України
https://orcid.org/0009-0000-2260-4751

РОЗВИТОК ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ЇХНІЙ ВПЛИВ НА ЕВОЛЮЦІЮ БЕЗПІЛОТНОЇ АВІАЦІЇ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

Здійснено комплексний системний аналіз взаємозв'язку між розвитком інформаційних технологій і трансформацією військової безпілотної авіації. Показано, що сучасні бойові дії, зокрема повномасштабна агресія проти України, засвідчили перехід безпілотних літальних апаратів від допоміжного засобу до провідного інструменту для розвідки, коригування вогню, проведення ударних операцій тощо.

Розкрито ключову роль інформаційних технологій у сучасній війні, визначено і проаналізовано критичні технології, які надають стратегічну й тактичну перевагу.

Дослідженням охоплено історичну еволюцію безпілотних літальних апаратів і деталізовано синергетичний вплив на їхній функціонал п'яти ключових ІТ-інновацій: штучний інтелект, сенсорна фузія, хмарні й периферійні обчислення, інтернет речей, мережеві архітектури роїв.

Використано (на теоретичному рівні) такі методи досліджень, як аналіз наукової літератури, системний та порівняльний аналіз.

***Ключові слова**: безпілотна авіація; БПЛА; дрони; штучний інтелект; сенсорна фузія; хмарні й периферійні обчислення; інтернет речей; мережеві архітектури роїв.*

UDC 327.5:911.3]:316.776.23] (02) DOI 10.59226/2786-6920.2.2025.28-40

VIEDIENIEIEV DMYTRO
Doctor of Historical Sciences, Professor,
Professor of the Department of History of
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute"
https://orcid.org/0000-0002-8929-9875

ORGANIZATIONAL-FUNCTIONAL AND SCIENTIFIC-CONCEPTUAL FEATURES OF CYBERNETIC COMBAT SYSTEMS OF THE LEADING COUNTRIES OF THE WORLD (FIRST QUARTER OF THE 21ST CENTURY)

The author's analysis of the state of scientific development of the problem raised allows us to state the need to prepare separate studies on the in-depth study of the organizational and functional structure, development trends and current tasks, forms and methods of activity of the cyber warfare forces of leading foreign states in order to take into account for the further development and improvement of the activities of the bodies and units of cyber defense of military formations and special services of Ukraine, timely detection and prevention of threats to the cyber sphere of the state.

The purpose of the article is to reveal the organizational and functional and conceptual features of the formation of the latest systems of cyber warfare of the leading countries of the world and to assess the characteristic threats that the modern stage of development of forces and means of intelligence and subversive activity in the network and virtual space poses to the national security of Ukraine.

It is proved that in the leading countries of the world the main trend is the creation of a set of departments, institutions (bodies) for cyber defense and cyber warfare. Cyber defense forces, as a rule, receive the status of a separate branch of the national armed forces by uniting units of electronic intelligence, electronic warfare, information and psychological operations, cryptographic support and cryptological support, geo-information support, information protection in information and telecommunications systems, etc. Currently, more than 60 countries have their own troops (bodies) for conducting cyber warfare - a set of measures aimed at exerting a managerial and/or destructive influence on the automated information and technological systems of the opposing side and protecting their own information and computing resources from such influence through the use of specially developed software and hardware, as well as conducting a system of specialized exercises.

In the author's opinion, in the future it seems appropriate to study in depth the doctrinal documents inherent in them, the experience of organizational and staffing structure, forms and methods of neutralizing threats in the cyberspace, the mechanism of using "non-governmental" hacker groups, the peculiarities of personnel selection, and to ensure that foreign innovations are taken into account in professional training and advanced training of employees of the information and cyber security and counterintelligence bodies of Ukraine.

Keywords: *unconventional strategy; information warfare; cyber warfare; cyber espionage; information security.*

Statement of the problem. Modern theorists of military science and special operations are united in recognizing that information confrontation (IC) has irreversibly become one of the leading components of military strategy and intelligence–subversive activity. The world's leading states

assign priority importance to the modernization and development of new strategies, technologies, forces, and means of information-psychological influence, as well as software and technical tools designed to damage computer and telecommunications systems. As evidenced by the experience of contemporary military conflicts, IC has become one of the primary forms of achieving strategic objectives (see, in particular, [1–3]).

At the same time, the concept of "cyberwarfare" has been firmly established, defined as "organized confrontation in the digital space, in which at least one of the parties is a state, conducted for political purposes and accompanied by the destruction of infrastructure and the infliction of other moral and material damage on society" [4, p. 18].

The seriousness of external destructive influences (attacks) on the cybernetic and governance spheres of Ukraine is outlined in the *Cybersecurity Strategy of Ukraine* dated August 6, 2021. From the perspective of this study, it is particularly important that the aforementioned document emphasizes the necessity of studying foreign experience in ensuring cybersecurity, which is directly linked to the need to overcome Ukraine's lag in this domain compared to the world's leading states [5].

The relevance of the problem addressed in this article is further enhanced by the importance of taking into account foreign experience in cyber confrontation and external threats to the information-network domain of Ukraine's national security in the context of the development and operation of the Command of Communications and Cybersecurity Forces of the Armed Forces of Ukraine. This command was established in February 2020 and, as of January 1, 2022, in accordance with the Law of Ukraine "On the Foundations of National Resistance," acquired the status of a separate branch of the Armed Forces of Ukraine [6].

Finally, a promising area of research is the cyber domain of the Russian–Ukrainian war, which is characterized by researchers as the "first cyber war" against Ukraine. This concept was articulated, in particular, during the plenary session *"The Impact of the World's First Cyber War on the State of Ukraine's National Security"* within the framework of the All-Ukrainian Scientific and Practical Conference *"Current Issues of Managing State Information Security"* (March 2024) [4, pp. 279–280].

Analysis of recent research and publications. The study of the characteristics of contemporary foreign experience in conducting confrontation in the electronic and networked domain has currently become one of the key research directions in Ukraine within the fields of cyber warfare and cybersecurity. According to the Ministry of Education and Science of Ukraine (2024), 54 higher education institutions were engaged in training specialists for the information security sector and conducting relevant research activities [4, p. 8]. Since 2023, the Administration of the State Service of Special Communications and Information Protection of Ukraine (SSSCIP) has established a Sectoral Council for the organization and coordination of the development of professional standards and professional qualifications in the fields of information technologies, cybersecurity, and information protection. Between 2021 and 2024, the number of officially recognized professions in the cybersecurity domain increased from two to twenty-seven [4, p. 8].

It should be noted that within the research segment of Ukraine's defense and security sector, a solid scientific school and corresponding research areas have been formed, focusing on the theory and practice of state cyber security. A significant place in these studies is devoted to analyzing foreign experience in organizing cyber warfare structures, as well as the forms and methods of their activities. Relevant specialized research is actively conducted at the Zhytomyr Military Institute named after S. P. Koroliov and at the Military Institute of Telecommunications and Information Technologies named after the Heroes of Kruty of the National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute."

A Cybersecurity Center and a scientific laboratory for countering cyber threats operate

within the Educational and Scientific Institute of Information Security and Strategic Communications of the National Academy of the Security Service of Ukraine. Specialized research on information and cyber security is also carried out by experts of the Center for Security Studies of the National Institute for Strategic Studies. The National University of Defense of Ukraine has become a major research hub in the field of cyber confrontation; since 2023, it has included the Institute of Information and Communication Technologies and Cyber Defense. Specialized academic events in this field are held on a regular basis [4; 7].

Focusing on existing scientific developments related to the problem under consideration, it is appropriate to mention a number of studies conducted by researchers from "power-oriented" scientific centers, in which external threats (adversaries) to Ukraine's cybersecurity were examined within a comprehensive analysis of problematic aspects of cyber defense. These studies addressed the infrastructure of Ukraine's cyber protection bodies and the ways of its reform, assessed the place and role of cyber defense within the Armed Forces of Ukraine, evaluated the level of protection of critical infrastructure facilities against cyberattacks, and developed practical recommendations for the draft Cyber Defense Strategy of Ukraine, as well as for the development of joint cyber defense forces [8–11].

Notably, a separate line of research has focused on the study of cyber confrontation as a component of the Russian-Ukrainian war, which has led to increased scholarly interest in the development of cyber warfare structures of the Russian Federation. Researchers have summarized the experience of cyber confrontation since the beginning of the war, including analyses of statistical data on cyberattacks, the organizational structure of both sides of the cyber conflict, new methods of applying cyber influence, and changes in the objectives of cyber operations depending on the situation in the main theater of military operations [see, for example: 12–21]. Within this research framework, an in-depth examination of the institutional system of cyber warfare in the Russian Federation, as well as the forms and methods of its aggressive actions in Ukraine's networked space, has been conducted.

Special emphasis should be placed on the scientific and practical significance of a series of publications devoted to studying the combat employment experience of signal and cyber security troops, prepared by the Main Command of the Signal and Cyber Security Troops of the Armed Forces of Ukraine and the Main Directorate of Communications and Cyber Security of the General Staff of the Armed Forces of Ukraine. Analytical work on the preparation of these publications was carried out by the Experience Generalization Group of the Staff Training Directorate of the Signal and Cyber Security Troops Command of the Armed Forces of Ukraine [22–23].

The Institute of Information and Communication Technologies and Cyber Defense of the National University of Defense of Ukraine has produced a series of collections of information and analytical materials dedicated to the combat experience of cyber defense as a factor of full-scale military operations (with Part 3 covering the period from late 2022 to mid-2023) [24]. These publications systematized materials useful for specialized research, particularly regarding the nature and statistics of enemy cyberattacks on Ukraine's critical infrastructure facilities. In addition, the Institute prepared several collections of information and analytical materials addressing current experience in ensuring information security during the period of full-scale war [25].

It should also be noted that Ukrainian researchers have been conducting long-term studies of foreign experience in information warfare [26]. At the same time, an analysis of the current state of scientific research on the issue indicates the need for dedicated studies aimed at an in-depth examination of the organizational and functional structure, development trends, current tasks, and forms and methods of activity of cyber warfare forces of leading foreign states. Such studies are necessary for the further development

and improvement of the activities of cyber defense bodies and units of Ukraine's military formations and special services, as well as for the timely identification and prevention of threats to the state's cyber domain.

Purpose of the article. The purpose of this article is to reveal the organizational, functional, and conceptual features of the formation of modern cyber confrontation systems in leading countries of the world, with a view to formulating recommendations for improving the cybersecurity system of Ukraine.

Presentation of the main material. In the context of so-called "remote wars" and non-conventional confrontation, several key directions in the development of means of information and psychological influence have become firmly established. These include, in particular: expanding the use of the global Internet and cellular communication networks for the dissemination of propaganda materials; the development of specialized software that enables the creation of alternative, self-organizing communication networks based on mobile phones without the use of base stations and bypassing official service providers; imitation of the activities of false user groups on social media, taking into account linguistic, cultural, and geographical characteristics of specific regions (ethnic groups, subcultures, etc.); deployment of wireless networks based on Wi-Fi and Bluetooth technologies that are not controlled by state authorities; and the extensive use of artificial intelligence [27–28].

The first quarter of the 21st century was marked by the emergence, in foreign conceptual and regulatory documents, of stable terms such as "cyber war," "cyber warfare," and "cyber attack," which denote the conduct of military confrontation and special operations in cyberspace. Warfare (subversive activities) in cyberspace has become a new form of interstate confrontation. At the same time, confrontation in cyberspace is also conducted within the broader framework of information operations, intelligence and subversive campaigns, and related activities. According to American experts, cyberspace has transformed into a global domain within the structure of the information space and consists of an interconnected network of information technology infrastructures, including the global information network – the Internet, telecommunications networks, computer systems, as well as embedded processors and controllers.

The military and political leadership of leading states views confrontation in cyberspace as one of the decisive factors influencing international relations and the achievement of national interests. For this purpose, multi-level managerial and functional systems of cyber confrontation are being established, along with relevant national and interstate (bloc-based) command-and-control bodies (commands, centers, etc.), so-called "cyber forces," and specialized units within the structure of intelligence and security services. Corresponding cyber warfare capabilities, forces, and means are also being developed.

The Internet itself has become the primary theater of military operations for uncontrolled destructive information expansion and a testing ground for the creation of advanced means of information warfare. Common destructive techniques include information injections, disinformation and false publications, information "contagion," distortion of facts, removal of information from context, and substitution of concepts. Modern means of information confrontation have acquired a networked character and parasitize social networks, messengers, forums, and digital platforms. As a result, a high-tech toolkit of cyber warfare has been formed [29].

The recognition of cyberspace as a domain of warfare and special operations has led to the expansion of activities by security agencies and intelligence services into the cyber domain. NATO's Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization of 19 November 2010 defined the task of coordinating national cyber defense capabilities and enhancing capacities to protect and restore national infrastructure following destructive cyberattacks. On the basis of this concept, a unified document – the "Cyber Security Action Plan" – has been developed. Its primary

objective is countering the Russian cyber threat. The document was further supplemented by the "Cyber Defence Action Plan," which addresses the use of cyberspace as an operational environment to counter threats from hostile states, terrorist and extremist organizations, and attacks on the "strategic communications" of Alliance members. In December 2020, the European Union presented a new Cybersecurity Strategy aimed at increasing the resilience of critical infrastructure sectors and countering external cyberattacks.

In leading countries of the world, a key trend is the establishment of a comprehensive system of agencies and institutions responsible for cyber defense and cyber confrontation. Cyber defense forces are typically granted the status of a separate branch of the national armed forces through the integration of units specializing in signals intelligence, electronic warfare, information and psychological operations, cryptographic and cryptologic support, geospatial intelligence, and information protection in information and telecommunications systems, among others. At present, more than 60 countries possess their own forces or bodies dedicated to cyber warfare – defined as a complex of measures aimed at exerting managerial and/or destructive influence on the automated information and technological systems of an adversary, while protecting one's own information and computing resources from such influence through the use of specially developed hardware and software tools, as well as through the conduct of specialized training systems. The United States, for example, established the United States Cyber Command (USCYBERCOM). Following the U.S. model, other countries – including the Netherlands, Germany, Spain, South Korea, and Japan – have introduced cyber commands, centers, or dedicated cyber units [13, pp. 219–223].

Among specialized cybersecurity bodies are the Cybersecurity and Infrastructure Security Agency (CISA) of the U.S. Department of Homeland Security, the United Kingdom's National Cyber Security Centre (NCSC), the Canadian Centre for Cyber Security, the National Cyber Security Centre of the Republic of Poland, the National Cyber and Information Security Agency of the Czech Republic, and the National Cyber Security Centre of Lithuania. In a number of states, such bodies form an integrated organizational community. In Germany, for instance, this includes the Federal Office for Information Security, the Bundeswehr Cyber and Information Domain Service, the Cyber Defence Center, and the Computer Emergency Response Team. In August 2020, this structure was further complemented by the Agency for Innovation in Cybersecurity, jointly established by the Federal Ministries of Defence and the Interior [30, p. 4; 31, p. 9].

A global trend in security policy is the strengthening of state regulation in cyberspace – including covert intervention by intelligence and law enforcement agencies – and the development of so-called public–private partnerships in the field of cybersecurity [32]. As early as June 2013, *The Washington Post* published the results of an investigative report on a classified cooperation program involving U.S. security agencies, primarily the signals intelligence branch of the National Security Agency (NSA), and leading private companies operating in the global information market, such as Microsoft, Yahoo, Google, Facebook, PalTalk, and others. The investigation revealed that the program provided for the transfer to intelligence services of data related to e-mail communications, text and video chats, user-uploaded photographs and video materials, and, in general, any data stored on the servers of private companies. Subsequently, NSA representatives acknowledged the existence of the program [33, pp. 64–65].

The relative importance of cyber operations in the arsenal of radical and terrorist groups has also been increasing. The well-known Palestinian group Hamas (together with hacker groups from other Arab states) increased the number of cyberattacks against the Israeli Ministry of Defense, Ministry of Foreign Affairs, and other government agencies fivefold in April 2021 alone—reaching up to 150,000 attacks per day. Consequently, the use of force to suppress cyber-subversive activities by

radical groups became a component of Israel's counterterrorism operation "Guardian of the Walls" in the Gaza Strip in 2021. This involved an interagency operation with the participation of the Israel National Cyber Directorate (INCD), Unit 8200 (signals intelligence and electronic warfare) of the Military Intelligence Directorate (AMAN), cyber units of the Ministry of Defense, the foreign intelligence service Mossad, and the Israel Security Agency (Shin Bet). As a result, more than ten Hamas cyber unit headquarters were destroyed, including the chief of Hamas cyber forces and the group's cyber command center [30, p. 5].

Cyber confrontation has thus become established as an innovative component of contemporary military art, particularly within the framework of the concept of Multi-Domain Operations (MDO). A number of doctrinal and guiding documents have been issued, including *The U.S. Army Concept for Multi-Domain Operations at Brigade Level and Above (2025–2045)*, *The Multi-Domain Operations Concept*, *Multi-Domain Battle: The Evolution of Combined Arms for the 21st Century (2025–2040)*, *The U.S. Army in Multi-Domain Operations – 2028*, as well as the NATO Cooperative Cyber Defence Centre of Excellence study *Cyber Power and Multi-Domain Operations in High-Intensity Conflict 2030*. MDO is understood as the principal form of warfare within a theater of operations, involving the synchronized application – by time, space, and objectives – of U.S. joint forces and coalition groupings across land, air, and maritime operations, as well as in space and cyberspace. At the operational and strategic levels of interagency headquarters, the establishment of a command-and-control body responsible for managing information processes and actions in cyberspace was envisaged. The conduct of MDO was planned to be carried out by joint or coalition groupings simultaneously across all operational environments, including the virtual domain (cyberspace confrontation), as defined in U.S. doctrinal documents. Multi-Domain Forces (MDF) were conceived as land-based formations capable of coordinating their actions in a network-centric manner with air, naval, space, and cyber units, while bypassing a traditional joint headquarters structure [34, pp. 62–64; 35].

Accordingly, in recent years the United States has begun forming permanent multi-domain units and formations. Multi-Domain Task Forces (MDTFs) are being established to integrate actions in cyberspace, outer space, the electromagnetic spectrum (electronic warfare), as well as land, air, and naval forces and long-range precision strike systems into a unified offensive platform. At the level of army corps, the creation of Multi-Domain Effects Cells (MDEC) is planned. For example, during the "Warfighter 25-02" exercise (November–December 2024), an MDEC was integrated into the U.S. 1st Army Corps, comprising special operations forces, land and air force units, the 11th Cyber Battalion, the 12th Psychological Operations Battalion, and representatives of the 56th Information Operations Group [36].

On 16–17 July 2025, the first specialized NATO conference organized by the U.S. Army Europe Command was held in Germany, bringing together more than 1,000 participants, including policymakers and representatives of the defense industry. One of the central themes of the conference was Multi-Domain Operations (MDO), encompassing, inter alia, the cyber and information domains. In particular, it was emphasized that the newly established 56th Multi-Domain Command in Europe is conducting relevant exercises under the Dynamic Front series, employing a unified "combat internet" (kill web). It was noted that MDO-type operations are becoming a "new military philosophy of NATO," while the war in Ukraine itself is being waged across multiple dimensions, including cyber and information spaces. The experience of cyber operations and the application of artificial intelligence was also examined [37].

It is also appropriate to draw attention to the rapid development of China's cyber warfare forces network. China has established the Central Commission for Cybersecurity and Informatization of the Communist Party of China, which serves as

the principal coordinating body for cybersecurity and is chaired personally by President Xi Jinping. The Commission's executive bodies include the Cyberspace Administration of China (the leading state authority for regulation and coordination in the field of information and cyber security), the Cybersecurity Crisis Management Center, and the Center for the Identification of Harmful and Illegal Information.

Particularly well known is "Bureau 61419," a cyber warfare entity within the Strategic Support Force (SSF) of the People's Liberation Army (PLA), which cooperates with a network of hacker groups. A notable example of the use of controlled hacker collectives for large-scale cyberattacks was the cyber operation against Japanese military enterprises and the Japan Aerospace Exploration Agency. China is also developing a peripheral network of cyber warfare centers abroad. For instance, in Papua New Guinea, the Chinese telecommunications giant Huawei constructed a data processing center for intercepted information of state importance originating from relevant Australian institutions. In addition, the PLA maintains separate Cyber Support Forces.

The Network Systems Department of the PLA Strategic Support Force is responsible for ensuring cybersecurity. It oversees specialized centers tasked with operations within adversary information networks and with the protection of China's own information systems. This structure includes units for cyber intelligence and counterintelligence, electronic and malware-based attacks, and antivirus defense. The Communications Directorate of the PLA General Staff operates the Hankou Training Center, which serves as the principal training base (range) for practicing forms and methods of confrontation in computer networks. In late July 2025, the PRC officially announced the dissolution of the Strategic Support Force and the creation of a new branch of the PLA – the Information Support Forces – to which the cyber warfare component will be transferred [37].

Within China's Ministry of State Security (MSS), the 13th Bureau—the Information Security Evaluation Center of the PRC – is responsible for the security of information systems of civilian state agencies (with the exception of the armed forces, where cybersecurity is handled by dedicated military structures and military counterintelligence). Counterintelligence units exercise oversight over users of global computer networks. Since 2015, the Ministry of Public Security has operated a "Cyber Police" with territorial subdivisions. This ministry also maintains a number of departments, institutes, and laboratories engaged in the development of computer viruses and "Trojan horse" programs [30, pp. 3–4; 31, p. 2].

In September 2025, a large-scale information campaign unfolded in leading Western countries concerning the activities of the hacker group *Salt Typhoon*, which is traditionally associated with China. The U.S. National Security Agency and the Federal Bureau of Investigation stated that the hackers' activities constituted "the largest cyber espionage operation in recent years," affecting more than 200 institutions in 80 countries, including government bodies and prominent political figures. Chinese companies Sichuan Juxinhe, Beijing Huanyu Tianqiong, and Sichuan Zhixin Ruijie were accused of engaging in cyber espionage and facilitating the activities of *Salt Typhoon*; these companies were described as cover entities for the Ministry of State Security of the PRC and the People's Liberation Army [39].

Ukrainian researchers, characterizing information-cognitive confrontation as a component of the ongoing Russian-Ukrainian war, emphasize that the Russian Federation employs a broad spectrum of information influence methods. These include cyberattacks aimed at disrupting information infrastructure and data exfiltration, fake news and disinformation campaigns, as well as the active use of bot networks on social media platforms to disseminate pro-Russian narratives, among other instruments [14–18].

In the Russian Federation, Information Operations Forces of the Armed Forces were established in 2014, and a cyber command was introduced within the General Staff of the Armed

Forces. The management and planning of information operations are carried out by the Information Confrontation Directorate ("Directorate 12-bis," or the 12th Directorate) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation. The 85th Special Purpose Center (military unit 26165) of the GRU of the General Staff is particularly active and is regarded as one of the centers for the development of malicious software (identified by the U.S. NSA as *Drovorub*). The Main Center for Special Technologies of the GRU has been accused by the U.S. side of cooperating with the hacker group *Sandworm Team*, which is blamed for the cyberattack on Ukraine's energy system. The 72nd Special Service Center (military unit 54777) is responsible for organizing psychological operations in cyberspace [30, p. 2; 40–41].

According to assessments by the UK Ministry of Defence, Russia's capacity to conduct operations in the "grey zone" (essentially one of the traditional theaters of "hybrid warfare") includes substantial cyber warfare capabilities, with the number of Russian special services units operating in cyberspace having increased severalfold. On 7 May 2021, the U.S. Cybersecurity and Infrastructure Security Agency (CISA), together with the U.S. National Security Agency, the FBI, and the UK National Cyber Security Centre, issued cybersecurity guidance on the tactics and techniques of Russia's Foreign Intelligence Service (SVR), titled *Operational Procedures of Cyber Actors Associated with the SVR*. At the same time, CISA recruited an additional 200 cyber warfare specialists [30, p. 2; 40–41; 42, p. 3].

According to a Microsoft report on hacker attacks in 2020–2021, Russia was responsible for 58% of all recorded attacks. The majority of these attacks targeted the United States (46%), followed by Ukraine (19%) and the United Kingdom (9%), while Belgium, Japan, and Germany together accounted for 3% of attacks [43, p. 78].

Since the beginning of the full-scale invasion, cybersecurity specialists of the Security Service of Ukraine (SBU) have detected and neutralized more than 3,500 cyberattacks on the electronic resources of critical infrastructure facilities and state authorities. According to the SBU, most cyberattacks conducted by the Russian Federation were aimed at destabilizing the operation of transport sector enterprises (37%), central government bodies (31%), energy sector enterprises (16%), the economic sector (13%), and entities providing social services to the population (3%) [12, p. 44].

It is appropriate to emphasize the negative synergistic effect generated by the growing use of artificial intelligence (AI) in conjunction with cyberattacks. According to experts, such a synthesis may radically transform the nature of subversive activities in the information environment, opening the way for crude distortions of reality and sophisticated manipulation of human consciousness on an unprecedented scale. Researchers argue that the integration of AI-based systems in the near future may lead to the generation of pseudo-reality, elevating information-psychological operations to a qualitatively new level and significantly complicating their detection [44–45].

Foreign intelligence services are closely monitoring the state of Russia's cyber activity against Ukraine during the Russian-Ukrainian war. As early as April 2022, cybersecurity authorities of the EU Council, the United States, the United Kingdom, Canada, Australia, and New Zealand released a joint report titled *Russian State-Sponsored and Criminal Threats to Critical Infrastructure*. At the same time, cyber intelligence and cyber forensics and response teams prepared weekly chronological situation reports on developments in cyberspace. The cyber situation was also discussed on 10–11 May 2022 at the international CYBERUK 2022 conference in Newport, the UK's principal annual cybersecurity event. Participants noted that "the Ukrainian state demonstrated considerable resilience in maintaining communicative openness." Ukraine displayed "remarkable cyber resilience" during the conflict, despite the identification of at least eight distinct variants of wiper malware used to attack Ukrainian assets. Nevertheless, the Ukrainian side

"responded successfully, contained the attacks, and rebuilt its systems" against the backdrop of continuous Russian cyberattacks since 2014 [40].

Conclusions and prospects for further research. The construction of aggressive information and cyber spaces has reached such a scale and produced such consequences that it is increasingly regarded by experts as a new dimension of geopolitical rivalry and geographical expansion. The level of protection of national cyberspaces has sharply declined. Ukraine suffers not only from "traditional" cybercrime but also from sophisticated, state-sponsored cyberattacks, which necessitates, at the national level, the formulation of a conceptual vision of global processes related to the development of cyberspace, the determination of the country's place within them, and an understanding of the prospects for statehood under conditions of a "new digital world order." This gives rise to a strategic need for a conceptual rethinking of the new cybersecurity reality in order to build an effective national cybersecurity system.

The study of foreign experience demonstrates that, in ensuring the information security of the state, a crucial role is played by legal institutions as instruments of normative regulation and protection of all spheres of social life—civil, administrative, criminal, and specialized information law. In leading countries of the world, national legislation on information policy and information security has been developed over a long period, forming the basis for corresponding state-legal systems of interrelated public authorities, organizations, and institutions responsible for implementing a set of legal norms and principles intended to regulate social relations in the information sphere.

From an organizational and functional perspective, foreign experience confirms the necessity of having both a system of governmental agencies (bodies) endowed with clearly defined "offensive" and information-security functions, and a leading coordinating authority in this domain. Valuable conclusions regarding the construction of a nationwide system of information confrontation and security can be drawn from an analysis of the corresponding system in the People's Republic of China. China's information confrontation system rationally integrates specialized coordinating and governing bodies at the highest levels of public administration (which ensures effective interagency mobilization of forces and resources, including scientific and educational potential), as well as departmental verticals of specialized management (primarily within the armed forces, intelligence and security services, and the diplomatic service). In essence, an interagency system of information confrontation bodies has been established. Particular emphasis is placed on counterintelligence, regime, and technical protection of information networks and the information-cognitive sphere of society as a whole.

With regard to further research into foreign structures (national systems) of cyber warfare and cybersecurity, it appears expedient to:

- conduct in-depth studies of their doctrinal documents, organizational and staffing structures, and the forms and methods used to neutralize threats in cyberspace;
- separately analyze the mechanisms by which "non-governmental" hacker groups are employed;
- ensure the prompt incorporation of foreign innovations into the processes of professional training and advanced education of personnel of Ukraine's information and cyber security and confrontation bodies.

Based on the study of foreign experience, a number of recommendations can be formulated for improving the domestic system of cybersecurity and cyber confrontation, in particular:

- enhancing interagency cooperation in countering cybersecurity threats at the national level and within the components of Ukraine's security and defense sector;
- intensifying international cooperation, including through partner intelligence and security services and specialized institutions, aimed at forming a collective cybersecurity system and preventing cyberattacks;
- ensuring proactive intelligence monitoring of the activities of foreign structures engaged in subversive actions in cyberspace;

- creating, through the agent-operational capabilities of Ukraine's intelligence bodies, appropriate positions of influence within foreign structures involved in subversive cyber activities, including so-called "non-governmental" hacker entities;
- strengthening efforts to promote cyber hygiene and cyber literacy among personnel of public administration bodies, critical infrastructure facilities, and the financial and economic sector, among others.

References

1. Krotiuk V. A. (ed.) (2021). *Viiny informatsiinoi epokhy: mizhdystsyplinarnyi dyskurs* [Wars of the Information Age: An Interdisciplinary Discourse]. Kharkiv : FOP Fedorko M. Yu. [in Ukrainian].

2. Viedienieiev D., Semeniuk O. (2024). *Rozvytok kontseptualnykh pohliadiv na informatsiine protyborstvo yak skladovu nekonventsiinykh (hibrydnykh) viin i konfliktiv (2013–2023 rr.)* [Development of conceptual views on information confrontation]. Odesa : Oldi+ [in Ukrainian].

3. Pievtsov H. V., Hordiienko A. M., Zalkin S. V., Sidchenko S. O., Feklistov A. O., Hudarkovskyi K. I. (2017). *Informatsiino-psykholohichna borotba u voiennii sferi* [Information and psychological warfare in the military sphere]. Kharkiv : Rozhko S. H. [in Ukrainian].

4. NA SBU (2024). Proceedings of the 15th All-Ukrainian scientific-practical conference *"Aktualni problemy upravlinnia informatsiinoiu bezpekoiu derzhavy"* (Kyiv, March 27, 2024) [Current problems of state information security management]. Kyiv, ch. I., sekts. 1 [in Ukrainian].

5. *Ukaz Prezydenta Ukrainy Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 travnia 2021 r. "Pro Stratehiiu kiberbezpeky Ukrainy" № 447/2021* [Decree of the President of Ukraine On the Resolution of the National Security and Defense Council of Ukraine dated April 14, 2021 "On the Cybersecurity Strategy of Ukraine" activity no. 447/2021]. (2021, August 6). Retrieved from: https://surl.li/ogmglw (accessed 21 June 2025) [in Ukrainian].

6. Ukrainskyi militarnyi portal (2019). *V ZSU formuiut dva novi komanduvannia.* [Two new commands are being formed in the Armed Forces of Ukraine]. Retrieved from: https://surl.li/mmkkum (accessed 10 May 2025) [in Ukrainian].

7. NUOU (2023). Proceedings of the scientific and practical seminar of the department of communication technologies and cyber security *"Dosvid planuvannia ta boiovoho zastosuvannia viiskovykh chastyn (pidrozdiliv) viiski zviazku ta kiberbezpeky Zbroinykh Syl Ukrainy. Problemni pytannia ta shliakhy yikh vyrishennia"* (Kyiv, March 23, 2023) [Experience in planning and combat use of military units (subunits) of the Signal and Cybersecurity Forces of the Armed Forces of Ukraine]. Kyiv [in Ukrainian].

8. Ternovyi O. V., Shkurenko O. M., Minenko L. M. (2023). *Problemni aspekty kiberoborony: mistse ta rol kiberzakhystu v Zbroinykh Sylakh Ukrainy* [Problematic aspects of cyber defense: the place and role of cyber defense in the Armed Forces of Ukraine]. *Suchasni informatsiini tekhnolohii u sferi bezpeky i oborony,* no. 1, pp. 23–31 [in Ukrainian].

9. Zhyvylo Ye. O., Dokil V. M. (2023). *Model metodyky otsiniuvannia spromozhnostei viisk zviazku ta kiberbezpeky Zbroinykh Syl Ukrainy shchodo vykonannia zavdan z vidbyttia voiennoi ahresii v kiberprostori* [Model of the methodology for assessing the capabilities of the communications and cybersecurity troops of the Armed Forces of Ukraine in performing tasks to repel military aggression in cyberspace]. *Suchasni informatsiini tekhnolohii u sferi bezpeky i oborony,* no. 1, pp. 32–40 [in Ukrainian].

10. Murasov R., Melnyk Ya. (2023). *Otsiniuvannia zakhyshchenosti kiberprostoru obiektiv krytychnoi infrastruktury Ukrainy* [Assessment of cyberspace security of critical infrastructure facilities in Ukraine]. *Suchasni informatsiini tekhnolohii u sferi bezpeky i oborony*, no. 1, pp. 41–44 [in Ukrainian].

11. Shypovskyi V. V. (2023). *Systema pokaznykiv otsiniuvannia kiberstiikosti informatsiinykh system obiektiv krytychnoi infrastruktury* [System of indicators for assessing the cyber resilience of information systems of critical infrastructure facilities]. *Zakhyst informatsii,* no. 1 (25), pp. 37–45 [in Ukrainian].

12. Strelbytska L. M., Strelbytskyi M. P., Palchyk M. L. (2022). *Zabezpechennia informatsiinoi ta kiberbezpeky v umovakh viiskovoi ahresii RF proty Ukrainy* [Ensuring information and cybersecurity in conditions of military aggression]. Kyiv : NA SBU [in Ukrainian].

13. Hora I. V., Kolesnyk V. A., Maliuk V. V., Khodanovych V. O., Cherniak A. M., Shcherbyna L. I. (2023). *Zlochyny proty informatsiinoi bezpeky derzhavy: poniattia, vyiavlennia, dosudove rozsliduvannia* [Crimes against the information security of the state]. Kyiv : NA SBU [in Ukrainian].

14. Mashtalir V. V., Shypovskyi V. V. (2023). *Analiz podii u kiberprostori u protsesi rosiisko-*

ukrainskoi viiny 2022 roku: vysnovky, rekomendatsii, zasvoieni uroky [Analysis of events in cyberspace during the russian-Ukrainian war of 2022]. *Nauka i oborona*, no. 4, pp. 48–56 [in Ukrainian].

15. Kyrychenko Yu. V., Serhiienko T. I., Slastin V. O. (2025). *Informatsiini viiny yak instrument hibrydnoi ahresii: ukrainskyi dosvid* [Information wars as a tool of hybrid aggression]. *Visnyk NTUU "KPI". Seriia: politolohiia, sotsiolohiia, pravo,* no. 1, pp. 89–95 [in Ukrainian].

16. Hrebnov H. (2023). *Informatsiinyi aspekt hibrydnoi viiny rosii proty Ukrainy* [The information aspect of russia's hybrid war against Ukrain]. *Ukrainskyi informatsiinyi prostir,* no. 1, pp. 107–118 [in Ukrainian].

17. Kresina I. O. (2018). *Osoblyvosti zastosuvannia krainoiu-ahresorom informatsiinykh tekhnolohii u hibrydnii viini* [Peculiarities of the use of information technologies by the aggressor country in hybrid warfare]. *Derzhava i pravo. Seriia: politychni nauky,* no. 81, pp. 27–41 [in Ukrainian].

18. Tverdokhlib Yu. M. (2019). *Informatsiino-psykholohichni operatsii u rosiisko-ukrainskii hibrydnii viini* [Information and psychological operations in the russian-Ukrainian hybrid war]. PhD thesis. Chernivtsi : ChNU imeni Yuriia Fedkovycha, 220 p. [in Ukrainian].

19. Shereshkova I. I., Klunnyk M. S. (2024). *Potentsial vykorystannia shtuchnoho intelektu v informatsiino-psykholohichnykh operatsiiakh rf* [The potential of using artificial intelligence in information and psychological operations in the russian federation]. Proceedings of the 15th All-Ukrainian scientific-practical conference *"Aktualni problemy upravlinnia informatsiinoiu bezpekoiu derzhavy".* (Kyiv, March 27, 2024). Kyiv : NA SBU, ch. I, sects. 1, pp. 265–266 [in Ukrainian].

20. Honcharenko A. A., Kucheruk M. M., Bihun V. M., Kryvenko Yu. M. (2023). Proceedings of the round table *"Aktualni pytannia zakhystu natsionalnoi derzhavnosti v suchasnykh umovakh"* (Kyiv, July 28, 2023). [Current issues of protecting national statehood in modern conditions]. Kyiv : NA SBU [in Ukrainian].

21. Zhytomyrskyi viiskovyi instytut imeni S. P. Korolova (2019). Proceedings of the scientificand practical conference *"Problemy teorii ta praktyky informatsiinoho protyborstva v umovakh vedennia hibrydnoi viiny"* (Zhytomyr, October 24-25, 2019) [Problems of the theory and practice of information confrontation in the conditions of hybrid warfare]. Zhytomyr : ZhVI [in Ukrainian].

22. NUOU (2023). *Informatsiinyi biuleten vyvchennia boiovoho dosvidu zastosuvannia viisk zviazku ta kiberbezpeky Zbroinykh Syl Ukrainy u rosiisko-ukrainskii viini 2022–2023 rokiv* [Information bulletin on the study of combat experience in the use of communications and cybersecurity troops of the Armed Forces of Ukraine]. Kyiv [in Ukrainian].

23. NUOU (2023). *Informatsiinyi biuleten vyvchennia boiovoho dosvidu zastosuvannia viisk zviazku ta kiberbezpeky Zbroinykh Syl Ukrainy u rosiisko-ukrainskii viini 2022–2023 rokiv* [Information bulletin on the study of combat experience in the use of communications and cybersecurity troops of the Armed Forces of Ukraine]. Kyiv [in Ukrainian].

24. Mashtalir V., Permiakov O., Mykus S., Koroliuk N. (2023). *Boiovyi dosvid z pytan kiberoborony, otrymanyi pid chas rosiisko-ukrainskoi viiny. Ch.3. (lystopad 2022 – cherven 2023 roku*) [Combat experience in cyber defense gained during the russian-ukrainian war].. Kyiv : NUOU [in Ukrainian].

25. Mashtalir V., Mykus S., Avramenko M., Avramenko D. (2023). *Boiovyi dosvid z pytan informatsiinoi bezpeky, otrymanyi pid chas rosiisko-ukrainskoi viiny. Ch. 2 (berezen 2022–liutyi 2023 roku)* [Combat experience in cyber defense gained during the russian-ukrainian war]. Kyiv : NUOU [in Ukrainian].

26. Malyk Ya. Yo., Bereza O. I. (2012). *Zabezpechennia informatsiinoi bezpeky Ukrainy u konteksti svitovoho dosvidu* [Ensuring information security of Ukraine in the context of world experience]. *Efektyvnist derzhavnoho upravlinnia,* no. 32, pp. 20–27 [in Ukrainian].

27. Rushchenko I. P., Zubar N. V. (2017). *Viiny informatsii* [Information wars]. *Oboronnyi visnyk,* no. 8, pp. 4–9 [in Ukrainian].

28. Snitsarenko P. M. (2020). *Informatsiina operatsiia Zbroinykh Syl Ukrainy yak intehruiucha forma voiennykh dii v informatsiinomu prostori* [Information operation of the Armed Forces of Ukraine]. *Nauka i oborona,* no. 1, pp. 37–42 [in Ukrainian].

29. Yaskevych A. (2024). *Internet yak nove seredovyshche suhestyvnoho manipuliatyvnoho vplyvu* [The Internet as a new medium of suggestive manipulative influence.]. Proceedings of the interdepartmental scientificand practical conference *"Posylennia spromozhnostei SB Ukrainy ta vzaiemodiia zi skladovymy sektoru bezpeky i oborony".* (Kyiv, September 24, 2024). Kyiv : NA SBU, ch. 1, pp. 265–267 [in Ukrainian].

30. NUOU (2020). *Informatsiina dovidka shchodo aktualnykh kiberzahroz (atak) v merezhi Internet ta dii providnykh krain svitu u sferi kiberbezpeky za serpen 2020 roku* [Information note on current cyber threats (attacks) in the Internet network and the activities of leading countries of the world in the sphere of cybersecurity for August 2020]. Kyiv [in Ukrainian].

31. NUOU (2021). *Informatsiina dovidka shchodo aktualnykh kiberzahroz (atak) v merezhi Internet ta dii providnykh krain svitu u sferi kiberbezpeky za traven 2021 roku* [Information note on current cyber threats (attacks) in the Internet and the activities of leading countries of the world in the sphere of cybersecurity in May 2021]. Kyiv [in Ukrainian].

32. NISD (2018). *Derzhavno-pryvatne partnerstvo u sferi kiberbezpeky: mizhnarodnyi dosvid ta mozhlyvosti dlia Ukrainy* [Public-private partnership in cybersecurity]. Kyiv [in Ukrainian].

33. Dubov D. V. (2014). *Kiberprostir yak novyi vymir heopolitychnoho supernytstva* [Cyberspace as a new dimension of geopolitical rivalry]. Kyiv : NISD [in Ukrainian].

34. Ivashchenko A. M., Hordiichuk V. V., Andriianova N. M. (2022). *Kontseptsiia bahatodomennykh operatsii ta yii zastosuvannia sylamy oborony* [The concept of multi-domain operations and its application by defense forces]. *Zbirnyk naukovykh prats Tsentru viiskovo-stratehichnykh doslidzhen Natsionalnoho universytetu oborony Ukrainy imeni Ivana Cherniakhovskoho,* vol. 3, pp. 62–67 [in Ukrainian].

35. Viedienieiev D. V., Semeniuk O. H. (2024). *Normatyvno-kontseptualni zasady vyznachennia funktsii informatsiinoho protyborstva u bahatosfernykh ("multydomennykh") operatsiiakh zbroinykh syl SShA* [Normative and conceptual principles for determining the functions of information confrontation]. *Yurydychnyi naukovyi elektronnyi zhurnal,* no. 1, pp. 24–28 [in Ukrainian].

36. Viedienieiev D. V. (2024). *Rozvytok zarubizhnykh naukovo-kontseptualnykh pohliadiv na "bahatosferni operatsii"* [Development of foreign scientific and conceptual views on "multi-spherical operations"]. Proceedings of the 5th International scientificand practical conference *"Ukrainske viisko: suchasnist ta istorychna retrospektyva"* (Kyiv, November 28, 2024). Kyiv : NUOU, pp. 342–343 [in Ukrainian].

37. Joseph Roukoz (2025). *LANDEURO.* Retrieved from: https://surl.li/jpqmxu (accessed 14 August 2025) [in English].

38. Amber Wang (2025). *How China's new Information Support Force gears military up for PLA modernisation*. Retrieved from: https://surl.lu/uoohwm (accessed 22 August 2025) [in English].

39. Hromov M. *FBR: kytaiski khakery atakuvaly blyzko 80 krain u mezhakh kampanii Salt Typhoon* [FBI: Chinese hackers attacked about 80 countries]. Retrieved from: https://surl.li/vouwch (accessed 2 September 2025) [in Ukrainian].

40. Hnatiuk S. (2022). *Kiberskladnyk rosiisko-ukrainskoi viiny: uroky ta otsinky mizhnarodnoi spilnoty* [The cyber component of the russian-ukrainian war]. Kyiv : NISD. Retrieved from: https://surl.li/lxhkiz (accessed 5 September 2025) [in Ukrainian].

41. Viedienieiev D., Seheda S. (2023). *Rozvytok struktury orhaniv psykholohichnykh operatsii Zbroinykh syl Rosii (2014–2021 rr.)* [Development of the structure of psychological operations bodies of the Russian Armed Forces (2014–2021)]. Proceedings of the International scientificand practical conference *"Sektor bezpeky i oborony Ukrainy na zakhysti natsional¬nykh interesiv: aktualni problemy ta zavdannia v umovakh voiennoho stanu"* (Khmelnytskyi, November 24, 2022). Khmelnytskyi : NA DPSU, pp. 885–887 [in Ukrainian].

42. NUOU (2020). *Informatsiina dovidka shchodo aktualnykh kiberzahroz (atak) v merezhi Internet ta dii providnykh krain svitu u sferi kiberbezpeky za hruden 2020 roku* [Information notes on current cyber threats (attacks) on the Internet]. Kyiv [in Ukrainian].

43. Slinko T. (2021). *Suchasni zahrozy informatsiinii bezpetsi krainy ta shliakhy yikh podolannia* [Modern threats to the country's information security and ways to overcome them]. *Ukrainskyi chasopys konstytutsiinoho prava,* no. 4, pp. 77–86 [in Ukrainian].

44. Bohomia V. I., Hudz A. S. (2023). *Shtuchnyi intelekt: suchasnyi stan i perspektyvy zastosuvannia* [Artificial Intelligence: Current State and Prospects]. *Suchasni informatsiini tekhnolohii u sferi bezpeky i oborony,* no. 1, pp.13–17 [in Ukrainian].

45. Shereshkova I. I., Klunnyk M. S. (2024). *Potentsial vykorystannia shtuchnoho intelektu v informatsiino-psykholohichnykh operatsiiakh rf* [The potential of using artificial intelligence in information and psychological operations in the russian federation]. Proceedings of the 15th All-Ukrainian scientific-practical conference *"Aktualni problemy upravlinnia informatsiinoiu bezpekoiu derzhavy".* (Kyiv, March 27, 2024). Kyiv : NA SBU, ch. I, sekts. 1, pp. 265–266 [in Ukrainian].

Received / Стаття надійшла до редакції: 19.09.2025
Revised / Прорецензовано: 30.09.2025
Accepted / Схвалено до друку: 15.10.2025

ВЄДЄНЄЄВ ДМИТРО ВАЛЕРІЙОВИЧ
доктор історичних наук, професор,
професор кафедри історії,
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
https://orcid.org/0000-0002-8929-9875

ОРГАНІЗАЦІЙНО-ФУНКЦІОНАЛЬНІ ТА НАУКОВО-КОНЦЕПТУАЛЬНІ ОСОБЛИВОСТІ СИСТЕМ КІБЕРНЕТИЧНОГО ПРОТИБОРСТВА ПРОВІДНИХ КРАЇН СВІТУ (ПЕРША ЧВЕРТЬ XXI СТ.)

Авторський аналіз стану наукової розробки порушеної проблеми дозволяє констатувати необхідність підготовки окремих досліджень щодо поглибленого вивчення організаційно-функціональної структури, тенденцій розвитку та актуальних завдань, форм і методів діяльності сил кіберзахисту провідних іноземних держав з метою врахування для подальшого розвитку та вдосконалення діяльності органів та підрозділів кіберзахисту військових формувань та спеціальних служб України, своєчасного виявлення та запобігання загрозам кіберсфері держави.

Метою статті є розкриття організаційно-функціональних та концептуальних особливостей формування новітніх систем кіберзахисту провідних країн світу та оцінка характерних загроз, які сучасний етап розвитку сил і засобів розвідувально-підривної діяльності в мережевому та віртуальному просторі становить для національної безпеки України.

Доведено, що у провідних країнах світу основною тенденцією є створення комплексу відомств, установ (органів) з кіберзахисту та кібервійни. Сили кіберзахисту, як правило, отримують статус окремого виду національних збройних сил шляхом об'єднання підрозділів радіоелектронної розвідки, радіоелектронної боротьби, інформаційно-психологічних операцій, криптографічного та криптологічного забезпечення, геоінформаційного забезпечення, захисту інформації в інформаційно-телекомунікаційних системах тощо. Наразі понад 60 країн мають власні війська (органи) для ведення кібервійни – комплексу заходів, спрямованих на здійснення управлінського та/або деструктивного впливу на автоматизовані інформаційно-технологічні системи протилежної сторони та захист власних інформаційно-обчислювальних ресурсів від такого впливу шляхом використання спеціально розроблених програмно-технічних засобів, а також проведення системи спеціалізованих навчань.

На думку автора, у майбутньому видається доцільним поглиблено вивчити властиві їм доктринальні документи, досвід організаційно-штатної структури, форми та методи нейтралізації загроз у кіберпросторі, механізм використання «неурядових» хакерських груп, особливості відбору персоналу, а також забезпечити врахування іноземних інновацій у професійній підготовці та підвищенні кваліфікації співробітників органів інформаційної та кібербезпеки та контррозвідки України.

Ключові слова: *неконвенційна стратегія; інформаційне протиборство; кібернетичні війни; кібершпигунство; інформаційна безпека.*

UDC 342.95:343.35]:355.45(477) DOI 10.59226/2786-6920.2.2025.41-48

HALAI VIKTORIIA
Doctor of Juridical Sciences, Professor,
Professor of the Department of State Security,
Kyiv Institute of the National Guard of Ukraine
https://orcid.org/0000-0003-1568-5068

VAULIN OLEKSANDR
Master's Degree Student,
Kyiv Institute of the National Guard of Ukraine
https://orcid.org/0009-0008-9743-5946

STATE ANTI-CORRUPTION POLICY OF UKRAINE AS AN ELEMENT OF ENSURING NATIONAL SECURITY UNDER CONDITIONS OF HYBRID AGGRESSION

The article examines the role of Ukraine's state anti-corruption policy as a component of national security in the context of hybrid aggression. The interrelationships between corruption risks and the vulnerability of state institutions are analyzed, as well as the mechanisms through which external pressure can exploit internal gaps.

Anti-corruption policy in the context of hybrid aggression should be considered as an integral element of national security, combining legal, institutional, operational and cultural and educational dimensions. It is necessary to shift the emphasis from exclusively repressive measures to comprehensive preventive mechanisms: strengthening the institutional capacity of bodies, clear legislative consolidation of powers and procedures, integration of digital services for transparency of public finances and procurement, as well as effective application of sanctions and international legal instruments for asset recovery.

The key components of the success of anti-corruption reform should be: independent judicial reform and the inevitability of responsibility, protection of whistle blowers and resource support for public control, large-scale educational initiatives to build integrity, and the political will of the leadership to consistently implement reforms.

To implement these measures, a comprehensive system for assessing the effectiveness of anti-corruption reforms should be introduced, combining quantitative and qualitative indicators, external reviews and regular independent audits. Such a system should include performance metrics (number of completed and convicted cases of top corruption, volume of assets returned, procurement transparency indices), process metrics (case review time, percentage of completed competitions for management positions) and trust metrics (sociological surveys, perception indices), as well as public feedback mechanisms that will allow for prompt policy adjustments based on verified data and identified risks.

Keywords: *anti-corruption policy; national security; hybrid aggression; institutional capacity; digitization.*

Statement of the problem. The study of state anti-corruption policy under conditions of hybrid aggression requires a comprehensive interdisciplinary approach that integrates security-related, institutional, and socio-cultural dimensions of the problem. An analysis of the interconnections between corrupt practices and the vulnerability of state institutions makes it possible to identify the

mechanisms through which external pressure can exploit internal deficiencies, and to formulate targeted directions for reforms and preventive measures. Of particular significance is the study of the transformation of corruption risks during periods of escalation of hybrid threats and the possibilities for their neutralization through public policy instruments.

The relevance of this problem is driven by the simultaneous impact of two interrelated factors. The first is the evolution of the very nature of threats to national security: in the twenty-first century, armed conflicts increasingly acquire the characteristics of hybrid aggression, combining open military action with instruments of informational, economic, and political pressure, as well as institutional subversion, including mechanisms of corrupt influence. In the context of Ukraine, which has been experiencing systemic hybrid aggression since 2014 and, since 2022, has faced a full-scale invasion by the Russian Federation, corruption has ceased to be merely an "internal" governance problem. Instead, it has become one of the key vulnerability factors of state resilience, which may be exploited by an external aggressor to weaken defense capabilities, undermine public trust in state institutions, and provoke socio-political destabilization.

Accordingly, state anti-corruption policy should be viewed as a set of institutional solutions, regulatory measures, and integrity-compliance practices, and thus as an integral component of national security. Its purpose lies in reducing the state's vulnerability to external influence and enhancing the internal cohesion of society. At the same time, under the pressure of the need for rapid responses to security challenges, Ukraine's anti-corruption institutions are developing strategic documents and programs that transform approaches to the prevention, detection, and investigation of corruption-related offenses in the context of martial law and hybrid risks.

This dual dynamic – namely, the intensification of external threats alongside the necessity for internal institutional reform – renders the present study particularly relevant for the development of public policy and the practice of public administration.

Analysis of recent research and publications. Recent scholarly publications and analytical studies demonstrate that the issue of state anti-corruption policy in Ukraine continues to attract sustained interest from a wide range of domestic researchers. Notably, Bogolepova A., Kovtun O. [1], Hanba O. [2], Hryshyna N., Rostovska K. [3], Demchik N. [4], Korchak N. [5], Naumchuk K. [6], Nesterenko K., Bulgakova O. [7], Novak A. [8], Ortinsky V. [9], Perederiy O., Hryhorenko Y. [10], Samoylenko L., Nazarenko S., Perun N. [12], Tarasenko N. [13], Khotynska-Nor O., Salenko O. [14], among others, have systematically developed both theoretical-methodological foundations and empirical indicators of the effectiveness of anti-corruption reforms. This scientific activity encompasses diverse approaches, ranging from institutional-legal analysis and evaluation of the regulatory framework to empirical studies of corruption risks within public administration, analysis of financial flows, and the study of corruption's impact on economic dynamics and public trust. Such diversity of research approaches underscores the multidisciplinary nature of the problem and the need for knowledge synthesis to inform an adequate response policy.

Contemporary studies on anti-corruption policy in Ukraine pay attention not only to scientific publications but also to normative legal acts that define strategic directions and mechanisms of state anti-corruption activity. In particular, the Law of Ukraine "On the Principles of State Anti-Corruption Policy for 2021–2025" [11] establishes the key principles, objectives, and instruments for implementing anti-corruption policy, serving as a foundation for analyzing institutional effectiveness and developing practical recommendations for improving the national anti-corruption strategy.

At the same time, despite a significant accumulation of scientific potential and numerous practical initiatives, anti-corruption policy remains one of the defining priorities of the state strategy, as its implementation has both direct and indirect consequences for key dimensions of national

security. Within this context, anti-corruption measures affect the state's ability to attract international support and investment, the quality of economic regulation, the competitiveness of the national market, and the level of public legitimacy and trust in public institutions. From a methodological perspective, this implies that assessing the effectiveness of anti-corruption policy cannot be limited solely to quantitative indicators of offenses or procedural investigation metrics; it must also consider composite indicators, including macroeconomic effects, institutional resilience, and changes in societal trust.

The importance of this issue is particularly acute under conditions of martial law and intensive European integration reforms, where traditional anti-corruption mechanisms face dual pressures: external security challenges and the need to align national regulatory and institutional frameworks with European standards. In such circumstances, anti-corruption policy requires not merely formal adaptation but substantive transformation of prevention, investigation, and asset recovery procedures. This includes the development of operational mechanisms to ensure the integrity of supply chains in the security and defense sector, enhanced oversight of strategically important public procurement, increased coordination among law enforcement, financial, and supervisory authorities, and the integration of international partner mechanisms into the functioning of domestic institutions.

Purpose of the article is to examine Ukraine's state anti-corruption policy as a component of national security under conditions of hybrid aggression, including assessing its effectiveness, analyzing institutional architecture and legal mechanisms, evaluating practical approaches to preventing corruption risks during wartime and post-war periods, and developing recommendations for improving legislation and the implementation of anti-corruption measures to enhance state resilience and public trust.

Presentation of the main material. Ukraine's anti-corruption policy in the context of hybrid aggression should be viewed as a multi-level, multidisciplinary, and highly dynamic component of national security. It integrates legal, organizational, institutional, and ideological-cultural measures aimed at preventing corruption risks, minimizing their impact on the country's defense capacity and resource potential, and ensuring transparency in the distribution of humanitarian aid and international transfers during and after armed conflict.

This perspective aligns with the conceptual positions of several contemporary studies. Hanba O. emphasizes the crisis nature of corruption and its capacity to undermine the ability of the security and defense sector to fulfill state protection functions [2, pp. 88–89]. Naumchuk K. argues for the institutional-administrative nature of anti-corruption policy as a set of state goals, measures, and decisions [6, p. 157]. Bogolepova A. and Kovtun O. demonstrate that the wartime context has stimulated anti-corruption institutions to perform non-traditional functions, from monitoring humanitarian aid to coordinating sanction lists [1, p. 253]. Nesterenko K. and Bulgakova O. underline that anti-corruption policy must remain a state priority even when significant resources are mobilized for defense [7, p. 100].

The integration of these approaches provides an analytical framework in which anti-corruption measures are conceptualized not only as legal regulation and criminal enforcement but also as a comprehensive set of preventive, organizational, technocratic, and socio-cultural initiatives. These initiatives are aimed at strengthening institutional resilience and countering the external aggressor's instrumentalization of corruption mechanisms.

Examining the evolution of the institutional architecture of Ukraine's anti-corruption policy reveals the transition from declarative norms to a complex system of specialized agencies and mechanisms that hold strategic significance for national security. Naumchuk K. proposes a periodization of anti-corruption policy development, identifying stages of emergence, establishment, initial implementation of international approaches, and institutional capacity building; this historical perspective is crucial for evaluating the readiness of institutions such as NABU, NACP, and ARMA [6, p. 157]. Specialized

anti-corruption prosecution and the High Anti-Corruption Court possess the necessary operational, legal, and personnel capacity to function under conditions of hybrid aggression.

Studies by Hanba O., Nesterenko K., and Bulgakova O. confirm that the mere existence of institutions does not guarantee effectiveness; critical factors include the quality of institutional support, integrity of recruitment procedures, legislative clarity of authority, access to operational resources, and judicial capacity [2, p. 92; 7, p. 101]. Historical analysis also highlights vulnerabilities such as fragmented reforms, political blockages, and constitutional debates, which have significantly undermined public trust in the anti-corruption system.

Practical Dimension of Anti-Corruption Policy in Wartime. In the practical context of wartime, anti-corruption agencies are compelled to combine classical functions – detection, investigation, and suppression of corruption – with security-oriented tasks. Bogolepova A. and Kovtun O. identify specific priorities of the National Agency on Corruption Prevention (NACP) during the war period, including the creation of the "War and Sanctions" portal to track assets of individuals involved in aggression, the formation of task forces to locate sanctioned assets, conducting anti-corruption expertise of legal acts, and ensuring transparency in humanitarian supplies and coordination of logistics chains [1, p. 253]. These practices demonstrate the adaptive potential of institutions – they cease to be narrowly focused on declarative functions and reactive measures, instead becoming active agents of economic and informational defense.

At the same time, Nesterenko K. and Bulgakova O. emphasize that the success of such initiatives depends on the integration of electronic services, restoration of public submission of asset declarations where security concerns allow, and transparent procedures for selecting agency leadership – all factors that directly influence the trust of citizens and international partners [7, p. 100].

Legal and Administrative Dimension. The legal and administrative-legal aspect of anti-corruption policy, thoroughly developed in the works of Hrishina N. and Rostovska K., requires the formalization of policy implementation mechanisms and the codification of administrative-legal categories that define the scope and limits of public authority intervention in corruption prevention [3, p. 33]. The authors stress that anti-corruption policy should be regarded as an administrative-legal category encompassing organizational, staffing, informational, and procedural measures implemented by executive authorities in interaction with civil society.

From this perspective, priority areas include: detailed normative regulation of agency functions, establishment of procedures for anti-corruption expertise, mechanisms for special inspections, formation of the Unified State Register of Persons Convicted of Corruption, and whistleblower protection provisions. These measures strengthen the administrative-legal infrastructure for prevention. Practical implementation must ensure agency autonomy from political pressure, professional integrity criteria, and ethical standards for public servants, which act as safeguards against politicization of anti-corruption efforts.

Monitoring and Evaluation. Quantitative and qualitative monitoring of the anti-corruption environment, including the use of the Corruption Perceptions Index (CPI), is a key element in assessing policy effectiveness and communicating results internationally. Nesterenko K. and Bulgakova O. note that, despite wartime conditions, Ukraine’s CPI indicators have demonstrated relative resilience or slight improvement, reflecting the durability of the anti-corruption system [7, p. 99]. However, the index has methodological limitations – it reflects expert and institutional perceptions rather than direct measurement of corruption incidents. Therefore, it should be complemented with domestic indicators such as the number of prosecuted cases, disclosure of public procurement, and the volume of recovered assets. Integrated monitoring systems combining international and national metrics provide a more accurate diagnostic tool and enable real-time policy adjustments [7, p. 99].

Law Enforcement and Operational Capacity. The anti-corruption law enforcement system requires in-depth analysis of organizational-operational capabilities and procedural interaction among subjects responsible for investigation and prosecution. Hanba O. and Naumchuk K. identify key issues: ambiguous distribution of powers between NABU, SAP, the National Police, SBU, and the Office of the Prosecutor General necessitates clearer coordination; there is a need to improve procedures for special inspections and investigations to promptly recover stolen or illicitly exported assets; the role of ARMA in managing confiscated assets requires legislative guarantees to ensure effective management and transparent redistribution for restoration purposes [2, p. 92; 6, p. 158].

Practical obstacles, including limited access to case materials, insufficient technical and analytical support, and prolonged judicial proceedings, exacerbate corruption risks and reduce the preventive capacity of anti-corruption measures. Consequently, strengthening the operational capacity of law enforcement agencies must be accompanied by judicial reform to ensure accountability and accelerate the adjudication of economic and corruption-related cases.

Cultural-Value, Civic, and International-Legal Dimensions of Anti-Corruption Policy. The cultural and value-based component of anti-corruption policy occupies a central role in the works of Hanba O. and other researchers, as without the establishment of a system of societal values, ethical norms, and integrity, state policy risks remaining declarative [2, p. 92]. The formation of an anti-corruption culture should occur through systematic educational initiatives, professional programs for public servants, integration of anti-corruption modules into higher and vocational education, as well as public awareness campaigns aimed at enhancing citizens' information hygiene and reducing tolerance for corruption. NACP's educational platforms, noted by Bogolepova A. and Kovtun O., highlight the importance of communicative and educational tools in fostering societal intolerance of corruption; however, these initiatives need to be scaled and reinforced with incentive and sanction systems to ensure long-term behavioral transformation [1, p. 254].

Civil society and public oversight mechanisms function as a "third party" in the architecture of anti-corruption policy. They not only monitor and expose corrupt practices but also contribute to building trust and legitimacy. During wartime, as emphasized by Nesterenko K. and Bulgakova O., as well as Bogolepova A. and Kovtun O., it is critical to maintain public access to operational data where security allows; restoring electronic declarations, ensuring transparency in procurement procedures, and making the distribution of reconstruction funds public are essential [1, pp. 254–255; 7, p. 100]. Support for independent investigative journalism, protection of whistleblowers, and the creation of platforms for collective expertise in public policies increase the likelihood of early detection of corruption schemes, thereby reducing their systemic impact.

The sanctions and international-legal dimension of anti-corruption strategy, effectively applied by NACP and other agencies during the war, has a dual effect. First, sanctions and mechanisms for freezing or confiscating assets increase economic pressure on entities contributing to aggression. Second, international legal instruments and cooperation with partners enhance the efficiency of asset recovery and create a legal framework for cross-border investigations [1, p. 253]. Successful use of sanctions and asset recovery requires high evidentiary standards, alignment of national legislation with international regimes, and coordination among financial, law enforcement, and diplomatic institutions.

The post-war reconstruction phase of Ukraine necessitates the integration of anti-corruption mechanisms into all recovery projects, from public procurement procedures and critical infrastructure restoration to regional social reintegration programs. Naumchuk K., Bogolepova A., and Kovtun O., alongside Nesterenko K. and Bulgakova O., propose coordinated practical measures: full digitalization and implementation of e-governance at all levels; minimization of discretionary and allocation functions through

automation and delegation of routine procedures; optimization of the size of the civil service while enhancing professional competencies; establishment of justified salary limits and transparent motivation systems that do not generate corruption risks; implementation of specialized candidate vetting for key positions; and creation and funding of effective mechanisms for public oversight with resource support at the local level [1, p. 255; 6, p. 160; 7, p. 254]. These measures are both technocratic and systemic, as they transform the rules of the game as well as the behavioral norms of participants in public relations.

Conclusions and prospects for further research.

1. Integrated Anti-Corruption Strategy in Hybrid Aggression Contexts. The analytical overview indicates that anti-corruption policy under conditions of hybrid aggression must become an integrated state strategy, encompassing clearly defined institutions, legislative and administrative mechanisms, technical tools, and cultural-educational initiatives. Such a policy should simultaneously perform functions of legal response, prevention, economic defense, and societal resilience building.

2. Anti-Corruption Policy as a Component of National Security**.** Anti-corruption policy in hybrid aggression contexts should be regarded as an inseparable element of national security, combining legal, institutional, operational, and cultural-educational dimensions. Emphasis must shift from exclusively repressive measures toward comprehensive preventive mechanisms: strengthening institutional capacity, legally formalizing powers and procedures, integrating digital services to ensure transparency in public finances and procurement, and effectively applying sanctions and international-legal instruments for asset recovery. At the same time, a robust monitoring system combining international indicators with specific national metrics is required to enable real-time policy adjustments based on verified data and to minimize vulnerabilities exploitable by external aggressors.

3. Integration of Anti-Corruption Measures into Post-War Reconstruction**.** Post-war implementation of anti-corruption measures should be organically embedded in reconstruction programs, including the digitalization of administrative services, automation of procedures, minimization of discretionary functions, transparent competitions for leadership positions, and enhancement of professional standards among personnel. Key elements for the success of anti-corruption reforms include independent judicial reform and the inevitability of accountability, protection of whistleblowers, resource-supported public oversight, large-scale educational initiatives to foster integrity, and the political will of leadership for consistent implementation of reforms. Only a coordinated strategy of this nature can transform anti-corruption policy into an effective tool for national defense and sustainable state recovery.

4. Pathways for Policy Improvement**.** Primary pathways for enhancing anti-corruption policy include digitalization, transparent procedures, professional capacity building, judicial system strengthening, whistleblower protection, international cooperation in sanctions and asset recovery, and the development of public oversight systems. These measures should be implemented in a coordinated manner, accompanied by monitoring and accountability mechanisms, ensuring that anti-corruption policy functions not only as an instrument of internal governance but also as an effective component of a comprehensive national defense strategy.

To implement these measures, a comprehensive system for evaluating the effectiveness of anti-corruption reforms should be introduced, combining quantitative and qualitative indicators, external review, and regular independent audits. This system should include:

- Outcome metrics – e.g., number of completed and adjudicated high-level corruption cases, volume of recovered assets, procurement transparency indices;
- Process metrics – e.g., case processing time, percentage of completed competitions for leadership positions;
- Trust metrics – e.g., sociological surveys, perception indices;

- Feedback mechanisms – enabling real-time policy adjustments based on verified data and identified risks.

Such a system will enhance the responsiveness, transparency, and resilience of Ukraine's anti-corruption infrastructure under conditions of hybrid threats and post-war reconstruction.

References

1. Boholiepova A., Kovtun O. (2022). *Aktualni problemy podolannia koruptsii v umovakh viiny u postvoiennyi period* [Current problems of overcoming corruption during the war in the post-war period]. *Litopys Volyni. Vseukrainskyi naukovyi chasopys,* no. 27, pp. 251–256. Retrieved from: https://surl.lt/goebym (accessed 5 August 2025) [in Ukrainian].

2. Hanba O. (2021). *Derzhavna antykoruptsiina polityka: poniattia, sutnist ta zahalni oznaky* [State anti-corruption policy: concept, essence and general features]. *Publichne pravo,* no. 4 (44), pp. 88–95. Retrieved from: https://surl.li/jxtica (accessed 5 August 2025) [in Ukrainian].

3. Hryshyna N. V., Rostovska K. V. (2021). *Derzhavna antykoruptsijna polityka yak administratyvno-pravova katehoriia* [State anti-corruption policy as an administrative-legal category]. *Yurydychnyi naukovyi elektronnnyi zhurnal*, no. 11, pp. 31–33. Retrieved from: https://surl.lu/lmxuqr (accessed 3 August 2025) [in Ukrainian].

4. Demchyk N. P. (2024). *Realizatsiia antykoruptsiinoi stratehii v Ukraini* [Implementation of anti-corruption strategy in Ukraine]. *Yurydychnyi naukovyi elektronnnyi zhurnal,* no. 3, pp. 289–292. Retrieved from: https://surl.lu/nbxtca (accessed 1 August 2025) [in Ukrainian].

5. Korchak N. (2024). *Protydiia koruptsii yak osnova zabezpechennia natsionalnoi bezpeky Ukrainy: okremi aspekty* [Countering corruption as a basis for ensuring Ukraine's national security: selected aspects]. *Visnyk Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. Seiia: natsionalna bezpeka.* Kyiv, vol. 2 (2), pp. 13–16. Retrieved from: https://surl.li/kgzjlc (accessed 5 August 2025) [in Ukrainian].

6. Naumchuk K. M. (2023). *Derzhavna antykoruptsiina polityka Ukrainy* [State anti-corruption policy of Ukraine]. *Ekonomika, upravlinnia ta administruvannia,* no. 2 (104), pp. 156–162. Retrieved from: https://surli.cc/gldlyg (accessed 2 August 2025) [in Ukrainian].

7. Nesterenko K. O., Bulhakova O. V. (2023). *Antykoruptsiina polityka Ukrainy v konteksti viiny* [Anti-corruption policy of Ukraine in the context of war]. *Visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia: pravo.* Uzhhorod, vol. 77 (2), pp. 98–101. Retrieved from: https://surl.li/mtgklo (accessed 10 August 2025) [in Ukrainian].

8. Novak A. (2017). *Natsionalna antykoruptsiina polityka: osoblyvosti ta osnovni chynnyky rozvytku v umovakh suchasnoho derzhavotvorennia* [National anti-corruption policy: features and main factors of development in the context of modern state-building]. *Derzhavne upravlinnia ta mistseve samovriaduvannia,* no. 3 (34), pp. 62–66 [in Ukrainian].

9. Ortynskyi V. (2020). *Rol hromadianskoho suspilstva ta ZMI u borotbi z koruptsieiu* [The role of civil society and media in combating corruption]. *Visnyk natsionalnoho universytetu "Lvivska politekhnika". Seriia: yurydychni nauky.* Lviv, vol. 3 (27), pp. 75–80. Retrieved from: https://surl.li/beiolb (accessed 3 August 2025) [in Ukrainian].

10. Perederii O. S., Hryhorenko Ye. I. (2023). *Antykoruptsiina bezpeka Ukrainy yak perspektyvnyi komponent derzhavnoi pravovoi polityky: teoretyko-pravovi aspekty* [Anti-corruption security of Ukraine as a prospective component of state legal policy: theoretical and legal aspects]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia: pravo*. Uzhhorod, vol. 79 (1), pp. 82–88. Retrieved from: https://surl.li/ongwql (accessed 5 August 2025) [in Ukrainian].

11. *Zakon Ukrainy "Pro zasady derzhavnoi antykoruptsiinoi polityky na 2021–2025 roky" № 2322-IX* [Law of Ukraine about the principles of state anti-corruption policy for 2021–2025 activity no. 2322-IX]. (2022, June 20). *Baza danykh "Zakonodavstvo Ukrainy".* Retrieved from:

https://surl.li/rijboz (accessed 5 August 2025) [in Ukrainian].

12. Samoilenko L. Ya., Nazarenko S. A., Perun N. V. (2024). *Vyklyky ta bariery v realizatsii antykoruptsiinoi polityky na natsionalnomu ta rehionalnomu rivni* [Challenges and barriers in the implementation of anti-corruption policy at national and regional levels]. *Ekonomichnyi prostir,* no. 194, pp. 87–91. Retrieved from: https://surl.lu/ntznci (accessed 5 August 2025) [in Ukrainian].

13. Tarasenko N. (2015). *Borotba z koruptsieiu v Ukraini: uspikhy, problemy, perspektyvy* [Fight against corruption in Ukraine: successes, problems, prospects]. *Ukraina: podii, fakty, komentari*, no. 19, pp. 27–40 [in Ukrainian].

14. Khotynska-Nor O. Z., Salenko O. V. (2024). *Koruptsia yak faktor delehitymatsii sudovoi vlady* [Corruption as a factor of judiciary delegitimization]. *Analitychno-porivnialne pravoznavstvo,* no. 1, pp. 665–669. Retrieved from: https://surl.li/arswxe (accessed 5 August 2025) [in Ukrainian].

Received / Стаття надійшла до редакції: 20.08.2025
Revised / Прорецензовано: 05.09.2025
Accepted / Схвалено до друку: 26.09.2025

ГАЛАЙ ВІКТОРІЯ ОЛЕКСАНДРІВНА
доктор юридичних наук, професор,
професор кафедри забезпечення державної безпеки,
Київський інститут Національної гвардії України
https://orcid.org/0000-0003-1568-5068

ВАУЛІН ОЛЕКСАНДР АНДРІЙОВИЧ
здобувач магістерського рівня освіти,
Київський інститут Національної гвардії України
https://orcid.org/0009-0008-9743-5946

ДЕРЖАВНА АНТИКОРУПЦІЙНА ПОЛІТИКА УКРАЇНИ ЯК ЕЛЕМЕНТ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ В УМОВАХ ГІБРИДНОЇ АГРЕСІЇ

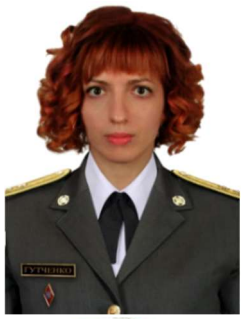
Досліджено роль державної антикорупційної політики України як складової національної безпеки в умовах гібридної агресії. Проаналізовано взаємозв'язок між корупційними ризиками і вразливістю державних інститутів, а також механізми, через які зовнішній тиск може експлуатувати внутрішні прогалини.

Окрему увагу приділено трансформації антикорупційних інституцій у період воєнного стану, застосуванню цифрових сервісів, міжнародних санкцій та системи публічного контролю. Акцентовано на тому, що ефективність антикорупційної політики залежить від якості інституційного забезпечення, прозорих процедур, інтеграції міжнародного досвіду та розвитку антикорупційної культури.

Запропоновано конкретні шляхи вдосконалювання антикорупційної політики, зокрема запровадження комплексної системи оцінювання ефективності антикорупційних реформ.

Ключові слова: *антикорупційна політика; національна безпека; гібридна агресія; інституційна спроможність; цифровізація.*

UDC 616-036.86:355.291.13:614.2 DOI 10.59226/2786-6920.2.2025.49-57



HUTCHENKO KATERYNA
Candidate of Medical Sciences, Leading Researcher,
Central Research Institute of the Armed Forces of Ukraine
https://orcid.org/0009-0008-6377-7745

KOZACHUK VIACHESLAV
Candidate of Technical Sciences, Senior Researcher, Leading Researcher,
Central Research Institute of the Armed Forces of Ukraine
https://orcid.org/0000-0002-0207-7461

HUTCHENKO ANDRII
Senior Lecturer at the Department,
Ivan Kozhedub National Air Force University
https://orcid.org/0009-0004-1748-6833

METHOD OF PLANNING MEDICAL AND PSYCHOLOGICAL REHABILITATION MEASURES FOR MILITARY PERSONNEL

One of the most pressing and problematic issues that arose during the Russian-Ukrainian war is improving the effectiveness of the medical and psychological rehabilitation system for servicemen of the Armed Forces of Ukraine. The peculiarity of this system lies in the need for a scientifically based approach to the planning and implementation of medical and psychological rehabilitation measures, taking into account not only clinical but also economic aspects. This creates a need to develop a comprehensive method based on mathematical models that will optimize the use of resources and improve the effectiveness of the medical and psychological rehabilitation system.

The purpose of this article is to develop a method for planning medical and psychological rehabilitation measures for military personnel.

A review of the literature has shown that most existing models of military rehabilitation focus on medical or psychological aspects without due consideration of economic efficiency and rational resource allocation. The scientific novelty of the article lies in the development of a method for planning medical and psychological rehabilitation measures for military personnel, which involves the use of cluster analysis, elements of queuing theory and programme-target management to prioritize applications based on the clinical condition of patients and available resources, which helps to improve the efficiency of the rehabilitation system in conditions of limited resources.

The article presents the formation of a rational queue of applications for medical and psychological rehabilitation, taking into account priority and resource availability, which allows for the most efficient distribution of medical, human and material resources. The practical application of the proposed method on the example of military personnel from the combat zone has shown the possibility of significantly improving the efficiency of the rehabilitation system by optimizing the time and labour intensity of procedures.

Further research prospects include determining the feasibility of using fuzzy clustering methods to improve the accuracy of forming a rational queue of military personnel for medical and psychological rehabilitation within the mass service system.

Keywords: *queuing theory; medical and psychological rehabilitation; method; system; military personnel; Armed Forces of Ukraine; resource optimization; planning; restoration of combat capability.*

Statement of the problem. In the process of analyzing the organization of medical care and the implementation of medical and psychological rehabilitation measures for military personnel in the context of large-scale hostilities in Ukraine, it has been established that key problems remain, such as the high level of systemic psycho-emotional exhaustion of personnel and the lack of adequate medical and economic justification for the planning of rehabilitation measures. These factors significantly reduce the effectiveness and timeliness of restoration the combat readiness of military formations, as well as lead to the irrational use of available medical, material, time and human resources within the functioning of the medical care system [1, 2].

According to the military medical service, more than 60% of military personnel who participated in combat operations require comprehensive rehabilitation measures, including medical and psychological rehabilitation. At the same time, the network of rehabilitation centres that existed at the beginning of 2022 was only 45 % staffed in terms of bed capacity and 52 % in terms of personnel, which led to queues for rehabilitation and delays in restoring the combat readiness of personnel [3].

At present, medical and psychological rehabilitation measures are planned mainly on the basis of clinical assessment of the soldier condition and the availability of free resources, without the use of mathematically sound methods.

Due to the lack of a structured mechanism for assessing the priority of medical and psychological rehabilitation, as well as economic justification for planned measures, the productivity of the existing forces and means of the medical and psychological rehabilitation system, which can be considered a mass service system, remained low [4]. In particular, some rehabilitation measures were prescribed without taking into account the clinical condition of military personnel, the intensity of their combat load and the predicted effectiveness of therapeutic intervention, which led to the irrational use of medical, human and financial resources [5]. In the process of preparing this article, data and approaches practiced at the Military Medical Clinical Centre of the Western Region and the Truskavets Medical Rehabilitation and Sanatorium Treatment Centre were taken into account. It was in these institutions that the need for unification of approaches to planning, taking into account resource constraints, was identified, which became the basis for the development of the proposed method.

Based on this, the issue of a scientifically sound approach to forming a rational queue for medical and psychological rehabilitation, as well as the development of a method for the medical and economic justification of rehabilitation measures in the healthcare system of military formations, is becoming particularly relevant [6, 7]. Its implementation will increase the effectiveness of restoring the combat readiness of military personnel and optimize the costs of medical services in conditions of limited resources [8].

Analysis of recent research and publications. on the organization of medical and psychological assistance to military personnel shows that the problem of medical and economic justification of planned rehabilitation measures has not been considered systematically enough. The main focus has been on the medical or psychological aspect separately, as well as on organizational approaches to the creation of rehabilitation structures [1–8].

Existing models that partially address the aspect of planning or the sequence of care provision can be divided into three groups [1, 3, 5]: analytical models based on the analysis of the treatment or rehabilitation process; probabilistic models based on statistics of intervention success and combat stress levels; regression models that take into account the influence of certain social, psychological or economic factors on the effectiveness of medical and psychological assistance.

The advantage of analytical and regression models is the ability to quantitatively assess the impact of key parameters (such as the degree of psycho-emotional stress, resource availability, etc.) on the effectiveness of rehabilitation measures [4, 6]. However, a disadvantage of regression models in particular is their dependence on a set of input factors that require experimental or empirical confirmation [2]. In addition, analytical models are mostly limited to two or three variables, and increasing the number of parameters significantly complicates calculations and reduces the reliability of results. Probabilistic models make it possible to assess the risks of relapse or ineffective rehabilitation based on statistical data, but they do not take economic factors into account [7].

On the other hand, models based on cluster analysis allow structuring the queues of military personnel for rehabilitation, taking into account both clinical and economic characteristics [5, 8]. Their advantage is the ability to flexibly manage the order of interventions, integrate medical indicators with cost and organizational factors, and adapt to changes in real time.

In this regard, an urgent task is to develop a method that will ensure effective planning of rehabilitation measures and rational allocation of available resources in the military medical system.

Purpose of the article is to develop a method for planning medical and psychological rehabilitation measures for military personnel.

Presentation of the main material. When a number of applications for medical and psychological rehabilitation of military personnel are received, a queue of such applications may be formed, the receipt and processing of which is determined by the discipline of queuing. The discipline of waiting determines the order in which applications are accepted into the rehabilitation system and their order in the queue, while the discipline of service determines the order in which applications are selected from the queue for the appointment of rehabilitation measures. Depending on the accepted order of processing applications, a distinction is made between systems with non-priority and priority disciplines.

Systems with non-priority disciplines consider applications to be equal. The following rules for selecting applications from the queue can be given as examples:

1) FIFO (First Input – First Output) discipline – the first application in the queue is selected;

2) LIFO (Last Input – First Output) discipline – the last application in the queue is selected;

3) discipline of selecting a request from the queue at random and several others.

In priority service disciplines, certain requests of one type are given preferential service over requests of another type in accordance with the established priority [3, 6].

The following types of priorities are distinguished:

1) Relative priorities – only taken into account when assigning a service request. When a rehabilitation channel becomes available, the priorities of the requests in the queue are compared, and service is provided to the request with the highest priority.

2) Absolute priorities – involve interrupting the rehabilitation of a low-priority request when a higher-priority request arrives. The interrupted request is returned to the beginning of the corresponding queue [7].

3) Mixed priorities – a combination of both types of priorities, where some requests are serviced without priority.

The task is more difficult when there are several priorities or when priorities are not ranked by degree of importance. In such cases, the rationality of the queue of requests is determined in several stages.

By a rational queue for medical and psychological rehabilitation, we mean a queue in which, within a specified time, the rehabilitation of military personnel will be carried out with the maximum effect of restoring combat readiness at minimum resource costs.

Let us consider the order of forming such a queue. Let there be a set of applications G, consisting of w types of rehabilitation measures with the number of applications $\overline{1,k}$ for each type. Within this process, it is advisable to consider the rehabilitation system as a queuing system (QS), where the objects of service are applications from military personnel for rehabilitation procedures. In an QS, queues are formed according to the types of interventions, and the efficiency of the system is assessed by indicators of load, service duration and resource utilization. Thus, a set of requests G is received by the QS, which forms w queues with a corresponding number of requests in each queue (Fig. 1). The method of forming a rational queue also requires knowledge of the initial state of requests, namely the duration of rehabilitation T_{rehab} and its labour intensity H_{rehab}.

From the perspective of QS theory, the maximum efficiency of the rehabilitation system is achieved when the productivity of processing the incoming flow of requests is maximum and the number of requests in the queue is minimum. To do this, requests with the minimum values of rehabilitation duration and labour intensity ($T_{обс}$, $H_{обс} \rightarrow min$) should be serviced first.

Based on this, the task *of the first stage* of the method is as follows: to select applications whose rehabilitation requires the least amount of time and resources. To solve this problem, applications in each of the w queues are clustered (using the k-means algorithm, applications in the queue are grouped into 3 clusters), resulting in the formation of $3w$ clusters from the set G: w clusters with $\{R\}$ applications with the lowest $T_{rehab\ and}$ H_{rehab} indicators, w clusters with $\{F\}$ applications with average indicators, and w clusters with $\{S\}$ applications with the highest indicators. Requests $\{R\}$ are sent to the QS for service, requests $\{F\}$ with average indicators remain in the queue, and requests $\{S\}$ with maximum indicators T_{rehab}, H_{rehab} are transferred for service to other rehabilitation centers with greater resources (Fig. 1).

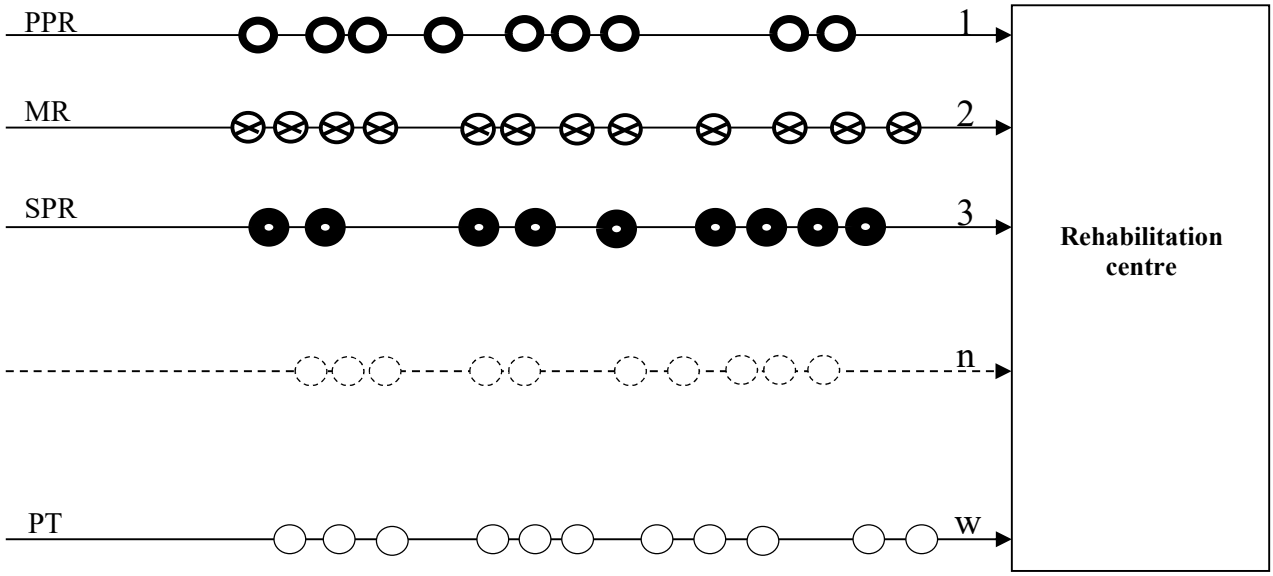


Figure 1 – Queues of applications for medical and psychological rehabilitation of military personnel (example). Source: developed by the authors

The task of *the second stage* of the method is to form a rational sequence of service for the {*R*} applications with the lowest T_{reab} *and* H_{reab} indicators, which were selected at the first stage. To solve this task, each request is described by a number of parameters, among which there must be a priority indicator. As an example, requests are characterized by parameters such as the duration of rehabilitation, labour intensity, combat load level, and degree of psychological exhaustion. The degree of combat stress can be considered a priority indicator.

After that, one cluster is formed from {*R*} applications according to the g-means algorithm based on the maximum compactness criterion, and the minimum distance from the cluster centre of each of {*R*} applications is determined:

$$W(S,c)=\sum_{k=1}^{K}\sum_{i} d(g_i,c_k),$$

where g_i is the vector of application parameters *i*, c_k is the centre of cluster *k*.

This distance is the ranking of applications to the QS by priority.

The minimization criterion is the sum of distances $d(g_i \; c_k)$ from objects g_i to the corresponding cluster centers (centroids) c_k [5].

Thus, the task of forming a rational queue of applications to the medical and psychological rehabilitation system is completed.

Similarly, a rational queue is formed for applications in clusters *w* from the set of applications {*F*} (applications with average indicators) that are waiting to be served in the queue.

An example of practical application (Fig. 1).

The initial data is as follows. There are 43 military personnel in the combat zone who require various types of rehabilitation: psychophysiological rehabilitation (PPR) – 9 people, medical rehabilitation (MR) – 12 persons, social-psychological rehabilitation (SPR) – 11 persons, psychotherapy (PT) – 11 persons.

The duration of rehabilitation varies from 4 to 22 days; labour intensity from 8 to 66 person-days; combat load from 1 to 5 points. The cost of rehabilitation measures varies from 2.33 thousand UAH to 2.35 thousand UAH.

After completing the first stage, 12 clusters were formed (Fig. 2): 4 clusters with low (so-called first-level clusters), medium (second level) and high (third level) indicators of duration and labour intensity.

There were 17 applications in clusters with the lowest T_{reb} *and* H_{reb} values, 11 applications in clusters with average values, and 15 applications in clusters with the highest T_{reb} and H_{reb} values.

The first-level clusters were formed as follows: psychophysiological rehabilitation – 4 applications (1, 4, 5, 8), medical rehabilitation – 5 applications (11, 15, 16, 19, 21), social and psychological rehabilitation – 3 (27, 28, 30), psychotherapy – 5 applications (33, 37, 41, 42, 43). Second-level

clusters: psychophysiological rehabilitation – 2 applications, medical rehabilitation – 3 applications, social and psychological rehabilitation – 3 applications, psychotherapy – 3 applications. Third-level clusters, respectively – 3, 4, 5, 3 applications.

At the second stage, in order to form a rational queue of applications placed in first-level clusters, a single cluster of low-level applications is formed and the applications are ranked according to their distance from the center of the cluster (Table 1).

Ranking applications according to the cluster centroid allows us to build a rational queue of applications. Table 1 shows how 17 applications, grouped into a single cluster, are distributed by distance to the center of this cluster – centroid. Each application has its own number, and they all belong to cluster number 1.

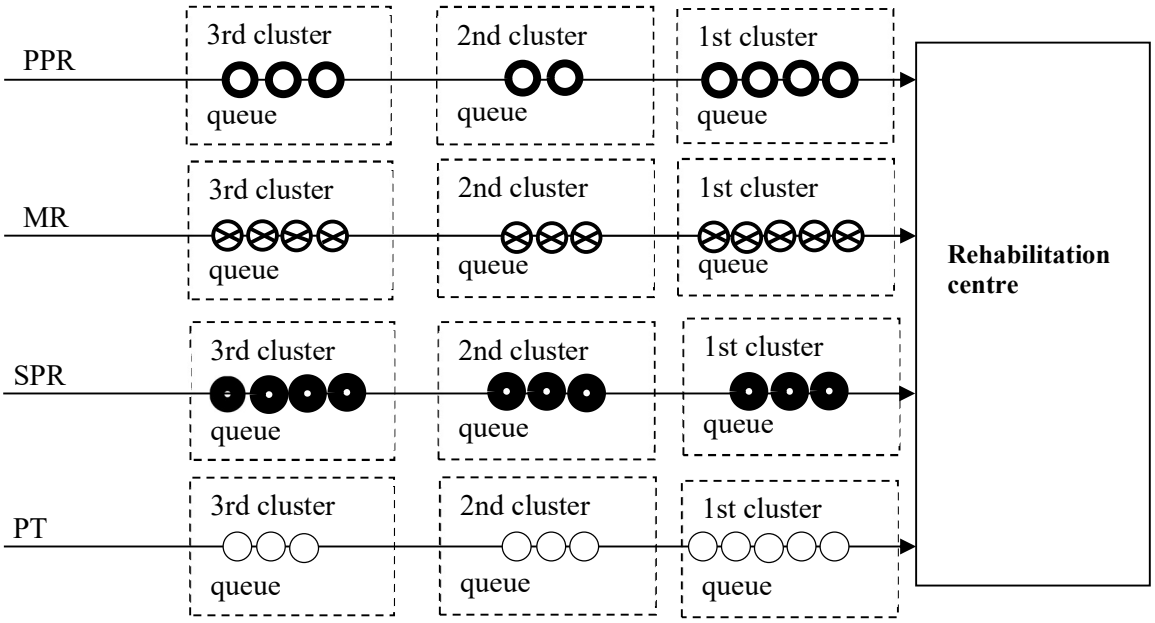


Figure 2 – Results of the first stage of clustering (example).
Source: developed by the authors

Table 1 – Distance of applications to the cluster centroid

Application number	Cluster number	Distance to the cluster center
1	1	0,6184146
4	1	0,6716266
5	1	0,5154355
8	1	0,6392021
11	1	0,2992313
15	1	0,4043581
16	1	0,2992313
19	1	0,3907396
21	1	0,2992313
27	1	0,5171861
28	1	0,3405352
30	1	0,2916174
33	1	0,8457961
37	1	0,7321997
41	1	0,7321997
42	1	0,8457961
43	1	0,7474904

The distance to the centroid shows how close the application is to the "typical" representative of the group. Smaller distance values mean that the application is more typical for the cluster, while larger values mean that it differs from the majority.

Applications with the smallest distance (e.g., No. 30, 11, 16, 21) are closest to the center and, accordingly, have priority for processing. Applications with a greater distance (e.g., No. 33, 42) are less typical and can be processed later.

This ranking helps to form an efficient order for processing applications, which increases the productivity of the system.

The cluster is formed using the g-means algorithm, which automatically determines the optimal number and structure of groups based on data analysis.

After ranking the applications, the optimized queue is shown in Fig. 3 and Table 2.

Table 2 presents the results of ranking 17 applications that were combined into a single cluster with low labour intensity and rehabilitation duration indicators. Each application has its own number, sequential place in the queue, and distance to the center of this cluster (centroid).

The queue is formed in such a way that the applications that are the most typical for this group are in the first place. For example, application No. 30 has the shortest distance to the centroid (0.2916), so it was given the highest priority. It is followed by applications No. 11, 16 and 21 – all with very similar distance values. This means that they also correspond well to the average profile of applications in the cluster.

In contrast, applications No. 33 and No. 42 have the greatest distance (0.8458), so they are placed at the end of the queue as they are less similar to the others and less of a priority for processing.

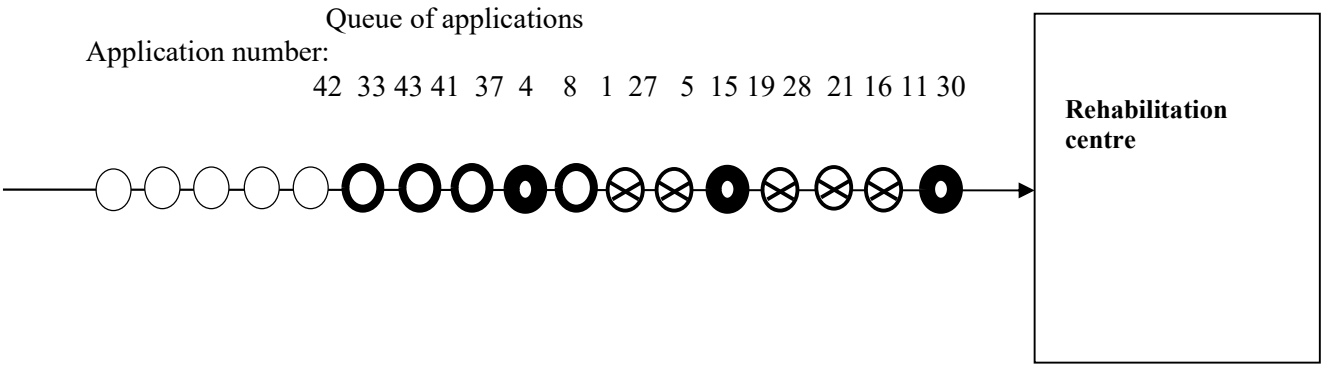


Figure 3 – Results of the second stage of clustering (example).
Source: developed by the authors

Table 2 – Ranking of the application queue

Application number	Number in the queue	Distance to cluster centre
30	1	0,2916174
11	2	0,2992313
16	3	0,2992313
21	4	0,2992313
28	5	0,3405352
19	6	0,3907396
15	7	0,4043581
5	8	0,5154355
27	9	0,5171861
1	10	0,6184146
8	11	0,6392021
4	12	0,6716266
37	13	0,7321997
41	14	0,7321997
43	15	0,7474904
33	16	0,8457961
42	17	0,8457961

This ranking method allows to create a rational queue for processing applications: first – the most typical ones, then the less typical ones. This increases the efficiency of the system, as it allows to quickly process the most "understandable" and predictable cases, using resources as efficiently as possible.

The analytical platform "Deductor–C", version 5.3, was used to perform the calculations.

The method was tested on a sample of data from military personnel who served in the combat zone, simulating real application flows. To implement the method, it is planned to gradually introduce it into the practical activities of the rehabilitation facilities of the Armed Forces of Ukraine by developing software that integrates with existing military medical information systems. The method allows to form rational rehabilitation queues based on priority, duration and complexity of procedures, as well as current supplies, which is particularly relevant in conditions of limited resources.

Conclusions and prospects for further research. A method for planning medical and psychological rehabilitation measures for military personnel has been proposed. It is based on the integration of program-target management and cluster analysis methods to organize and prioritize medical and psychological rehabilitation measures. The proposed approach makes it possible to take into account the multiplicity of parameters of needs for rehabilitation measures and the resource capabilities of the system.

Prospects for further research include determining the feasibility of using fuzzy clustering methods to improve the accuracy of forming a rational queue of military personnel for medical and psychological rehabilitation within the mass service system.

References

1. Sukharieva, V., Kozhyna, H., Chernenko, I., & Lytvynenko, V. (2025). Pathophsychological features of stress-related disorders in combatants. *Eastern Ukrainian Medical Journal,* no. 13 (1), pp. 122–129. DOI: https://doi.org/10.21272/eumj.2025;13(1):122-129 [in English].

2. Yakimets, V. M., Pechyborshch, V. P., Voronenko, V. V., Yakimets, V. V., Pechyborshch, O. V., Nikonenko, A. V., & Slabky, G. O. (2023). Guaranteed psychological assistance and rehabilitation of servicemen is a component of national security. *Bulletin of Social Hygiene and Health Care Organizations of Ukraine,* no. 3, pp. 41–50. DOI: https://doi.org/10.11603/1681-2786.2022.3.13435 [in English].

3. Surhund N., Verba H. (2024). *Osoblyvosti psykholohichnoi reabilitatsii viiskovosluzhbovtsiv na etapi vidnovlennia* [Features of psychological rehabilitation of servicemen at the recovery stage]. *Psychology Travelogs,* no. 3, pp. 47–56. DOI: https://doi.org/10.31891/PT-2024-3-5 [in Ukrainian].

4. Rybchych I. Ye., Khoroshenko M. V., Kupiak S. R. (2022). *Formuvannia derzhavnoi polityky medyko-psykholohichnoi reabilitatsii viiskovosluzhbovtsiv na etapi adaptatsii do sotsialno-ekonomichnykh umov* [Formation of state policy of medical and psychological rehabilitation of servicemen at the stage of adaptation to socio-economic conditions]. *Dniprovskyi naukovyi chasopys publichnoho upravlinnia, psykholohii, prava,* no. 5 (5), pp. 28–32. DOI: https://doi.org/10.51547/ppp.dp.ua/2022.5.5 [in Ukrainian].

5. Vasylenko S. (2020). *Psykholohichna reabilitatsiia v systemi psykholohichnoho zabezpechennia pidhotovky ta zastosuvannia viisk ZSU v suchasnykh umovakh* [Psychological rehabilitation in the system of psychological support for the training and deployment of the Armed Forces of Ukraine under modern conditions]. *Visnyk Natsionalnoho universytetu oborony Ukrainy,* vol. 51 (1), pp. 5–10. DOI: https://doi.org/10.33099/2617-6858-2019-51-1-5-10 [in Ukrainian].

6. Chaban O. H. (2014). *Shliakhy stvorennia efektyvnoi systemy medychnoi reabilitatsii* [Ways of creating an effective system of medical rehabilitation]. *Aktualni problemy navchannia ta vykhovannia liudei z osoblyvymy potrebamy*, no. 11 (13), pp. 207–218. Retrieved from: https://ap.uu.edu.ua/article/33 (accessed 25 June 2025) [in Ukrainian].

7. Kokun O. M., Moroz V. M., Lozinska N. S., Pishko I. O. (2021). *Psykholohichna profiklatyka psykhotravmatyzatsii viiskovosluzhbovtsiv* [Psychological prevention of servicemen's psychotraumatization]. Kyiv : NDTs HP ZSU [in Ukrainian].

8. Sydorenko V. M., Ivanov O. P. (2018). *Reabilitatsiia viiskovosluzhbovtsi – uchasnykiv boiovykh dii v systemi medychnoho zabezpechennia Zbroinykh Syl Ukrainy* [Rehabilitation of combatant servicemen in the medical support system of the Armed Forces of Ukraine]. Khmelnytskyi : Khmelnytskyi natsionalnyi universytet [in Ukrainian].

Received / Стаття надійшла до редакції: 04.07.2025
Revised / Прорецензовано: 18.07.2025
Accepted / Схвалено до друку: 29.07.2025

ГУТЧЕНКО КАТЕРИНА СЕРГІЇВНА
кандидат медичних наук,
провідний науковий співробітник,
Центральний науково-дослідний інститут Збройних Сил України
https://orcid.org/0009-0008-6377-7745

КОЗАЧУК В'ЯЧЕСЛАВ ЛЕОНІДОВИЧ
кандидат технічних наук, старший науковий співробітник,
провідний науковий співробітник,
Центральний науково-дослідний інститут Збройних Сил України
https://orcid.org/0000-0002-0207-7461

ГУТЧЕНКО АНДРІЙ ГЕННАДІЙОВИЧ
старший викладач кафедри,
Харківський національний університет Повітряних Сил
Збройних Сил України імені Івана Кожедуба
https://orcid.org/0009-0004-1748-6833

МЕТОД ПЛАНУВАННЯ ЗАХОДІВ МЕДИКО-ПСИХОЛОГІЧНОЇ РЕАБІЛІТАЦІЇ ВІЙСЬКОВОСЛУЖБОВЦІВ

Одним із найбільш актуальних і проблемних питань, що постали під час російсько-української війни, є підвищення ефективності функціонування системи медико-психологічної реабілітації військовослужбовців Збройних Сил України. Особливість цієї системи полягає в необхідності науково обґрунтованого підходу до планування та реалізації заходів медико-психологічної реабілітації з урахуванням не тільки клінічних, а й економічних аспектів. Відтак виникає потреба у розробленні цілісного методу, який на основі математичних моделей дасть змогу оптимізувати використання ресурсів і підвищити ефективність системи медико-психологічної реабілітації.

Розроблено метод планування заходів медико-психологічної реабілітації військовослужбовців, що передбачає використання кластерного аналізу, елементів теорії масового обслуговування та програмно-цільового управління з метою впорядкування черговості заявок з огляду на клінічний стан пацієнтів і наявні ресурси. Зазначений метод сприятиме підвищенню ефективності функціонування системи реабілітації в умовах обмеженого ресурсного забезпечення.

Здійснено формування раціональної черги заявок на медико-психологічну реабілітацію з урахуванням пріоритетності та ресурсної забезпеченості, що уможливлює максимально ефективний розподіл медичних, кадрових і матеріальних ресурсів. Практичне застосування запропонованого методу у процесі відновлення військовослужбовців із зони бойових дій показало значне підвищення ефективності системи реабілітації за рахунок оптимізації часу і трудомісткості процедур.

Ключові слова: *теорія масового обслуговування; медико-психологічна реабілітація; метод; система; військовослужбовці; кластеризація; оптимізація ресурсів; планування; відновлення боєздатності.*

UDC 623.462.22(075.8) DOI 10.59226/2786-6920.2.2025.58-69

IVANETS HRYHORII
Candidate of Technical Sciences, Associate Professor,
Senior Researcher, Ivan Kozhedub National Air Force University
https:/orcid.org/0000-0002-4906-5265

HORIELYSHEV STANISLAV
Candidate of Technical Sciences, Associate Professor,
Associate Professor of the Department of Tactics,
National Academy of the National Guard of Ukraine
https://orcid.org/ 0000-0003-1689-0901

IVANETS MYKHAILO
Candidate of Technical Sciences, Senior Researcher,
Leading Researcher – Leading Test Engineer,
State Research Institute for Testing and Certification
of Armament and Military Equipment
https:/orcid.org/0000-0002-3106-7633

DEFINING THE FREQUENCY DEPENDENCIES OF THE RADAR CROSS SECTION OF LENS SIMULATORS OF AIR TARGETS FOR VARIOUS DIELECTRIC MATERIALS

Maintaining air defense units within the Armed Forces of Ukraine and the National Guard of Ukraine in constant combat readiness to perform combat tasks requires conducting live-fire exercises with modern air targets during military training of personnel. Air targets simulate real enemy air attack weapons and are used as false air targets during combat operations. One of the most promising passive simulators of the radar cross section of air targets in the radar wave range is the multilayer Luneburg lens.

When creating such lens simulators, the discreteness of change and frequency dependence of dielectric permeability, as well as additional technological errors, lead to a decrease in their radar cross section compared to theoretical values. This circumstance must be taken into account when creating specific targets or false air targets.

An algorithm has been developed for a computational and experimental method of estimating the real values of the radar cross section of passive simulators based on Luneburg lenses using an anechoic chamber. The measurement and assessment of the real value of the radar cross section of lens simulators is based on the use of a reference reflector in the form of a metal sphere with a known radar cross section.

The results of experimental studies have shown that the radar cross section indicators of air target simulators depend on the dielectric material, technology, and irradiation frequency.

Keywords: *radar cross section; air target simulator; Luneburg lens; dielectric material; technology; reference sphere; anechoic chamber.*

Statement of the problem. Maintaining air defense units (ADU) within the Armed Forces of Ukraine and the National Guard of Ukraine in constant combat readiness to perform combat tasks requires conducting live-fire exercises with modern air targets during military training. Air targets simulate real modern enemy air attack weapons, as well as false targets during combat operations. The main element of the target equipment of modern and promising target UAVs is the means of simulating the radar cross section (RCS) of various types of air targets. Currently, in the leading countries of the world and the European Union, the most promising direction for the creation of passive RCS simulators of air targets in the radar wave range is the use of multilayer spherical Luneburg lenses (LL), which differ from each other in geometric dimensions, material and shape of the metallised surface [1, 2]. Selecting the necessary parameters allows for a significant increase in RCS (by tens of times) and the simulation of more significant targets [3].

The use of LL in air target simulators significantly reduces the cost of training air defence units, increases the realism of training exercises and creates universal targets for various combat scenarios.

Various dielectric materials are used to manufacture spherical LLs, as well as various dielectric composite materials, which include synthetic polymers and dielectric substances. When creating spherical air target simulators in the form of multilayer LLs, the properties of the dielectric material, the discreteness of the change in dielectric permeability, and the failure to comply with the manufacturing technology lead to a deterioration in their RCS values compared to what is theoretically possible.

In view of the above, there is a need to study the influence of dielectric material and LL manufacturing technology on the RCS values of air target simulators manufactured on their basis. This must be taken into account when creating air targets and false air targets with specified RCS values at a specific frequency of their irradiation.

Analysis of recent studies and publications. Analysis of the state of current research in the field of using dielectric materials with different properties, manufacturing technology features, and the use of spherical LLs as passive air target simulators has shown that these issues are covered in a number of works. Research [3] examines the properties of dielectric and various composite materials that can be used to manufacture spherical LLs, in particular foam dielectric materials, expanded polystyrene, foam plastic, etc. Composite dielectric materials include synthetic polymers and various ceramic powders. They are lightweight and have good dielectric properties, which allows for the creation of various spherical LL designs.

The authors of studies [4-7] describe spherical LLs manufactured using various three-dimensional printing technologies. Thus, studies [4, 5] present an approach to creating spherical LLs with radial holes, while studies [6, 7] consider spherical LLs in the form of dielectric cubes of various sizes. The authors investigated how the dielectric permittivity and loss tangent of equivalent lens materials can be influenced by the shape of the holes, the direction of the holes, and the porosity. However, this technology has only been used to create LLs with two layers, which does not allow for a complete reduction in the discreteness of changes in dielectric permittivity.

In works [8, 9], the creation of multilayer LLs with a smooth dielectric permittivity was considered. In this case, an approach was used in which the dielectric permittivity of each layer is constant but changes discretely from one layer to another. The authors note that the implementation of LLs with more than 10 layers is impractical and does not lead to significant changes in the characteristics of the lens. In practice, 4-6 layer lenses are the most technologically feasible.

In addition, the authors of [9] conducted a comparative analysis of various methods of layer-by-layer approximation of spherical LLs, in particular: dividing the lens into layers by refractive index, uniform division by dielectric permeability, and uniform division by radius. The research showed that the best approximation of dielectric permittivity to the theoretical law of change for a six-layer LL is achieved by uniform division into layers by radius. In this case, the average absolute error of approximation of dielectric permittivity to the theoretical value is no more than 6.7%.

The processes of manufacturing LLs by printing on a 3D printer using inkjet polymerisation technology are discussed in [10]. The peculiarity of such LLs is that the structure of the lens body includes electromagnetic crystals. At the same time, a heterogeneous dielectric is used as the main material of the lens body. The parameters of the dielectric are changed by controlling its filling

density during 3D printing. When creating an LL, the dielectric permeability should vary from two units in the centre to one unit near the surface.

The research [11] provides examples of the implementation of multilayer LLs from elements in the form of hemispheres of different radii. These elements are made of porous dielectric or polystyrene foam. The authors note that this manufacturing method is complex, and errors in the accuracy of the layers as they increase in size lead to a deterioration in the "reflective" characteristics of the lens.

The authors of publications [12-15] have conducted research on the effectiveness of using corner and lens simulators of modern air targets. The results of the research showed that among corner simulators, the square simulator provides the highest RCS, but at the same time it has the narrowest indicatrices in both planes and a less robust design. The widest monostatic indicatrices in both planes are provided by triangular simulators, which determines their advantages in use, despite their relatively low RCS value. Under conditions of identical geometric dimensions, simulators based on LL have the highest RCS and allow covering the entire radar wavelength range and simulating the RCS of most modern air targets. At the same time, simulators based on a spherical LL with a metallised segment in the form of a "cap" provide the highest RCS.

Thus, the analysis of the publications has shown that the influence of dielectric material and manufacturing technology on the RCS of air target simulators based on multilayer spherical LLs has not been sufficiently studied. When designing air target simulators, failure to take these issues into account can lead to devices with unplanned RCS values, the appearance of RCS instability in different frequency ranges, degradation and temperature instability, and other serious technical problems.

The purpose of this article is to study the influence of dielectric material and manufacturing technology on the RCS of air target simulators based on multilayer spherical LLs for consideration when creating air targets and decoys with specified RCS values.

To achieve this goal, the following tasks must be solved:

– to propose a methodological approach for assessing the impact of dielectric material and manufacturing technology features on the RCS of air target simulators based on spherical LLs;

– conduct experimental studies to evaluate the real RCS of air target simulators based on multilayer spherical LLs;

– to evaluate the RCS ratio of air target simulators based on multilayer spherical LLs made of different dielectric materials.

Presentation of the main material. The main characteristic of air attack weapons, such as radar targets, is their RCS. RCS characterises the reflective properties of the target and determines its energy characteristics of secondary radiation at the reception point and does not depend on the intensity of the primary wave.

One of the most acceptable and promising passive simulators of the RCS of air targets in the radar wave range is an LL, which is a multilayer sphere with different values of dielectric permittivity of the layers and, accordingly, their refractive indices.

For a classic LL without losses, the dielectric permittivity varies smoothly along the radius of the sphere from $\varepsilon=1$ at the surface of the lens to $\varepsilon=2$ at the centre of the lens, in accordance with the law [16]:

$$\varepsilon(a)=2-\left(\frac{a}{r}\right)^2, \qquad (1)$$

where $\varepsilon(a)$ is the function of the change in the dielectric permittivity of the lens;

r is the radius of the lens, m;

a is the radial coordinate of an arbitrary point inside the lens, m.

If part of the surface of a spherical lens is metallised, it becomes an RCS simulator, which acts in a spatial angle equal to the angle covering the metal coating. The paper considers passive RCS simulators based on spherical dielectric LLs, part of the surface of which is metallised in the form of a "cap" (segment). The reflection of an electromagnetic wave in a dielectric sphere occurs from the metallised surface. The maximum monostatic RCS [12, 15] in this case is determined by the aperture method using the formula:

$$S_L = 4\frac{\pi^3 r^4 f^2}{c^2}, \qquad (2)$$

where S_L is the monostatic RCS of an LL with a metallised segment in the form of a "cap", m^2;

f is the frequency of electromagnetic radiation, Hz;

C is the speed of light, m/s.

When manufacturing spherical LLs, it is necessary to have a dielectric material that allows for a continuous change in dielectric permittivity $\varepsilon(a)$ according to the gradient law (1). In real conditions, it is practically impossible to accurately implement this law. Therefore, in practice, a multilayer structure is created with a stepwise approximation of the law of change in dielectric permittivity. In this case, within one layer of such structure, the dielectric permittivity is constant, and the accuracy of the approximation to the characteristics of an ideal lens with a smooth change in dielectric permittivity is ensured by the number and thickness of the layers. The greater the number of layers, the more accurate the approximation of the characteristics of a real lens and the closer it is to the ideal. The most technologically advanced is the creation of a 4-6 layer lens. The RCS of spherical LLs used as air target simulators depends not only on their absolute dimensions and irradiation frequency, but also on the properties of the dielectric material and the LL manufacturing technology. When creating spherical lens simulators in the form of multilayer structures, the discreteness of the change in dielectric permeability and additional technological errors lead to a decrease in their RCS value compared to the theoretically possible one.

Six-layer spherical LLs with cubic holes made of various dielectric materials are considered as RCS simulators in this research. These LLs have radii of 4.5 cm and a metallised segment in the form of a "cap". The lenses are manufactured using 3D printing technology from two types of dielectric materials: PET and PETG. Polyethylene terephthalate glycol (PETG) is a thermoplastic polyester that provides high chemical resistance and durability. PETG is an adaptation of PET (polyethylene terephthalate), where "G" stands for glycol. PETG has greater strength and durability, is more impact resistant and is better suited to higher temperatures. Due to its low moulding temperatures, PETG is easy to mould under vacuum and pressure or to bend. PETG is a transparent amorphous material with a glass transition temperature of 80-85°C and a melting point of 180-230 C. The density of PETG is 1.26-1.28 kg/dm^3. The dielectric permeability of PETG is in the range of 2.81–3.3 [17]. Unlike PETG, PET plastic is prone to crystallisation at high temperatures, which makes it opaque and weakens its structure.

The paper investigates six-layer spherical LLs made of different dielectric materials based on uniform division of the lens into layers according to dielectric permittivity [9, 13, 17]. In this case, the dependence of dielectric permittivity on radius is divided into parts with equal steps of $\varepsilon(a)$, i.e., the radii of the layers are $r = a_1, a_2 \ldots a_{N-1}, a_N = const$. To calculate the dielectric permittivity, the expression $\varepsilon_i^{'} = \varepsilon\left(a_{i-1} + 0{,}5 \cdot \left(a_i - a_{i-1}\right)\right)$ is used, i.e., the average value in each layer of the lens. Thus, we obtain a uniform division by dielectric permeability (by $\varepsilon(a)$). Such an approximation function allows us to approximate the change in dielectric permeability to a smooth law (1) by changing the density of the dielectric filling in the lens design.

Table 1 shows the parameters of the LL layers with a uniform division of the lens into layers according to dielectric permeability [9].

Table 1 – Parameters of LL layers

Layer parameters	**Layer number**					
	1	2	3	4	5	6
Relative layer radius, (a_i / r)	0,4082	0,5774	0,7071	0,8165	0,9129	1
Dielectric permeability of layers, $\varepsilon_i^{'}$	1,9583	1,7571	1,5875	1,4197	1,2523	1,0851

Source: developed by the authors

The appearance of spherical LLs and their cross-section are shown in Fig. 1.

a *b*

Figure 1 – Appearance of LLs (a) and their cross-section (b)
Source: developed by the authors

To take into account the influence of dielectric material and manufacturing technology on the RCS of air target simulators based on spherical LLs, we introduce the concept of a reduction factor, which shows how many times the actual RCS of the simulator is less than the theoretical (calculated) value. The RCS reduction factor is the ratio of the theoretical (calculated) RCS value of a lens simulator to its actual (experimental) value for a given irradiation frequency. It characterises the dependence of the real EPR of the LL on the dielectric material and the features of the manufacturing technology and shows how much it will change compared to the theoretical value. For an air target simulator based on a metallised spherical LL in the form of a "cap", the RCS reduction factor $K_{зн}$ is determined as follows:

$$K_{зн} = \frac{S_L}{S_0}, \qquad (3)$$

where S_L is the theoretical (calculated) value of the RCS of the LL with a metallised segment in the form of a "cap" (2), m^2;

S_0 is the actual (experimental) value of the RCS of an LL with a metallised segment in the form of a "cap", m^2.

The algorithm for assessing the influence of dielectric material and manufacturing technology features on the RCS value of air target simulators based on spherical LLs is as follows.

Step 1. Describe the material, dimensions, and manufacturing technology features of the spherical LLs selected for the experiment.

Step 2. For the selected LLs, the theoretical values of the RCS for a given irradiation frequency are evaluated. For each metallised spherical LL in the form of a "cap", the theoretical (calculated) monostatic value of the RCS is determined in accordance with formula (2).

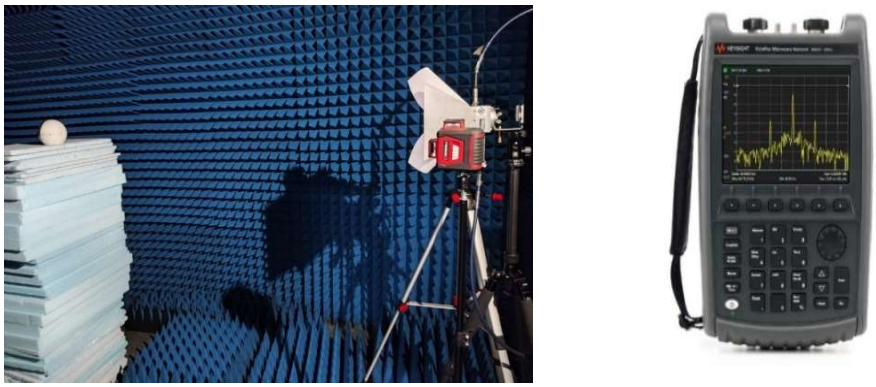
Step 3. The actual values of the RCS of spherical LLs are determined experimentally depending on the irradiation frequency.

Step 4. For the selected LLs, the RCS reduction indicators are calculated according to formula (3).

Step 5. The results are analysed and conclusions are drawn.

Measurements of the actual (experimental) RCS values of the LLs S_0 were carried out in an anechoic chamber (AC). An anechoic chamber is a special room whose walls are covered with radio-absorbing material that has a low reflection coefficient in a wide range of frequencies and angles when a plane electromagnetic wave strikes it.

Fig. 2 shows a general view of the anechoic chamber and the equipment of the experimental measuring stand, which includes: transmitting and measuring antennas, a laser level (Fig. 2a), and a portable vector network analyser (FieldFox microwave analyser) (Fig. 2b).



a *b*

Figure 2 – Measuring stand equipment
(a – transmitting and measuring antennas and laser level;
b – KeysightN9951A – portable FieldFox microwave analyser)
Source: developed by the authors

The experimental setup (measuring stand) in this configuration allows measuring the monostatic RCS of objects in the 4-15 GHz frequency range.

The measurement of the real RCS value of spherical LLs is based on the use of a reference reflector with a known RCS S_E. The essence of the method is that the power of the received signal reflected both from the reference reflector P_E with a known RCS S_E and from spherical LLs, the RCS of which must be determined P, is measured. Then the real (experimental) value of the RCS of spherical LLs S_0 is calculated using the formula:

$$S_0 = S_E \frac{P}{P_E}, \quad (4)$$

where S_E *is* the RCS of the reference reflector, m^2;

P – power of the received signal from spherical LLs, dB;

P_E – power of the received signal from the reference reflector, dB.

Since the power of the received signals is measured in decibels, the ratio (P / P_E) is written as follows:

$$\frac{P}{P_E} = 10^{0,1 \cdot U}, \quad (5)$$

where $U = P - P_E = 10 \lg P - 10 \lg P_E = 10 \lg (P / P_E)$ *is* the difference between the received signals, dB.

Taking into account expression (5), expression (4) will take the form:

$$S_0 = S_E \cdot 10^{0,1 \cdot U}. \quad (6)$$

A metal sphere with a radius of $a = 4,5$ cm was selected as the reference reflector (reference) for the RCS during the experiment. The following formulas are used to calculate the RCS of the reference sphere [18]:

$$S_E = S_m \cdot F(ka), \quad (7)$$

where

$$S_m = \pi a^2, \quad (8)$$

$$F(ka) = \left| \frac{2}{ka} \sum_{n=1}^{\infty} (-1)^n \cdot (2n+1) \cdot \left\{ \frac{J_n(ka)}{h_n^{(1)}(ka)} - \frac{\frac{d}{ka}(ka \cdot J_n(ka))}{\frac{d}{ka}(ka \cdot h_n^{(1)}(ka))} \right\} \right|^2, \quad (9)$$

$$J_n(ka) = \sqrt{\frac{\pi}{2ka}} \cdot J_{n+\frac{1}{2}}(ka), \quad (10)$$

$$h_n^{(1)}(ka) = \sqrt{\frac{\pi}{2ka}} \cdot H^{(1)}_{n+\frac{1}{2}}(ka), \quad (11)$$

a – sphere radius, m;

S_m – maximum RCS of the reference (sphere), m^2;

$k = \frac{2\pi}{\lambda}$ – wave number, m^{-1};

$J_n(ka)$ – spherical Bessel function;

$h_n^{(1)}(ka)$ – Hankel spherical function;

$J_{n+\frac{1}{2}}(ka)$ – Bessel function of the first kind;

$H^{(1)}_{n+\frac{1}{2}}(ka)$ – Hankel function of the first kind.

Taking this into account, the RCS values of the standard (sphere) with a radius of $a = 4,5$ cm depending on the irradiation frequency are shown in Fig. 3.

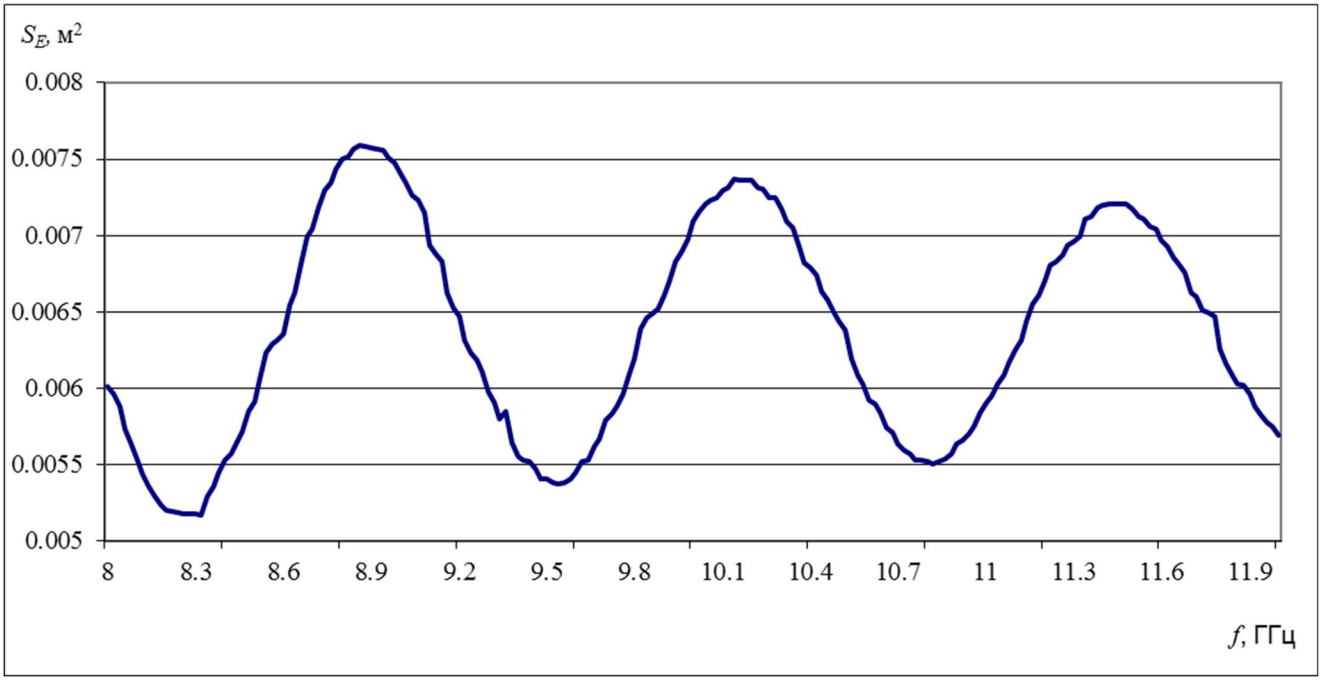


Figure 3 – RCS values of the reference sphere depending on the irradiation frequency
Source: developed by the authors based on data [18]

When conducting the experiment, the minimum distance $R_{\min}$ to the spherical LLs is determined in accordance with expression [19]:

$$R_{\min} = \frac{\pi \cdot f \cdot a^2}{\Delta\phi \cdot c}, \qquad (12)$$

where $\Delta\phi = \frac{\pi}{8}$ *is* the maximum phase error at the edge of the reference being studied.

Thus, the methodology of the computational-experimental method for measuring the real values of the RCS of spherical LLs is as follows:

a) for a given irradiation frequency, using an experimental setup (measuring stand), the anechoic chamber measures the power of the reflected signals in decibels from the spherical LL (P) and the reference (P_E) respectively;

b) based on the experimental data, the difference between the received signals U in decibels is found;

c) the RCS of the reference metal sphere S_E is calculated in accordance with expression (7);

d) The theoretical monostatic RCS of spherical LLs S_0 are calculated for a given irradiation frequency in accordance with expression (6).

e) the obtained results are analysed and conclusions are formulated.

The frequency dependencies of the theoretical RCS value and the actual RCS values for LLs made of PET and PETG materials are shown in Fig. 4.

Analysis of the results obtained (Fig. 4) showed that the reflective properties of LLs depend both on the dielectric material from which they are made and on the irradiation frequency. At some frequency ranges, the reflective properties (RER) of lenses made of PETG-type dielectric material exceed the reflective properties (RER) of lenses made of PET-type dielectric material, while in other frequency ranges, the opposite is true – lenses made of PET dielectric material exceed the reflectivity (RER) of lenses made of PETG dielectric material.

The dependence of the RER reduction coefficient $K_{зн}$ on frequency for LLs made of PET and PETG materials is shown in Fig. 5.

Analysis of the results obtained (Fig. 5) showed that the RCS reduction coefficients of LL also depend on both the dielectric material from which they are made and the irradiation frequency. For LLs made of PET-type dielectric material, the RCS reduction coefficient $K_{зн}$ ranges from 1.45 to 2.43, and for LLs made of PETG-type dielectric material, it ranges from 1.53 to 2.27.

The average value of $K_{зн}$ for LLs made of PET-type dielectric material is 1.95, i.e. on average, the actual RCS value of such a lens is 2.9 dB less than the theoretical value. The average value of $K_{зн}$ for LL made of PETG-type dielectric material is 1.86, i.e., on average, the actual RCS value of such a lens is 2.7 dB less than the theoretical value.

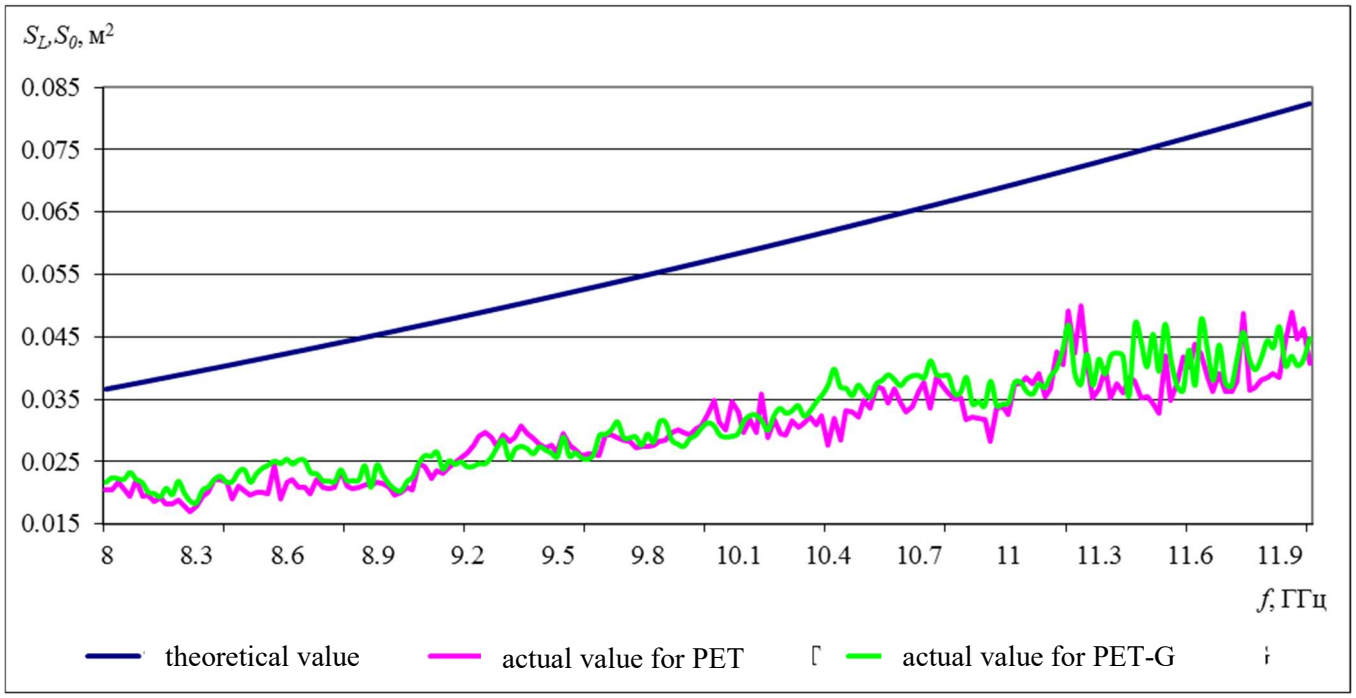


Figure 4 – Frequency dependencies of the theoretical and actual values of the RCS for LLs with a metallised segment in the form of a "cap" for dielectric materials of the PET and PETG type

Source: developed by the authors

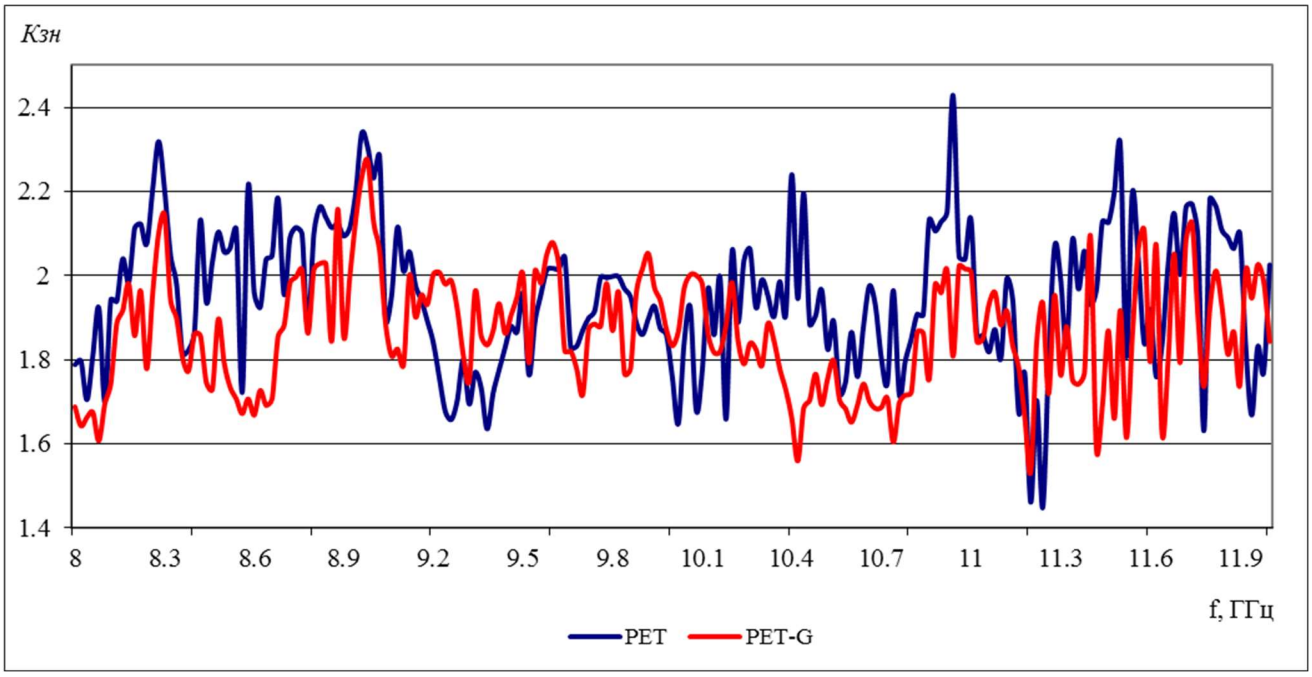


Figure 5 – Dependence of the RCS reduction coefficient on frequency for LL with a metallised segment in the form of a "cap" for dielectric materials such as PET and PETG

Source: developed by the authors

Thus, the results of experimental studies have shown that the reflective properties of a lens made of PETG dielectric material exceed the reflective properties (RER) of lenses made of PET dielectric material by 0.2 dB.

Conclusions and prospects for further research.

1. When manufacturing air target simulators based on multilayer LL, the properties of dielectric material, the discreteness of dielectric permittivity changes, and the peculiarities of manufacturing technology lead to a decrease in their RCS compared to the theoretical value. A methodological approach is proposed for assessing the impact of these factors on the magnitude of the change in the real RCS of air target simulators relative to the theoretical value.

2. An algorithm has been developed for a computational and experimental method of evaluating the real values of the RCS of air target simulators based on multilayer spherical LLs using anechoic chambers. The measurement and evaluation of the real RCS value of spherical LLs is based on the use of a reference reflector in the form of a metal sphere with a known RCS.

3. The results of experimental studies have shown that the RCS reduction indicators of air target simulators compared to theoretical values for PET and PETG type dielectric materials depend both on the dielectric material from which they are made and on the irradiation frequency. The average value of the RCS reduction coefficient for LLs made of PET-type dielectric material is about 2.9 dB, and for LLs made of PETG-type dielectric material, it is about 2.7 dB.

The results of the study will be used in practice in the design of compact and inexpensive air target simulators with specified reflective characteristics, as well as in the creation of false targets that complicate the work of enemy air defence systems.

Further research should be focused on identifying frequency dependencies of the

characteristics of new, cheaper and more effective dielectric materials that can be used to create air target simulators.

Reference

1. NATO (2021). Military unmanned systems. Annual Handbook. Iss. 29. Shephard [in English].

2. Military System & Technology (2025). Air target: Power of Precision. Retrieved from: https://surl.li/grkggl (accessed 25 February 2025) [in English].

3. Bor, J., Lafond, O., Merlet, H., L Bars, P., HimdiI, M. (2014). Foam Based Luneburg Lens Antenna at 60 GHz. *Progress In Electromagnetics Research Letters,* no. 44, pp. 1–7. DOI: https://doi.org/10.2528/PIERL13092405 [in English].

4. Changsheng, D., Ziqing, C., Yong, L., Haidong, W., Chao, J., Shiwes, Y. (2017). Permittivity of composites used for Luneburg lens antennas by drilling holes based on 3-D printing technique. *Journal of Terahertz Science and Electronic Information Technology,* no. 15 (4), pp. 646–651[in English].

5. Liang, M., Ng, W. R., Chang, K., Gbele, K., Gehm, M. E., Xin, H. (2014). A 3-D Luneburg Lens Antenna Fabricated by Polymer Jetting Rapid Prototyping. *IEEE Transaction on Antennas and Propagation,* no. 62 (4), pp. 1799–1807 [in English].

6. Larimore, Z., Jensen, S., Good, A., Lu, A., Suarez, J., Mirotznik, M. (2018). Additive Manufacturing of Luneburg Lens Antennas Using Space-Filling Curves and Fused Filament Fabrication. *IEEE Transaction on Antennas and Propagation,* no. 66 (6), pp. 2818–2827 [in English].

7. Xin, H., Liang, M. (2017). 3D printed microware and THz devices using polymer jetting techniques. *Proceeding of the IEEE*, no. 105 (4), pp. 737–755 [in English].

8. Fuchs, B., Coq, Le L., Lafond, O., Rondineau, S. (2007). Design optimization of multishell Luneburg Lenses. *IEEE Trans. AP*, no. 55 (2), pp. 283–289 [in English].

9. Ivanets H. V., Horielyshev S. A., Ivanets M. H., Voinov V. V., Stavytskyi O. M., Baulin D. S. (2025). *Rozrobka metodyky posharovoi aproksymatsii sferychnykh linz Liuneberha* [Development of a method for layer-by-layer approximation of Lüneberg spherical lenses]. *Vyprobuvannia ta sertyfikatsiia,* no. 1 (7), pp. 58–66. DOI: https://doi.org/10.37701/ts.07.2025.07 [in Ukrainian].

10. Kubach, A., Shoykhetbrod, A., Herschel, R. (2017). 3D Printed Luneburg Lens for Flexible Beam Steering at Millimeter Ware Frequencies. *IEEE 47th European Microwave Conference (EuMC),* pp. 234–247 [in English].

11. Baev, S., Hadjistamov, B., Dankov, P. (2009). Luneburg Lenses as Communication Antennas. *Annuaire de l'Universite de Sofia "St. Kliment Ohridski", Faculte de Physique,* no.102, pp. 67–84 [in English].

12. Volynets V. L., Mamonova N. L., Nelson O. V. (2014). *Porivnialnyi analiz pasyvnykh zasobiv imituvannia efektyvnoi ploshchi rozsiiuvannia povitrianykh tsilei* [Comparative analysis of passive means of simulating the radar cross section of air targets]. *Zbirnyk naukovykh prats Derzhavnoho naukovo-doslidnoho instytutu aviatsii*, no.10 (17), pp. 66–71 [in Ukrainian].

13. Baldauf, J., Lee, S.-W., Lin, L., Jeng, S.-K., Scarborough, S. M., Yu, C. L. (1991). High frequency scattering from trihedral corner reflectors and other benchmark targets: SBR versus experiment. *IEEE Transactions on Antennas and Propagation*, no. 39 (9), pp. 1345–1351. DOI: https://doi.org/10.1109/8.99043redf [in English].

14. Zaker, Reza & Sadeghzadeh, Arezoo. (2020). Passive techniques for target radar cross section reduction: A comprehensive review. *International Journal of RF and Microwave Computer-Aided Engineering*, no. 30 (8), e22411. DOI: https://doi.org/10.1002/mmce.22411 [in English].

15. Ivanets H. V., Voinov V. V., Horielyshev S. A., Nakonechnyi O. A., Ivanets M. H., Vasylieva O. M., Bashtakov Ye. H. (2024). *Obgruntuvannia dotsilnosti stvorennia perspektyvnykh povitrianykh mishenei na*

osnovi linz Liuneberha [Justification of the feasibility of creating promising air targets based on Luneberg lenses]. *Visnyk Natsionalnoho tekhnichnoho universytetu "KhPI". Seriia: mashynoznavstvo ta SAPR,* no. 2, pp. 60–67. DOI: https://doi.org/10.20998/2079-0775.2024.2.07 [in Ukrainian].

16. Sayanskiy, A., Glybovski, S, Akimov, V., Belov, P., Meshkovskiy, I. (2017). Broadband 3D Luneburg lensen based on met-amaterials of radially diverging dielectric rods. *IEEE Antennas and Wireless Propagation Letters*, no. 16, pp. 1520–1523 [in English].

17. Malkin, A. I., Knyazev, N. S. (2017). Dielectric permittivity and permeability measurement system. *REIT,* pp. 45–51. Retrieved from: https://surl.li/qiiyem (accessed 2 May 2025) [in English].

18. Mozharov Ye. O., Halkin N. K. (2018). *Kalibruvannia shyrokosmuhovoho stendu dlia vymiriuvannia kharakterystyk obiektiv* [Calibration of a broadband stand for measuring the characteristics of objects]. *Zhurnal radioelektroniky,* no. 10, pp. 15–25 [in Ukrainian].

19. Skosyrov V. M. (2012). *Pidvyshchennia informatyvnosti radiolokatsiinykh system na osnovi tekhnolohii nadshyrokosmuhovykh syhnaliv* [Increasing the information content of radar systems based on ultra-wideband signal technologies]. *Zhurnal radioelektroniky,* no. 7, pp. 1–10 [in Ukrainian].

Стаття надійшла до редакції / Received: 05.06.2025
Revised / Прорецензовано: 20.06.2025
Accepted / Схвалено до друку: 25.06.2025

ІВАНЕЦЬ ГРИГОРІЙ ВОЛОДИМИРОВИЧ
кандидат технічних наук, доцент,
старший науковий співробітник,
Харківський національний університет
Повітряних Сил імені Івана Кожедуба
https:/orcid.org/0000-0002-4906-5265

ГОРЄЛИШЕВ СТАНІСЛАВ АНАТОЛІЙОВИЧ
кандидат технічних наук, доцент,
доцент кафедри тактики,
Національна академія Національної гвардії України
https://orcid.org/ 0000-0003-1689-0901

ІВАНЕЦЬ МИХАЙЛО ГРИГОРОВИЧ
кандидат технічних наук, старший дослідник,
провідний науковий співробітник – провідний інженер-випробувач,
Державний науково-дослідний інститут випробувань і сертифікації
озброєння та військової техніки
https:/orcid.org/0000-0002-3106-7633

ДОСЛІДЖЕННЯ ЧАСТОТНИХ ЗАЛЕЖНОСТЕЙ ЕФЕКТИВНОЇ ПОВЕРХНІ РОЗСІЮВАННЯ ЛІНЗОВИХ ІМІТАТОРІВ ПОВІТРЯНИХ ЦІЛЕЙ ДЛЯ РІЗНИХ ДІЕЛЕКТРИЧНИХ МАТЕРІАЛІВ

Підтримання підрозділів протиповітряної оборони у складі частин Збройних Сил України та Національної гвардії України у постійній бойовій готовності до виконання бойових завдань передбачає під час військових навчань з особовим складом проведення бойових стрільб по сучасних повітряних мішенях. Повітряні мішені імітують реально існуючі засоби повітряного нападу противника, а під час ведення бойових дій використовуються як хибні повітряні цілі. Одним із найперспективніших пасивних імітаторів ефективної поверхні розсіювання повітряних цілей у радіолокаційному діапазоні хвиль є багатошарова лінза Люнеберга.

Під час створення таких лінзових імітаторів дискретність зміни й частотна залежність діелектричної проникності, а також додаткові технологічні похибки призводять до зменшення значення їх ефективної площі розсіювання порівняно з теоретичними. Цю обставину необхідно брати до уваги у процесі створення конкретних мішеней або хибних повітряних цілей.

Розроблено алгоритм розрахунково-експериментального способу оцінювання реальних значень ефективної поверхні розсіювання пасивних імітаторів на основі лінз Люнеберга з використанням безлунної камери. Вимірювання та оцінювання реального значення ефективної поверхні розсіювання лінзових імітаторів ґрунтується на використанні еталонного відбивача у вигляді металевої сфери з відомою ефективною поверхнею розсіювання.

Результати експериментальних досліджень засвідчили, що показники ефективної поверхні розсіювання імітаторів повітряних цілей залежать як від діелектричного матеріалу, технології, так і від частоти опромінення.

Ключові слова: *ефективна поверхня розсіювання; імітатор повітряної цілі; лінза Люнеберга;*

UDC 623.1/.3

DOI 10.59226/2786-6920.2.2025.70-78

KOSTRYTSIA SERHII
Candidate of Technical Sciences, Associate Professor,
Associate Professor of the Department Technical mechanics,
Ukrainian State University of Science and Technologies
https://orcid.org/0000-0002-7922-0975

MOSKALOV HENNADII
Senior Lecturer at the Department of Military Training
of Specialists of the State Special Service of Transport,
Ukrainian State University of Science and Technologies
https://orcid.org/0000-0001-9989-8014

KHRYPKO IVAN
cadet
Ukrainian State University of Science and Technologies
https://orcid.org/0009-0002-5759-8798

DEVELOPMENT OF A MOBILE SHELTER DESIGN IN UNSTABLE SOILS FOR PROTECTION OF DEFENSE FORCES PERSONNEL FROM ENEMY'S MEANS OF ATTACK

Over the past centuries, the rapid development of fortification equipment for strongholds has been clearly evident during periods of active hostilities. The dynamic progress of armaments and the direct experience of warfare are powerful catalysts for the continuous search for innovative forms, advanced designs, the latest materials and specialised equipment. The main goal of this search is to ensure the maximum preservation of own firepower and human resources.

The problem of soldiers' survival is especially critical on the front line of defence, where they are under constant, intense enemy fire control. Fortifications built in such extreme conditions are often of primitive design and demonstrate a low ability to effectively protect personnel from modern weapons. As a rule, such fortifications are built directly on the ground, manually, using available materials and structures, dominated by wood elements.

However, in the context of the hostilities that have unfolded on the territory of Ukraine, there is a serious problem with the availability of natural wood reserves of the required quality and in sufficient quantity directly in the conflict zone. This creates difficulties associated with the need to organise complex and costly timber deliveries from remote regions. In this regard, it is important to find alternative engineering solutions that would provide the military with reliable shelters without depending on local resources.

One of the promising ways to solve this problem may be the development and implementation of a mobile collapsible shelter made of lightweight but durable metal elements. The key requirement for such a kit is its weight, which should be optimised to ensure that it can be transported and installed by one person without significant physical effort. This will allow each soldier to independently and quickly set up the shelter at their position and use it repeatedly, depending on the tactical situation and the need to move. Such mobility and autonomy in providing protection can significantly increase the survival rate of personnel on the contact line.

Keywords: *mobile collapsible shelter; self-installation; fortifications; metal structures.*

Statement of the problem. In conditions of direct contact with the enemy, when setting up defensive positions, personnel who are manually constructing the positions are poorly protected. In the horizontal projection of the position, they are protected from small arms fire and debris by an earthen parapet. In the vertical projection of the position, there is no protection. With the advent of modern weapons, the level of losses increases significantly. Therefore, it is very important to create conditional safety at this stage of the work. The solution to this problem may be the development of a mobile, individual, collapsible metal shelter that can be quickly installed in the side wall of a trench. When danger arises, soldiers will be able to quickly take cover, which significantly increases their level of safety and, on a larger scale, the level of safety of the unit. The design of such a shelter will be proposed in this article.

Analysis of recent research and publications. In the period after the World War I, the approach to the construction of fortifications changed. Influenced by positional warfare and improvements in weapons (aircraft ammunition, chemical weapons), new trends in defence organisation emerged: dispersal of units across the defence area, construction of long-term underground fortifications, and improvement of field fortifications to protect personnel [1, pp. 204-207]. In field fortifications, dugouts and shelters of a non-reinforced construction provided more reliable protection for soldiers, but their construction required time, materials and, most importantly, trained specialists [2, pp. 101-105].

Simpler and more common structures and shelters for personnel were in the form of niches and dugouts in trenches. Their construction was mainly without supports, i.e. the stability of the ceiling, walls of dugouts and niches was ensured by the outline of the earthwork and the strength of the earth mass in which the structure was located. There were shelters whose outlines were reinforced with improvised means (boards, half-logs, brushwood), no calculations were made for reinforcing the walls and ceiling, and the outline and design of the shelters were passed on as combat experience [3, p. 7].

Different countries had their own ways and experiences of using fortifications. In NATO member countries, the active use of niches and dugouts took place after the participation of the United States in the Vietnam War. Learning from the enemy's experience, the American military built a single trench for firing in the form of a cup, which was equipped, in the course of combat operations, with a niche for shelter and rest. In the Soviet Union, their purpose, design and construction sequence were described in guidelines and manuals. They were made from wooden shields, wooden frames or planks. The guidelines specified their dimensions and the type of soil in which they should be used. No calculations were provided. S. Gerbanovsky and A. Yermolaev dealt with issues of fortification and the development of field engineering structures, describing practical experience of their use in wars and armed conflicts.

Due to the widespread use of metal elements and structures in public life, solutions and constructions for bolted metal structures for the construction of fortifications began to appear. In the 1960s, NATO guidelines and instructions considered the use of corrugated metal sheets for the construction of shelters, bunkers, and command posts. The protective structure was assembled with bolts and was in the form of an arch [4, pp. 30-31]. Such structures were intended to be used in a backfilled design. The Soviet army used designs for prefabricated metal fortifications (KVS-A, KVS-U) in an underground design.

Thus, summarising the above:

1. Niches have long been used as a means of protecting personnel during combat operations.
2. The only material used to make niches is wood.
3. There are metal prefabricated structures with bolted connections, but their calculations are not provided.

In view of the above, there is a clear lack of in-depth scientific justification and calculation methods for designing niches in trenches. Previous studies have focused on describing structures and rules for their use, without providing engineering calculations. There is a particularly urgent need to develop such calculations for modern materials and conditions, which will improve the effectiveness of personnel protection and optimise the construction process. This highlights the relevance of this study, which aims to develop a prefabricated metal structure for individual shelters in trench niches at unit strongpoints to improve their protective properties.

The purpose of the article is to highlight the calculations for shelters, check the strength of the structure, provide recommendations for its intended use, and draw attention to the need to provide units with structures that will effectively prevent soil from collapsing under load.

Presentation of the main material. One of the main types of fortifications is trenches. The construction of trench shelters, as part of the fortification equipment of a unit strongpoint, is a critically important task for preserving the lives of military personnel. Fortifications allow defensive combat to be conducted and provide basic protection against most of the damaging effects of enemy weapons [5, p. 38]. Niches can also be used to store ammunition and other supplies. The crumbling and collapse of unfortified niches under load prevents them from being used for their intended purpose.

To achieve the goal of this work, the following tasks are to be solved:

- draw and calculate the structure to determine the necessary materials;
- develop a structure based on the calculation scheme;
- conduct experimental tests to determine the technical characteristics of the structure;
- describe the sequence of installation of the structure and provide recommendations for placing the design in the trench wall;
- conduct an e analysis of the increase in the survivability of units as a result of using individual shelters.

This work proposes a structure for a mobile shelter for personnel and ammunition, which is installed in a niche cut into the side wall of the trench and provides basic protection from collapses (Fig. 1, 2).

The proposed structure is a steel parallelepiped (without a front wall) reinforced with stiffening ribs consisting of: four upper corners to which a 1500 x 600 steel sheet is attached, and four corner posts to which 500 x 600 side steel sheets and a 1500 x 500 wall are attached. The overall dimensions of the assembled structure are 1500 x 500 x 600 mm, and when disassembled, 1500 x 500 x 60 mm. The main structural elements are made of 3 mm thick hot-rolled steel sheet and 40 x 4 mm and 63 x 5 mm equal-sided angles. Material is steel St.3. The weight of the structure kit is 70 kg. M8 bolts and nuts are used to connect the structural elements.

Figure 1 – View of the assembled shelter from the wall side

Source: photo developed by the authors

Figure 2 – View of the shelter from the front

Source: photo developed by the authors

The finite element method (FEM) was chosen as the method for studying the stress-strain state of the mobile shelter structure. FEM is currently the main tool for engineering analysis due to the availability of computer software packages that not only implement the FEM calculation process, but also have a convenient interface for entering initial data, controlling the calculation process and processing the calculation results. In this work, the Structure CAD (SCAD) software package [6, 7] was used to perform the calculations.

The essence of the finite element method is that the structure is broken down into a number of small but finite elements. The latter are called finite elements (hereinafter FE), and the process of breaking down is called discretisation. Finite elements are connected at nodal points.

Depending on the type of structure and the nature of its deformation, FE can have different shapes: beams, plates (triangular and rectangular) and volumetric FE (tetrahedrons or parallelepipeds). Beam and plate FE were used to construct the finite element model of the shelter.

Calculations are performed for the first limit state under the action of a vertical distributed load from the pressure of loose soil at a depth of 1.2 m – the depth of the horizontal sheet of the load-bearing structure. For the calculation, we assume the density of loose soil to be

$\gamma = 1{,}3$ т/м^3, а $= 1{,}5$ м, в $= 0{,}6$ м, $h = 1{,}2$ м.

We determine the volume of soil that creates pressure on the horizontal sheet of the structure $V = a \times b \times h = 1{,}5 \times 0{,}6 \times 1{,}2 = 1{,}08$ м^3

Soil mass $m = V \times \gamma = 1{,}08 \times 1{,}3 = 1{,}4$т

Weight of soil $F = m \times g = 1{,}4 \times 9{,}81 = 13{,}6$кН

Distributed load $P = \frac{F}{S} = \frac{13{,}6}{0{,}9} = 15{,}1$кН/м^2

We assume a distributed load of 15.1кН/м^2 .

Finite element analysis. Calculation scheme.

A finite element 3-D model of the shelter structure was constructed using beam and plate finite elements in the Structure CAD environment (Fig. 3) and is intended for calculating and evaluating the strength of the structure.

The frame calculation diagram is shown in Fig. 4. It consists of rod elements with a cross-section in the form of angles, the dimensions of which are indicated above.

After loading the model, the programme provides an overview of the deformed structure (Fig. 5). The greatest deformation is observed on the upper plate elements.

Analysing the values of displacements from the action of vertical load (Fig. 6), it can be concluded that along the Z-axis, the greatest displacement occurs in the middle of the upper plate and amounts to -27 mm (Fig. 7), along the X-axis – 2 mm (side sheets, Fig. 8), and along the Y-axis – 8 mm (rear sheet, Fig. 9).

Stress fields under the action of a vertical distributed load are shown in Fig. 10 The most stressed area of the sheet is marked in dark grey and amounts to 226 MPa (Fig. 11).

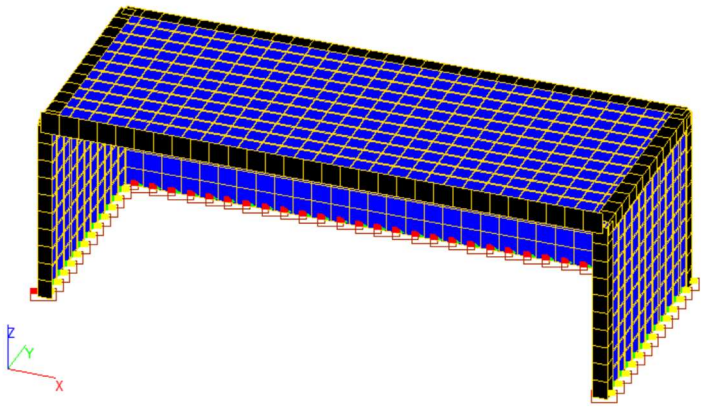


Figure 3 – Finite element shelter structure
Source: model developed by the authors

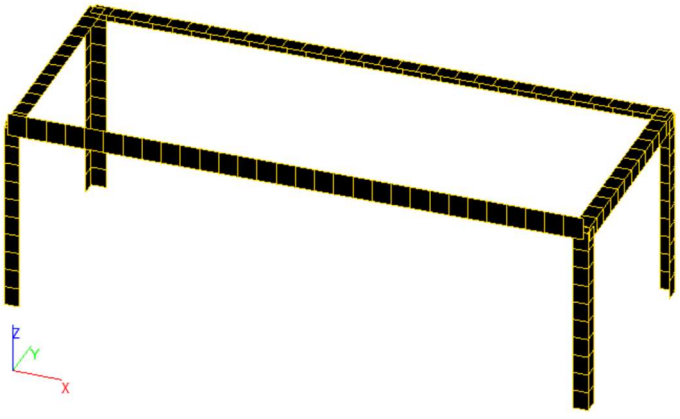


Figure 4 – The frame of the structure consists of angles to which steel sheets are attached
Source: model developed by the authors

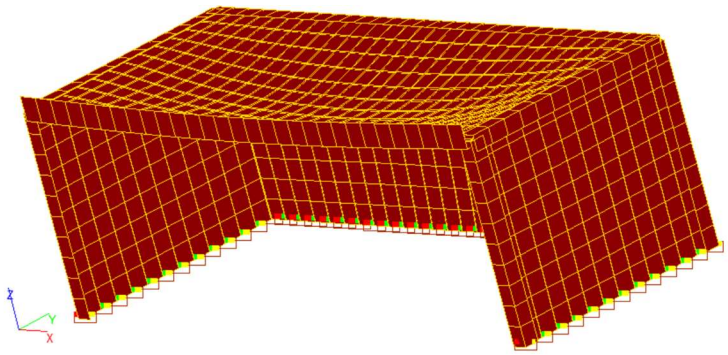


Figure 5 – View of the deformed structure
Source: model developed by the authors

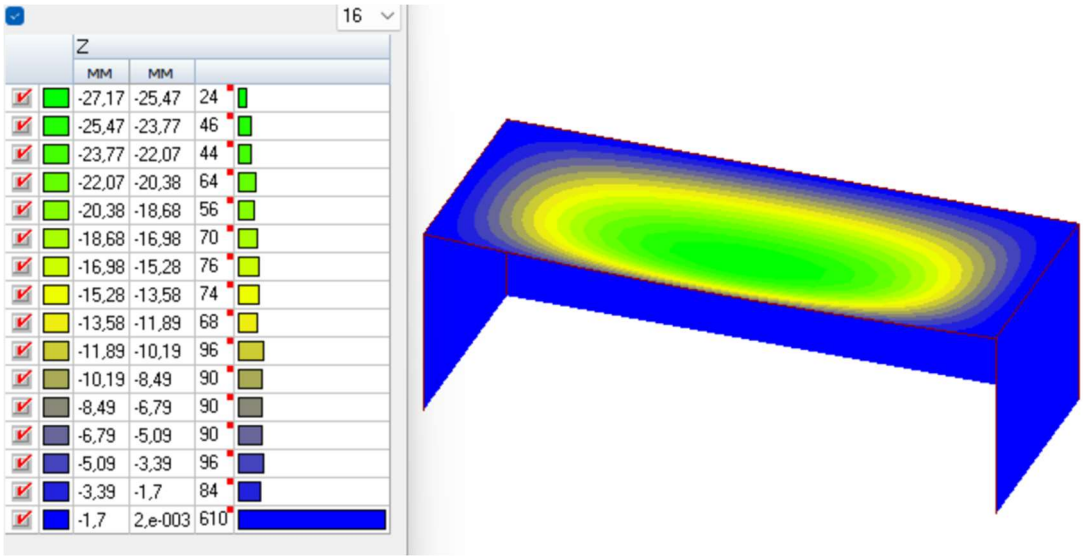


Figure 6 – General view of model displacements
Source: model developed by the authors

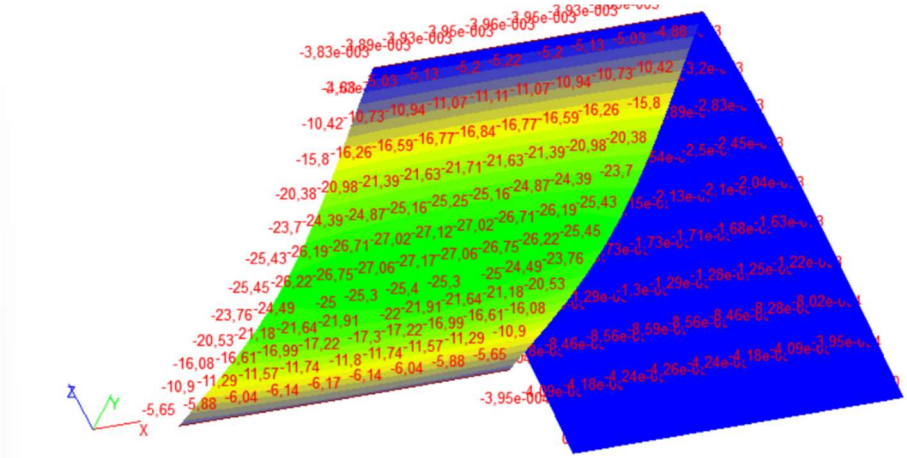


Figure 7 – Maximum numerical values of displacements along the Z axis.
Source: model developed by the authors

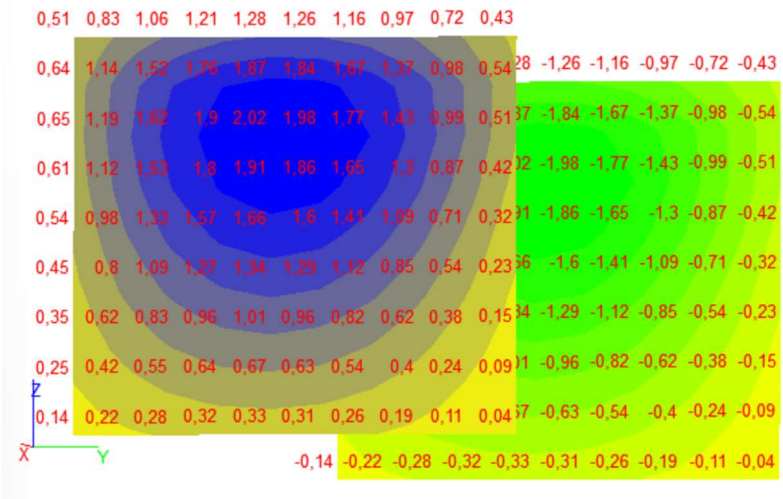


Figure 8 – Maximum numerical values of displacements along the X-axis
Source: model developed by the authors

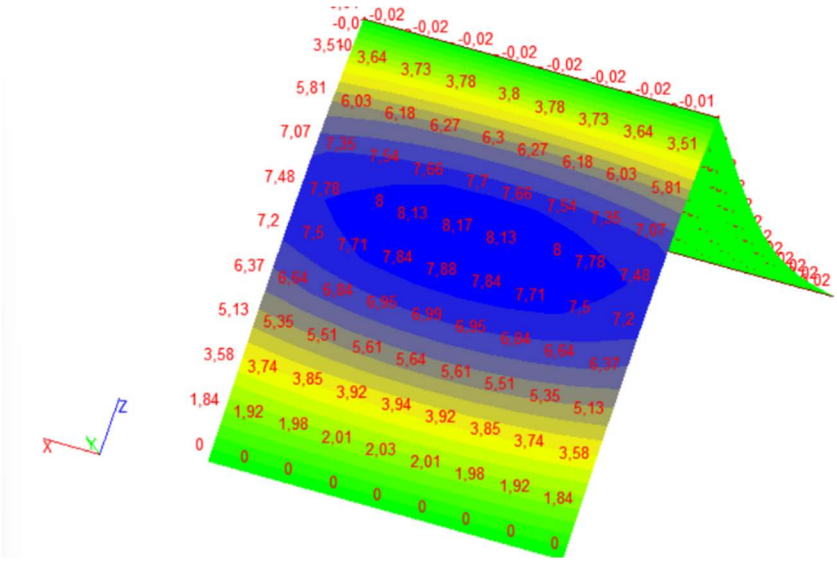


Figure 9 – Maximum numerical values of displacements along the Y-axis
Source: model developed by the authors

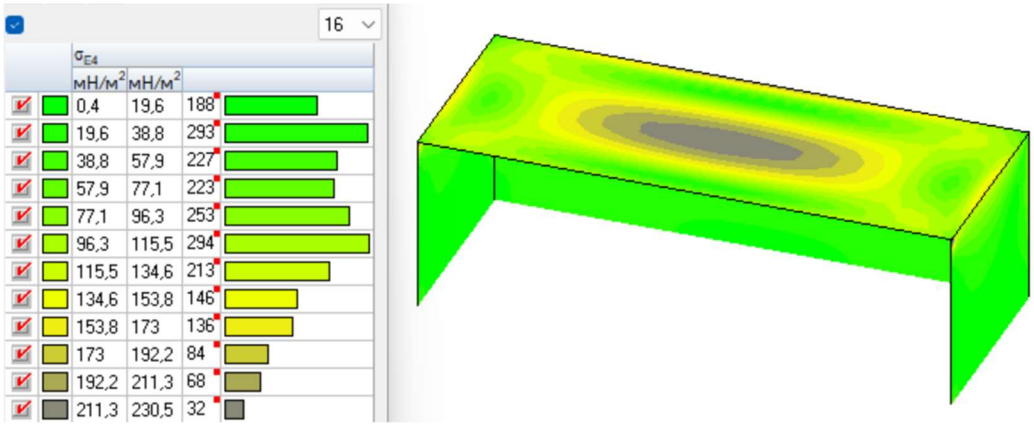


Figure 10 – General view of stresses
Source: model developed by the authors

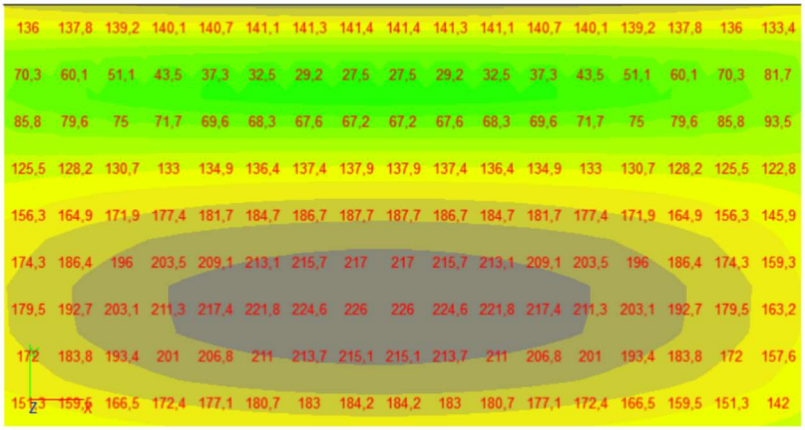


Figure 11 – Maximum numerical values of stress in the upper plate elements
Source: model developed by the authors

Analysis of the calculation results showed that the maximum equivalent stresses (according to the 4th theory of strength) in the structural elements of the shelter are 226 MPa and do not exceed the yield strength of St.3 steel – 245 MPa [8, p. 5]. Thus, the structure can withstand a calculated distributed load of 15.1 kH/м^2 s and can be used for its intended purpose.

The calculations, design development and practical application can be the subject of further study and development.

Sequence of work on the construction of the shelter:

1. Preparatory work for the construction of niches.

Dig out a niche according to the dimensions of the shelter. The volume of soil removed from the trench wall is ≈0,5 м^3 . Time required to construct the niche $30 - 35$ (хв) ;

2. Assembling the structure.

Install vertical elements (side elements and wall) in the trench opposite the niche and connect them with bolts using corner brackets; Attach a horizontal sheet with a 63 x 63 x 5 mm corner bracket to the connected vertical elements;

3. Installing the structure.

Install the structure in the niche and tighten the bolts. The time required to assemble the structure and install it in the trench niche is 45 minutes.

4. Dismantling the structure.

The dismantling of the structure is carried out in the reverse order of its installation and assembly. The dismantling time is 15 minutes.

Recommendations for installation. For ease of use, an OSB sheet measuring 1500 x 500 x 3 mm can be used (Fig. 2).

To close the niche from the trench side, wooden shields and other improvised means can be used to protect and camouflage the shelter (not considered in this work).

When constructing the shelter, it is important to remember that when digging out the niche, the protective top layer of soil (at least 1 m) must be preserved, and the bottom of the shelter must be at least 30 cm above the bottom of the trench to prevent flooding by surface water.

In special conditions (sand, high groundwater levels), it is advisable to install the shelter on the ground, protecting it around the perimeter with loose gabion structures. In the vertical projection of the positions, it is possible to lay bags with local soil in 1-2 rows [9, pp. 90-94].

Analysis of the improvement of unit survivability as a result of using individual shelters. It should be noted that the time and labour intensity of work on the construction of group shelters (covered trenches, dugouts) are significantly higher than those of the structure under consideration. The average time required to construct a shelter is 1.5 hours, and a covered trench is 2 hours 20 minutes. One of the criteria for increasing the survivability of a unit is the time it takes to construct fortifications and occupy them, as well as the time it takes for the enemy to detect their location [10, p. 5]. Therefore, the construction of shelters in the side walls of trenches is a priority measure.

Conclusions and prospects for further research.

The design of the proposed mobile shelter has been verified by calculations and can be used to protect personnel in conditions of loose soil up to 1.5 m thick.

This structure is not intended to withstand a direct hit from an artillery shell or equivalent external load, but it is effective in protecting against primary and secondary debris from enemy weapons; it significantly reduces the impact of the blast wave (especially when using side shields).

A single copy of the proposed shelter was manufactured and sent to one of the Defence Forces units, where it received positive feedback – the shelter design increases the protective properties of the unit stronghold. It is advisable to place such a shelter next to the place where a soldier is firing in a trench, as this will significantly reduce the time it takes to take cover in the event of a sudden barrel, mortar or rocket salvo fire, drops and other means of destruction from UAVs. At the same time, based on the results of field use, there are suggestions to refine the structure in order to reduce the overall weight and add protective doors to the kit.

Based on the results of the work description, the following areas for improvement of the structure are identified:

1. Connection of structural elements. The proposed structure features bolted connections. It takes 45 minutes to assemble. To reduce assembly time, it is advisable to use welded canopy-type connection elements for vertical and horizontal structural elements.

2. Protective and camouflage elements on the trench side were not considered in this work, although they are of great importance. Options for the side wall on the trench side: wooden shield, camouflage net, metal hatch, or a combination of these options.

References

1. Rudyk O. I. (2014). *Zmina pidkhodiv do budivnytstva dovhotryvaloi fortyfikatsii naprykintsi XIX – na pochatku XX st.* [Changes in Approaches to the Construction of Long-Term Fortification in the Late 19th – Early 20th Century]. *Naukovi pratsi istorychnoho fakultetu Zaporizkoho natsionalnoho universytetu*. Zaporizhzhia, vol. 39, pp. 204–207 [in Ukrainian].

2. Diakov S. I., Kolos O. L., Verstivskyi A. A. et al. (2018). *Viiskovi fortyfikatsiini sporudy* [Military Fortifications]. Lviv : NASV [in Ukrainian].

3. KSP (2025). *PVP 11-92(439).56: metodychni rekomendatsii z inzhenernoho obladnannia pozytsii (z urakhuvanniam dosvidu rosiisko-Ukrainskoi viiny 2024–2025 rokiv*) [PVP 11-92(439).56: Methodological Recommendations for Engineer Equipment of Positions (Considering the Experience of the russian-Ukrainian War 2024–2025)]. Kyiv [in Ukrainian].

4. Field Manual. FM 5-103: Survivability. Headquarters Department of the Army. Washington, DC, 10 June 1985 [in English].

5. MOU (2016). *Boiovyi statut mekhanizovanykh i tankovykh viisk Sukhoputnykh viisk Zbroinykh Syl Ukrainy. Chastyna I. Vzvod, viddilennia, ekipazh* [Combat Regulations of Mechanized and Tank Troops of the Land Forces of the Armed Forces of Ukraine. Part I. Platoon, Section, Crew]. Kyiv [in Ukrainian].

6. Bazhenov V. A., Perelmuter A. V., Shyshov O. V. (2013). *Budivelna mekhanika. Kompiuterni tekhnolohii i modeliuvannia* [Structural Mechanics. Computer Technologies and Modeling]. Kyiv : VIPOL [in Ukrainian].

7. SCAD Soft. Retrieved from: https://scadsoft.com (accessed 30 May 2025) [in Ukrainian]

8. *DSTU 8803:2018. Prokat tovstolystovyi z vuhletsevoi stali zvychainoi yakosti. Tekhnichni umovy* [DSTU 8803:2018. Hot-rolled Carbon Steel Plates of Ordinary Quality. Technical Specifications]. (2018, September 21). Kyiv : UkrNDNTs [in Ukrainian]

9. Kolos O. L. (2016). *Obgruntuvannia dotsilnosti zastosuvannia habionnykh konstruktsii pry fortyfikatsiinomu obladnanni raioniv (pozytsii) viisk (syl)* [Substantiation of the Expediency of Using Gabion Structures in the Fortification Equipment of Areas (Positions) of Troops (Forces)]. *Viiskovo-tekhnichnyi zbirnyk*, no. 14, pp. 90–94. DOI: https://doi.org/10.33577/2312-4458.14.2016.90-94 [in Ukrainian].

10. Shevchenko V. K., Voloshchenko O. I., Bobrun O. V. (2020). *Sposib vyznachennia velychyny vplyvu fortyfikatsiinoho obladnannia na zhyvuchist systemy upravlinnia viiskamy (sylamy) v operatsii (boiovykh diiakh)* [A Method for Determining the Magnitude of the Impact of Fortification Equipment on the Survivability of the Troop (Force) Command and Control System in an Operation (Combat Actions)]. *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony*, no. 1 (37), pp. 179–184. DOI: https://doi.org/10.33099/2311-7249/2020-37-1-179-184 [in Ukrainian].

Received / Стаття надійшла до редакції: 23.07.2025
Revised / Прорецензовано: 30.07.2025
Accepted / Схвалено до друку: 15.08.2025

КОСТРИЦЯ СЕРГІЙ АНАТОЛІЙОВИЧ
кандидат технічних наук,
доцент кафедри технічної механіки,
Український державний університет науки і технологій
https://orcid.org/0000-0002-7922-0975

МОСКАЛЬОВ ГЕННАДІЙ ЮРІЙОВИЧ
старший викладач
кафедри військової підготовки спеціалістів Держспецтрансслужби,
Український державний університет науки і технологій
https://orcid.org/0000-0001-9989-8014

ХРИПКО ІВАН СЕРГІЙОВИЧ
здобувач освіти,
Український державний університет науки і технологій
https://orcid.org/0009-0002-5759-8798

РОЗРОБЛЕННЯ КОНСТРУКЦІЇ МОБІЛЬНОГО УКРИТТЯ У НЕСТІЙКИХ ҐРУНТАХ ДЛЯ ЗАХИСТУ ОСОБОВОГО СКЛАДУ СИЛ ОБОРОНИ ВІД ЗАСОБІВ УРАЖЕННЯ ПРОТИВНИКА

Активний розвиток фортифікаційної науки відбувається у періоди ведення війн. Удосконалення озброєння і досвід війни змушують здійснювати пошук нових форм, конструкцій, матеріалів і обладнання для збереження своїх вогневих засобів і людських ресурсів. Особливо гостро постає питання виживання військових на першій лінії оборони в умовах постійного вогневого контролю противника.

Однак, в умовах бойових дій, що розгорнулися на території України, існує серйозна проблема з наявністю природних запасів деревини необхідної якості та в достатній кількості безпосередньо в зоні конфлікту. Це створює труднощі, пов'язані з необхідністю організації складних та дорогих поставок деревини з віддалених регіонів. У зв'язку з цим важливо знайти альтернативні інженерні рішення, які б забезпечили військових надійними укриттями без залежності від місцевих ресурсів.

Проаналізовано наявні фортифікаційні споруди. Споруди, що будуються в умовах постійного вогневого контролю противника, мають примітивну конструкцію і низьку здатність до захисту особового складу. Вони облаштовані вручну з використанням підручних матеріалів і конструкцій, а найчастіше – із дерев'яних елементів. З огляду на те, що на території України, де відбуваються бойові дії, природні запаси деревини необхідної якості дуже незначні, необхідно або підвозити деревину з іншої місцевості, або шукати альтернативні рішення.

Розроблено і запропоновано мобільне збірно-розбірне укриття, виготовлене з металоелементів. Вага найважчого елемента комплекту дає змогу переносити його одній людині. Військовослужбовець здатен самостійно встановити укриття і використовувати його багаторазово.

Ключові слова: *фортифікаційні споруди; ніша для укриття; утримання обвалів; мобільні укриття.*

UDC [351.75 : 340.13] : 351.743 «364» DOI 10.59226/2786-6920.2.2025.79-87

KUVAKIN SERHII
Candidate of Juridical Sciences, Associate Professor,
Associate Professor of the Department of Social and Humanitarian Disciplines,
Kyiv Institute of the National Guard of Ukraine
https://orcid.org/0000-0003-1032-6736

PROBLEMS OF REGULATORY REGULATION OF THE PARTICIPATION OF NGU UNITS IN THE IMPLEMENTATION OF MEASURES OF THE LEGAL REGIME OF MARTIAL STATE AS THE BASIS OF ENSURING STATE SECURITY

This study analyzes the problems of regulatory regulation of the participation of the National Guard of Ukraine units in the implementation of measures of the legal regime of martial law as the basis for ensuring state security. The article emphasizes that during the legal regime of martial law, the law enforcement and defense vectors of the National Guard of Ukraine are combined. It is noted that among the main duties and functions assigned to the National Guard of Ukraine is the implementation of measures of the legal regime of martial law, however, in today's conditions there is insufficient legal regulation of the powers of the National Guard of Ukraine during participation in these measures in wartime, which affects the quality of the implementation of the tasks set by the state.

It was determined that the purpose of applying the measures of the legal regime is to avert the threat, repel armed aggression and ensure national security, eliminate the threat of danger to the state independence of Ukraine, its territorial integrity. It was established that a special role in the implementation of the measures of the legal regime of martial law belongs to the units of the National Security Service, which operate not in isolation, but in close cooperation with public authorities, law enforcement agencies and the Armed Forces of Ukraine in order to create appropriate conditions for the formation of a safe living environment as the basis of security throughout the territory of Ukraine. The measures to ensure the legal regime of martial law are classified and restrictive, control, defensive and law enforcement measures are characterized.

The need to reform the regulatory framework for interaction between the National Security Service and other security and defense forces is emphasized and is an important task for improving the security system of Ukraine. At the legislative level, there is a need to further improve the legal regulation of interaction between security and defense sector entities. The Law of Ukraine "On the Legal Regime of Martial Law", although it defines the main provisions, requires the development of additional by-laws that would regulate specific aspects of interaction between the National Guard of Ukraine and other law enforcement agencies when performing tasks to ensure state security, which will ensure the effective use of resources, avoid duplication of functions, and increase the efficiency of decision-making in modern conditions.

Keywords: *security; military personnel; military formations; martial law; measures; defense; law enforcement function.*

Statement of the problem. In connection with the armed aggression of the Russian Federation against Ukraine, from February 24, 2022, on the basis of a Decree of the President of Ukraine approved by the Verkhovna Rada of Ukraine, a regime of martial law was introduced – one in which our state had never been since the proclamation of its sovereignty and independence. Despite the fact that at that time there was a real threat to the national security of the state and there existed a relevant legislative framework regulating most of the key issues that could potentially arise during wartime, there was no practice of its application. In this period of uncertainty, all state and non-state institutions began to restructure their activities to meet the contemporary realities of war; this process continues to this day. The National Guard of Ukraine was no exception, despite having sufficient

experience through active participation in combat operations since 2014, defending Ukraine's state sovereignty and territorial integrity.

In legal scholarship and publications on state security and defense, it has repeatedly been emphasized that the National Guard of Ukraine is a universal military formation belonging to the state's security and defense sector, because in peacetime it performs law enforcement functions and is part of the security forces, whereas in wartime it transforms into a component of the defense forces. Therefore, "the NGU's simultaneous belonging both to the security forces in peacetime and to the defense forces under the legal regime of martial law, on the one hand, testifies to the uniqueness and multifunctionality of this military formation and, on the other, requires a comprehensive approach to its development and further functioning" [1, p. 24].

During the operation of the legal regime of martial law, these two vectors of the NGU's activities are combined, since this military formation must ensure both the law enforcement and defense directions simultaneously. Thus, M. O. Yermoshyn and T. A. Sutiushev emphasize that "the Guard's military formations carry out service-and-combat (operational) tasks within the main types and forms of service-and-combat activity and actions of the National Guard of Ukraine at the strategic level, during routine service, and under states of emergency and martial law" [2, pp. 21–22].

Among the main duties and functions assigned to the NGU is the implementation of measures under the legal regime of martial law; however, under current conditions there is insufficient legal regulation of the powers of the National Guard of Ukraine when participating in the above measures during wartime, which affects the quality of fulfillment of tasks assigned by the state – thus determining the relevance and practical significance of the chosen area of research.

Analysis of recent research and publications. The theoretical framework for studying the principal areas of the NGU's activity under the legal regime of martial law, which has also revealed specific problematic issues, is constituted by the scholarly works of V. M. Aleksandrov [11], Yu. V. Allerov [13], D. A. Vlasenko [4], M. O. Yermoshyn [2], O. F. Kobzar [9], Yu. M. Kolomiets [10], O. V. Kryvenko [13], M. O. Ktitorov [1], A. V. Martyniuk [5], M. O. Semenyshyn [7], V. V. Sokurenko [14], R. V. Stefanchyshen [6], T. A. Sutiushev [2], D. V. Shvets [7], D. O. Shleha [8], and other Ukrainian scholars. The analysis of available literature sources and the scholarly ideas of researchers who have produced substantial theoretical contributions demonstrates that many aspects related to the activity of the National Guard of Ukraine under the legal regime of martial law remain insufficiently developed to this day. Among them, issues of legal regulation of the powers of the National Guard of Ukraine in performing its assigned tasks while implementing measures under the legal regime of martial law—particularly in de-occupied territories and areas close to combat operations—are of particular importance and require more detailed study.

The purpose of the article is to examine the problems of legal regulation of the NGU's powers in implementing measures under the legal regime of martial law, and to substantiate and уточнити (clarify) the role and place of NGU units in the course of their implementation.

Presentation of the main material. Pursuant to Part 1 of Article 1 of the Law of Ukraine "On the Legal Regime of Martial Law," martial law is a special legal regime introduced in Ukraine or in certain areas thereof in the event of armed aggression or a threat of attack, or a threat to Ukraine's state independence and territorial integrity. It provides for granting the relevant state authorities, military command, military administrations, and local self-government bodies the powers necessary to avert a threat, repel armed aggression, and ensure national security, eliminate threats to Ukraine's state independence and territorial integrity, as well as for the temporary, threat-conditioned restriction of constitutional rights and freedoms of individuals and citizens and the rights and legitimate interests of legal entities, with the duration of such restrictions specified [3].

Given the statutory definition of this type of legal regime, martial law is characterized by the restriction of certain constitutional rights and freedoms of citizens, specific powers of public authorities and military administrations, and the introduction of special control measures. These features are aimed at achieving the primary objective of martial law – protecting the state and its citizens from a military threat [4, pp. 14–15].

In A. V. Martyniuk's view, the martial law regime constitutes a special form or special approach to the legal regulation of social relations and processes in the state resulting from the occurrence of certain events and circumstances that threaten national security, territorial integrity, the

constitutional order, state sovereignty, and Ukraine's independence. The introduction of this regime is an extraordinary measure implemented in the presence of real and significant threats; it is characterized by certain restrictions on a range of human and civil rights and freedoms, the rights and legitimate interests of collective entities, and by specific features of the activity and interaction of public authorities. A particular role and attention in the context of introducing and operating the martial law regime is assigned to military formations and law enforcement agencies tasked with countering the very threats that give rise to this legal regime. A representative of both the military and law enforcement components of the state is the National Guard of Ukraine, which takes an active part in ensuring the martial law regime, as stipulated in the Law of Ukraine "On the National Guard of Ukraine" [5, p. 163].

Pursuant to the Law of Ukraine "On the Legal Regime of Martial Law," which establishes a range of measures introduced for the duration of this legal regime, R. V. Stefanchyshen considers such measures to be a type of extraordinary temporary administrative and legal measures implemented by public administration entities jointly with military command on the basis of direct methods of influence, in the manner prescribed by special legislation and within the scope of powers, and qualitatively aimed at ensuring national security and preserving statehood under conditions of restricting constitutional rights and freedoms of individuals and citizens, as well as the rights and legitimate interests of legal entities [6, p. 169]. At the same time, D. A. Vlasenko defines measures to ensure the legal regime of martial law as a set of legal, organizational, and administrative actions aimed at maintaining public security and order, ensuring national security, and protecting citizens' rights and freedoms during the period of martial law. These measures involve temporary restrictions of citizens' rights and freedoms, as well as granting additional powers to state authorities and military command that are necessary and sufficient for an effective response to threats to national security [4, p. 15].

The purpose of applying measures under the legal regime is to avert threats, repel armed aggression, and ensure national security, as well as eliminate threats to Ukraine's state independence and territorial integrity. Clearly, measures under the legal regime of martial law differ in their specific tasks and intended outcomes. However, for any of these measures, the ultimate goal is to ensure an appropriate state of social relations within the country in terms of an adequate level of national security, positioning Ukraine as an independent state, and preserving its territorial integrity [6, p. 167].

During the operation of the legal regime of martial law, by decision of the National Security and Defense Council of Ukraine enacted in the established manner by a Decree of the President of Ukraine, military formations established in accordance with the laws of Ukraine are involved, together with law enforcement agencies, in solving tasks related to the introduction and implementation of measures under the legal regime of martial law, in accordance with their purpose and the specifics of their activity [3].

A special role in implementing measures under the legal regime of martial law belongs to NGU units, which do not act in isolation but in close cooperation with public authorities, law enforcement agencies, and the Armed Forces of Ukraine in order to create appropriate conditions for forming a safe living environment as the basis of security throughout the territory of Ukraine.

The main characteristics of measures under the legal regime of martial law are as follows:

1. the subjects responsible for their introduction are the military command together with military administrations, acting independently or with the involvement of executive authorities, the Council of Ministers of the Autonomous Republic of Crimea, and local self-government bodies;
2. the normative basis for their application is a Decree of the President of Ukraine, approved by the Verkhovna Rada of Ukraine, on the introduction of martial law in Ukraine or in certain areas thereof;
3. the main objective is to protect the state and citizens from a military threat in order to ensure national security;
4. they are imperative in nature;
5. the powers granted are discretionary and are exercised taking into account the situation, terrain, and other relevant factors;
6. they are based on the Constitution and laws of Ukraine; however, a significant body of regulation is implemented at the level of subordinate legal acts, which, in the vast majority of cases, are interagency in nature;
7. they apply to all natural and legal persons regardless of the form of ownership;
8. they are based not only on national legislation but also on the norms of international humanitarian law.

Pursuant to Part 1 of Article 8 of the Law of Ukraine "On the Legal Regime of Martial Law," a broad range of measures for ensuring the legal regime of martial law is defined. In D. A. Vlasenko's view, these measures may be classified according to several criteria. First, restrictive measures aimed at the temporary limitation of certain rights and freedoms of citizens – such as freedom of speech, assembly, movement, and other rights that may pose a threat to national security. Second, control measures that establish enhanced oversight over the activities of business entities, public authorities, and citizens in order to prevent sabotage and intelligence-subversive activities. The third category comprises defense measures, which include strengthening the state's defense capability, mobilization, organization of military service, and civil protection of the population. The fourth important element is law enforcement measures aimed at maintaining public order, suppressing offenses related to national security, conducting pre-trial investigations, and bringing perpetrators to justice [4, p. 15]. Supporting this classification – which we adopt as a baseline – we will apply it when identifying the problems of legal regulation arising in the course of the NGU's implementation of measures under the legal regime of martial law.

The substantive content of measures under the legal regime of martial law is manifested through the exercise of statutorily established powers that have an executive–administrative nature. A settled approach interprets powers (competences /authorities) as a concept denoting the set of rights and duties vested in a subject for the performance of its functional mandate. Depending on the approach, the list of rights and duties constituting such powers may be exhaustive or may include referral norms that allow rights and duties to be established by other regulatory legal acts. Powers always reflect authoritative prescriptions because they: are exercised exclusively by duly authorized subjects; constitute a potentially available means of influence of the authorized subject; are secured by a rule of law; and are implemented exclusively within the framework of public-law relations [6, pp. 167–168].

Restrictive Measures Implemented by NGU Units

Protecting and safeguarding the life, rights, freedoms, and legitimate interests of citizens, society, and the state is one of the NGU's core missions. However, during martial law in Ukraine, in order to ensure the country's defense and preserve its security, certain rights and freedoms may be limited by law, while fundamental rights enshrined in the Constitution remain inviolable. In this period, NGU servicemen are vested with additional powers, in particular to ensure compliance with curfew, check citizens' identification documents, inspect belongings, vehicles, baggage and cargo, service premises and citizens' dwellings, enforce a special regime of entry and exit, restrict freedom of movement of citizens, foreigners, and stateless persons, as well as regulate vehicle movement, etc. In the vast majority of cases, these additional powers, insofar as they restrict citizens' rights, duplicate the powers of officers of the National Police, for whom they are part of everyday practice. However, the level of legal regulation of such powers for NGU servicemen must be more detailed; that is, mechanisms of their practical application require systematization and should, accordingly, be enshrined at the level of interagency orders. Thus, "legislation should establish clear procedures for restricting citizens' rights and freedoms, such as freedom of assembly and freedom of speech, while adhering to the principle of proportionality and minimizing interference. At the same time, it is important to enshrine mechanisms for the legal protection of citizens against unlawful actions by public authorities and officials during the implementation of martial law measures. It is also worth introducing special procedures for considering citizens' complaints regarding decisions of public authorities under martial law, which will contribute to the protection of their rights" [7, p. 200].

Control Measures

The National Guard of Ukraine, as a military formation with law enforcement functions, ensures the protection of public security and order, as well as the protection of state sovereignty. It performs tasks related to guarding state institutions and strategic facilities, thereby ensuring the protection of the population and territories. Thus, in addition to performing tasks on the front line, the NGU carries out control measures of a law-enforcement orientation. NGU servicemen perform duties at checkpoints, participate in law enforcement tasks in de-occupied and frontline areas, carry out stabilization measures, are engaged in counter-sabotage activities, and counter sabotage-and-reconnaissance groups.

Determining the place of the National Guard of Ukraine within the system of law enforcement

bodies cannot be accomplished without taking into account the nature and forms of its interaction with other law enforcement structures. Under current legislation, the NGU is part of the system of the Ministry of Internal Affairs of Ukraine, which in itself determines its close institutional and functional interaction with the National Police, the State Border Guard Service, the State Migration Service, and other bodies within the internal affairs system. The nature of this interaction lies in coordinating actions when carrying out joint tasks related to maintaining public order, ensuring a state of emergency or martial law regime, participation in counterterrorism measures, operational-search activities, and ensuring the protection of the state border. In practice, such interaction is manifested in joint service, joint patrols, checkpoint control, ensuring public security during mass events, evacuation of the civilian population from combat zones, participation in territorial defense measures, and the like [8, p. 138].

Defense Measures

Under the legal regime of martial law, a particularly important role among the components of the defense forces is played by NGU operational-purpose military units, which ensure the performance of tasks related to conducting military (combat) operations to repel the armed aggression of the Russian Federation. These entities are capable, at an appropriate level, together with units of the security and defense sector, of fulfilling combat tasks and conducting combat operations.

O. F. Kobzar emphasizes that the National Guard of Ukraine is currently one of the security and defense sector units most actively engaged in repelling Russia's attack and, accordingly, its service-and-combat activity today is continuous and diverse. The structure of the National Guard of Ukraine is complex, as it comprises units and subunits of several types (by purpose): units guarding state-significance facilities; units and subunits protecting diplomatic missions, consular institutions of foreign states and representations of international organizations in Ukraine; military units responsible for maintaining public order; convoying units and subunits; operational-purpose units; special-purpose units, etc. In essence, structurally the National Guard of Ukraine is analogous to a branch of the Armed Forces of Ukraine (it does not include arms branches, but it does include types of military units) [9, pp. 13–14].

When implementing defense measures, NGU operational-purpose military units are subordinated to the Commander-in-Chief of the Armed Forces of Ukraine, as are other units of the state's defense and security forces. At the same time, when taking direct part in combat operations, problems are observed due to legal gaps in the interaction between the NGU and other units of the security and defense sector–especially with regard to measures involving interaction and coordination.

Law Enforcement Measures

Within the law enforcement system, the National Guard of Ukraine occupies a significant place due to the specific nature of the functions assigned to it. The effective use of NGU units is one of the key conditions for maintaining public order and security and will contribute to a systematic counteraction to crime, suppression of unlawful encroachments, and ensuring the security of citizens and society. In this context, the NGU's role is to create conditions for forming a safe living environment in the state as a basis of internal security and as one of the principal factors in deterring the armed aggression of the Russian Federation. Of course, it should be noted that these aspects of law enforcement activity are performed by the National Guard of Ukraine in peacetime as well. However, as A. V. Martyniuk notes, during martial law and the confrontation with armed aggression, the role of the National Guard of Ukraine as a subject ensuring a secure environment is significantly strengthened, because – given the threats and challenges posed by hostilities – there arises a need for stricter and more effective measures, including involving servicemen who, nevertheless, may also implement police-type measures [5, p. 117].

Defense Measures

Under the legal regime of martial law, a particularly important role within the defense forces is played by the NGU's operational-purpose military units, which ensure the performance of tasks related to conducting military (combat) operations to repel the armed aggression of the Russian Federation. It is precisely these entities that are capable – together with other units of the security and defense sector – of carrying out combat missions and conducting hostilities at an appropriate level.

O. F. Kobzar emphasizes that the National Guard of Ukraine is currently among the security and defense sector entities most actively engaged in repelling Russia's attack and, accordingly, its service-and-combat activity today is continuous and diverse. The structure of the National Guard of Ukraine is complex, as it includes units and subunits

of several types (by their functional purpose): units guarding state-significance facilities; units and subunits protecting diplomatic missions, consular institutions of foreign states, and representations of international organizations in Ukraine; military units responsible for maintaining public order; convoy units and subunits; operational-purpose units; special-purpose units, etc. In essence, the National Guard of Ukraine is structurally analogous to a branch of the Armed Forces of Ukraine (it does not include arms branches, but it does include types of military units) [9, pp. 13–14].

When implementing defense measures, NGU operational-purpose military units are subordinated to the Commander-in-Chief of the Armed Forces of Ukraine, as are other units of the state's defense and security forces. At the same time, when the NGU takes direct part in combat operations, problems become apparent due to legal gaps in its interaction with other units of the security and defense sector– especially with regard to measures involving interaction and coordination.

Law Enforcement Measures

Within the law enforcement system, the National Guard of Ukraine occupies a significant place due to the specific nature of the functions assigned to it. Effective use of NGU units is one of the key conditions for maintaining public order and security; it contributes to systematic counteraction to crime, suppression of unlawful encroachments, and ensuring the safety of citizens and society. In this context, the NGU's role is to create conditions for forming a safe environment for the state's vital activity as a basis of internal security and as one of the main factors in deterring the armed aggression of the Russian Federation. Of course, it should be noted that these aspects of law enforcement activity are carried out by the National Guard of Ukraine in peacetime as well. However, as A. V. Martyniuk notes, during martial law and the confrontation with armed aggression, the role of the National Guard of Ukraine as a provider of a secure environment is significantly strengthened because, given the threats and challenges posed by hostilities, there arises a need for stricter and more effective measures, including the involvement of servicemen who, nevertheless, may also perform police-type measures [5, p. 117].

At the same time, the National Guard of Ukraine often performs tasks related to maintaining public order and security that overlap with the competences of the National Police of Ukraine, which may create misunderstandings and a lack of coordination in practical actions.

Interaction between the National Police and the National Guard is necessary for the effective execution of service-and-combat tasks during martial law. Joint patrols, searches and detentions, as well as maintaining public order during mass events help create conditions for the safety of the population. After the de-occupation of Ukrainian territories where hostilities took place, law enforcement agencies perform tasks related to restoring public order, preventing crime, and ensuring the rule of law. Under the difficult conditions that arise in de-occupied territories, interaction between these state institutions is also necessary for organizing humanitarian corridors and delivering various forms of assistance to the local population [10, pp. 105–106].

When performing tasks under martial law, the NGU is often engaged in combat operations while also ensuring public order in liberated territories. Particular attention is paid to guarding critical state facilities, maintaining public order, and participating in joint operations with the Armed Forces of Ukraine and the Security Service of Ukraine (SBU) to counter terrorism and other threats to state security. The National Guard of Ukraine also plays an important role in escorting prisoners of war and ensuring security in temporarily occupied territories [11, p. 81].

Thus, the National Guard of Ukraine plays a key role not only in maintaining public order, guarding state facilities, and countering terrorism, but also expands its tasks under the conditions of modern warfare to include combat operations, in particular the escort of prisoners of war and the maintenance of security in temporarily occupied territories.

The issue of escorting prisoners of war during active hostilities deserves special attention. This task requires a high level of coordination between the National Guard of Ukraine, the Armed Forces of Ukraine, and other security structures in order to ensure an adequate level of safety both for prisoners of war and for personnel. Insufficient coordination may lead to unforeseen risks during prisoner-of-war escort operations, which in turn may have negative consequences for both military personnel and civilians.

In de-occupied territories, units of the National Police and the National Guard face a wide range of shared tasks that can be achieved through constructive interaction. Such tasks include:

1. ensuring public order: street patrols, protection of public places, and prevention of mass disturbances; under difficult post-liberation conditions, mixed patrols are formed that include police officers and NGU servicemen;

2. demining territories: joint work with engineering units to clear areas of explosive hazards;

3. protection of citizens' rights, including documentation of human rights violations and war crimes;

4. protection of strategic facilities, i.e., ensuring security at critical infrastructure facilities, including power plants, bridges, hospitals, etc. [10, p. 104].

Therefore, improving interaction and coordination among entities responsible for implementing measures under the legal regime of martial law is a multi-faceted process that requires comprehensive, systemic efforts. Coordinated and effective work of public authorities, military structures, law enforcement bodies, civil society organizations, and international partners will contribute to building a resilient national security system capable of countering threats and ensuring stability under this legal regime.

In addition to the above issues, there are also problems related to the NGU's interaction with other law enforcement bodies during mass disturbances. For example, the NGU may act together with the National Police of Ukraine, the Security Service of Ukraine, and local authorities. However, the absence of clear boundaries regarding the distribution of functions among these structures leads to uncoordinated actions and duplication of efforts, which may affect response speed and the effectiveness of suppressing disturbances [12, p. 21]. Although, under current legislation, the National Guard of Ukraine is the main subject responsible for suppressing mass disturbances. When carrying out measures to suppress mass disturbances, the National Guard of Ukraine coordinates the activities of forces and resources of law enforcement agencies involved in terminating such unlawful actions.

Conclusions and prospects for further research.

The legal regulation of the implementation of measures under the legal regime of martial law requires a comprehensive approach, strict compliance with legislation, and coordinated work of all state and non-state structures. This makes it possible to ensure effective governance in crisis situations, protect citizens' rights, and maintain order and stability in the country.

At the legislative level, there is a need to further improve the legal regulation of interaction among subjects of the security and defense sector. Although the Law of Ukraine "On the Legal Regime of Martial Law" defines the basic provisions, it requires the development of additional subordinate regulations that would govern specific aspects of cooperation between the National Guard of Ukraine and other security structures when performing tasks aimed at ensuring state security. Such regulation would enable more effective use of resources, prevent duplication of functions, and increase the speed of decision-making under current conditions.

Improving interaction and coordination among entities involved in ensuring the implementation of measures under the legal regime of martial law in Ukraine is a necessary condition for an effective response to threats to national security. A comprehensive approach that includes the introduction of modern technologies into the NGU's activities can significantly increase the effectiveness of martial law measures and ensure national security in the present circumstances.

The need to reform the regulatory framework governing interaction between the NGU and other structures is an important task for improving Ukraine's security system. It is proposed to introduce clearer cooperation algorithms that would define the specific roles and tasks of each structure within the security and defense forces and avoid situations in which an NGU serviceman must simultaneously apply norms from numerous legal acts and rely on laws and subordinate regulations governing the activities of other law enforcement and militarized structures. Such situations substantially reduce the professional quality of the NGU's performance of its assigned tasks.

References

1. Ktitorov M. O. (2022). *Rozvytok spromozhnostei Natsionalnoi hvardii Ukrainy v umovakh pravovoho rezhymu voiennoho stanu* [Development of the capabilities of the National Guard of Ukraine under the legal regime of martial law]. *Naukovyi visnyk Kyivskoho instytutu Natsionalnoi hvardii Ukrainy*, no. 1, pp. 24–31. DOI: https://doi.org/10.59226/2786-6920.1.2022.24-31 [in Ukrainian].

2. Yermoshyn M. O., Sutiushev T. A. (2020). *Osnovni vydy i formy sluzhbovo-boiovoi diialnosti i dii Natsionalnoi hvardii Ukrainy* [Main types and forms of military service and actions of the National

Guard of Ukraine]. *Chest i zakon*, no. 4 (75), pp. 18–24. https://doi.org/10.33405/2078-7480/2020/4/75/220549. [in Ukrainian].

3. *Zakon Ukrainy "Pro pravovyi rezhym voiennoho stanu" № 389-VIII* [Law of Ukraine about the Legal regime of martial law activity no. 389-VIII]. (2015, May 12). *Vidomosti Verkhovnoi Rady Ukrainy*. 2015, no. 28. art. 250. Retrieved from: https://surl.lu/wbdcvs (accessed 24 September 2025) [in Ukrainian].

4. Vlasenko D. A. (2024). *Administratyvno-pravove zabezpechennia realizatsii zakhodiv pravovoho rezhymu voiennoho stanu* [Administrative and legal support for the implementation of measures of the legal regime of martial law]. Extended abstract of PhD thesis. Kharkiv : KhNUVS, p. 26. Retrieved from: https://surl.li/kirqoq (accessed 28 September 2025) [in Ukrainian].

5. Martyniuk A. V. (2024). *Administratyvno-pravove zabezpechennia vykonannia Natsionalnoiu hvardiieiu Ukrainy zavdan z terytorialnoi oborony* [Administrative and legal support for the implementation of territorial defense tasks by the National Guard of Ukraine]. PhD thesis. Kharkiv : KhNUVS, p. 213. Retrieved from: https://surl.lu/gltevl (accessed 28 September 2025) [in Ukrainian].

6. Stefanchyshen R. V. (2023). *Zakhody pravovoho rezhymu voiennoho stanu yak riznovyd administratyvnykh pravovykh zakhodiv* [Measures of the legal regime of martial law as a type of administrative legal measures]. *Derzhava ta rehiony. Seriia: pravo*, no. 4 (82), vol. 2. pp. 165–170. DOI: https://doi.org/10.32782/1813-338X-2023.4.2.30 [in Ukrainian].

7. Shvets D. V., Semenyshyn M. O. (ed.) (2022). *Politseiska yurysdyktsiia v umovakh voiennoho stanu* [Police jurisdiction in martial law conditions]. Odesa : Helvetyka. Retrieved from: https://surl.lu/fxhvqo (accessed 30 September 2025) [in Ukrainian].

8. Shleha D. O. (2025). *Mistse Natsionalnoi hvardii Ukrainy u systemi pravookhoronnykh orhaniv* [The Place of the National Guard of Ukraine in the System of Law Enforcement Agencies]. *Tsentralnoukrainskyi visnyk prava ta publichnoho upravlinnia,* vol. 2 (10), pp. 135–141. DOI: https://doi.org/10.32782/cuj-2025-2-16 [in Ukrainian].

9. Kobzar O. F. (2023). *Poniattia ta zmist sluzhbovo-boiovoi diialnosti Natsionalnoi hvardii Ukrainy* [The concept and content of the service and combat activities of the National Guard of Ukraine]. *Naukovyi visnyk KI NHU*, no. 1, pp. 11–15. DOI: https://doi.org/10.59226/2786-6920.1.2023.11-15 [in Ukrainian].

10. Kolomiiets Yu. M. (2024). *Vzaiemodiia Natsionalnoi politsii ta Natsionalnoi hvardii Ukrainy pid chas voiennoho stanu: osoblyvosti vykonannia zavdan na deokupovanykh terytoriiakh* [Interaction of the National Police and the National Guard of Ukraine during martial law: features of task performance in the deoccupied territories]. *Pivdennoukrainskyi pravnychyi chasopys*, vol. 4, pp. 103–108. DOI: https://doi.org/10.32850/sulj.2024.4.18 [in Ukrainian].

11. Aleksandrov V. M. (2020). *Sektor bezpeky i oborony Ukrainy v mekhanizmi realizatsii oboronnoi funktsii derzhavy* [The security and defense sector of Ukraine in the mechanism of implementing the defense function of the state]. *Chasopys Kyivskoho universytetu prava,* no. 4, pp. 78–82. DOI: https://doi.org/10.36695/2219-5521.4.2020.13 [in Ukrainian].

12. Kobzar O. F., Romashko O. M. (2023). *Zmist i sutnist masovykh zavorushen yak obiekta prypynennia pidrozdilamy Natsionalnoi hvardii Ukrainy* [The content and essence of mass riots as an object of suppression by units of the National Guard of Ukraine]. *Chest i zakon,* no. 2, pp. 19–23. DOI: https://doi.org/10.33405/20787480/2023/2/85/282526 [in Ukrainian].

13. Allerov Yu. V., Kryvenko O. V. (2018). *Rol i mistse Natsionalnoi hvardii Ukrainy u strukturi sektoru natsionalnoi bezpeky i oborony Ukrainy* [The role and place of the National Guard of Ukraine in the structure of the national security and defense sector of Ukraine]. *Nauka i oborona*, no. 3, pp. 3–9. DOI: https://doi.org/10.33099/2618-1614-2018-4-3-3-9 [in Ukrainian].

14. Sokurenko V. V. (2021). *Pidhotovka kadriv dlia sektoru bezpeky i oborony yak peredumova zabezpechennia natsionalnoi bezpeky Ukrainy* [Training personnel for the security and defense sector as a prerequisite for ensuring the national security of Ukraine]. *Pravo i bezpeka*, no. 3 (82), pp. 209–218. DOI: https://doi.org/10.32631/pb.2021.3.24 [in Ukrainian].

Received / Стаття надійшла до редакції: 19.09.2025
Revised / Прорецензовано: 30.09.2025
Accepted / Схвалено до друку: 10.10.2025

КУВАКІН СЕРГІЙ ВЯЧЕСЛАВОВИЧ
кандидат юридичних наук, доцент,
доцент кафедри соціально-гуманітарних дисциплін,
Київський інститут Національної гвардії України
https://orcid.org/0000-0003-1032-6736

ПРОБЛЕМИ НОРМАТИВНОГО РЕГУЛЮВАННЯ УЧАСТІ ПІДРОЗДІЛІВ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ У ВИКОНАННІ ЗАХОДІВ ПРАВОВОГО РЕЖИМУ ВОЄННОГО СТАНУ ЯК ОСНОВИ ЗАБЕЗПЕЧЕННЯ ДЕРЖАВНОЇ БЕЗПЕКИ

Проаналізовано проблему нормативного регулювання участі підрозділів Національної гвардії України у виконанні заходів правового режиму воєнного стану як основи забезпечення державної безпеки. Під час дії правового режиму воєнного стану правоохоронний і оборонний вектори діяльності Національної гвардії України поєднуються, і до основних обов'язків та функцій додається виконання заходів правового режиму воєнного стану. Однак в умовах сьогодення правове регулювання повноважень Національної гвардії України під час участі у зазначених заходах здійснюється недостатньо, що часом позначається на якості виконання поставлених державою завдань.

Визначено, що метою застосування заходів правового режиму є відвернення загрози, відсіч збройної агресії та забезпечення національної безпеки, усунення загрози державній незалежності України, її територіальній цілісності. Акцентовано на особливій ролі у реалізації заходів правового режиму воєнного стану підрозділів Національної гвардії України, які діють не ізольовано, а у тісній взаємодії з органами публічної влади, правоохоронними органами та Збройними Силами України задля створення відповідних умов формування безпечного середовища життєдіяльності як основи безпеки на всій території України. Здійснено класифікацію заходів забезпечення правового режиму воєнного стану й охарактеризовано обмежувальні, контрольні, оборонні та правоохоронні заходи.

Наголошено на необхідності реформування нормативної бази щодо взаємодії між Національною гвардією України та іншими структурами сил безпеки й оборони, що є важливим завданням для вдосконалювання безпекової системи України.

Ключові слова: *безпека; військовослужбовці; військові формування; воєнний стан; заходи; оборона; правоохоронна функція.*

UDC 351.746.1:355.4(4-672HATO) DOI 10.59226/2786-6920.2.2025.88-94

KURASHKEVYCH ANDRII
Candidate of Military Sciences, Associate Professor,
Head of the Department of Tactical and Special Disciplines,
Bohdan Khmelnytsky National Academy of the State Border Guard Service of Ukraine
https://orcid.org/0000-0001-9496-5708

TUSHKO DMYTRO
Senior Lecturer, Department of Border Guard Service,
Bohdan Khmelnytsky National Academy of the State Border Guard Service of Ukraine
https://orcid.org/ 0000-0002-1697-5836

ANALYSIS OF FOREIGN EXPERIENCE IN CAPABILITY-BASED OPERATIONAL PLANNING OF BORDER SECURITY UNITS OF NATO MEMBER AND PARTNER COUNTRIES

The article is devoted to the analysis of foreign experience in operational planning in the field of border security based on the capabilities of units from NATO member and partner countries. The methodology of Capability-Based Planning is examined, which ensures flexibility and adaptability of the management system in a dynamic environment. Tools for assessing readiness and interoperability are analyzed, including NATO standards, inspections, training, and modeling. Directions for adapting Alliance standards to Ukrainian realities are identified, in particular the integration of NDPP elements, which contributes to enhancing the efficiency of managing the forces and resources of the State Border Guard Service of Ukraine (SBGSU). The conducted study allows for a number of key conclusions regarding the potential adaptation of foreign operational planning experience to improve the effectiveness of Ukraine's border units.

Keywords: *operational planning, unit capabilities, NATO, border security, interoperability, State Border Guard Service of Ukraine.*

Statement of the problem. In the context of modern geopolitical challenges and the intensification of hybrid threats, ensuring reliable protection of the state border has become a key element of Ukraine's national security. At the same time, an analysis of operational planning practices within the State Border Guard Service of Ukraine (SBGSU) reveals several inconsistencies that define the scientific problem of this study.

Firstly, there is a contradiction between the legislative requirements for Ukraine's Euro-Atlantic integration and the actual lack of an adapted methodology for assessing the capabilities of border units. Ukraine's National Security Strategy and the Concept for the Development of the Security and Defense Sector envisage the implementation of NATO standards, including the NATO Defense Planning Process (NDPP). However, the regulatory and legal acts of the SBGSU do not contain specific mechanisms for applying a "capability-based planning" approach instead of the traditional "threat-based planning".

Secondly, there is a theoretical gap between the threat-oriented planning concept established in Ukrainian public administration science and the modern capability-based planning paradigm that predominates in NATO member countries. Domestic research has primarily focused on analyzing specific challenges and risks, whereas the methodology for developing universal, flexible, and resilient capabilities of border units remains insufficiently studied.

Thirdly, a practical contradiction has been identified between the need for rapid response to

unpredictable hybrid threats and the limitations of the existing tools for objectively assessing the readiness of units to perform tasks across a broad spectrum. Practice shows that current planning approaches often prove ineffective in rapidly changing operational environments, as they are oriented toward known past threats rather than the development of adaptive response capabilities.

These contradictions highlight the need for a scientific justification of a methodology for capability-based operational planning of individual border guard units, taking into account the tools of the NATO Defense Planning Process, such as standardization (STANAGs), joint exercises, inspections, and modeling. This constitutes a relevant scientific problem for improving Ukraine's border security system in the context of Euro-Atlantic integration.

Analysis of recent research and publications. The assessment of combat capabilities of military units, including border units, is a key element in ensuring national security. A methodological approach to this issue requires a thorough analysis of the factors affecting the effectiveness of task execution under increasingly complex operational conditions. Both global and domestic scientific literature pay significant attention to this problem, developing comprehensive models and methodologies. However, a critical review of the literature indicates the absence of a universal solution for assessing the capabilities of border units specifically under dynamic hybrid threat conditions, which combine military, migration, and information challenges. This creates a gap that must be addressed by formulating a new research objective.

In his work *"Assessment of Combat Readiness and Capabilities of Military Units"* (2014) [3], Klaus Fontan proposes a matrix approach for analyzing combat potential, which takes into account material and technical support, morale and psychological state, level of training, and adaptability to asymmetric threats using nonlinear models. While this approach is effective for general military formations, it is insufficiently adapted to the specifics of border units, where asymmetric threats (illegal migration, smuggling) and the need for interagency cooperation dominate. Fontan's matrix tends to overemphasize quantitative factors, overlooking the daily-changing dynamics of the border operational environment.

David Chandler and Tim Rivers, in their work *"Modern Border Security: Challenges and Solutions"* (2017) [4], critique traditional quantitative methods as insufficient and propose qualitative indicators, such as management flexibility, decision-making speed, and interaction effectiveness. While their approach is relevant to the border security context, it remains largely descriptive, lacking clear integration of quantitative and qualitative metrics into a unified model. Moreover, the authors do not provide tools for real-time operational assessment, which limits applicability for units with constrained resources.

The Ukrainian researcher V. Ilchenko, in the monograph *"Assessment of Operational Capabilities of Border Units under Hybrid Warfare Conditions"* (2020) [1], develops a multi-level system of criteria, including intelligence capabilities, the use of drones/sensors, and communication resilience. While this system accounts for hybrid threats, it primarily emphasizes technological aspects, underestimating the human factor (morale and psychological resilience during prolonged rotations) and integration with tactical-level assessment. Additionally, the model lacks validation against real border operation data.

Jan Kowalski, in *"Modeling Operational Situations at the Border"* (2019) [2], employs simulation models to forecast scenarios considering stochastic factors. Although mathematical modeling is useful for operational planning, it is too abstract for assessing the capabilities of a specific unit, does not account for real constraints (e.g., lack of field data), and does not offer simplified tools for commanders in the field.

Thus, the literature analysis [1–4] demonstrates progress in the development of assessment models; however, none of them address the challenge of providing a comprehensive, dynamic evaluation of border units' capabilities that accounts for the specifics of hybrid threats, resource limitations, and the need for operational applicability. The absence of an integrated approach – combining quantitative and qualitative indicators with practical tools for tactical-level use – forms the basis for the study's objective: to develop a universal methodology for assessing the capabilities of border units, oriented toward real-world operational conditions.

The purpose of the article is to examine NATO methodologies for assessing and developing the capabilities of border units and to identify prospective directions for their implementation in the operational practices of the State Border Guard Service of Ukraine, taking into account the experience of Alliance partner countries.

Presentation of the main material. The modern development of border security systems is characterized by the search for new, effective

management tools capable of adequately responding to hybrid threats and dynamic challenges. In this context, capability-based operational planning for individual border protection units serves as a key element in enhancing the state's defensive capacity.

Operational planning in border security should be understood as the process of defining long-term goals, priorities, and pathways for their achievement, aimed at creating a balanced and resource-supported response system for potential and emerging risks. It forms the foundation for the development of concepts, programs, and action plans that ensure the resilience of the state border. The concept of *"capabilities of border protection units"* encompasses an integrated set of material-technical, informational, personnel, and organizational elements that determine the ability of a specific structural component (e.g., a border post, brigade, or operational center) to effectively perform assigned tasks within its designated area of responsibility. This includes not only the availability of equipment and personnel but also their interaction, level of training, adaptability of procedures, and the capacity to operate under complex conditions.

The place and role of the capability-based approach (*Capability-Based Planning*) within NATO's defense and security planning system is central. As one of the main architects of modern security standards, the Alliance has shifted from planning focused on specific past threats toward a more flexible and universal approach. Its essence lies in developing capabilities that enable member and partner countries to counter a broad spectrum of unpredictable challenges rather than preparing for a single scenario. This methodology is implemented through a set of instruments, among which the NATO Defence Planning Process (NDPP) plays a key role. It is designed to identify the capabilities required by the Alliance, assess the existing national resources, and subsequently align national development plans to address identified gaps.

For border agencies of NATO member states and their partners, this entails the integration of their operational planning into the broader context of collective security. In practice, this is expressed through comprehensive capability assessments of each significant border protection unit to ensure compliance with NATO standards regarding interoperability, mobility, and resilience. For example, the ability of a partner country's border service to rapidly deploy a mobile checkpoint, integrate intelligence data from allied systems, or provide logistical support for troop movements is directly linked to the Alliance's overall capacity to respond to crises.

Thus, national-level operational planning transforms from an isolated process into a component of collective efforts, where capability analysis of individual border units becomes the basis for decisions regarding funding, technical modernization, and operational training. This integration facilitates the creation of interoperable and complementary border security systems, significantly enhancing the effectiveness of countering transnational threats across the Euro-Atlantic area.

The organization of operational planning in NATO member states exhibits several distinctive features that differentiate it from national defense and security management systems, as it is based on a multi-level structure, clear principles, and well-developed coordination mechanisms among participating countries. Strategic documents within the Alliance are developed with the need to ensure collective security and interoperability of armed forces across nations, requiring consistency in the approaches to the development, planning, and implementation of key defense policies.

The structural model of NATO planning is built hierarchically. The strategic level is represented by foundational and conceptual documents such as the NATO Strategic Concept, Political Directives, and the Annual Defence Planning Directive. These documents define general political and military guidelines for all Alliance members. The next level consists of medium- and short-term defense plans, which specify tasks and resources. This structure ensures a balance between long-term vision and flexibility in responding to current challenges. Multinational headquarters, committees, and specialized NATO agencies play a key role in coordinating and monitoring the implementation of decisions.

The principles of operational planning in NATO are grounded in democratic decision-making, with consensus as a key principle, ensuring equal participation of all members in shaping security policy. At the same time, the approach combines collective responsibility with the preservation of national sovereignty in defense. Planning is based on threat forecasting, analysis of the international security environment, and assessment of the existing and potential capabilities of allies. Systematic approaches, mutual transparency, resource coordination, and standard interoperability are fundamental principles that determine the

effectiveness of operational planning within the Alliance.

The mechanisms for developing NATO strategic documents follow a clearly defined procedure, including stages of information collection, formulation of political and military assessments, consultations among national delegations, approval within relevant committees, and final endorsement at the level of the North Atlantic Council. A critical tool is the NATO Defence Planning Process (NDPP), which ensures alignment of national force development plans with collective objectives. NDPP provides a framework for identifying the capabilities required to execute collective defense, crisis response, and stabilization operations.

The experience of integrating national strategies with NATO's collective standards demonstrates that member states maintain their own approaches to defense policy while simultaneously adapting them to overarching Alliance requirements. This adaptation occurs through the standardization of terminology, planning procedures, management norms, and logistical support. A critical aspect of this process is the shift from traditional resource-based planning to capability-based planning, which allows for consideration not only of quantitative indicators but also qualitative characteristics of military units, including their training level, technological equipment, and ability to operate effectively in a multinational environment.

Integrating national strategies into NATO's system involves a continuous adaptation process, as the security environment evolves under the influence of new challenges, including cyber threats, hybrid warfare methods, and the need to develop high-tech capabilities. Consequently, strategic documents not only define long-term objectives but also provide mechanisms for the operational updating of priorities. This approach fosters high dynamism in strategic planning and creates conditions for effective cooperation among allies within the collective security framework.

In summary, the distinctive features of NATO operational planning include a clearly structured document hierarchy, adherence to the consensus principle, transparency and interoperability, and the use of effective mechanisms for integrating national defense strategies into a collective security system. These elements ensure a comprehensive and flexible approach, enabling efficient resource utilization among member states and guaranteeing a high level of readiness to respond to current and future challenges.

In the context of modern geopolitical challenges, NATO's capability-based approach acquires particular significance for strengthening the border security of partner countries. This methodological framework, focused on the assessment and development of specific operational capabilities, enables the adaptation of NATO standards to unique national contexts, ensuring effective integration of partners into the collective defense architecture. In border units of countries such as Ukraine, Georgia, and Moldova, the implementation of this approach supports a transformation from reactive to proactive border protection strategies, emphasizing hybrid threats including cyberattacks, migration crises, and unconventional conflicts.

The adaptation of NATO's methodology to national needs involves flexible adjustment of standards, such as STANAGs, to local realities. In Ukraine, for instance, the Individual Partnership Action Plan (IPAP) and the Defense Capacity Building (DCB) initiative integrate NATO elements into reforms of the State Border Guard Service, focusing on anti-corruption measures, personnel training, and equipment modernization. This includes the implementation of integrity standards developed with NATO support, adapted to Ukrainian legislation, emphasizing civilian oversight and social guarantees for border personnel.

In Georgia, adaptation emphasizes regional challenges in the Black Sea basin: NATO trust funds and training centers strengthen territorial defense capabilities, integrating Georgian border units into multinational exercises that account for post-conflict recovery specifics. Moldova, in turn, applies the approach through the Parliamentary Security Element (PSE), highlighting interoperability with NATO in countering cross-border threats, considering its neutral status and limited resources, with a focus on peacekeeping preparation, such as KFOR missions.

Implementation results in the border security domain demonstrate significant improvements in effectiveness. In Ukraine, Operation UNIFIER with Canadian partners facilitated experience-sharing on countering Russian hybrid tactics, enhancing intelligence networks and internal threat detection, with border system interoperability increasing by 40% according to NATO's 2022 report. In Georgia, strengthened capabilities stabilized borders with occupied territories, reducing incidents by 25% through joint patrols and training. Moldova advanced in demining and special operations,

integrating NATO standards into national doctrine, enabling participation in international missions and reducing vulnerability to separatist risks. Overall, this approach not only strengthens national security but also promotes regional stability, exemplifying a successful hybrid adaptation model, where global standards are transformed into localized resilience tools.

Key instruments for assessing and developing border unit capabilities under modern conditions are determined by the need to harmonize national security systems with international standards, particularly NATO standards. In the border security domain, special attention is given to three main components – doctrinal provisions, personnel training, and interoperability. NATO's doctrinal documents establish a unified conceptual framework that enables border units to operate according to agreed principles and tactical approaches. This provides the possibility to integrate national border security strategies into collective defense plans, ensuring their alignment with regional and global security systems.

Training represents the second key instrument, as the preparedness of border personnel directly affects their ability to execute tasks in both national and international contexts. The implementation of educational programs modeled on NATO standards fosters the development of practical skills among service members, addressing contemporary challenges ranging from countering illegal migration and transnational crime to operating effectively in crisis conditions.

A third critically important factor is interoperability, which involves the standardization of procedures, terminology, technical standards, and communication systems. Ensuring interoperability allows border units from different countries to rapidly coordinate efforts in joint operations.

The assessment of readiness, effectiveness, and interoperability of border formations is carried out through a range of methods, with inspections, joint exercises, and operational scenario modeling occupying a leading role. Inspection activities provide an objective picture of unit capabilities and help identify areas requiring improvement. NATO-standardized training and exercises serve simultaneously as tools for assessment and development, as practical task execution allows verification of actual readiness and adjustment of tactical and organizational approaches. Modern simulation technologies for combat and crisis scenarios enable testing of border units' capacity to operate effectively in dynamic environments characterized by high uncertainty.

Thus, the key instruments for assessing and developing the capabilities of border units are based on a combination of doctrinal, educational, and technological solutions that harmonize national actions with NATO standards. This approach not only enhances the efficiency of state border protection but also forms the foundation for integration into collective security systems, enabling border units to operate across a broad spectrum of contemporary security challenges.

Current challenges in border security require the State Border Guard Service of Ukraine (SBGSU) to implement innovative approaches to operational planning grounded in successful foreign practices. Analysis of leading countries' experience highlights the necessity of a comprehensive approach to adapting international standards while taking into account the specifics of the national border control system.

European experience, particularly practices from Frontex and EU member states' border services, demonstrates the effectiveness of risk-based planning and integrated border management. Adapting these approaches to Ukrainian conditions requires consideration of the country's geopolitical situation, the length of its borders, and the nature of threats. The U.S. operational planning model, exemplified by U.S. Customs and Border Protection, underscores the importance of technological innovation and interagency coordination, which can be successfully implemented in the domestic context.

A key aspect of adaptation is the creation of a flexible planning system that combines long-term strategic perspectives with the capacity for operational response to evolving security challenges. Ukraine's national specifics, including the need to ensure European integration and counter hybrid threats, necessitate the development of tailored approaches to operational planning.

Prospects for the development of the State Border Guard Service of Ukraine's (SBGSU) operational planning system include the implementation of digital technologies for scenario forecasting and modeling, the establishment of continuous monitoring of the effectiveness of strategic initiatives, and the enhancement of analytical capabilities. Cultivating a culture of strategic thinking among leadership and creating mechanisms for the regular updating of strategic documents will ensure system adaptability to new

challenges. Integration with European standards and practices will contribute to improved border control effectiveness and strengthening of national security.

Conclusions and prospects for further research. The conducted study allows for several key conclusions regarding the possibilities of adapting foreign experience in operational planning to enhance the efficiency of Ukrainian border units. The proposed approach, combining quantitative and qualitative criteria for capability assessment, proves practically valuable for identifying "bottlenecks" in the functioning of border detachments. Analysis of NATO and partner countries' practices has demonstrated the effectiveness of shifting from threat-specific planning to capability-based planning (Capability-Based Planning), which provides flexibility and adaptability in a dynamic security environment. Experiences from countries such as Georgia and Moldova, as well as Ukraine's own results within the framework of the Individual Partnership Action Plan (IPAP), confirm that integrating Alliance standards significantly increases interoperability, professional competence of personnel, and technological modernization.

Thus, the primary vector for the development of the SBGSU operational planning system should be deeper integration with NATO principles and mechanisms, including the implementation of risk-based approaches, digitalization of monitoring and modeling processes, and the development of interagency coordination. This will ensure not only enhanced national defense capability but also increased security resilience across the region.

References

1. Ilchenko V. O. (2020). *Otsinka operatyvnoi spromozhnosti prykordonnykh pidrozdiliv v umovakh hibrydnoi viiny* [Assessment of the operational capability of border units in the conditions of hybrid warfare]. Kyiv : NUOU [in Ukrainian].
2. Kovalskyi Ya. P. (2019). *Modeliuvannia operatyvnykh sytuatsii na kordoni* [Modeling of operational situations at the border]. Varshava : Viiskova akademiia [in Ukrainian].
3. Fontan K. (2014). *Otsinka boiovoi hotovnosti ta spromozhnosti viiskovykh pidrozdiliv* [Assessment of the combat readiness and capability of military units]. Berlin : Viiskove vydavnytstvo [in Ukrainian].
4. Chendler D. A., Rivers T. L. (2017). *Suchasna prykordonna bezpeka: vyklyky ta rishennia* [Modern border security: challenges and solutions]. Vashyngton : Vydavnytstvo natsionalnoi bezpeky [in Ukrainian].

Received / Стаття надійшла до редакції: 13.10.2025
Revised / Прорецензовано: 24.10.2025
Accepted / Схвалено до друку: 29.10.2025

КУРАШКЕВИЧ АНДРІЙ ПЕТРОВИЧ
кандидат військових наук, доцент,
начальник кафедри тактико-спеціальних дисциплін,
Національна академія Державної прикордонної служби України
імені Богдана Хмельницького,
https://orcid.org/0000-0001-9496-5708

ТУШКО ДМИТРО АНАТОЛІЙОВИЧ
старший викладач кафедри прикордонної служби,
Національна академія Державної прикордонної служби України
імені Богдана Хмельницького
https//orcid.org/ 0000-0002-1697-5836

АНАЛІЗ ЗАРУБІЖНОГО ДОСВІДУ ОПЕРАТИВНОГО ПЛАНУВАННЯ НА ОСНОВІ СПРОМОЖНОСТЕЙ ОКРЕМИХ ПІДРОЗДІЛІВ ОХОРОНИ КОРДОНІВ КРАЇН-ЧЛЕНІВ ТА КРАЇН-ПАРТНЕРІВ НАТО

Стаття присвячена аналізу зарубіжного досвіду оперативного планування у сфері безпеки кордонів з урахуванням можливостей підрозділів країн-членів та партнерів НАТО. В умовах сучасних геополітичних викликів та посилення гібридних загроз забезпечення надійного захисту державного кордону має ключове значення для національної безпеки України. Водночас, аналіз практики оперативного планування в Державній прикордонній службі України виявляє низку суперечностей, що призводять до наукової проблеми дослідження.

Сучасний розвиток систем безпеки кордонів характеризується пошуком нових ефективних інструментів управління, здатних адекватно реагувати на гібридні загрози та динамічні виклики. У цьому контексті оперативне планування, що базується на можливостях окремих підрозділів охорони кордону, є ключовим елементом підвищення обороноздатності держави.

Розглянуто методологію Capability-BasedPlanning (Планування на основі можливостей), яка забезпечує гнучкість та адаптивність системи управління в умовах динамічного середовища. Було проаналізовано інструменти оцінки готовності та взаємодії, включаючи стандарти НАТО, інспекції, навчання та моделювання. Визначено напрямки адаптації стандартів Альянсу до українських реалій, зокрема, інтеграція елементів НДПП, що сприяє підвищенню ефективності управління силами та засобами ДПСУ. Проведене дослідження дозволяє зробити низку ключових висновків щодо можливостей адаптації зарубіжного досвіду оперативного планування для підвищення ефективності діяльності прикордонних підрозділів України. Таким чином, основним вектором розвитку системи оперативного планування Державної прикордонної служби України має бути подальша глибока інтеграція з принципами та механізмами НАТО, зокрема шляхом впровадження ризик-орієнтованого підходу, цифровізації процесів моніторингу та моделювання, а також розвитку міжвідомчої координації. Це забезпечить не лише підвищення обороноздатності на національному рівні, але й підвищення безпекової стабільності всього регіону.

***Keywords**: оперативне планування, спроможності підрозділів, НАТО, прикордонна безпека, взаємосумісність, Державна прикордонна служба України.*

UDC 355.1:(81’42+81’23) DOI 10.59226/2786-6920.2.2025.95-104

LYSYCHKINA IRYNA,
Candidate of Philologycal Sciences, Associate Professor,
Professor of the Department of Philology and Military Translation,
Kyiv Institute of the National Guard of Ukraine
https://orcid.org/0000-0002-2050-9379

LYSYCHKINA OLHA,
Candidate of Philologycal Sciences, Associate Professor,
Professor of the Department of Philology and Military Translation,
Kyiv Institute of the National Guard of Ukraine
https://orcid.org/0000-0002-9511-9615

COLLECTIVE CONSCIOUSNESS OF MILITARY PERSONNEL: THE SIGNIFICANCE OF COMMON KNOWLEDGE BASE AND CULTURAL HERITAGE

The article examines the formation of collective consciousness among military personnel through the prism of a common knowledge base and cultural heritage. The relevance of this research is determined by contemporary challenges and threats to Ukraine's national security, particularly in the context of cognitive warfare, which emphasises the need to develop a unified system of values, behavioural patterns, and professional identity within the military community. The collective consciousness of military personnel ensures the harmonisation of ideas, values and norms of behaviour, creating psychological resilience and the ability to resist disinformation, manipulation and cognitive attacks. Particular attention is paid to military personnel's awareness of prominent Ukrainians and their achievements as an element of a common knowledge base that contributes to the formation of collective identity, patriotism and shared historical memory.

The results of an empirical study of military personnel's awareness of prominent Ukrainians, conducted using a questionnaire, showed a high level of awareness in the fields of history and science (Pylyp Orlyk, Ilya Mechnikov, Igor Sikorsky), an average level in professionally significant and scientific and technical issues (Petro Prokopovych, Boris Paton), and a lower level in the field of culture and sports (Bohdan Stupka, Valeriy Lobanovskyi). Gender differences were identified, as female respondents were significantly more likely to give correct answers to questions than male respondents. The presence of spelling errors and instances of no response indicates superficial awareness and a need for improved educational training.

Scientific observations show that knowledge about prominent Ukrainians not only shapes collective consciousness and professional identity, but also increases the cognitive resilience of military personnel in situations of information pressure. Consistency of knowledge and values within the group contributes to maintaining morale, strengthening collective unity and active citizenship, which is especially important in the context of modern hybrid threats.

Keywords: *collective consciousness; military personnel; common knowledge base; cultural heritage; patriotism; professional identity.*

Statement of the problem. In the current context of global challenges and threats to Ukraine's national security, the issue of forming and developing collective consciousness among military personnel is becoming particularly relevant. The collective consciousness of military personnel is shaped by various factors, among which a shared knowledge base and cultural heritage play a particularly important role. These elements create the foundation for the formation of a unified worldview, value system, and behavioral patterns that are critical to the functioning of a military organization. In this context, awareness of the names of prominent individuals and their

achievements is a crucial component of a shared knowledge base. Such knowledge helps create shared values and identity within the professional community, particularly among military personnel.

Given the multifaceted nature of this issue, it is important to address the theoretical and practical aspects of shaping the collective consciousness of military personnel, key influencing factors, and the development of recommendations for optimizing this process in the context of modern realities.

Analysis of recent research and publications. The issue of collective consciousness and its formation through the lens of a common knowledge base and cultural heritage has drawn the attention of many researchers in the fields of psychology, sociology, and pedagogy. M. Sliusarevsky emphasizes the importance of shared experience and social unity [1]. The research by V. Kupriychuk "The role of national cultural heritage in the formation of Ukrainian identity" [2] highlights the relationship between cultural identity and the preservation of the historical memory of generations for the future. Several scientific papers [3; 4; 5; 6] have been devoted to analysing modern approaches to the development of collective consciousness in the information society. Scientists considered the narrative as a tool for shaping the collective consciousness of military personnel [7], emphasizing the importance of "integrating narratives into culture, education, and upbringing at both the national level and promoting these narratives at the international level" [8].

The analysis of recent publications suggests a growing scientific interest in the topic of collective consciousness of military personnel [9; 10], as well as the role of a common knowledge base and cultural heritage in its formation. Researchers emphasize the multidisciplinary nature of this problem and the need to take into account contemporary sociocultural and information-technological realities. At the same time, despite the significant amount of theoretical work, there is a lack of empirical research that would enable a quantitative assessment of the influence of various factors on the formation of the collective consciousness of military personnel.

The purpose of this article is to determine the level of awareness among military personnel regarding the names of prominent Ukrainians and their achievements, as an essential component of a common knowledge base, as well as the role of this awareness in shaping collective consciousness.

Presentation of the main material. The formation of collective consciousness involves understanding and agreeing on ideas, values, and identities within a professional community. Familiarity with the names of prominent figures and their achievements, as well as general knowledge, can play an important role in this process, especially in five areas:

defining values and goals;

recreating a shared history;

creating a positive image of the professional community;

stimulating patriotism and pride;

supporting identification and mutual understanding.

The names of prominent people are often associated with specific values and achievements. Knowledge of their achievements allows the professional community to determine which values and goals are important to them independently, as well as which common values unite them. Awareness of the names of prominent individuals and their contributions can serve as the basis for creating a shared history of a group or community. In this context, understanding the shared achievements of individuals can contribute to the formation of collective self-determination. Knowing the names of prominent figures can influence the construction of a positive image, because if compatriots are noted for their great achievements and positive contributions, this can help to increase the self-esteem and attractiveness of the group to new members. Knowledge of the history and achievements of famous people can stimulate patriotism and pride in one's country, nation, or community. This can support internal unity and a positive perception of belonging. General knowledge about prominent figures can create points of common contact between different members of the community, which promotes mutual understanding and the formation of a common identity.

Achieving the set goal required empirical research, which employed a questionnaire method to ensure the relative objectivity and representativeness of the results obtained. The electronic questionnaire was distributed using the snowball method. A total of 239 respondent questionnaires were processed. The vast majority of respondents (94.6%) are servicemen of the National Guard of Ukraine, 1.3% are servicemen of the Armed Forces of Ukraine, 0.8% are representatives of other military formations, and 2.1% are persons who are not servicemen. The age composition of the sample is determined by the specifics of the respondents' professional military activities: 89.5%

of the study participants are aged 18 to 30; 7.9% are in the 31–40 age group; 1.7% are in the 41–50 age group; and 0.8% are over 50 years old. The gender composition of the respondents (75.1% of the total number of respondents were men) generally reflects the gender imbalance in the military sphere.

The questionnaire "Knowledge, perceptions, value priorities" was devoted to the level of respondents' awareness of prominent Ukrainians. This section included ten statements about famous figures. The task was to indicate their surnames. To make the task easier, respondents were given the first letter of the corresponding surname.

We will present the results obtained from this questionnaire and comment on them in terms of the formation of collective consciousness.

The first question concerned the author of the world's first constitution. The answers to this question are shown in Fig. 1. Almost three-quarters of respondents (72.6%) answered this question correctly (Pylyp Orlyk). 18.1% of respondents did not provide any answer, and 1.7% admitted that they did not know the answer. It should be noted that when determining the percentage of correct answers, answers containing spelling errors (within 5%) were accepted (such as: Orlik, Pilip Orlyk, etc.). 94.2% of female respondents answered this question correctly.

The second question concerned the inventor of the first frame hive, as Ukraine confidently maintains its place among the world's top three honey producers. Petro Prokopovych was mentioned by 56.5% of respondents, with some answers containing spelling errors (within 5%). 30.8% of respondents did not provide an answer, and 3.4% admitted that they did not know the correct answer. 87.2% of female respondents answered this question correctly. The answers to this question are shown in Fig. 2.

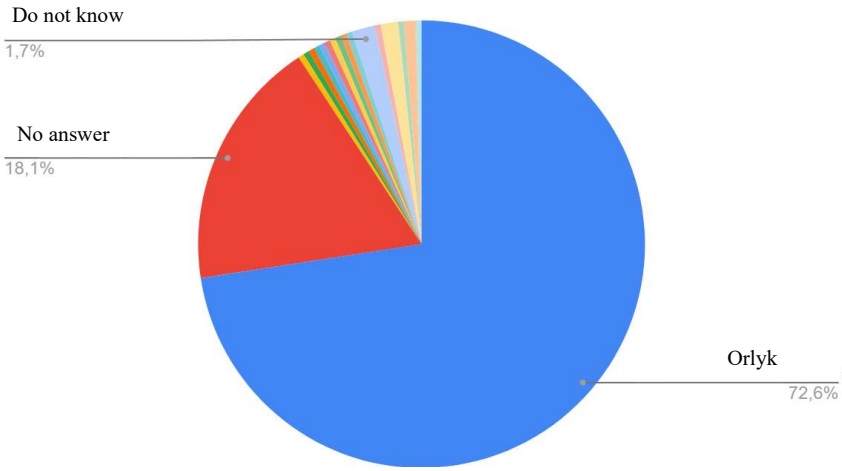


Figure 1 – Answers to question 1. O... – author of the world's first constitution (Constitution of the Rights and Freedoms of the Zaporizhzhia Army, April 5, 1710). For comparison, the US Constitution was adopted in 1787

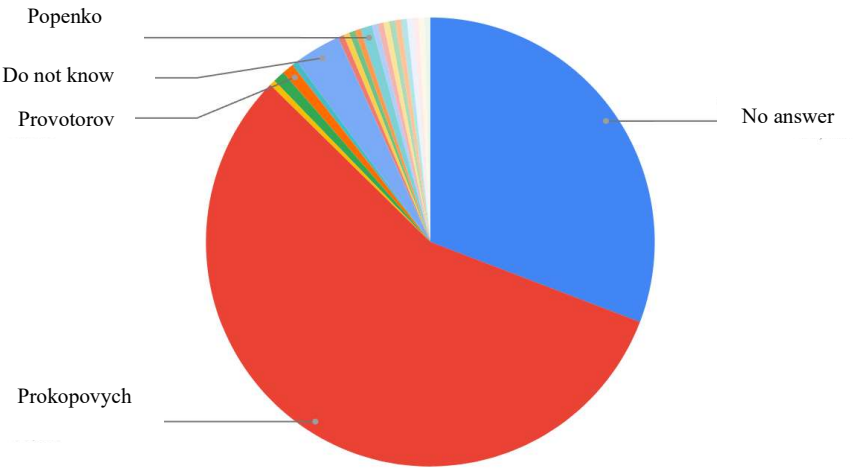


Figure 2 – Answers to question 2. P... – inventor of the first frame hive
Ukraine confidently maintains its place among the world's top three honey producers

The third question concerned the inventor of helicopters. The answers to this question are shown in Fig. 3. Unlike the subject area of the previous question, respondents are more familiar with aviation technology and military equipment, so 65% of respondents correctly identified the inventor of helicopters (Igor Sikorsky). 27.4% of respondents did not provide an answer, 2.1% said they did not know the answer, and 2.5% of respondents named Serhii Korolov. We consider this to be evidence of insufficient knowledge, a possible tendency to give an answer even if unsure, which can be idiomatically described as "I hear the bell but don't know where it is." 82.4% of female respondents answered this question correctly.

The fourth question concerned a famous bacteriologist and immunologist. Illia Mechnikov was identified by 58.6% of respondents, which indicates that the respontents have general knowledge of prominent figures in the history of science and medicine. As with the answers to the previous questions, almost a third of respondents did not provide any answer (29.1%), 3.4% said they did not know the answer, and 3.8% chose Mykhailo Pirohov under the letter M (possibly influenced by the figure of the outstanding surgeon Mykola Pirohov). We have no explanation for the next most common answer (0.8% – Mykhailo Ivanovskyi), as we are not familiar with any Ukrainians with this surname in the field of medicine. 80.4% of respondents answered this question correctly. The answers to this question are shown in Fig. 4.

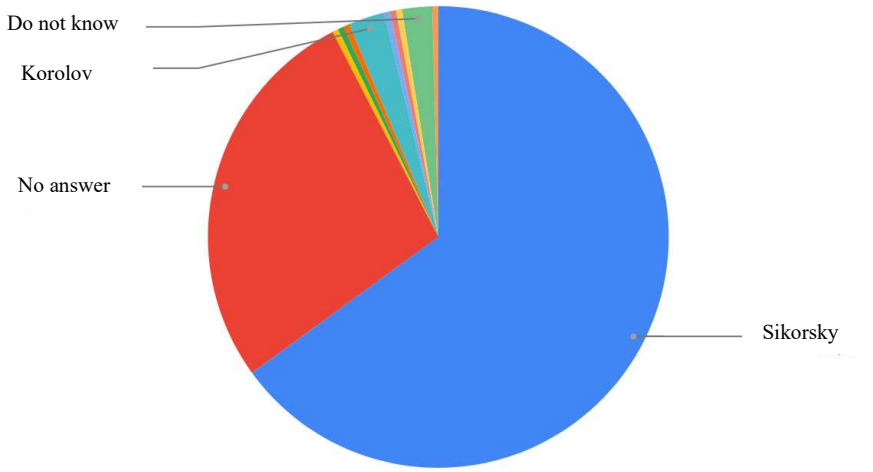


Figure 3 – Answers to question 3. S... – inventor of helicopters. Under his leadership, the Grand and Illia Muromets aircraft were created, and 75 four-engine bombers were built

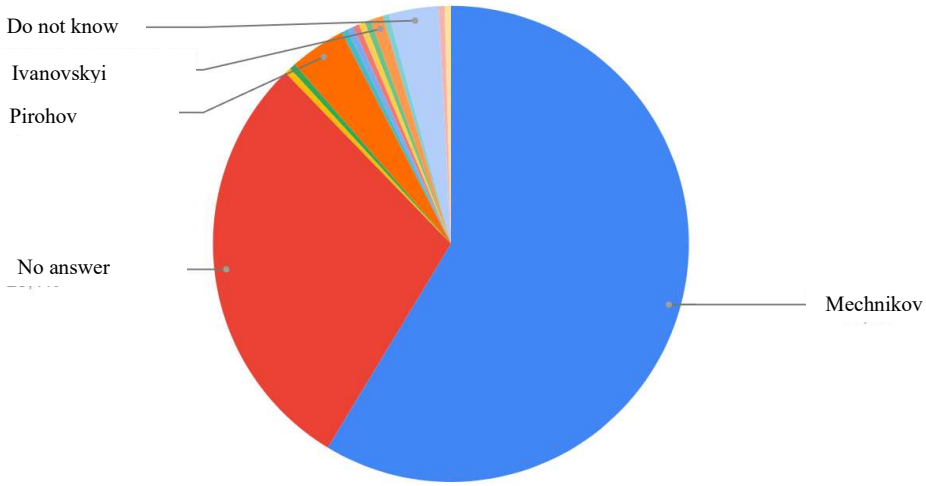


Figure 4 – Answers to question 4. M... is a famous bacteriologist and immunologist. He was born in the Kharkiv region. In 1908, the scientist was awarded the Nobel Prize in Physiology and Medicine for his research in immunology

The theme of cinema and theatre arts was explored in question 5. When answering this question, respondents in many cases moved away from the Ukrainian context and suggested actors and actresses whose names begin with the letter S: Sylvester Stallone (14.35%), Jason Statham (3%), Sergei Bondarchuk (2.1%), Steven Seagal (0.8%), which shows the global influence of foreign cinema on the consciousness of the respondents. Ukrainian actor Bohdan Stupka was named as a world-famous actor by 21.1% of respondents. Other answers included well-known figures who are not/were not actors at all: theatre director Konstantin Stanislavsky (1.3%), American film director Steven Spielberg (5.5%), and American writer Stephen King (1.3%). Such answers may indicate a lack of clarity in the understanding of artistic professions and their representatives by the professional community under study. 35.4% of respondents did not provide any answer to this question, 2.5% admitted that they did not know. 26.5% of respondents answered this question correctly. The answers to this question are shown in Fig. 5.

The sixth question logically followed on from the previous one and concerned musical creativity. 60.8% of respondents correctly identified Mykola Leontovych as the author of "Shchedryk," while 4.6% attributed the authorship to another prominent Ukrainian composer, Mykola Lysenko, which may indicate possible confusion among well-known Ukrainian composers or a lack of sufficient knowledge. 90.4% of female respondents answered this question correctly. Approximately one-third of respondents (26.6%) did not provide an answer, indicating that they did not know (1.7%), which is consistent with the general trend: almost one-third of respondents refused to answer the questions in this section of the questionnaire. The answers to this question are shown in Fig. 6.

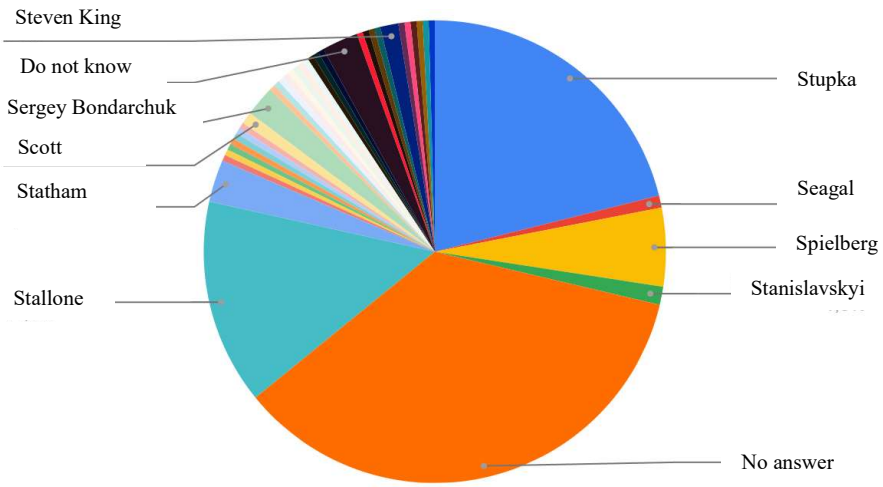


Figure 5 – Answers to question 5. S… – world-renowned actor

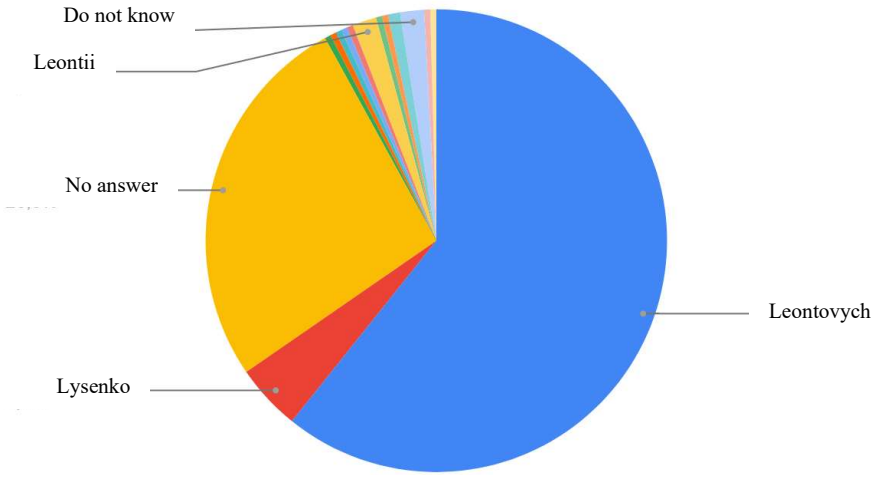


Figure 6 – Answers to question 6. L... is an outstanding musician, one of the founders of the Ukrainian national school of composition and the author of the most popular arrangement of 'Shchedryk', which is played every year before the New Year holidays all over the world

The seventh question concerned a scientist in the field of welding. The answers to this question are shown in Fig. 7. Slightly more than half of the respondents correctly identified Borys Paton (53.2%) as the answer to this question, with answers containing spelling errors (Poton, Patton, etc.) and incorrect names (Mykola, etc.) also considered correct. 75.5% of female respondents answered this question correctly. We have no explanation as to why respondents gave other answers (writer (?) Pavlo Zahrebelnyi (0.4%), Petro (?) Lazarenko (0.8%), surgeon (?) Pirohov (2.5%)). 33.8% of respondents did not provide an answer at all, and 0.8% did not know the answer.

Awareness of outstanding Ukrainians in sport was tested by the eighth question. The answers to this question are shown in Fig. 8. The fact that less than half of the respondents correctly identified the surname of the outstanding football coach Valeriy Lobanovskyi (49.8%), even though military personnel are usually interested in football, indicates the transience of time and the respondents' focus on the present day in terms of sports subjects that are not reflected in school curricula, as well as a lack of awareness of major football events or features of the game in the past. We believe that the names of contemporary football coaches of clubs and national teams should not pose any difficulties. 55.1% of respondents answered this question correctly. 34.6% of respondents did not answer, and 3.4% indicated they did not know the answer. Interestingly, incorrect answers to this question were more often given by men aged 18–30.

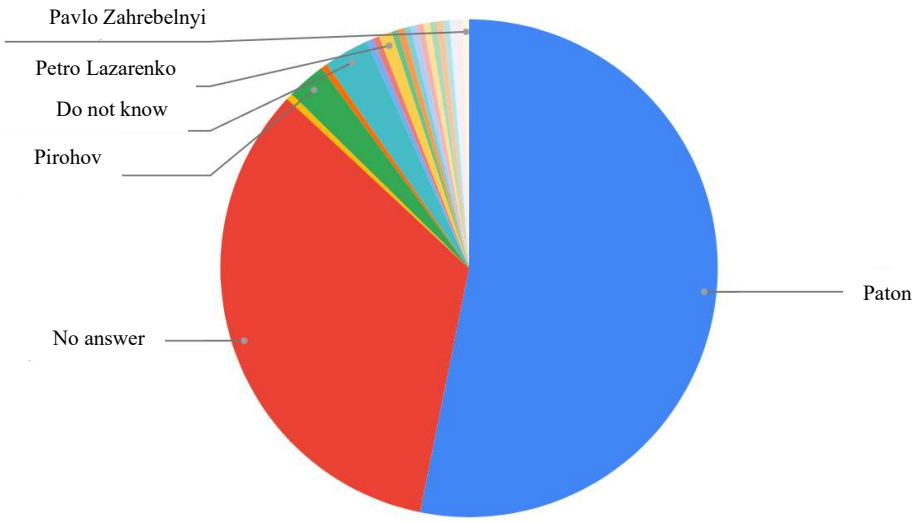


Figure 7– Answers to question 7. P... – thanks to his developments, it became possible to use welding in outer space and welding of living tissues, which was recognised worldwide as an unprecedentedly effective method in surgery

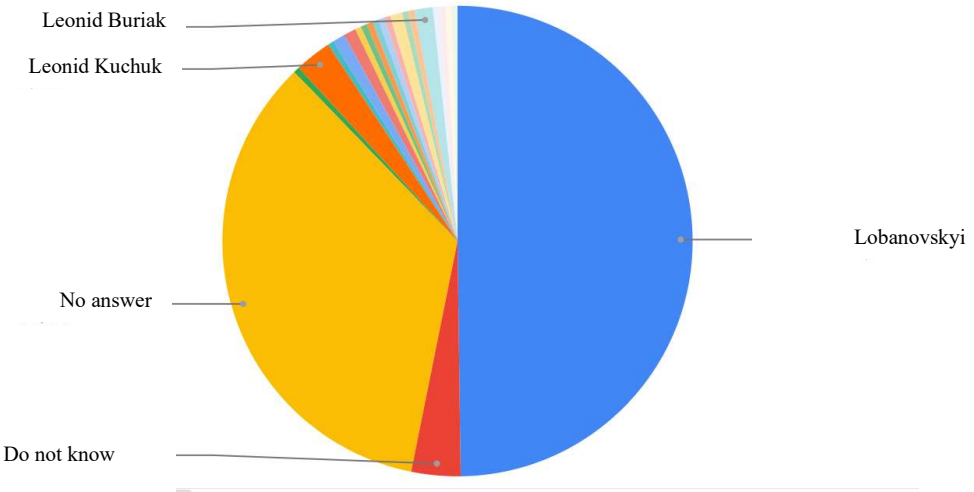


Figure 8 – Answers to question 8. L... – thanks to his talent, Dynamo Kyiv managed to reach the Champions League semi-finals, beating Barcelona. To date, no other Ukrainian team has been able to match this achievement from the 1990s.

The ninth question concerned Ukrainian literature. The answers to this question are shown in Fig. 9. 63.7% of respondents correctly named Lina Kostenko. Writer Olha Kobylianska and poet Lesia Ukrainka, whose surname begins with the letter K (Kosach), were named by 2.1% and 1.7% of respondents, respectively. 24.1% of respondents did not answer this question. 82.4% of female respondents answered this question correctly.

The last question in the questionnaire was about a world-famous cardiac surgeon. The answers to this question are shown in Fig. 10. Unexpectedly for the questionnaire developers, 61.6% of respondents correctly identified Mykola Amosov. 84% of female respondents answered this question correctly. 30.8% of respondents did not answer at all, and 3.8% did not know the answer.

Analysis of the data obtained reveals certain patterns in respondents' awareness of prominent Ukrainians and their contributions to various fields, which is important for shaping the collective consciousness of the professional community.

A high level of correct answers was recorded in questions related to historical and scientific figures such as Pylyp Orlyk, Illia Mechnikov, and Igor Sikorsky. This fact suggests that respondents possess a sufficient level of knowledge in the fields of national history and science, which is likely related to patriotic education and the specifics of military training.

It is worth noting that a gender difference exists in the level of awareness, as female respondents consistently demonstrate a significantly higher percentage of correct answers than male respondents in most questions. This fact may indicate that women pay more attention to educational and cultural topics, as well as a difference in motivation to participate in the survey and provide answers.

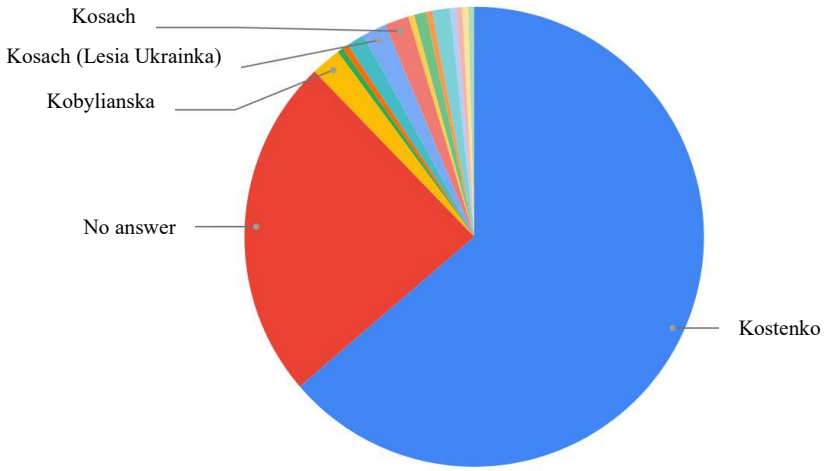


Figure 9 – Answers to question 9. C... – courage, loyalty to principles, and skilful words characterise this talented poet. Her works are studied in schools. Her poems have become modern classics

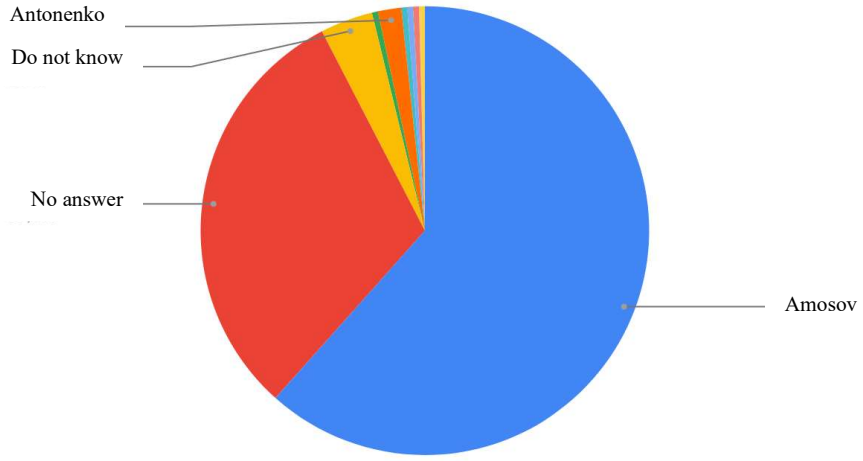


Figure 10 – Answers to question 10. A... is one of the world's most famous cardiac surgeons, who, thanks to his tireless work and talent, has become a legend in Ukrainian and world medicine

The results indicate a lower level of awareness among respondents in the field of culture and sports. In particular, questions about famous Ukrainian actors and football coaches (Bohdan Stupka, Valeriy Lobanovskyi) received a significantly lower percentage of correct answers. This indicates the influence of global popular culture, as well as insufficient attention to national cultural and sporting achievements of the past century in educational and training programmes, which, in turn, may reduce the potential for the formation of national and professional identity.

Respondents demonstrate an average level of awareness of professional and scientific achievements that are not directly related to historical education (Prokopovich's frame hive, Borys Paton's welding developments). This highlights the need for more active implementation of knowledge about scientific and technical achievements in the professional training and patriotic education process.

Errors in responses and the presence of alternative associations (for example, confusing Mechnikov with Pirohov, Sikorsky with Korolov) indicate the existence of superficial awareness, where respondents have heard the names of famous figures but do not always associate them with specific achievements.

A significant proportion of respondents refused to answer certain questions (especially in the field of culture and science), which may indicate a lack of confidence in their knowledge and a need for stronger educational training to shape collective consciousness. At the same time, the lower level of awareness in the field of culture and sports indicates potential areas for improvement in educational and training programmes aimed at integrating national cultural heritage and sporting achievements into the process of forming a common identity among military personnel.

Conclusions and prospects for further research. Knowledge about prominent figures and their achievements is one of the key tools for shaping the collective consciousness of a professional community, as it helps to identify common values, create a positive image and stimulate pride in belonging to a group. This awareness lays the foundation for a shared history and identity, providing points of connection between community members and fostering their internal unity and mutual understanding. Consistent responses may indicate the active participation of respondents in civic life and an interest in important aspects of history. This can shape awareness of the importance of knowledge and active participation in public processes.

Most respondents answered questions related to contemporary issues, art and literature, and professionally relevant subject areas correctly, which may indicate the significant influence of interests and educational programmes on the expansion of knowledge among members of this professional community. The difference in responses between different age and socio-cultural groups may indicate that interests and awareness vary depending on these factors. This may influence the formation of a collective consciousness, highlighting the achievements of domestic inventors in a crucial field.

Female respondents were more likely to answer questions correctly, indicating greater awareness of the names of prominent Ukrainians.

The presence of spelling errors is due to the fact that some respondents have the information but may have difficulty writing or choosing the right words. This may be an element of identification and characterise a group with certain characteristics.

The proportion of those who do not know the answer or did not provide an answer may indicate opportunities for improving education and awareness. Such answers can serve as an incentive to provide additional educational information and contribute to the growth of intellectual awareness. The results indicate the need to increase the level of general education in order to raise citizens' awareness in various fields, including history, culture, science and medicine.

We consider the following areas to be promising for further research: studying the impact of educational programmes and cultural initiatives on the level of awareness, analysing the dynamics of collective consciousness formation in the professional community of military personnel, and developing tools for the systematic improvement of citizens' cultural, scientific and historical competence.

References

1. Sliusarevskyi M. M. (2023). *Suspilna yednist v umovakh povnomasshtabnoi viiny: nabutky i vyklyky* [Social Unity in the Conditions of Full-scale War: achievements and challenges]. Proceedings of the scientificand practical conference *"Filosofsko-sotsiolohichni ta psykholoho-pedahohichni problemy pidhotovky osobystosti do vykonannia zavdan v osoblyvykh umovakh"* (Kyiv, November 23, 2023). Kyiv : NUOU, pp. 28–32 [in Ukrainian].

2. Kupriichuk V. M., Troshchynskyi V. P. (ed.), Skurativskyi V. A., Yarosh N. P., Sytnyk P. K., Kravchenko M. V., Peshetnikov Yu. Ye., Karlova V. V., Fesenko H. L., Derbak A. P., Burmistrova V. A. (2018). *Rol natsionalnoi kulturnoi spadshchyny u formuvanni ukrainskoi identychnosti* [The Role of National Cultural Heritage in the Formation of Ukrainian Identity]. *Formuvannia ukrainskoi identychnosti v umovakh suchasnykh vyklykiv: teoretychni i politychni aspekty*. Kyiv : NADU, pp. 78–106 [in Ukrainian].

3. Potapenko V. (ed.), Tyshchenko Yu., Kaplan Yu. (ed.), Stepyko M., Valevskyi O. (2024). *Analiz osnovnykh tendentsii u sferi kolektyvnykh identychnostei ukrainskoho suspilstva: vyklyky natsionalnii bezpetsi* [Analysis of Main Trends in the Sphere of Collective Identities of Ukrainian Society: challenges to national security: analytical report]. Kyiv : NISD. DOI: https://doi.org/10.53679/NISS-analytrep.2024.13 [in Ukrainian].

4. Kyrychenko V. V. (2020). *Osobystist u suchasnomu informatsiinomu suspilstvi* [Personality in Modern Information Society]. Zhytomyr : ZhDU im. Ivana Franka [in Ukrainian].

5. Hudmanian A. H. (ed.), Yahodzinskyi S. M. (ed.) (2020). *Sotsialni komunikatsii informatsiinoho suspilstva: teoretychni ta prykladni aspekty* [Social Communications of Information Society: Theoretical and Applied Aspects]. Kyiv : Talkom [in Ukrainian].

6. Sardak A. (2024). *Fenomen natsionalnoi identychnosti v umovakh informatsiinoi viiny* [The Phenomenon of National Identity in the Conditions of Information War]. *Zhurnal sotsialnoi ta praktychnoi psykholohii,* no. 3, pp. 87–91. DOI: https://doi.org/10.32782/psy-2024-3-14 [in Ukrainian].

7. Lysychkina I. O., Lysychkina O. O. (2023). *Naratyv yak instrument formuvannia kolektyvnoi svidomosti viiskovosluzhbovtsiv* [Narrative as a Tool for Forming the Collective Consciousness of Military Personnel]. *Zbirnyk naukovykh prats Natsionalnoi akademii Natsionalnoi hvardii Ukrainy*, vol. 2 (42), pp. 58–62. DOI: https://doi.org/10.33405/2409-7470/2023/2/42/293345 [in Ukrainian].

8. Koval, V., Krymets, L. (2023). Morale and morality in the Armed Forces of Ukraine: NATO approaches and the national direction of implementation. *Visnyk of the National Defence University of Ukraine*, vol. 72 (2), pp. 58–68. DOI https://doi.org/10.33099/2617-6858-2023-72-2-58-68 [in English].

9. Ilchenko O. A. (2024). *Rol ZMI u formuvanni masovoi svidomosti ta kolektyvnoi svidomosti viiskovosluzhbovtsiv (za materialamy anketuvannia)* [The Role of Mass Media in the Formation of Mass Consciousness and Collective Consciousness of Military Personnel (based on questionnaire materials)]. *Vcheni zapysky TNU imeni V. I. Vernadskoho. Seriia: filolohiia, zhurnalistyka,* vol. 35 (74), no. 2 (2), pp. 254–258. DOI: https://doi.org/10.32782/2710-4656/2024.2.2/40 [in Ukrainian].

10. Krymets L. (2020). *Tsinnisni aspekty formuvannia mentalnosti viiskovosluzhbovtsiv Zbroinykh Syl Ukrainy* [Value Aspects of Forming the Mentality of Military Personnel of the Armed Forces of Ukraine]. *Visnyk Natsionalnoho universytetu oborony Ukrainy*, vol. 49 (1), pp. 155–160. DOI: https://doi.org/10.33099/2617-6858-2018-49-1-155-160 [in Ukrainian].

Received / Стаття надійшла до редакції: 18.09.2025
Revised / Прорецензовано: 09.10.2025
Accepted / Схвалено до друку: 15.10.2025

ЛИСИЧКІНА ІРИНА ОЛЕКСІЇВНА
кандидат філологічних наук, доцент,
професор кафедри філології та військового перекладу,
Київський інститут Національної гвардії України
https://orcid.org/0000-0002-2050-9379

ЛИСИЧКІНА ОЛЬГА ОЛЕКСІЇВНА
кандидат філологічних наук, доцент,
професор кафедри філології та військового перекладу,
Київський інститут Національної гвардії України
https://orcid.org/0000-0002-9511-9615

КОЛЕКТИВНА СВІДОМІСТЬ ВІЙСЬКОВОСЛУЖБОВЦІВ: ЗНАЧЕННЯ СПІЛЬНОЇ БАЗИ ЗНАНЬ І КУЛЬТУРНОЇ СПАДЩИНИ

Досліджено формування колективної свідомості військовослужбовців крізь призму спільної бази знань і культурної спадщини. Актуальність проблеми зумовлена сучасними викликами й загрозами національній безпеці України, зокрема в контексті когнітивної війни, що потребує розвитку єдиної системи цінностей, поведінкових патернів і професійної ідентичності у військовій спільноті. Колективна свідомість військовослужбовців забезпечує узгодження ідей, цінностей і норм поведінки, створюючи психологічну стійкість і здатність протистояти дезінформації, маніпуляціям та когнітивним атакам.

Особливу увагу приділено обізнаності військовослужбовців щодо видатних українців та їхніх досягнень як елемента спільної бази знань, що сприяє формуванню колективної ідентичності, патріотизму та спільної історичної пам'яті.

Результати емпіричного дослідження обізнаності військовослужбовців із видатними українцями, що було реалізоване методом анкетування, показали високий рівень обізнаності у сфері історії та науки, середній – у професійно значущих і науково-технічних питаннях, нижчий – у сфері культури й спорту. Виявлено гендерні відмінності: респондентки порівняно з чоловіками значно частіше давали правильні відповіді на запитання. Орфографічні помилки і відсутність відповідей демонструють поверхову обізнаність і потребу у посиленні освітньої підготовки.

Наукові спостереження свідчать, що знання про видатних українців не лише формує колективну свідомість і професійну ідентичність, а й підвищує когнітивну стійкість військовослужбовців у ситуаціях інформаційного тиску. Узгодженість знань і цінностей у групі сприяє підтриманню моралі, зміцненню колективної єдності та активній громадянській позиції, що особливо важливо в умовах сучасних гібридних загроз.

Ключові слова: *колективна свідомість; військовослужбовці; спільна база знань; культурна спадщина; патріотизм; професійна ідентичність.*

UDC 358.1 DOI 10.59226/2786-6920.2.2025.105-124

LYKHOLOT OLEKSANDR
PhD, Professor of the Department of Missile Troops and Artillery,
National Defence University of Ukraine
https://orcid.org/0000-0003-3418-9529

HOLOVCHENKO OLEH
PhD, Professor of the Department of Missile Troops and Artillery,
National Defence University of Ukraine
https://orcid.org/0000-0003-3715-7872

DEMIANIUK ANDRII
PhD, Docent of the Department of Missile Troops and Artillery,
National Defence University of Ukraine
https://orcid.org/0000-0003-0961-4431

METHODOLOGY FOR PLANNING A CONCENTRATED FIRE STRIKE WHEN PLANNING JOINT FIRE SUPPORT IN MODERN ARMED CONFLICTS

The article improves the methodology for planning a concentrated fire strike through the use of a joint targeting cycle. In addition, the use of a methodology for determining the enemy's center of gravity for a specific decisive condition allows for the identification of a group of targets that are critical vulnerabilities and/or critical needs, which will significantly increase the effectiveness of such a strike. Furthermore, the use of improved criteria for describing the indicators of the methodology for determining the priority of targets makes it possible to select the most critical targets during the preparation and delivery of the strike. The use of the nonlinear programming method – 'two functions' at the stage of assigning appropriate means allows for the most effective use of the capabilities of joint fire support forces and means, and at the planning stage allows for an assessment of its possible effectiveness.

Keywords: *joint fire support; concentrated fire strike; center of gravity; prioritization of targets; capabilities; two-function method; targeting.*

Statement of the problem. The armed aggression of the Russian Federation against Ukraine has brought to the forefront the issue of improving the model of state defense organization, which has necessitated a review of the content of the theory and practice of domestic military art. Modern domestic operational art is developing in accordance with the principles of comprehensive defense of Ukraine and taking into account the introduction of the principles and standards of NATO member states into the defense forces.

The characteristic features of the modern operational environment include: blurring of the differences between peacetime and wartime, between the front and the rear; the strengthening of the role of high-precision, robotic and weapons based on new physical principles; the expansion of the range of participants in military conflicts to

include friendly, neutral and hostile forces, the local population, international and non-governmental organizations, and the media; an increase in the proportion of irregular formations in the enemy's combat strength; and the growing role of asymmetric actions.

The presence of these features in the operational environment increases the complexity of preparing and conducting operations in modern conditions. Success in an operation is based on the ability to make rational decisions quickly in conditions of uncertainty, which must be ensured by the use of advanced operational planning techniques by military command and control bodies. One aspect of improving operational planning is to improve the planning of combined fire support in operations and as a component of joint fire support planning (JFSP) – planning a concentrated fire strike (CFS) in the interests of the operation as a whole and in the course of performing a specific operational task or the most important tasks of the operation.

Under current conditions, JFS is the basis for defeating enemy forces and a decisive factor in achieving the objectives of an operational (strategic) force grouping. At the same time, a concentrated fire strike, as a component of the JFSP process, which is delivered jointly by the firepower of several components (ground, sea, air) against important enemy targets in a specific area over a short period of time, allows fire to be directed at elements of the enemy's centre of gravity, significantly reducing its capabilities.

The lessons learned in repelling the armed aggression of the Russian Federation point to a number of inconsistencies and discrepancies, both theoretical and practical, in the planning of JFSP, which in turn lead to a reduction in its effectiveness, including during the planning and delivery of CFS.

The main ones are:

changes in typical targets due to changes in the qualitative composition of weapons;

the use of new types of foreign-made ammunition with new characteristics that were not considered in previous operational and tactical calculation methods;

new standards for the consumption of missiles and ammunition for striking enemy targets have not been defined, taking into account the replacement of the nomenclature of ammunition for both missile forces and artillery (MFA) and the Air Force (AF) and Ground Forces (GF);

the procedure for planning the use of strike unmanned systems (US) has not been defined;

enemy countermeasures using electronic warfare (EW) against high-precision missiles, aerial bombs, ammunition and components of unmanned systems, both reconnaissance and strike, are not taken into account;

the priority of enemy targets and the effectiveness of each element of firepower against enemy targets are not taken into account when planning CFS.

In addition, when planning JFSP in operations, including CFS, the level of training of military command personnel in determining the importance (criticality) of targets and the procedure for direct planning of CFS remains insufficient, primarily due to the lack of adequate planning methods.

In view of the above, there is a need to conduct research on improving the methodology for planning concentrated fire strikes when planning combined fire support in modern armed conflict operations.

Analysis of recent research and publications. The problems of planning concentrated fire strikes were studied in works [1–4], the participation of unmanned systems in them [3, 5–7] and the prioritization of targets in [4, 8–10].

However, the issue of systematizing the actions of officials at the joint fire support center when planning concentrated fire strikes by improving existing methods or creating new ones, including determining the priority of targets while taking into account compatibility with standardized procedures used by NATO member countries, has not been fully researched.

With regard to the distribution of a certain type of resource, the aforementioned works [4, 11–14] considered the distribution of one or two types of resources, both homogeneous and heterogeneous. At the same time, the issue of determining the interrelated distribution of several types of heterogeneous resources, such as the forces and means of JFSP participating in the CFS, by target objects was not considered.

In addition, the issue of determining the enemy's centre of gravity for planning CFS and achieving a certain decisive condition for the design of the operation was not investigated.

The purpose of the article is to improve the methodology for planning a concentrated fire strike when planning joint fire support in modern armed conflicts.

Presentation of the main material. Given the transition of the Armed Forces of Ukraine to the standards of planning and conducting operations used by the armies of NATO member countries, it is advisable to use the concepts found in their theory in order to achieve full compatibility. Therefore, for planning CFS, it is proposed to use the joint targeting cycle [15] (Fig. 1).

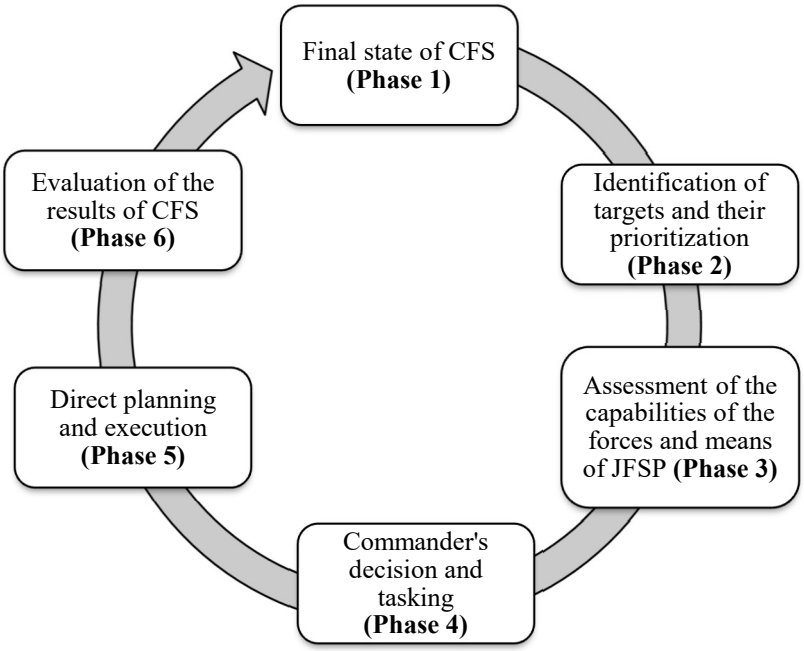


Figure 1 – Joint targeting cycle

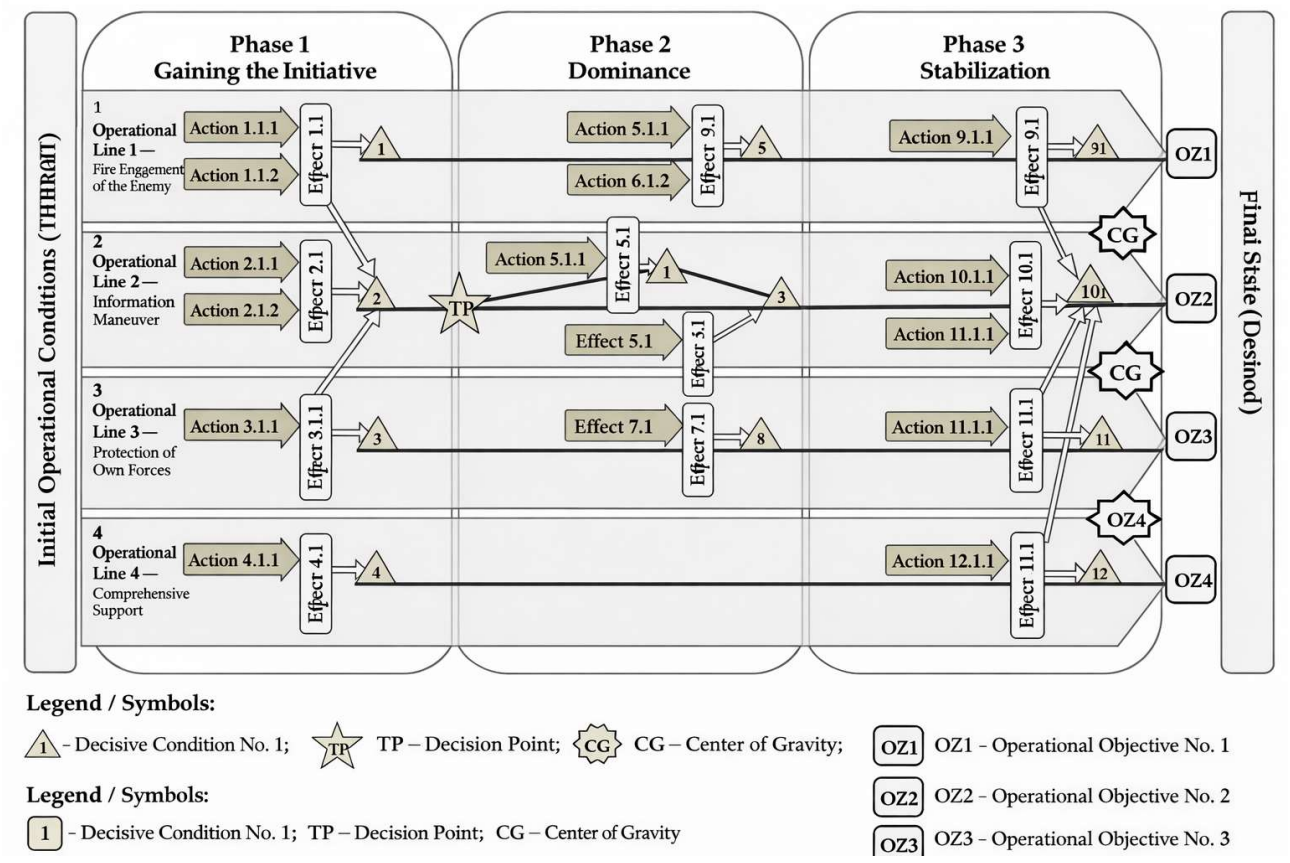


Figure 2 – Example of an operation design

1. Final state of the joint targeting operation (phase 1).

This phase involves:

formulating the final (desired) result of the CFS (from the developed operation design in accordance with the specific operational task and the decisive condition to be achieved during the operation) [16] Fig. 2;

determination of the enemy's center of gravity (CoG) to the decisive condition at a certain stage of the operation and its critical vulnerabilities [17];

formulation of the objectives and conditions for conducting the CFS.

The center of gravity is the main source of power that ensures the strength of an actor (participant in a military conflict), freedom of action or will to fight. Determining the center of gravity in an operation is based on identifying the critical capabilities, critical requirements and critical vulnerabilities of each actor.

Critical capabilities enable their forces, adversaries, or other participants to accomplish their tasks. Critical requirements are the conditions, resources, and means associated with critical capabilities. Critical vulnerabilities are those aspects or components of critical requirements that are deficient or vulnerable to direct or indirect action that can be taken by the opposing side.

One of the important results of operational planning is to identify ways to influence the centers of gravity of actors (the enemy, one's own, other participants in the conflict) sufficient to achieve the objectives of the operation by strengthening and protecting one's own center of gravity and weakening or destroying the enemy's center of gravity. There are two approaches to influencing centers of gravity: direct and indirect.

The direct approach attacks the enemy's center of gravity or its main forces using armed combat directly against the enemy. The indirect approach usually focuses on avoidance or other ways of rendering armed combat ineffective, rather than on the physical destruction of the enemy's center of gravity. In some cases, an indirect approach may require a series of operations (actions) against several critical vulnerabilities of the enemy. In other cases, it may involve a single operation (action) against several particularly critical vulnerabilities, but without armed engagement with the enemy's main forces. The choice of approach is a matter of weighing factors such as the balance of power between the parties, the capabilities of one's own forces, the types of critical vulnerabilities of the enemy, acceptable levels of risk, available time, and so on.

A decisive condition is a combination of circumstances, consequences, or a specific key event, critical factor, or function, the realization of which allows for a sufficient advantage over the enemy or significantly contributes to the fulfilment of the operational task. Decisive conditions are determined based on the results of assessing the situation and analyzing centers of gravity. A decisive condition is defined as desirable at a specific point in time in the future, which is considered decisive, and is formulated in the past tense.

Examples of decisive conditions include: fire superiority over the enemy in the operational group's attack zone has been achieved; the enemy's main strike force has been stopped; irregular enemy forces have been neutralized.

An operational effect is a recognizable change in the behavioral or physical state of a system (the system may be: a group of troops; targets, infrastructure; the local population, etc.) resulting from one or more actions. An operational effect supports the formation of one or more decisive conditions and is formulated in simple language without adverbs in the perfect tense.

Examples of operational effect formulations include: the main forces of the enemy's first echelon are surrounded; the enemy's division command system is suppressed; important state facilities in the defense zone of the operational troop grouping are protected.

The action ensures the implementation of one or more operational effects within the framework of the joint functions of the combined forces in operations, which are as follows: command and control; information support; firepower; manoeuvre; defense; support (reconnaissance,

logistics, medical, morale and psychological support).

Usually, an action can be implemented in a specific form, primarily in the form of military operations. The action is formulated in simple language in the past tense. Examples of action formulations include: a second concentrated fire strike was delivered, focusing on the enemy's tank army; a counteroffensive operation was carried out by an operational-tactical group of troops; illegal armed formations in a specific area were blocked (disarmed, defeated); the state border was covered (reinforced) in threatening areas.

The development of operational design is based on determining the logical sequence of decisive conditions, operational effects and actions, which can be arranged in relation to each other in the form of a sequence or a branch. In operational design, sequences and branches are considered as elements of an algorithmic structure.

Under the influence of a dynamic operational environment, the centers of gravity of participants are constantly changing. Therefore, the determination and analysis of the center of gravity should be considered an iterative process that occurs continuously throughout the preparation and conduct of an operation.

The center of gravity is determined based on the results of factor analysis and participant assessment, which results in the identification of critical capabilities, critical requirements and critical vulnerabilities for each participant.

Figure 3 provides one method for using the CoG analysis matrix; other methods can be used to analyze a participant's physical CoGs at the command level.

Some analysts prefer to first identify the decisive capabilities (abilities) that a participant needs to perform its (predictable) tasks, and only then determine the main entity that possesses most of these decisive capabilities. Others may first identify CoG as part of the process that determines how a participant (predictably) will perform their tasks. However, considering that CoG analysis is a continuous and repetitive process, the sequence of actions is irrelevant.

2. Defining objectives and their priority (phase 2).

This phase involves:

forming a list of critical enemy targets (high pay-off targets, HPTs) that relate to a specific center of gravity [18, 19] according to the following structure:

a) target number and name;

b) target classification;

c) source of intelligence information;

d) time of detection and confirmation of the target;

e) location of the target (area or coordinates);

f) type and brief description of the target, etc.

preliminary verification (assessment) of risks, collateral (incidental) losses and compliance with the norms of international humanitarian law (IHL);

determination of the priority of targets [18, 19].

Prioritization of targets should be carried out in accordance with the indicators of the analysis of the significance of enemy objects (CARVER methodology: Criticality, Accessibility, Recouperability, Vulnerability, Effect, Recognizability) [18–20].

All targets in the enemy's group should be considered in terms of their relationship with other elements of its operational structure. The value of each enemy target will change as the operational situation changes, requiring the use of time-sensitive methods that respond to changes in the situation. The criticality of a target will depend on several factors, the main ones being:

time – how quickly will the result of hitting the target affect the course of the operation?

quality – what percentage of the enemy's forces or its rear and infrastructure targets will be reduced by successful fire on the specified target?

effectiveness – how will the destruction of a specific target affect the achievement of the operation's objectives?

theory of relativity – how many targets are there? What are their positions? How is their relative value determined? What will happen in the system or complex ‘flow’?

<table>
<tr><td colspan="2">Purpose of a concentrated fire strike (CFS)
(Assumed) principal tasks (goals) and probable methods of conducting actions for their employment (to achieve these goals) at the level of the command conducting the analysis.</td></tr>
<tr><td>Center of gravity (CoG)
Identify CoG conditions that should exist and conditions that must be avoided to achieve the purpose of the concentrated fire strike (CFS).
Required conditions should be reflected in one's own tasks; if not, they must be reviewed.
Conditions to be avoided should be reflected in the rules of engagement and other constraints.</td><td>Critical capabilities
Identifying the critical capabilities of the center of gravity (CoG) involves assessing whether the CoG possesses the key abilities required to accomplish its tasks (achieve its objectives).
Some capabilities may be weak; in such cases, the corresponding critical vulnerabilities must be identified.
Critical capabilities necessary for accomplishing the participant's tasks (achieving its objectives) may also be lacking; in that case, support from an entity possessing the missing capabilities becomes a critical requirement of the CoG.</td></tr>
<tr><td>Critical vulnerabilities
For each identified critical vulnerability, assess its impact on the critical capability and determine its relationship to the required CoG condition.
For each critical vulnerability, identify and estimate the probable effect (impact) that demonstrates how the critical vulnerability can be exploited to create the required CoG conditions. Can we achieve the planned effects by delivering a concentrated fire strike (CFS), and by what actions? What accompanying risks exist? Are there undesirable effects? What combination of effects can create the required CoG condition?</td><td>Critical requirements
Each critical capability of the center of gravity (CoG) should be considered in terms of critical requirements – the conditions, resources, and/or means necessary for the CoG to employ its capabilities.
There will usually be overlap in the requirements for employing different critical capabilities, but attention should be paid to which critical capability is associated with which requirement.</td></tr>
<tr><td colspan="2">Conclusions
Conclusions should be formulated as elements for further planning, for example: purpose, tasks (objectives), decisive conditions, effects, actions, rules for the use of force (rules of engagement), restrictions on the use of force, etc.</td></tr>
</table>

Figure 3 – Centre of Gravity Analysis Matrix

Based on the above, the criteria for deciding whether to target a target and determining its priority are ranked. Table 1 shows an option for ranking the criticality criteria of enemy targets.

As can be seen from the data in Table 1, the importance ranking of a target (from 1 to 10) directly depends on the degree of its impact on the course of the operation as a whole and the fulfilment of operational (tactical) tasks in particular. At the same time, given that the result of fire impact on the enemy can be achieved through the accessibility of the object, the next element for assessing enemy objects is its accessibility. This element determines the ability of fire support assets to achieve a successful result of fire impact on an enemy target. Another important aspect of prioritizing enemy targets is taking into account factors that may hinder or facilitate their effective destruction.

There are four main steps in determining the accessibility of targets that can be destroyed, namely: the ability to destroy the target without direct threat from the enemy; the ability to determine the results of the fire impact; the ability to destroy the target without damaging the surrounding environment; the ability to destroy the entire target, rather than its individual elements.

Factors considered when assessing accessibility may include, but are not limited to: active and passive early warning systems (air defense systems, ground-based reconnaissance radar stations,

counter-battery radars, etc.); the presence of electronic warfare elements (for the use of high-precision munitions); type of terrain and its use; fortification equipment system; concealment and cover of individual target elements; location of the facility in populated areas where the use of certain means of destruction is impossible; other natural or synthetic obstacles or barriers; sudden changes in climatic and weather conditions.

Accessibility is determined in terms of the relative ease or difficulty of implementing a set of measures aimed at destroying the target. With this in mind, it is recommended to rank these criteria, which will then be taken into account when assessing targets that will be considered as possible targets for JFSP forces and means during a concentrated fire strike. Table 2 shows one possible option for ranking the criteria for the accessibility of enemy targets.

As can be seen from Table 2, the importance ranking of a target (from 1 to 10) reveals a directly proportional relationship between the accessibility of an enemy object for destruction and the degree of its openness and observability, as well as the complexity of the terrain on which it is located.

Given that the assessment of an enemy target, which may subsequently be taken as a target, will be influenced by its ability to be restored or replaced in a timely manner, the next element for its assessment is its recuperability, measured in time.

Factors to be considered when assessing recuperability include, but are not limited to, the availability of: handy equipment such as railway cranes, dry docks and the removal of serviceable parts and assemblies from damaged equipment for the repair of damaged weapons; restoration and replacement through reduction; availability of spare parts; equivalent repair kits that provide backup for critical equipment or components, as well as the consequences of economic embargoes and labour unrest.

Therefore, taking into account the varying recuperability of the target over time, it is proposed to rank these criteria, which will subsequently be taken into account when assessing targets. Table 3 shows the ranking of criteria for the recuperability of enemy targets.

Table 1 – Ranking of criteria for the criticality of enemy targets

Criteria for criticality	Ranking of importance
Crucial for the overall success of the operation.	10
Important for the success of current combat operations.	9
Timely and convincing consequences for current combat operations.	8
Significantly affects the course of combat operations.	7
Moderate contribution to combat operations, not critical to success.	6
Failure to take targeted action may negatively complicate the operation.	5
Requires focus in future plans.	4
Failure to apply firepower will result in the involvement of more forces and resources.	3
The effect provided by the target may not be realized in the future.	2
Mostly unimportant, the consequences will not hinder combat operations	1

Table 2 – Ranking of criteria for accessibility of enemy targets

Accessibility criteria	Rank of importance
Stationary, fully accessible, no early warning systems for determining fire results.	10
Stationary, accessible. Insufficient information about radio-electronic suppression, no natural obstacles.	9
Accessible, reliably reconnoitered, terrain type partially complicates access to the target.	8
Accessible, individual elements behind artificial obstacles. Terrain partially affects the use of certain weapons.	7
Partially accessible, individual elements are fortified. High-precision weapons are required.	6
Partially accessible, it may not be possible to accurately determine the structure of the target, there is a possibility of early warning systems or radio-electronic suppression elements.	5
Partially accessible, natural or artificial obstacles, high probability of early warning systems or radio-electronic suppression, possibility of counter-battery fire from the enemy.	4
Difficult to access, requires significant forces and resources, difficult terrain, some elements are hidden. Impossible to use certain weapons.	3
Accessible with great difficulty and expenditure of significant resources. The target can only be destroyed by certain types of weapons.	2
Minimal accessibility, early warning systems (counter-battery radars) reliably identified, elements of the target are hidden or located in a populated area.	1

Table 3 – Ranking of criteria for the Recuperability of enemy targets

Criteria (for recovery (replacement, repair or substitution) required	Rank of importance
1 month or more	10
2–3 weeks	9
up to 2 weeks	8
1 week	7
5–6 days	6
3–4 days	5
up to 72 hours	4
up to 48 hours	3
on the same day or the next	2
up to 12 hours	1

Based on Table 3, the importance ranking of the target (from 1 to 10) will increase depending on the time for which the corresponding object from the enemy's group will be put out of action. Based on the data in the table, there is also a logical dependence of the sensitivity of a specific target to the firepower of the forces and means of the JFS, with the same amount of weapons. Thus, for evaluation purposes, its vulnerability is accepted, which is characterized as the inability to withstand the impact of firepower and the presence of a significant number of weak points in one or more elements of the target (object of attack). This factor shows how sensitive the target is to fire damage, as

well as what consequences can be caused by the same amount of ammunition (missiles, bombs).

When determining the vulnerability of a target, the scale of the critical component is compared with the attacker's ability to destroy or damage it. In general, the attacking element may tend to: select specific components; cause permanent damage; prevent or stop the effect of cannibalization (donating individual elements to other objects); maximize effects by using materials on site; force the target to self-destruct.

In particular, vulnerability depends on: the nature and design of the target; the amount of damage required; available assets (e.g., personnel, expertise, motivation, weapons, explosives, and equipment).

Taking this into account, Table 4 shows the ranking of criteria according to which the damage caused to the target object is determined, which will be accepted for damage in the future.

According to Table 4, the importance ranking of an object (from 1 to 10) directly depends on its ability to withstand the fire impact of various types of weapons and the amount of resources involved in the attack.

Taking into account the intention and purpose of the fire impact on the enemy, as well as the possible consequences of such an impact, the effect factor is accepted for assessment, which will occupy one of the main places in the process of assessing an object (group of objects) when using the CARVER matrix, and it is closely related to the criticality indicator of objects. The effect of fire is a measure of the possible military, political, economic, psychological and sociological impacts not only on the target, but also beyond it. The type and magnitude of the desired effects will help in the process of planning the use of force to select the object and its main elements for destruction. In this context, the effect refers to all significant effects, desired or not, that may occur after the destruction of the object in question.

Table 4 – Ranking of enemy target vulnerability criteria

Vulnerability criteria	Rank of importance
The target (its main individual elements) will be hit by debris during the fire attack	10
Individual elements of the target are critical, vulnerable individual elements (open manpower)	9
Individual elements of the object are critical, the object is vulnerable to individual elements.	8
The object is vulnerable to all means of destruction, in particular, general support artillery and all types of multiple launch rocket systems.	7
The facility is vulnerable to most means of destruction, in particular artillery and mortars.	6
The facility is vulnerable to certain types of means of destruction, in particular long-range artillery and medium- and long-range multiple launch rocket systems	5
The facility is invulnerable to certain types of weapons and requires constant fire. High-precision weapons may be used.	4
The facility is invulnerable to some weapons, but damage can be caused by powerful fire from forces and weapons.	3
The target is invulnerable to most types of weapons, but can be destroyed by long-range multiple launch rocket systems and, to some extent, by general support artillery.	2
The target is invulnerable to all types of weapons except tactical missile systems and long-range multiple launch rocket systems.	1

Effects may include: initiation of countermeasures; incapacitation of forces and means; repression against the civilian population; collateral damage to other targets.

Possible consequences may be hypothetical and should be identified as assumptions. The consequences of striking a single target may vary considerably at the tactical, operational and strategic levels.

Taking this into account, these criteria have been ranked and will be taken into consideration when assessing enemy targets that may be considered as possible targets. Table 5 shows the ranking of criteria for the effect of striking enemy targets.

It is also important how long ago and by what means of reconnaissance the enemy target was reconnoitered. This information will indicate the reliability of reconnaissance information about the enemy target. Therefore, it is also proposed to take into account the factor of target recognizability (identification) when applying the CARVER matrix. This factor represents the degree to which the target can be recognized by various means of reconnaissance, primarily artillery reconnaissance, under different conditions. Weather has an obvious and significant impact on the visibility of targets that do not reveal themselves through active radiation or sound and wave emissions. Rain, snow, and ground fog can interfere with observation. Areas with sparse vegetation and adjacent high ground create favourable conditions for reconnaissance. Distance, time of day, and season should also be taken into account.

Other factors affecting recognition include the size and structural complexity of the target, the presence of its distinctive features, the presence of camouflage or concealment, and the technical complexity and preparation of fortification equipment.

Therefore, taking into account the type of reconnaissance used to detect the target, the time elapsed since its detection, and weather conditions, the recognition criteria were ranked, which can be taken into account in the future during the overall assessment of targets using the CARVER matrix. Table 6 shows an option for ranking the criteria for recognizing enemy objects.

Table 5 – Ranking of criteria for the effect of striking enemy targets

Effect criteria (from striking a target)	Rank of importance
Will have the maximum possible positive effect on the results of the operation.	10
Will have a positive effect on the results of the operation.	9
Will have a positive effect on individual stages of the operation.	8
Will have a moderate effect on the results of the operation.	7
Will have a slight positive effect on the overall situation in the combat zone.	6
Will not have a significant positive effect on the overall situation in the combat zone.	5
Will not have a positive effect on the stages of the operation, excessive use of resources.	4
Little significant positive effect, possible negative impact on the operation.	3
Will not have a positive effect, negative effects from its destruction are predicted.	2
Will not have a significant positive effect on the operation, negative effects are predicted.	1

Table 6 – Ranking of criteria for recognizing enemy objects

Recognition criteria	Rank of importance
Clearly observed by reconnaissance means, all elements of the object are grouped together.	10
Observed by reconnaissance means at present or earlier, the object continues its activity in the area.	9
Reconnaissance by artillery reconnaissance, the object reveals itself by various types of radiation.	8
Reconnaissance with a high degree of reliability, characteristic features confirm that the object has not changed location.	7
Reconnaissance conducted within 1 hour, low mobility, possibility of movement. Further reconnaissance possible.	6
Reconnaissance conducted within 3 hours, some elements changed on the ground, low manoeuvrability.	5
Reconnaissance conducted by agents, difficult weather conditions hampering reliability of reconnaissance.	4
Recently scouted, manoeuvrable, no further scouting or possibility of misinformation.	3
Scouted for a long time, weather conditions prevent identification of the object.	2
Scouted a long time ago, no scouting signs detected, possible movement of the object.	1

As Table 6 shows, the importance ranking of an object (from 1 to 10) depends on the technical capabilities of the reconnaissance means used to detect it, the reliability of the reconnaissance data about it, and the possibility of real-time observation, which in turn will make it possible to observe the results of the fire impact on a given enemy object.

The use of this methodology for prioritizing enemy objects for acceptance as possible targets for further destruction during the delivery of CFS, using the CARVER matrix to prioritize objects, taking into account factors such as criticality, accessibility, recoverability, vulnerability, effect and recognizability, ensures the use of limited resources to achieve objectives at all levels of military command.

3. Assessment of the capabilities of the forces and means of JFS (phase 3).

This phase involves assessing the combat capabilities of existing forces and means of JFS (MFA, AF aviation, GF, reconnaissance, EW, UAVs, air defense (AD), special operations forces, etc.) by the following components [21, 22]:

firepower (lethal and non-lethal): depth of action; number of objects that can be simultaneously and sequentially hit with the required expenditure of missiles (bombs), ammunition, strike UAVs; altitudes at which forces and assets (FA) of JFSP are capable of operating; frequency ranges at which electronic warfare (EW) assets are capable of creating interference;

manoeuvring capabilities: capabilities to manoeuvre to specific areas of launch (firing) positions (UAV launch), aviation action lines; fire manoeuvring capabilities (repeated launch taking into account reloading);

reconnaissance capabilities: depth of action of the means; accuracy of determining the coordinates of enemy targets; ability to engage enemy targets with means of JFSP (targeting and engaging MFA, UAVs, etc.); ability to assess the results of damage inflicted on enemy targets (photo and video recording).

The capabilities of military aviation units, MFA, strike unmanned aerial vehicles (UAVs) and electronic warfare units should be understood as a set of quantitative and qualitative indicators that characterize the ability of a military unit (subunit) to perform specific tasks to engage the enemy with air strikes, missile strikes, strike UAVs, artillery

fire, suppression by electronic warfare means, and to manoeuvre within the established time frame in specific conditions.

At the same time, the combat capabilities of a military unit are a set of quantitative and qualitative indicators that characterize the potential combat capabilities of a military unit, provided that it is fully manned, trained and supplied with all types of resources.

The initial data for calculating the participation of aviation, MFA, strike UAVs, and electronic warfare units in the strike are:

the composition, position, and probable nature of the enemy's actions;

objective assessment of the enemy's grouping (critically important targets of the operational link);

the chosen method (order) of performing the assigned tasks of the JFS, suppression by electronic warfare means (construction of a concentrated fire strike),

the capabilities of aviation, MFA, strike UAVs and electronic warfare means to influence enemy targets.

When planning a strike, special attention is paid to ensuring the high effectiveness of the first launch of missiles and artillery fire for the reliable destruction of the most important objects of the enemy's troop control system and its air defense means in the areas of operation of strike aviation groups.

Therefore, it is necessary to consider the combat capabilities of aviation, MFA, strike UAVs and electronic warfare means and their impact on strike planning in the operation.

The combat capabilities of aviation are characterized by spatial, temporal and combat effectiveness indicators.

The spatial indicators of combat capabilities determine the maximum distance of lines, zones and boundaries of areas (districts) in which aviation units (formations, groupings) are capable of conducting combat operations.

Spatial indicators include:

tactical radius, which is the maximum distance from the base airfield that aviation can travel to perform a combat mission and return to the departure airfield. The tactical radius depends on fuel reserves, combat load, group composition, the nature of the combat mission, meteorological conditions and the choice of the optimal flight mode;

the combat zone, which is limited by near, far and lateral boundaries;

the depth of combat operations is the size of the space above enemy territory in which aircraft are capable of striking the enemy and depends on the depth of basing and tactical radius.

Time indicators are:

mobility – the time required to complete a combat mission, calculated from the moment the combat mission is assigned (received) to the moment the strike is delivered (interception of an air target, transmission of reconnaissance data, etc.).

The time required to prepare for a repeat sortie directly affects mobility and the intensity of combat operations.

A quantitative indicator of the intensity of combat operations is combat stress – the number of aircraft sorties (helicopter sorties) that a unit (formation) performs during a certain period of time (day, night, 24 hours). The unit of combat stress is the norm of combat flights per crew, unit (part) per day.

According to [23], the Air Force of the Ground Forces is capable of striking small-sized moving and stationary ground targets in conditions of visual visibility and without it. Striking enemy targets with unguided aviation missiles (UAM) from horizontal flight is effective for striking linear, planar and group targets that are densely concentrated in the direction of the helicopter's flight. Firing from horizontal flight at extremely low altitudes (25-100 m) is performed on open stationary targets located on relatively flat terrain.

In conditions of saturation of the combat zone with enemy air defense systems, the use of UAM is carried out in the ‘climb’ mode (from a hover) from extremely low altitudes without leaving or with a short-term entry into the zone of action of enemy anti-aircraft missile systems.

The combat capabilities of the MFA are determined by its firepower, depth of destruction, manoeuvrability, readiness time for fire missions, and capabilities for reconnaissance of enemy targets [24, 25].

Let us consider the combat capabilities of missile forces, which are characterized by: the number of targets that can be struck simultaneously; the degree of damage inflicted; the depth of damage; the time required to prepare for a strike; and manoeuvrability.

During the Russian-Ukrainian war, the transition of missile forces and artillery units to new types of weapons significantly changed the capabilities of missile units to destroy enemy targets. This is

primarily due to new missile systems and types of missiles (with their performance characteristics) and, accordingly, the capabilities of a single combined launch by a missile (reactive artillery) brigade (division). At the same time, weapons that were in service before the war continue to be used.

When determining the number of targets that can be hit by a single launch of a missile brigade (division), it is necessary to take into account the number of launchers in them and the operational rate of missile consumption per target.

Analysis [26] shows that the operational rate of missile consumption is 2–4 missiles per target, depending on the launch task and the accuracy of determining its location.

The time required to prepare for the execution of tasks of JFSP depends on the condition, location and readiness of the strike assets, as well as the missiles. The manoeuvrability of missile and rocket brigades is determined by their ability to move and deploy into combat formation.

Thus, taking into account the combat capabilities of missile forces, planning their participation in CFS must be carried out in two stages – the stage of preparation for the strike and the stage of the strike itself.

The firepower of artillery is characterized by the scope of tasks and measured by the number of enemy targets that an artillery unit (subunit) can destroy, ruin or suppress with a given degree of damage in specific conditions.

When planning the use of artillery to inflict damage, in accordance with current guidelines (manuals).

A decisive factor that determines the minimum and maximum sizes of group targets that can be destroyed with the required degree of damage and a specified number of guns, mortars, and multiple launch rocket systems is the parameters of the projectiles that destroy them.

The established norms are currently based purely on mathematical calculations under classic conditions of warfare and troop tactics.

Due to the significantly developed capabilities of round-the-clock reconnaissance at all tactical depths and changes in the tactics of artillery units (by gun, by platoon on a large front), the ability to provide the necessary fire density during combat in a limited time is limited. At the same time, the probability of hitting targets under observation has increased to 70%, including with the use of high-precision shells such as Excalibur, Bonus, Smart, and Copperhead.

It is particularly important to take into account the accuracy of determining the coordinates of targets. The requirements for the accuracy of determining the coordinates of targets are determined by the mean circular error, which should not exceed 30-60 m for rifled artillery and 70-80 m for rocket artillery.

The depth of artillery strikes is determined depending on the tactical and technical characteristics of the weapons, the depth of the unit location in the operational structure, and the available ammunition and charges for them.

The time required for artillery to be ready to perform its tasks of JFSP in a strike depends on the type of artillery unit weapons and the readiness of the firing positions.

The combat capabilities of UAVs are characterized by spatial and temporal indicators and indicators of combat effectiveness.

The spatial characteristics of externally piloted UAVs include the tactical radius, which is the maximum distance from the base airfield that a UAV can travel to perform a combat mission and return to the departure airfield. The tactical radius depends on fuel reserves, combat load, group composition, the nature of the combat mission, meteorological conditions, and the choice of the optimal flight mode.

The type of strike UAV and the type of onboard weapon are selected when planning combat operations based on the characteristics of the target, the time of day specified for the strike (day, night), the distance to the target, etc.

Their use must be synchronized with the use of aviation, MFA, electronic warfare and air defense systems.

The combat actions of strike UAV units to destroy the enemy are primarily focused on the tactical and operational levels of warfare, targeting the enemy forces and assets and the infrastructure that directly supports them, and may indirectly lead to strategic consequences by eliminating the enemy ability to pursue its strategy of fighting with ground forces. Reconnaissance and strike unmanned aerial systems, strike UAVs, and “loitering munition” type UAVs are designed to engage enemy troops, ground (sea) targets, mainly small and mobile targets, primarily at the front line of defense, in tactical and immediate operational depth, as well as for aerial mining.

At the same time, the use of aviation units and strike UAVs will be heavily dependent on meteorological conditions. This dependence will be

linked not only to weather conditions in the vicinity of airfields (launch sites) but also in the vicinity of targets (for certain categories of aviation munitions and types of strike UAVs).

The special capabilities of electronic warfare (EW) assets are characterized by the number of intelligence sources detected per hour, the number of targets that can be simultaneously suppressed, the maximum range of EW assets, and the number of objects and troops protected from high-precision weapons strikes.

When preparing a strike, air reconnaissance, artillery reconnaissance and electronic reconnaissance forces and means must be focused on reconnaissance, refinement (additional reconnaissance) and constant monitoring of targets.

Thus, the combat capabilities of aviation, MFA, strike UAVs and electronic warfare means allow for the reasonable planning of the stages of preparation for and delivery of JFSP in Defense Forces operations.

4. Commander's decision and assignment (phase 4).

This phase involves developing a schedule for preparing and conducting CFS using the forces and resources of JFSP, including a list of targets to be struck and directive documents that will convey combat missions to subordinate units (subdivisions).

The CFS schedule should contain information on:

the goals and tasks to be performed by the forces and means of JFSP during the CFS operation;

the composition of the forces and means involved in the preparation and conduct of the CFS operation;

the list of targets;

the distribution the forces and means of reconnaissance forces, taking into account their capabilities for reconnaissance and further reconnaissance of the location of targets;

the distribution of CFS (lethal and non-lethal) among targets, taking into account the priority of targets and the capabilities of firepower;

the option for constructing the CFS (graphical representation of the option for the actions of the forces and means of the JFSP distributed in time (operational and astronomical time scale) according to combat control signals during the preparation and delivery of the CFS at the time of launch (time 'P') determined by the head of the JFSP center, according to the signal (time 'C') or from the time of explosion (time 'B') of missiles, aerial bombs, and ammunition in the areas of targets being struck).

When constructing the CFS schedule, the JFSP center decides how best to synchronize actions in order to generate the greatest effect by using available resources or to achieve the required effect with the least expenditure. In doing so, the following tasks are solved:

Synchronization is the establishment of a sequence of actions and corresponding effects (impacts) in time, space and purpose in order to achieve decisive conditions. Thus, the JFSP centre establishes the comprehensive use of all available capabilities to achieve (create) decisive conditions. The main advantage of synchronized actions is the ability to achieve synergy from the use of different resources and to strengthen levers of influence by creating effects and using them throughout the entire area of operations.

Synergy is the ultimate goal of all synchronization efforts. Synergy is the cumulative result or outcome of individual actions; it is greater than the sum of the results of the individual parts if they act individually (not synchronized). Synergy is the result of effective synchronization. In practice, this means integrating and synchronizing actions aimed at achieving a goal (completing a task). This approach is also closely linked to the idea of a comprehensive approach.

Leverage is used when the impact of an action is greater in proportion to the effort expended. Leverage can be achieved by focusing the strengths of combined forces against the weaknesses of the enemy in order to achieve decisive conditions. Other instruments of power may also be used as part of a comprehensive approach.

When developing a CFS, it is essential to consider:

a) the priority of targets;

b) the numbers and names of targets;

c) who, when and where each target is identified;

d) who, when, how and with what effect each target is struck;

e) who determines the results of the strike.

At the same time, the distribution of reconnaissance and firepower resources should be carried out on the basis of an existing mathematical method that takes into account the capabilities of the components of the JFSP process as much as possible, and in general, the selection of one option from a certain set of options that will best ensure the

achievement of the specified goal of its implementation.

Taking into account the above and considering the composition of reconnaissance and firepower assets that can be used in the preparation and delivery of CFS, we can conclude that these assets are heterogeneous, have different capabilities, and averaging them into a single type will lead to large errors in calculations. Therefore, the most appropriate method for distributing reconnaissance and firepower assets is the two-function method.

In general, the essence of the two-function method is to find an assignment matrix $\left\|\vartheta_{kl}^{0}\right\|_{NS}$, that maximizes the objective function F [27, 28]:

$$F = F(\vartheta) = \sum_{l=1}^{S} \Theta_l \left(1 - \prod_{k=1}^{N} \varepsilon_{kl}\right),$$

where l – target number indicator $(1 \ldots S)$;

k – specific type of means number indicator $(1 \ldots N)$;

S– number of targets;

N – number of types of means;

Θ – importance coefficient of a specific type of target;

ω – probability of impact on the t arget;

ε – probability of the opposite event(no impact on the target);

ϑ – indicator of the assignment of a specific type of sample to a specific target;

F – target function (degree of implementation) of the capabilities of firepower against enemy objects (targets), which can be achieved by distributing them among targets, $0 \le F \le 1$).

with certain restrictions:

$$\sum_{l=1}^{S} \vartheta_{kl} = 1, \quad k = 1 \ldots N$$

And under additional conditions:

$$\left.\begin{array}{l} \vartheta_{kl} \in \{1;0\}, \\ 1 \ge (\varepsilon_{kl} = 1 - \omega_{kl}) \ge 0, \\ \Theta > 0 \end{array}\right\} \quad \begin{array}{l} k = 1 \ldots N, \\ l = 1 \ldots S. \end{array}$$

Therefore, given a certain number of different types of active agents $k = 1 \ldots N$ each of them, when acting on l-th object (target) ($l = 1 \ldots S$) with its relative weight (importance) Θ_l affects with a probability of ω_{kl}. It is necessary to make such a distribution that the target effect will reach its maximum value. At the same time, at each t step of the calculations, the fact of assigning a certain type of agent to a certain target is recorded with an indicator $\vartheta_{kl} = 1$ ($\vartheta_{kl} = 0$ – in case of non-assignment). The decision is recorded in the form of a chain of calculations or by forming a matrix of assignments $\left\|\vartheta_{kl}^{0}\right\|_{NS}$. However, under such conditions, the maximum value of the target function F takes on any positive value and is only informative.

If the weight of the entire set of objectives $\sum_{l=1}^{S} \Theta_l = 1$ [28], it can be assumed that the objective function F, which is achieved by determining the maximum element $\max \Delta_{kl}$ of the resource allocation matrix at each step, taking into account both the gain Δ_{kl}^{+} in the case of assigning k resource to l objective, and the loss Δ_{kl}^{-} in the case of not assigning k resource to a specific target, will express the degree of firepower impact on enemy targets that needs to be achieved. In addition, this approach will make it possible, provided that $F^{(t)} \ge F_{\text{заданого}}^{(t)}$, to determine the degree of impact on enemy targets (objectives) achieved through the allocation of appropriate resources, i.e. to ascertain the achievability of the established degree of impact on enemy targets with the available quantity of certain types of appropriate resources.

The completion of the work of the JFSP centre at this stage is the approval of the Schedule for the preparation and tasks of the CFS and orders to the JFSP forces and means involved in the preparation and conduct of the CFS.

5. Direct planning and execution (phase 5).

The execution of strike missions is a cyclical process of dynamic targeting, which includes the following stages (F2T2EA) [19, 29]:

1. find, which includes reconnaissance and detection;

2. fix, which includes positive identification, determination of exact coordinates and available time;

3. track, which includes prioritizing reconnaissance data, tracking the object and updating its vulnerability data;

4. target, which includes target confirmation, decisions on the use of firepower, requirements for assessment and determination of collateral damage;

5. engage, which involves executing the order to engage the target and controlling and conducting the operation;

6. assess, which includes evaluating the results of the fire and reporting to the senior commander with recommendations for possible re-engagement.

During this stage, it is recommended that officials at the JFSP center re-prioritize the engagement of enemy targets within the area of responsibility of the operational group of troops (forces), taking into account the collection, processing and analysis of situation data.

Based on the results of the re-prioritization, the enemy objects and the sequence of their destruction are specified, with subsequent communication of the specified tasks to the subordinate forces and means of the JFSP, which are involved in the application of the CFS. Therefore, in the process of performing dynamic target identification, it is recommended to use software tools that will allow increasing the efficiency of decision-making by the officials responsible for this.

Phase 5 is considered completed when the planned CFS is delivered (applied).

6. Evaluation of the results of the CFS (phase 6).

The evaluation of the results of the CFS is the final in this cyclical process, during which an assessment of the complex of measures that took place during the five previous phases is carried out. The process of evaluating the definition of targets, taking into account their priority, makes it possible to determine whether the goal of implementing fire impact on the enemy has been achieved, taking into account the created effects.

The results of phase 6 are an assessment of combat losses, an assessment of the effectiveness of ammunition, an assessment of associated losses and recommendations for a second strike. Based on the analysis of the assessment of the implementation of fire impact on the enemy, an assessment of the effects of combined fire support is also carried out, not only the physical and functional effect, but also the operational one, with an accompanying psychological effect. In the absence of the desired effects, probable causes are considered and proposals are made to the commander based on the initial data on the implementation of fire impact on the enemy, namely: if it is not possible to suppress a critical object due to the fact that certain conditions for its operation were not taken into account, certain actions are prepared to prohibit action in accordance with its functional purpose for a certain period of time; or if in certain directions it is not possible to achieve the effect of hindering movement, perhaps a more rational solution would be to remotely lay a minefield in order to hinder the enemy's maneuver.

Phase 6 is considered completed when the commander provides a report on the results of the CFS.

Conclusions and prospects for further research. Thus, the article improves the methodology for planning a concentrated fire strike when planning joint fire support in modern armed conflicts. The improved methodology meets the requirements of doctrinal documents of NATO member states, allows for more effective planning and delivery of CFS to enemy targets in accordance with the defined purpose of the CFS in operations. Also, the use of the nonlinear programming method – the "two-function" method at the stage of assigning the appropriate reconnaissance and fire impact means allows for the most effective use of the capabilities of the available forces and means of JFSP, and reducing the total weight of enemy targets accepted in the CFS to one allows for an assessment of the possible effectiveness of the CFS at the planning stage.

Further areas of research are proposed to develop a work schedule for officials of the JFSP center for the preparation and delivery of CFS in operations, which will allow for streamlining their activities and substantiating certain recommendations. In addition, the possibility of implementing this methodology in software solutions will allow automating the activities of officials of the JFSP center and reducing the time for management decisions.

References

1. Semenenko O., Mytchenko S., Dobrovolskyi Yu., Remez A., Yarmolchyk M., Tverdokhlib Yu. (2024). *Evoliutsiia form i sposobiv zastosuvannia uhrupovan viisk (syl): tendentsii zbroinoi borotby* [Evolution of forms and methods of using cluster weapons (syl): tendencies of armed conflict Evolution of forms and methods of using cluster weapons (syl): tendencies of armed conflict]. *Sotsialnyi rozvytok i bezpeka*, vol. 14, pp. 33–52. DOI: https://doi.org/10.33445/sds.2024.14.3.3 [in Ukrainian].

2. Zahorka O. M., Polishchuk S. V., Uvarova T. V., Zahorka I. O. (2024). *Peredbachennia zastosuvannia protyvnykom form voiennykh dii pid chas stratehichnoho planuvannia rozvytku zbroinykh syl* [Consideration of the use of military forms by the enemy during the strategic planning of the development of the armed forces]. *Zbirnyk naukovykh prats Tsentru voienno-stratehichnykh doslidzhen Natsionalnoho universytetu oborony Ukrainy,* vol. 1 (80), pp. 6–12. DOI: https://doi.org/10.33099/2304-2745/2024-1-80/6-12 [in Ukrainian].

3. Semenenko O., Koval V., Vodchyts O., Dobrovolskyi Yu. (2024). *Multydomenna operatsiia – suchasnyi pohliad na adaptatsiiu form i sposobiv voiennykh dii do transformatsii seredovyshcha vyklykiv ta zahroz* [Multi-domain operations – a contemporary view on the adaptation of forms and methods of military action to the transformation of the environment of threats and challenges]. *Mizhnarodnyi naukovyi zhurnal "Military Science"*, vol. 2 (1), pp. 17–34. DOI: https://doi.org/10.62524/msj.2024.2.1.02 [in Ukrainian].

4. Khimchenko O. (2021). *Metodychnyi pidkhid shchodo otsinky mozhlyvostei protyvnyka z urazhennia vazhlyvykh obiektiv boiovoho potentsialu zbroinykh syl i voienno ekonomichnoho potentsialu derzhavy* [Methodological approach to estimating the enemy's ability to strike important objectives of the combat potential of the armed forces and the military-economic potential of the state]. Proceedings of the interdepartmental scientific-practical conference *"Uroky zbroinoi ahresii Rosii proty Ukrainy – voienno-stratehichni aspekty"* (Kyiv, April 29, 2021). Kyiv : NUOU im. I. Cherniakhovskoho, pp. 116–121 [in Ukrainian].

5. Horbulin V. (2020). *Yak peremohty Rosiiu u viini maibutnoho* [How Russia won the victory in the war of the future]. Kyiv : Brait Buks [in Ukrainian].

6. Zhyvotovskyi R. M., Horobets Yu. O. (2016). *Analiz sposobiv zastosuvannia bezpilotnykh aviatsiinykh kompleksiv* [Analysis of methods for using unmanned aerial vehicles]. *Systemy ozbroiennia i viiskova tekhnika*, vol. 4 (48), pp. 16–21 [in Ukrainian].

7. Semenenko, O., Ostrovskyi, S., Movchan, A., Melnychenko, A., Stolinets, S., & Petrenko, S. (2024). The role and place of swarms of unmanned systems in operations (combat operations) and options for their use. *Social Development and Security*, no. 14 (5), pp. 75–86. DOI: https://doi.org/10.33445/sds.2024.14.5.7 [in English].

8. Repilo Yu., Holovchenko O., Riman O. (2023). *Metodyka vyznachennia priorytetnosti raketnykh ta artyleriiskykh pidrozdiliv dlia yikh osnashchennia bezpilotnymy systemamy* [Methodology for determining the priority of missile and artillery divisions for their equipment with unmanned systems]. *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony,* vol. 47 (2), pp. 55–66. DOI: https://doi.org/10.33099/2311-7249/2023-47-2-55-66 [in Ukrainian].

9. Horbenko V., Kireienko V. (2024). *Metodyka vyznachennia vazhlyvosti obiektiv protypovitrianoi oborony v protsesi planuvannia operatsii z vykorystanniam metodu faktornoho analizu* [Methodology for determining the importance of anti-aircraft defense objectives in the process of planning operations using the factor analysis method]. *Povitriana mits Ukrainy*, vol. 2 (7), pp. 36–42. DOI: https://doi.org/10.33099/2786-7714-2024-2-7-36-42 [in Ukrainian].

10. Zvyhlianych S., Orlov S., Balabukha O., Kolomiitsev O., Openko P. (2022). *Propozytsii shchodo vyboru kombinatsii nazemnykh obiektiv protyvnyka, shcho vrazhaiutsia pry planuvanni vohnevykh udariv z urakhuvanniam potochnoho stanu danykh obiektiv* [The proposal was to select a combination of enemy ground targets, which would be considered when planning fire strikes, taking into account the current state of these targets]. *Zbirnyk naukovykh prats Derzhavnoho naukovo-doslidnoho instytutu vyprobuvan i sertyfikatsii ozbroiennia ta viiskovoi tekhniky*, vol. 11 (1), pp. 47–54. DOI: https://doi.org/10.37701/dndivsovt.11.2022.06 [in Ukrainian].

11. Horbenko V. M., Korshets O. A., Kuvshynov O. V. (2021). *Otsiniuvannia variantiv rozpodilu zavdan v spilnii aviatsiinii hrupi*

pilotovanoi ta bezpilotnoi aviatsii [Evaluation of the distribution options is a task in the general aviation group of piloted and unmanned aviation]. *Systemy ozbroiennia i viiskova tekhnika*, vol. 4 (68), pp. 14–20. DOI: https://doi.org/10.30748/soivt.2021.68.02 [in Ukrainian].

12. Hrabchak V. I., Suprun V. M., Bystryk Yu. S. (2014). *Matematychna model optymalnoho rozpodilu zasobiv urazhennia* [Mathematical model of optimal distribution of attractive insults]. *Viiskovo-tekhnichnyi zbirnyk*, vol. 1 (10), pp. 16–23 [in Ukrainian].

13. Zalivan O. V., Zaika V. F., Taran I. A. (2006). *Ratsionalnyi rozpodil zasobiv vyiavlennia ta vohnevoho urazhennia mizh obiektamy na poli boiu* [Rational distribution of the effect of the detection of fire damage between objects on the battlefield]. *Systemy ozbroiennia i viiskova tekhnika*, vol. 2 (6), pp. 53–55 [in Ukrainian].

14. Maistrenko, O., Khoma, V., Lykholot, O. et al. (2021). Devising a procedure for justifying the need for samples of weapons and weapon target assignment when using a reconnaissance firing system. *Eastern-European Journal of Enterprise Technologies,* vol. 5, no. 3 (113), pp. 65–74. DOI: https://doi.org/10.15587/1729-4061.2021.241616 [in English].

15. Joint Fires and Targeting Handbook. United States Joint Forces Command. (2007, October 19) [in English].

16. Allied Joint Publication AJP-5, Edition A, Version 2, Allied Joint Doctrine for the Planning of Operations. (May 2019) [in English].

17. Holovanov A. V. (2021). *Planuvannia operatsii operatyvnoho uhrupovannia viisk za standartamy NATO* [Planning of operations of the operational group of units according to NATO standards]. Kyiv : NUOU im. Ivana Cherniakhovskoho [in Ukrainian].

18. FM 3-60. Army Targeting. Headquarters, Department of the Army. Washington, DC (2023, August 11) [in English].

19. ATP 3-60. Targeting. Headquarters, Department of the Army. Washington, DC (2015, May 7) [in English].

20. Repilo Yu., Prymirenko V., Demianiuk A. (2023). *Metodyka vyznachennia priorytetnosti obiektiv protyvnyka dlia pryiniattia yikh yak mozhlyvykh tsilei z metoiu vohnevoi pidtrymky z vykorystanniam matrytsi CARVER* [Methodology for prioritizing the opponent's objectives to achieve their possible goals using the method of fire support using the CARVER matrix]. *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony*, vol. 47 (2), pp. 155–166. DOI: https://doi.org/10.33099/2311-7249/2023-47-2-155-166 [in Ukrainian].

21. Skliar O. V. (2025). *Udoskonalena metodyka otsiniuvannia vohnevykh mozhlyvostei viiskovykh chastyn ta pidrozdiliv viisk protypovitrianoi oborony Sukhoputnykh viisk* [Improved methodology for estimating the potential of aircraft parts and classifying aircraft for anti-aircraft defense Land aircraft]. *Povitriana mits Ukrainy,* vol. 1 (8), pp. 23–29. DOI: https://doi.org/10.33099/2786-7714- 2025-1-8-23-29 [in Ukrainian].

22. Holovchenko O., Shevtsov R., Lykholot O., Kislov M., Potapov M., Stoliaruk V. (2025). *Metodyka otsiniuvannia vohnevykh mozhlyvostei viiskovykh formuvan artylerii sukhoputnykh viisk zbroinykh syl rosiiskoi federatsii v operatsii (boiu)* [Methodology for assessing the potential of artillery formations of ground forces of the russian federation in operation (combat)]. *Collection of Scientific Papers "ΛΟΓΟΣ"* (2025, May 9; Cambridge, UK), pp. 198–210. DOI: https://doi.org/10.36074/logos-09.05.2025.038 [in Ukrainian].

23. DNDI aviatsii (2024). *Analiz efektyvnosti zastosuvannia aviatsiieiu nekerovanykh aviatsiinykh raket (informatsiino-analitychni materialy)* [Analysis of the effectiveness of the use of aviation unmanned aircraft missiles (information and analytical materials). Kyiv [in Ukrainian].

24. NDTs RViA (2020). *Boiovyi statut artylerii Sukhoputnykh viisk Zbroinykh Syl Ukrainy (bryhada (polk), bryhadna artyleriiska hrupa). Chastyna 1* [Combat status of artillery of the Land Forces of the Armed Forces of Ukraine (bryhada (regiment), bryhadna artilleriiska hrupa). Kyiv [in Ukrainian].

25. KSV (2017). *Boiovyi statut raketnykh viisk Sukhoputnykh viisk Zbroinykh Syl Ukrainy. Raketna bryhada, reaktyvnyi artyleriiskyi polk (dyvizion, batareia)* [Combat status of rocket forces of the Ground Forces of the Armed Forces of Ukraine. Rocket brigade, reactive artillery regiment (division, battery). Kyiv [in Ukrainian].

26. KSV (2021). *Nastanova z pidhotovky raketnykh viisk Sukhoputnykh viisk ZS Ukrainy (bryhada (reaktyvna artyleriiska bryhada), dyvizion, batareia, viddilennia, vzvod, obsluha)* [Arrangement of the missile installations of the Land Forces of Ukraine (brigade (reactive artillery brigade), division, battery, divisions, platoon, service). Kyiv [in Ukrainian].

27. Permiakov Yu., Atrokhov A. (2005). *Osnovy modeliuvannia boiovykh dii viisk* [Basics of modeling combat vehicles]. Kyiv : NAOU [in Ukrainian].

28. Maistrenko, O., Khoma, V., Lykholot, O. et al. (2021). Devising a procedure for justifying the need for samples of weapons and weapon target assignment when using a reconnaissance firing system. *Eastern-European Journal of Enterprise Technologies*, vol. 5, no. 3 (113), pp. 65–74. DOI: https://doi.org/10.15587/1729-4061.2021.241616 [in English].

29. Riman O., Holovchenko O., Shevtsov R., Ishchenko O., Lykholot O., Rodionov E. (2024). *Pidvyshchennia rezultatyvnosti vohnevoi pidtrymky raketnymy viiskamy i artyleriieiu v operatsiiakh (diiakh) za rakhunok vprovadzhennia tsyklu tarhetuvannia u protses operatyvnoho planuvannia* [Increasing the effectiveness of fire support by rocket launchers and artillery in operations (divisions) due to the introduction of the targeting cycle in the process of operational planning]. *Grail of Science*, no. 35, pp. 114–121. DOI: https://doi.org/10.36074/grail-of-science.19.01.2024.019 [in Ukrainian].

Received / Стаття надійшла до редакції: 08.09.2025
Revised / Прорецензовано: 23.09.2025
Accepted / Схвалено до друку: 25.09.2025

ЛИХОЛЬОТ ОЛЕКСАНДР ВІКТОРОВИЧ
доктор філософії,
професор кафедри ракетних військ і артилерії,
Національний університет оборони України
https://orcid.org/0000-0003-3418-9529

ГОЛОВЧЕНКО ОЛЕГ ВОЛОДИМИРОВИЧ
доктор філософії,
професор кафедри ракетних військ і артилерії,
Національний університет оборони України
https://orcid.org/0000-0003-3715-7872

ДЕМ'ЯНЮК АНДРІЙ ВОЛОДИМИРОВИЧ
доктор філософії,
доцент кафедри ракетних військ і артилерії,
Національний університет оборони України
https://orcid.org/0000-0003-0961-4431

МЕТОДИКА ПЛАНУВАННЯ ЗОСЕРЕДЖЕНОГО ВОГНЕВОГО УДАРУ ПІД ЧАС ПЛАНУВАННЯ ОБ'ЄДНАНОЇ ВОГНЕВОЇ ПІДТРИМКИ У СУЧАСНИХ ЗБРОЙНИХ КОНФЛІКТАХ

Удосконалено методику планування зосередженого вогневого удару внаслідок застосування циклу об'єднаного таргетування. Використання методології визначення центру тяжіння противника для певної вирішальної умови дає змогу виділити групу критичних об'єктів ураження, які належать до центру тяжіння, і таким чином значно підвищити ефективність зосередженого вогневого удару. Так само під час підготовки й завдавання удару завдяки вдосконаленим критеріям опису показників методології визначення пріоритетності об'єктів ураження можливо вибрати найбільш критичні об'єкти.

Застосування методу нелінійного програмування «двох функцій» на фазі призначення відповідних засобів дає змогу максимально ефективно використати можливості сил і засобів об'єднаної вогневої підтримки й на етапі планування здійснити оцінювання його можливої ефективності.

Ключові слова: *об'єднана вогнева підтримка; зосереджений вогневий удар; центр тяжіння; пріоритетність об'єктів ураження; можливості; метод двох функцій; таргетування.*

UDC 342.951:623.36 (477) DOI 10.59226/2786-6920.2.2025.125-131

MARCHENKO MAKSYM
Candidate of Juridical Sciences,
Doctoral Student,
Kharkiv National University of Internal Affairs
https://orcid.org/0009-0006-0078-8346

CONCEPT AND FEATURES OF THE LEGAL STATUS OF MINE ACTION OPERATORS IN UKRAINE

The article is devoted to defining the essence and features of the legal status of mine action operators in Ukraine. The concept of the "legal status of a mine action operator" is defined, as well as the mandatory condition for its acquisition – the presence of certified specialists, technical equipment, communication means, and a management system that confirm the operator's capacity to conduct mine action activities. It is established that a distinctive feature of the legal status of a mine action operator is the execution of strictly certified processes, which represent the practical aspects of his activity, rather than governmental powers. It has been clarified that not only obtaining certification, but also concluding liability insurance contracts for potential harm to the environment and/or the health and property of third parties, is a mandatory condition for a mine action operator to carry out their activities.

Keywords: *legal status, mine action, operator, certification, monitoring, humanitarian demining, explosive devices, mine action measures.*

Statement of the problem. The armed aggression of the Russian Federation against Ukraine has brought the issue of mine action safety into sharp focus, which has now become extremely urgent. Today, Ukraine is one of the most heavily mined countries in the world, creating a significant threat to the lives and health of civilians, complicating socio-economic recovery, and return to peaceful life. Under such conditions, the effective functioning of the mine action system becomes a key instrument for the sustainable development of affected territories.

As of June 2022, the area of territories in Ukraine potentially contaminated with explosive devices exceeded 174,000 km² – nearly 25% of the country's total area. By the end of 2024, thanks to the efforts of Ukrainian and international mine action operators, approximately 35,000 km² had been cleared [1, p. 14]. It is precisely the mine action operators who play the primary role in the practical implementation of mine action measures. However, the legal definition of the concept "mine action operator," as well as their status, powers, rights, and responsibilities, remains insufficiently regulated, creating difficulties in coordinating actions, monitoring the quality of work, licensing, involvement of international assistance, and ensuring personnel safety. Therefore, studying the concept and status of mine action operators is important from the perspective of administrative law and for the development of an effective, safe, and transparent mine action system in Ukraine.

Analysis of recent research and publications. The issue of the legal status of mine action operators has so far not received adequate attention in Ukrainian legal scholarship. In the scientific literature, this topic has been studied only fragmentarily, which creates a need for its

comprehensive analysis. Among the few studies, particular attention should be given to the work of O. M. Botnarenko, who analyzes specific elements of the legal status of mine action entities, in particular operators, focusing on their powers [2]. In turn, O. A. Boiko, P. I. Haman, and S. I. Pavlov concentrate on the procedural aspects of acquiring, suspending, and terminating the legal status of mine action operators [3].

However, these studies are isolated and do not form a cohesive scientific basis for understanding the legal nature of mine action operators. This further highlights the gap in the scholarly examination of the legal aspects of mine action and underscores the relevance of further theoretical development of the concept and features of the legal status of such entities.

The purpose of the article is to define the concept and features of the legal status of mine action operators in Ukraine.

Presentation of the main material. The national standards of Ukraine describe mine action as "activities aimed at reducing the social, economic, and environmental impact of explosive ordnance" [4]. Similarly, the concept of "mine action" and the list of mine action entities are defined by the Law of Ukraine "On Mine Action" dated December 6, 2018, No. 2642-VIII. According to Part 2 of Article 6 of this Law, one of the entities of mine action is the mine action operator. The latter is understood by the legislator as authorized divisions of central executive authorities, enterprises, institutions, and organizations regardless of ownership form, including international and foreign entities involved in conducting mine action measures [5]. This allows us to conclude that the primary legislative act defining the legal status of a mine action operator in Ukraine is the Law "On Mine Action."

It should be noted that, according to the legislative definition, "mine action operators" are exclusively legal entities. In legal doctrine, the legal status of a legal entity is generally understood as the position established by law, encompassing its set of rights and obligations. The legal status includes the following elements: 1) legal personality; 2) rights and obligations established by law; 3) guarantees of established rights; 4) the entity's liability for failure to fulfill obligations [6].

According to Article 28 of the Law of Ukraine "On Mine Action," mine action operators, as performers of mine action measures, acquire their status from the moment they receive a certificate of compliance for the mine action processes they conduct, in accordance with current legislation [5].

Currently, the procedure for obtaining a certificate by mine action operators is regulated by the Resolution of the Cabinet of Ministers of Ukraine dated February 2, 2024, No. 123, "On Approval of the Procedure for Implementing an Experimental Project on the Certification of Mine Action Operators and Mine Action Processes." The aim of the experimental project is to establish a unified approach to the certification of mine action operators and mine action processes by introducing, for the duration of the project, a procedure for issuing certificates of compliance to operators. According to this procedure, in order to undergo certification (initial or repeated), a mine action operator must submit an application to the certification authority in the state language. If the applicant does not have the right to the status of a mine action operator under Part 3 of Article 28 of the Law of Ukraine "On Mine Action," the certification authority denies consideration of the application and notifies the applicant via email or the Diia Portal within two working days. If there are no grounds for refusal, the certification authority initiates the procedure for initial certification [7].

It should be noted that the initial certification procedure for a mine action operator includes four stages: 1) organizational stage – verification of the applicant's legal, financial, managerial, and quality capacities; 2) operational stage – assessment of technical and practical capabilities based on submitted documents; 3) on-site assessment –

confirmation of the applicant's compliance with standard procedures and legal requirements; 4) analysis and decision – independent expert evaluation of results, followed by a certification decision. In the case of a positive decision, a certification agreement is concluded within three working days, outlining the obligations of the parties and requirements for maintaining compliance during the validity of the certificate. The operator's status is granted from the moment the certificate is received for at least one of the declared processes, including: non-technical survey; technical survey; manual demining; mechanical demining; use of mine detection canine units; clearance of combat zones; demining of water bodies; neutralization (destruction) of mines/explosive remnants of war; and informing the population about risks associated with mines and explosive remnants of war. Legislation also allows for the expansion of the certification scope, i.e., the list of mine action processes covered by a compliance certificate may be supplemented with a new, separate mine action process [7].

Thus, a mine action operator carries out demining measures, and their competencies depend on their legal status, scope of activity, and the processes that have been certified. These activities represent practical aspects of the operator's work rather than governmental powers [2, p. 701].

The list of entities that have acquired the status of mine action operators is maintained by the National Mine Action Authority in accordance with the procedure approved by the Resolution of the Cabinet of Ministers of Ukraine dated November 3, 2021, No 1150. As of June 2025, over 100 mine action operators have been certified in Ukraine. This significant number of operators indicates the creation of a demining market in Ukraine, the involvement of international organizations, and the broad development of government operators' mine action capacities [1, p. 48].

According to the national standard DSTU 8820-3:2024 "Mine Action. Management Processes. Part 3. Information Management System," mine action operators are the main entities of mine action responsible for collecting and consolidating data. They collect, verify, and timely submit information regarding the implementation of mine action measures to the Mine Action Center (hereinafter – MAC) or the Humanitarian Demining Center (hereinafter – HDC). Typically, they are the primary source of data on the execution of mine action measures and perform the following activities: 1) collect reliable data during their operations and provide it promptly to the MAC/HDC according to established requirements;

2) manage data and information related to the organization's operations, ensuring their preservation. To carry out information management activities in mine action, the mine action operator also designates a responsible person and ensures their access to the necessary resources and professional training [8].

It should be noted that the MAC develops an Instruction on Planning the Implementation of Mine Action Processes by Certified Operators of Mine Actions. This instruction provides certified operators of mine actions with guidance on internal planning procedures, organization, and coordination of their activities, as well as on preparing and submitting applications to start or continue mine action processes in territorial communities in de-occupied areas of Ukraine.

After completing certification of mine action processes and obtaining the certificate, the operator of mine actions sends an official letter to the MAC indicating readiness to perform the certified mine action processes. The second stage involves obtaining approval from territorial communities for conducting mine action processes through the Secretariat of the National Mine Action Authority. At this stage, the MAC conducts a detailed analysis and plans the implementation of processes, taking into account the declared capacities of the mine action operator and the needs of territorial communities.

Subsequently, the mine action operator submits an application to the MAC to obtain an order from the MAC Head for the organization of humanitarian demining processes no later than 10 calendar days before the day on which the mine action operator intends to start the relevant processes. The mine action operator also organizes interaction with local authorities and self-governance bodies. According to DSTU 8820:2023 "Mine Action. Management Processes. Basic Provisions," no later than 10 calendar days before the day on which he intends to begin the implementation of mine action processes in the territory of the relevant united territorial community, sends a notification to the address of such community and regional military administration about the start of the implementation of such processes in order to ensure the participation of citizens at the relevant stages of their implementation. If the mine action operator cannot conduct mine action processes due to a security situation, he must notify the MAC in writing, which then redistributes territories and issues a new order for organizing humanitarian demining. This order, issued by the MAC no later than seven working days from the receipt of the application, specifies the personnel involved, equipment, interaction procedures with other mine action entities, geographic information on the location of operations, timelines, and reporting procedures. After receiving the MAC Head's order, the mine action operator begins activities not earlier and not later than the date indicated in the order. During operations, the mine action operator conducts daily detailed planning, organization, coordination, and analysis of mine action measures, improving management aimed at achieving the final result, in accordance with the certified processes [9]. It should be noted that, in addition to obtaining the certificate and the MAC Head's order, the mine action operator before the mine action process must also conclude liability insurance for potential damage to the environment and/or the health and property of third parties, under insurance class 13 as defined in Article 4 of the Law of Ukraine "On Insurance" dated November 18, 2021, No. 1909-IX (Article 31 of the Law of Ukraine "On Mine Action") [5].

As of today, 101 mine action operators are active in Ukraine, of which 93 are domestic companies or structures and 8 are foreign representations. Thirty-two operators belong to state structures, including emergency rescue units of the State Emergency Service, military units of the State Special Transport Service, and the Armed Forces of Ukraine [3, p. 5]. Besides state bodies, non-state operators play an important role in humanitarian demining. These are categorized as: 1) commercial organizations (LLC) that operate for profit and are often involved in fulfilling state contracts; 2) local non-profit organizations – public organizations and charitable foundations conducting mine action through grant support or international donor funds; 3) international non-profit organizations – such as HALO Trust, Danish Refugee Council (DRC), Norwegian People's Aid (NPA), Mines Advisory Group (MAG), etc., implementing humanitarian mine action projects in the spere of mine actions with international funding [1, p. 19].

Although various entities can serve as mine action operators, there are certain specific restrictions on how they conduct activities. In particular, non-governmental mine action operators are prohibited from carrying out humanitarian demining on the areas within 20 km of the line of contact and/or the state border [3]. At the same time, it should be noted that the large number of state and non-state mine action operators complicates effective planning and task management. For example, there have been cases where non-state operators suspended work on areas that were subsequently cleared by state agencies, and vice versa – operators received typical demining assignments after the same territory had already been surveyed by rapid response units and all explosive devices removed. This highlights the need

for clear regulations regarding the coordination of demining processes [1, p. 54].

Legislation provides for monitoring mine action operators' compliance with certification requirements, as well as grounds for temporary suspension or revocation of a mine action operator's certificate. It should be noted that in May 2025, the Cabinet of Ministers of Ukraine amended Resolution No. 123 dated February 2, 2024. The updated Procedure for Maintaining the Register of Mine Action Operators introduces new grounds for suspending a certificate of compliance, for example, if a mine action operator do not perform the intended work for two years, the certificate may be suspended. A mechanism for unscheduled monitoring of operators has also been introduced in cases of: submission of an application by the operator to the certification authority (in paper or electronic form via the Diia Portal); notification of violations that threaten work quality, personnel safety, the environment, or the state; an incident involving explosive devices resulting in death or injury; identification of non-compliance during verification of DSTU 8820:2023 requirements; a legally binding court decision [5]. Thus, the process of regulatory development and improvement of the legal status of mine action operators in Ukraine remains dynamic, reflecting the need to to update it in accordance with adapt to practical requirements and security challenges in the field of mine action.

Conclusions and prospects for further research. Thus, the legal status of a mine action operator should be understood as the set of rights, obligations, requirements, and legal responsibilities established by national legislation, which collectively define the legal position of an entity authorized to carry out mine action measures. The key features of the legal status of a mine action operator can be summarized as follows: 1) conducting mine action activities solely on the basis of a certificate; 2) possessing certified specialists, technical equipment, communication means, and a quality management system in accordance with standards; 3) concluding liability insurance contracts for potential harm to the environment and/or the health and property of third parties before conducting certified processes; 4) exclusive rights to technical survey of territories, humanitarian demining, and destruction of explosive devices; 5) inability to conduct certified processes without interaction with the Mine Action Center, the Humanitarian Demining Center, local authorities, and self-government bodies; 6) obligation to adhere to principles of transparency and accountability, ensured through periodic monitoring of activities; 7) possibility of losing legal status and being held legally liable in the event of violations.

Given that the legal status of mine action operators is still evolving, it is advisable to amend the Law of Ukraine "On Mine Action" and related normative acts to ensure legal clarity regarding the competencies, guarantees, responsibilities, and other elements of the legal status of both state and non-state operators. Specifically, it is proposed that Article 28 of the law establish distinctions between state and non-state operators, define their rights, obligations, and limits of liability, and provide for the possibility of forming mixed teams of state and non-state operators to work in complex or hazardous territories with clearly defined distribution of authority.

Prospects for further research lie in the development of new proposals for improving the legal status of mine action operators and mechanisms for its practical implementation.

References

1. Yensen S., Klark E., Merion P., Zhuromska D., Hoch D., Kalinin R. (2025). *Bila knyha onovlennia instytutsiinoi arkhitektury protyminnoi diialnosti v Ukraini* [White Paper on the Renewal of the Institutional Architecture of Mine Action in Ukraine]. Instytut hlobalnykh zmin Toni Blera.

Retrieved from: https://surl.li/vnnqcx (accessed 2 August 2025) [in Ukrainian].

2. Botnarenko O. M. (2025). *Rozmezhuvannia povnovazhen u sferi protyminnoi diialnosti: subiekty, kompetentsii, problemy praktychnoi realizatsii* [Distribution of powers in the field of mine action: actors, competences, and problems of practical implementation]. *Natsionalni interesy Ukrainy,* no. 6 (11), pp. 692–703. DOI: https://doi.org/10.52058/3041-1793-2025-6(11)-692-703 [in Ukrainian].

3. Boiko O. A., Haman P. I., Pavlov S. I. (2025). *Humanitarne rozminuvannia v Ukraini: derzhavna polityka i derzhavne upravlinnia* [Humanitarian demining in Ukraine: state policy and public administration]. *Publichne upravlinnia i polityka,* no. 5 (9), pp. 1–12. DOI: https://doi.org/10.70651/3041-2498/2025.5.13 [in Ukrainian].

4. *DSTU 8820-1:2023. Protyminna diialnist. Protsesy upravlinnia. Chastyna 1. Systema upravlinnia yakistiu* [State Standard 8820-1:2023. Mine action. Management processes. Part 1. Quality management system]. (2024, March 1). Retrieved from: https://surl.li/kryamq (accessed 8 August 2025) [in Ukrainian].

5. *Zakon Ukrainy Pro protyminnu diialnist № 2642-VIII* [Law of Ukraine about the Mine Action activity no. 2642-VIII]. (2018, December 6). Retrieved from: https://surl.li/tqcsfs (accessed 2 August 2025) [in Ukrainian]

6. Parasiuk V. M., Parasiuk M. V. (2018). *Osoblyvosti pravosubiektnosti yurydychnoi osoby* [Features of the legal personality of a legal entity]. *Visegrad Journal on Human Rights*, no. 2, pp. 139–145 [in Ukrainian].

7. *Postanova Kabinetu Ministriv Ukrainy "Pro zatverdzhennia Poriadku realizatsii eksperymentalnoho proiektu shchodo sertyfikatsii operatoriv protyminnoi diialnosti ta protsesiv protyminnoi diialnosti" № 123* [Resolution of the Cabinet of Ministers of Ukraine "On the approval of the Procedure for the implementation of a pilot project on the certification of mine action operators and processes" activity no. 123]. (2024, February 2). Retrieved from: https://surl.li/rwlvtm (accessed 2 August 2025) [in Ukrainian].

8. *DSTU 8820-3:2024. Protyminna diialnist. Protsesy upravlinnia. Chastyna 3. Systema upravlinnia informatsiieiu* [State Standard 8820-3:2024. Mine Action. Management Processes. Part 3. Information Management System]. (2024, June 1). Retrieved from: https://surl.li/vgcvrv (accessed 3 August 2025) [in Ukrainian].

9. Tsentr protyminnoi diialnosti (2025). *Instruktsiia shchodo planuvannia vykonannia protsesiv protyminnoi diialnosti sertyfikovanymy operatoramy protyminnoi diialnosti* [Instruction on Planning the Implementation of Mine Action Processes by Certified Mine Action Operators]. (2025, February 3). Retrieved from: https://surl.li/jxnlem (accessed 2 August 2025) [in Ukrainian].

Received / Стаття надійшла до редакції: 05.08.2025
Revised / Прорецензовано: 25.08.2025
Accepted / Схвалено до друку: 29.08.2025

МАРЧЕНКО МАКСИМ ЮРІЙОВИЧ
кандидат юридичних наук, докторант,
Харківський національний університет внутрішніх справ
https://orcid.org/0009-0006-0078-8346

ПОНЯТТЯ ТА ОСОБЛИВОСТІ ПРАВОВОГО СТАТУСУ ОПЕРАТОРІВ ПРОТИМІННОЇ ДІЯЛЬНОСТІ В УКРАЇНІ

Визначено сутність та особливості правового статусу операторів протимінної діяльності в Україні. Сформульовано поняття «правовий статус оператора протимінної діяльності», а також обов'язкову умову його набуття – наявність сертифікованих фахівців, технічного обладнання, засобів зв'язку, системи управління, що підтверджує спроможність оператора здійснювати протимінну діяльність.

Установлено особливість правового статусу оператора протимінної діяльності, що полягає у здійсненні оператором суто сертифікованих процесів, що є практичними аспектами його діяльності, а не владними повноваженнями. З'ясовано, що не лише отримання сертифіката, а й укладення договору страхування відповідальності за шкоду, яку може бути завдано довкіллю та/або здоров'ю і майну третіх осіб, становить обов'язкову умову здійснення оператором протимінної діяльності.

Ключові слова: *правовий статус; протимінна діяльність; оператор; сертифікація; моніторинг; гуманітарне розмінування; вибухонебезпечні предмети; протимінні заходи.*

UDC 355.4

DOI 10.59226/2786-6920.2.2025.132-140

POLIAKOV VADYM
Chief of the Center for Postgraduate Education,
Kyiv Institute of the National Guard of Ukraine
https://orcid.org/0000-0002-8434-2336

LEHENCHUK SERHII
Senior Lecturer of Department of Reconnaissance,
Kyiv Institute of the National Guard of Ukraine
https://orcid.org/0009-0008-3993-7104

DEFENSIVE COMBAT IN MODERN CONDITIONS: LESSONS FROM THE RUSSIAN-UKRAINIAN WAR

An analysis has been conducted on the changes in the organization and conduct of defensive combat since the beginning of the Russian Federation's aggression in 2014 and after the full-scale invasion in 2022 to the present time. The work examines the transformation of methods for conducting defensive combat, the use of the latest technologies and engineering support, from positional defense during the ATO (JFO) period to modern high-tech and maneuverable defense. Special attention is given to mutual situational awareness on the battlefield, caused by the widespread use of UAVs, including FPV drones, which have enabled high-precision strikes at the level of small units, and the increasing role of electronic warfare.

Changes in the tactics of mechanized units and the implementation of a decentralized command model (Mission Command) in the Ukrainian defense forces have been studied. The work includes a comparative analysis of the stages of the war, conclusions regarding key changes, and a forecast of the further development of defensive combat.

Keywords: *Ukrainian Defense Forces, defensive battle, offensive battle, tactics, stronghold, enemy, situational awareness, unmanned aerial vehicles.*

Statement of the problem. The russian-Ukrainian war, which is the largest armed conflict in Europe since World War II, has led to the realization that views on conducting combat operations on land, in the air, and at sea have become completely or partially outdated.

Technical progress and rapid technological development are quickly and radically changing the nature of combat, both offensive and defensive. Therefore, commanders and personnel of the Ukrainian defense forces have to adapt instantly and change their tactics.

Defensive battle, as a type of combat, has undergone fundamental changes. Classic approaches aimed at deterring massive mechanized breakthroughs through positional and deeply echeloned defense have proven insufficiently effective in the context of the significant technological leap demonstrated by both sides of the conflict.

This highlights the need to analyze these changes and identify the factors that caused them in order to predict the likely future development of defensive combat.

Analysis of recent research and publications. The topic of the russian-Ukrainian war and the transformation of modern military art is actively researched by both Ukrainian and foreign analytical centers, military experts, and scientists.

Thus, the authors of [1] analyzed the use of troops (forces) and combat experience during the initial stage of russian large-scale invasion and provided relevant recommendations for their implementation in the activities of military command bodies and military units (subunits) of the Armed Forces of Ukraine. However, this study covers February–March 2022, which is only one stage of the russian-Ukrainian war.

The British Royal United Services Institute (RUSI) makes a significant contribution to the analysis of tactical changes in the theater of war. Its reports, particularly in works [2, 3], examine the processes of adaptation, changes in the use of artillery, armored vehicles, electronic warfare, and support forces by both sides of the conflict, as well as issues of air support and air defense. However, the authors only briefly touch upon the specifics of combined arms tactics and their changes during the war.

The American Institute for the Study of War (ISW) in its daily "Assessments of the russian Offensive Campaign" [4] provides an analysis of the actions of the parties and changes on the contact line of the parties, but does so at the operational and strategic levels, and also touches on the military-political features of the russian-Ukrainian confrontation, which is beyond the scope of this study.

A number of publications in specialized Ukrainian and foreign resources are devoted to the technological aspect of the russian-Ukrainian war, in particular the active development of unmanned systems. Publications [5, 6] reveal changes in combat tactics with the advent of unmanned systems. In article [7], the author analyzes the economic and tactical impact of FPV technologies on the course of combat operations. These findings are reflected in this study.

The change in management philosophy and the introduction of decentralization principles (Mission Command) in the Ukrainian defense forces are described in works [8, 9], which allowed us to consider the evolution of defensive combat through the prism of management system development.

The issue of ensuring situational awareness on the battlefield was considered in publications [11, 12, 13] as an important component of the management system in the Ukrainian defense forces, which played a significant role in the evolution of Ukrainian military art and tactics in particular.

Despite the significant number of publications, some of them are general in nature. Other studies focus on specific features of modern combined arms warfare, such as the use of unmanned systems or the issue of decentralization of military command, or examine a specific stage of the war. Some works consider the russian-Ukrainian war at the highest, operational, or strategic levels and cannot be fully utilized in this study.

Thus, there is currently a lack of research that synthesizes the evolution of defensive combat in all its components, in particular, technological, engineering, tactical, and managerial, which determines the relevance of this work.

The purpose of the article is to analyze the development of forms and methods of defensive combat based on the experience of the russian-Ukrainian war in 2014–2025 in order to identify key trends, problems, and prospects, which will allow us to predict the further development of defensive combat.

Presentation of the main material. The anti-terrorist operation (ATO), and later the joint forces operation (JFO) from 2014 to 2022, formed a unique combat experience for the Ukrainian defense forces. This stage became the basis for the subsequent transformation of defensive combat. An analysis of this period is key to understanding both the strengths and certain limitations with which the Armed Forces of Ukraine and other military formations entered the new phase of the war.

After the active phase of warfare in 2014–2015, the front stabilized. This period was characterized by a relatively static line of contact, where the main efforts of the parties were focused on holding their positions rather than conducting deep offensive operations (combat operations).

Combat activity was mainly reduced to episodic combat clashes, local battles for individual combat positions, strongholds, or key areas of terrain (objects), artillery duels, and the use of sniper and sabotage-reconnaissance groups. The defense forces of Ukraine, adhering to political restrictions, trying to minimize civilian casualties and infrastructure destruction, deliberately avoided large-scale offensive actions.

The nature of the conflict had a profound impact on the tactics and psychology of the troops. On the one side, it allowed them to gain considerable experience in defensive combat under constant fire, improve their skills in camouflage, engineering, and countering sabotage threats. On the other hand, eight years of positional defense inevitably led to the formation of a certain "tactical nearsightedness."

Unit commanders became accustomed to thinking in terms of holding a specific combat position or platoon strongpoint. This formed a persistent psychological and doctrinal dependence on the physical line of combat engagement. As a result, when the front suddenly became dynamic and extended on February 24, 2022, this inertia of thinking, geared toward positional rather than maneuverable defense, became one of the challenges that complicated the response to the rapid advance of russian troops, especially in the southern direction.

In conditions of positional warfare, the platoon strongpoint became the basis of defense. In accordance with the requirements of the Combat Regulations for Mechanized and Tank Forces, Part III (platoon, squad, crew), the platoon strongpoint occupies an area up to 400 meters wide and 300 meters deep [10]. It consists of combat positions for three mechanized squads and attached units (if available), firing positions for infantry fighting vehicles or armored personnel carriers and other attached firepower, as well as the platoon commander's command and observation post.

Combat positions of units should generally be located in one or two lines. The engineering equipment of the platoon's strongpoint was primarily aimed at protecting personnel from small arms fire and damage from artillery shells and mines. It included trenches and communication passages. Covered trenches and dugouts were equipped for personnel, and trenches were equipped for combat equipment.

The fire system should be based on the classic principle: the fire zones of the units should overlap, creating a continuous zone of destruction in front of the front line of defense. However, the overall concept of defense remained linear. The depth of defense was minimal, and the main focus was on holding the first line of trenches. This model, effective for low-intensity conflict, proved insufficiently resistant to massive artillery bombardments, air strikes, and large-scale assaults, which became apparent after the start of the full-scale invasion.

During the anti-terrorist operation and joint forces operation, artillery mainly performed counter-battery tasks, striking targets on the front line and in the enemy's immediate tactical depth. However, changes in its usage were prompted by the introduction of unmanned aerial vehicles (UAVs).

It was at this stage that the defense forces of Ukraine began to actively use UAVs for reconnaissance and artillery fire correction. This experience in the use of UAVs began to be systematized and incorporated into the training programs of artillery units. The use of drones made it possible to significantly reduce the time needed to prepare data for firing, increase the accuracy of fire, and reduce ammunition consumption. In fact, during this period, the foundations were laid for the creation of integrated "reconnaissance and strike complexes," which fully revealed their potential after February 24, 2022.

At the same time, it should be noted that during the ATO (JFO) period, UAVs were used primarily for reconnaissance and fire correction, rather than as a means of fire. Their number was limited, and their capabilities were significantly lower than those of modern UAVs. However, during this time, the Ukrainian defense forces were able to gain experience, train a significant number of operators, and develop new techniques and methods of action, which became the basis for deterring the enemy at the beginning of the full-scale invasion. The

decentralized acquisition and development of technologies in 2014-2021 became a prerequisite for the introduction of decentralized command and tactical innovations that characterize Ukrainian defense forces at the present stage.

The full-scale invasion by the russian federation has been a catalyst for an unprecedented technological transformation of the battlefield. The speed with which new technologies have been introduced, adapted, and scaled has fundamentally changed the nature of defensive combat, rendering many traditional approaches obsolete.

The most fundamental change brought about by the russian-Ukrainian war was the situational awareness of commanders, both on our side and on the enemy's. This is the ability to quickly perceive, understand, and predict events on the battlefield, which has a critical impact on the successful completion of combat missions. The widespread availability and extensive use by both sides of relatively inexpensive reconnaissance UAVs, such as commercial quadcopters (e.g., DJI Mavic, Autel) and small aircraft-type UAVs, has resulted in virtually no "blind spots" remaining in tactical depth.

Any concentration of troops, movement of combat vehicles, or deployment of artillery batteries is highly likely to be detected by enemy reconnaissance and, in some cases, strike UAVs within minutes. Experience shows that the time from target detection to fire strike has been reduced to a period of several to ten minutes, depending on the level of command and control and the type of firepower. This makes classic tactics based on covert concentration of forces for an attack almost impossible to implement. The concept of "fog of war," described by Carl von Clausewitz, which for centuries defined the uncertainty of the combat situation, has been largely eliminated at the tactical level.

The commander's situational awareness had a significant impact on the preparation and conduct of defensive combat. First, military units (subunits) on the defensive gained a significant advantage, as they were able to see the enemy's intentions and preparations for offensive actions in advance and inflict damage while the enemy was still advancing and deploying into battle formations. Second, the concept of a secure rear in the tactical depth of both sides disappeared. Any area within 10–15 km (and it is constantly increasing) from the line of contact is under constant surveillance. This factor significantly complicates logistics, rotation, evacuation of the wounded, and restoration of combat capability of units. Third, this has forced both sides to radically change their tactics, moving from actions as part of units to the use of small, maximally dispersed, and mobile groups capable of rapid movement and camouflage.

However, it is important to understand that situational awareness is not absolute or static. The activity of electronic warfare (EW) assets, weather conditions, time of day, and terrain create a mosaic of visible and invisible areas, and their boundaries are constantly changing. Thus, modern combined arms combat has turned into a "war for visibility," where success in battle depends not only on the ability to hit the target, but also on the ability to create a local "zone of transparency" for one's own forces, while simultaneously plunging the enemy into an artificially created "fog of war."

While reconnaissance UAVs provided commanders with situational awareness, strike FPV (First-Person View) drones made it extremely lethal. These small, fast, and maneuverable devices, originally designed for racing and hobbies, were quickly adapted for military usage. Equipped with a warhead, they became a mass-produced, cheap, and extremely effective guided weapon.

The cost of a FPV drone is incomparably lower than that of an anti-tank missile or artillery shell. This has enabled battalion, company, and even platoon-level units to deliver high-precision strikes against armored vehicles, fortifications, and enemy forces at distances of tens of kilometers.

This revolution radically changed the economics of war. The cost of destroying important targets, such as tanks or self-propelled guns, fell thousands of times. This forced both sides to urgently review the role and design of combat vehicles, equipping them with additional protection (anti-drone protection, electronic warfare systems), which, however, is not always effective. For defensive units, an additional threat from the air has emerged,

in addition to classic means of air attack. This requires new approaches to camouflage and fortification equipment for positions.

At the same time, this technological evolution is leading to a gradual reduction in the number of personnel on the front line. Since situational awareness and battlefield lethality make it practically fatal for humans to be in open areas or large gatherings, this stimulates the development of unmanned ground platforms for logistics, the installation of mine and explosive engineering barriers, fire support, and medical evacuation.

Parallel to the development of unmanned systems, countermeasures have also evolved. Electronic warfare has transformed from a type of combat support to one of the key elements of modern combined arms warfare. The effectiveness of any radio-controlled drone directly depends on its ability to overcome enemy electronic warfare measures.

The russian armed forces, having significant experience in this area since Soviet times, were able to deploy a dense network of electronic warfare systems on the front lines [14]. In response, the parties are constantly working to improve the resilience of unmanned systems to electronic warfare. This includes the use of transmitters with rapid frequency changes, more powerful antennas, and the development of drones that are less dependent on radio channels and satellite navigation. Thus, the presence of an effective "dome" created by electronic warfare systems over combat positions can completely disorient the enemy, depriving them of their advantages in both aerial reconnaissance and the use of strike drones. This creates opportunities for conducting offensive operations, maneuvering, or rotating units.

The next stage in the development of unmanned systems was the use of fiber optic cables to transmit control signals, making drones immune to radio interference, as well as the introduction of artificial intelligence elements for autonomous navigation using visual landmarks (known as machine vision) and automatic target acquisition. This requires new approaches and solutions to counter such challenges.

Under the influence of new threats, primarily drones and high-precision munitions, the very structure of combat positions has changed. The main principle has become avoidance of concentration and maximum dispersion.

Instead of large dugouts designed for an entire platoon, which are attractive and easy targets for precision strikes by FPV drones or artillery shells, infantry units are increasingly using individual shelters or shelters designed for two to three people, known as "foxholes" or simply "holes" (burrows). They are much less noticeable, and their destruction does not result in large instantaneous losses.

Trenches and communication passages have become deeper, providing better protection from debris and allowing safer movement at full height, especially during the evacuation of the wounded. Not only shelters for combat equipment, but also careful camouflage of positions has become a mandatory element. Standard camouflage equipment is widely used, as well as special anti-drone nets that physically prevent FPV drones from hitting equipment or entering shelters. Recently, such nets have also been installed on logistics routes (roads).

In addition, the role of false combat and firing positions has grown significantly. Equipment mock-ups, imitation trenches, and firing positions allow the enemy to be misled, forcing them to waste ammunition on non-existent targets and expose their own firepower. Thus, defensive engineering equipment has evolved from simply creating physical protection to actively shaping a false perception of the battlefield in the enemy's mind.

Technological and engineering changes on the battlefield inevitably led to a profound transformation in the philosophy of troop management. Rigid, hierarchical command models and tactics designed for large units proved ineffective. Instead, flexibility, local initiative, and the ability of small groups to act autonomously within a single plan came to the fore.

One of the key differences between the Ukrainian Defense Forces and the russian federation armed forces is their approach to management. Since 2014, the Ukrainian Defense Forces have been implementing a decentralized command philosophy known in NATO as Mission Command. The essence of this approach is that the senior commander determines the overall intent (purpose) of the battle (operation) and allocates the necessary resources but gives subordinate commanders maximum freedom in choosing the means to achieve this goal [8, 9].

This model, based on trust, a high level of training, and personal initiative on the part of junior officers and sergeants, contrasts sharply with the rigid, centralized command structure traditional in the russian army. In the russian system, any decision must be approved by a senior commander, and local initiative is discouraged and often punished.

In today's "transparent" and extremely dynamic battlefield, where the situation can change from one minute to the next, centralized micromanagement becomes physically impossible and counterproductive. There is simply no time to report to higher headquarters and receive orders. The ability of a squad, platoon, or company commander to independently assess the situation, make an adequate decision, and take responsibility becomes a decisive factor not only in the completion of the task but also in the survival of the unit. The experience gained in the ATO (JFO), where Ukrainian commanders often operated in conditions of unstable communications and unclear orders, became the basis for this approach. Thus, decentralization of command became not just a borrowed doctrine, but a necessity that turned into a key asymmetric advantage.

Given the impact of the above factors on the course of combat operations and war in general, tactics have also undergone significant changes. The extreme lethality of the modern battlefield, caused by the widespread use of artillery and drones, has made classic defensive tactics, based on maintaining a continuous front line with large units, practically impossible. Any concentration of personnel is immediately detected and becomes a target for fire.

This led to a fundamental change in the tactics of infantry units. First, small infantry groups became the main combat unit on the battlefield. Such groups are less noticeable, more mobile, and more flexible. Second, the nature of combat itself changed. Due to dense engineering barriers and constant aerial surveillance, advancement is only possible along narrow, predetermined "channels" i.e. forest strips, building ruins, folds in the terrain, etc. Combat has turned into a series of small-group clashes for control of individual shelters, reminiscent of urban warfare.

There has been a conceptual shift from line defense to area defense. The unit's task now is not so much to physically hold certain combat positions, strongpoints, or defense areas, but rather to establish fire control over a specific area of terrain. Defense is built as a network of dispersed, well-camouflaged, and interconnected firing positions and shelters. When an enemy attempting to advance is detected, it is fired upon, and crossfire is opened from several positions. After that, the groups can quickly change positions to avoid return fire. Such tactics require each soldier to have a high level of individual training, impeccable camouflage skills, terrain orientation, and the ability to operate as part of a small combat group.

In general, the results of studying the nature of changes in the conduct of defensive combat during the russian-Ukrainian war can be summarized in the table below.

The changes in the preparation and conduct of defensive combat were also caused by changes in the enemy's tactics.

Table 1 – Comparative characteristics of defensive combat elements by stages of war

Element	ATO / JFO Period (2014–2022)	Initial Stage of the Invasion (2022)	Positional Stage (2023–2025)
Basic tactical unit	Platoon in a strongpoint	Battalion/company in mobile defense	Small infantry group
Nature of defense	Static, positional defense of fixed positions	Mobile defense, fighting in urban areas	Deeply echeloned, zonal defense
Reconnaissance	Visual observation, limited use of UAVs for fire adjustment	Human intelligence, Bayraktar TB2 UAVs, partner intelligence support, initial use of small copter-type UAVs	Widespread employment of small UAVs at squad, platoon, and company levels
Field fortifications	Trenches, trench systems, dugouts, local strongpoints	Unprepared or hastily constructed fighting positions, use of natural and artificial obstacles	Deeply echeloned defensive lines, dense engineer obstacles, "foxholes / burrows"
Firepower / fires	Artillery duels, mortars, small arms	Massed use of artillery, ATGMs, Bayraktar TB2 strikes	Integration of "UAV–artillery", FPV drones as precision weapons, cluster munitions
Command and control	Centralized command with limited local initiative	Crisis command and control, accelerated transition to decentralization	Wide implementation of decentralized command and control (Mission Command)

After the initial stage of full-scale invasion, the Armed Forces of the russian federation, realizing the ineffectiveness of the battalion tactical group (BTG) concept, also demonstrated their ability to adapt, albeit reactively. Realizing that BTGs were unable to perform their tasks in the current conditions, the russian command switched to a functional distribution of forces and tactics for using assault units. A typical example is assault units such as "Storm-Z," staffed mainly by convicts, which are used for the most dangerous offensive operations. Trained units, such as airborne troops and marines, are used to build on successes in key areas.

The main offensive tactic of the russian troops has been the so-called "meat assaults." These are waves of attacks carried out with minimal armored vehicle support. The main goal of such attacks is not so much to capture territory as to identify the firing positions of Ukrainian units, force them to use up their ammunition, and exhaust them physically and morally. Once Ukrainian positions have been identified and suppressed by artillery and air strikes, more highly trained assault groups enter the fray.

Subsequently, the enemy's main tactic in offensive combat became the use of light vehicles, motorcycles, ATVs, and even electric scooters to quickly move assault groups as close as possible to the front line of Ukrainian defense forces. This forced the intensified use of explosive and non-explosive engineering barriers in the directions of the enemy's advance. Today, the main tactic of the enemy's offensive actions is the continuous use of small infantry groups of 2–3 people with the task of crossing the front line of our forces, accumulating, and consolidating their positions deep within the battle lines. At the same time, the russian command actively uses strike UAVs to cut off the logistics routes of Ukrainian defense forces. It should be noted that this enemy tactic is effective and allows for the advancement of units, albeit at the cost of significant losses.

In defense, russian troops rely on powerful engineering equipment and superiority in artillery and aviation. Their defensive tactics are rigid, static, and designed to destroy enemy forces in pre-prepared "fire pockets" (kill zones).

Conclusions and prospects for further research. The experience of the russian-Ukrainian war, especially its full-scale phase, has led to significant changes in the theory and practice of defensive combat. Analysis of this evolution allows us to draw several general conclusions.

Defensive combat has evolved from static, linear positional defense to dynamic, zone control of the terrain. Whereas defense used to be based on the concentration of manpower and firepower in prepared strongpoints, today the key factors for success are information superiority, speed of response, and the ability to conduct dispersed operations. The decisive factor is no longer the number of forces and means, but the speed of the "detection-identification-destruction" cycle. Technologies, in particular unmanned systems and electronic warfare means, have evolved from

auxiliary means to system-forming elements of defense that determine its very architecture. Situational awareness and the battlefield, which has become extremely lethal, have negated the value of massive strikes by troops supported by combat equipment and brought to the fore the tactics of small infantry groups and cheap but massive high-precision weapons.

The further evolution of defensive combat will likely move toward even greater robotization and autonomization of the battlefield. The struggle for dominance in the electromagnetic spectrum will only intensify. We can expect the mass emergence of "drone swarms" controlled by artificial intelligence, capable of collective, coordinated action without direct operator intervention. At the same time, ground-based robotic systems will be developed to take on the most dangerous tasks: assault operations, clearing passages through engineering barriers, logistics, and medical evacuation from the front lines. The development of situational awareness systems, communication channel stability, and the ability to process huge amounts of intelligence data in real time will play a significant role in combat operations. The advantage will go to the side that can implement advanced technological solutions faster and integrate them more effectively into its military art and organizational structure.

The prospect for further research in this area is to study the development and changes in offensive combat tactics: Similar to this study, it is necessary to analyze how the forms and methods of conducting an offensive have changed in the context of situational awareness and the widespread use of various types of strike UAVs and ground-based robotic platforms.

References

1. TKP 7-000(162)01.01. Heneralnyi shtab Zbroinykh Syl Ukrainy (2022). *Zbirnyk materialiv vyvchennia boiovoho dosvidu rosiisko-ukrainskoi viiny 2022 roku : taktychna publikatsiia Holovnoho upravlinnia doktryn ta pidhotovky Heneralnoho shtabu spilno z zatsikavlenymy strukturnymy pidrozdilamy naukovo-doslidnykh ustanov Zbroinykh Syl Ukrainy.* Kyiv [in Ukrainian].
2. Watling, J., Reynolds, N. (2023). Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine. Royal United Services Institute, Special Report. Retrieved from: https://static.rusi.org/403-SR-Russian-Tactics-web-final.pdf (accessed 23 August 2025) [in English].
3. Watling, J., Reynolds, N. (2025). Tactical Developments During the Third Year of the Russo-Ukrainian War. Royal United Services Institute. Retrieved from: https://surl.li/mvozwt (accessed 23 August 2025) [in English].
4. Institute for the Study of War (2025). Russian Offensive Campaign Assessment. Retrieved from: https://surl.li/sbjtvt (accessed 23 August 2025) [in English].
5. Militarnyi (2025). *Yak BPLA dokorinno zminyly sutnist pikhotnoho boiu* [How UAVs have fundamentally changed the nature of infantry combat]. Retrieved from: https://surl.li/lrnhlu (accessed 29 August 2025) [in Ukrainian].
6. Texty.org.ua (2023). *Drony vsiudy. Yak tekhnolohichna revoliutsiia na poli boiu v Ukraini zminiuie suchasnu viinu – WP* [Drones are everywhere. How a technological revolution on the battlefield in Ukraine is changing modern warfare – WP]. Retrieved from: https://surl.li/euytmd (accessed 26 August 2025) [in Ukrainian].
7. Kyiv Post (2025). *Revoliutsiia FPV-droniv v Ukraini: yak vony zminyly khid viiny* [The FPV drone revolution in Ukraine: how they changed the course of the war]. Retrieved from: https://www.kyivpost.com/uk/post/47569 (accessed 26 August 2025) [in Ukrainian].
8. Korendovych V. S., Chirikalov O. S. (2020). *Problema detsentralizatsii upravlinnia viiskamy (sylamy) v hibrydnii viini* [The problem of decentralization of command of troops (forces) in hybrid warfare]. *Nauka i oborona*, no. 3, pp. 32–40 [in Ukrainian].
9. Texty.org.ua (2022). *Yak detsentralizovanyi pidkhid dopomahaie SOU u viini z avtorytarnoiu Rosiieiu* – The Economist [How a decentralized approach helps the SOU in the war against authoritarian Russia – The Economist] Retrieved from: https://surl.lt/nmvatm (accessed 29 August 2025) [in Ukrainian].
10. *Boiovyi statut mekhanizovanykh ta tankovykh viisk Sukhoputnykh viisk Zbroinykh Syl Ukrainy. Chastyna III. Vzvod, viddilennia, ekipazh tanka : zatv. nakazom komanduvacha Sukhoputnykh viisk Zbroinykh Syl Ukrainy № 238* [Combat statute of mechanized and tank troops of the Land Forces of the Armed Forces of Ukraine Part 3. Platoon, squad, tank crew activity no. 238]. (2016, May 25). Kyiv : Alerta [in Ukrainian].
11. Lutseviat O. I., Voloshyn I. I., Yaroshenko Ya. V. Rohovets O. V. (2024). *Faktory, shcho vplyvaiut na efektyvnist systemy sytuatsiinoi obiznanosti z urakhuvanniam informatsii vid bezpilotnykh aviatsiinykh kompleksiv v operatsii uhrupovannia obiednanykh syl* [Factors affecting the effectiveness of the situational awareness system considering information from unmanned aerial systems in the operation of the joint forces grouping]. *Povitriana mits Ukrainy,* no. 2 (7), pp. 24–30 [in Ukrainian].
12. Militarnyi (2022). *Ukraina predstavyla vlasnu systemu sytuatsiinoi obiznanosti Delta*

[Ukraine has presented its own Delta situational awareness system]. Retrieved from: https://surl.lu/bmnffi (accessed 30 August 2025) [in Ukrainian].

13. АрміяInform (2025). *Masshtabna tsyfrovizatsiia: navishcho viiskovym systema sytuatsiinoi obiznanosti DELTA. Interviu* [Large-scale digitalization: why the military needs the DELTA situational awareness system. Interview]. Retrieved from: https://h7.cl/1eVlY (accessed 30 August 2025) [in Ukrainian].

14. TsUL (2024). *Dovidnyk viiskovoho zviazkivtsia. Zasoby radioelektronnoi borotby ta rozvidky, yaki vykorystovuiutsia rosiiskoiu federatsiieiu* [Military Signalman's Handbook. Electronic warfare and reconnaissance tools used by the russian federation]. Kyiv. Retrieved from: https://h7.cl/1eVud (accessed 30 August 2025) [in Ukrainian].

Received / Стаття надійшла до редакції: 10.10.2025
Revised / Прорецензовано: 23.10.2025
Accepted / Схвалено до друку: 31.10.2025

ПОЛЯКОВ ВАДИМ ЮРІЙОВИЧ
начальник центру післядипломної освіти,
Київський інститут Національної гвардії України
https://orcid.org/0000-0002-8434-2336

ЛЕГЕНЧУК СЕРГІЙ ВІКТОРОВИЧ
старший викладач кафедри розвідки,
Київський інститут Національної гвардії України
https://orcid.org/0009-0008-3993-7104

ОБОРОННИЙ БІЙ В СУЧАСНИХ УМОВАХ: УРОКИ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

Проведено аналіз змін в організації та веденні оборонного бою з початку агресії Російської Федерації у 2014 році та після повномасштабного вторгнення у 2022 році до теперішнього часу. У роботі розглядається трансформація методів ведення оборонного бою, використання новітніх технологій та інженерного забезпечення, від позиційної оборони в період АТО (ООС) до сучасної високотехнологічної та маневреної оборони. Особлива увага приділяється взаємній ситуаційній обізнаності на полі бою, спричиненій широким використанням БПЛА, включаючи FPV-дрони, які дозволили завдавати високоточних ударів на рівні невеликих підрозділів, та зростаючою роллю радіоелектронної боротьби. Досліджено зміни в тактиці механізованих підрозділів та впровадження децентралізованої моделі командування (Mission Command) в українських силах оборони. Робота включає порівняльний аналіз етапів війни, висновки щодо ключових змін та прогноз подальшого розвитку оборонного бою.

Досвід російсько-української війни, особливо її повномасштабної фази, призвів до значних змін у теорії та практиці оборонного бою. Аналіз цієї еволюції дозволяє зробити низку загальних висновків.

Оборонні бої еволюціонували від статичного, лінійного утримання позицій до динамічного, зонального контролю місцевості. Якщо раніше основою оборони була концентрація живої сили та вогневих засобів у підготовлених опорних пунктах, то сьогодні ключовим фактором успіху є інформаційна перевага, швидкість реагування та здатність до проведення розосереджених дій.

Подальша еволюція оборонного бою, ймовірно, рухатиметься в напрямку ще більшої роботизації та автономності на полі бою.

Ключові слова: *Сили оборони України, оборонний бій, наступальний бій, тактика, опорний пункт, противник, ситуаційна обізнаність безпілотні літальні апарати.*

UDC 355.45:342.9:004.056(477) DOI 10.59226/2786-6920.2.2025.141-148

ROMASHKO Oleh
Senior Lecturer, Department of State Security,
Kyiv Institute of the National Guard of Ukraine
https://orcid.org/0000-0003-1601-1591

WAYS TO ENHANCE THE SECURITY OF MILITARY ACTIVITIES UNDER THE LEGAL REGIME OF MARTIAL LAW

The article examines the key problems of ensuring the security of military activities under the legal regime of martial law. Based on the analysis of current regulatory acts and scientific publications, it is established that legislative regulation remains fragmented, the level of cybersecurity of critical infrastructure is insufficient, risk management lacks a comprehensive approach, and the psychological training of military personnel requires systematic improvement. External and internal threats are identified, including hybrid forms of warfare, information and psychological operations, and cyberattacks that significantly affect the state's defense capability. As a result of the study, the following ways to enhance the security of military activities have been identified: improvement of the regulatory framework in line with international standards, development of interagency coordination, strengthening of cyber defense, modernization of technical equipment, and expansion of psychological support programs for personnel. The obtained results are important for strengthening Ukraine's defense capacity, ensuring the resilience of critical infrastructure, and reducing risks in the modern context of hybrid warfare. Prospects for further research are related to the development of models for assessing military risks and the integration of artificial intelligence technologies into the field of security.

Keywords: *martial law; military activity; risks; threats; military personnel; regulatory acts; information and psychological operations; security; cybersecurity.*

Statement of the problem. Under the legal regime of martial law, issues of the security of military activities become critically important, as risks to personnel, the civilian population, and strategic facilities increase significantly. An analysis of current legislation shows that the regulatory framework governing the activities of the defense forces remains fragmented and requires improvement, particularly with regard to a clear definition of the powers of military administrations and the interaction between military and civilian institutions [1; 2]. At the same time, the level of cybersecurity protection of critical infrastructure is insufficient. Research indicates a growing number of cyberattacks on the public sector and defense facilities, which creates additional threats to national security [3; 4]. The management of military risks also remains problematic, since modern mechanisms for forecasting hostilities and mathematical models are used only sporadically and are not integrated into the decision-making system [5]. An equally urgent challenge is insufficient psychological training of servicemen: according to scholars, a significant proportion of personnel in the security and defense sector experience elevated levels of stress and psychological exhaustion, which reduces their resilience and combat effectiveness [6].

These factors determine the need for a comprehensive approach to the security of military activities, including improving the legal regulation of military operations, strengthening cybersecurity protection of critical facilities, developing a risk-management system, and introducing programs of psychological training and rehabilitation for servicemen. Such an approach will enable the state to rapidly adapt to a dynamic security environment, effectively counter military threats, and ensure stable functioning throughout the entire period of armed conflict.

Analysis of recent researchs and publications. The issue of the security of military activities under martial law is addressed in the works of many Ukrainian scholars. O. O. Hlushchenko [7]

examines the function of ensuring state security during martial law, emphasizing the role of legislative mechanisms and organizational decisions. At the same time, his work is limited to a general analysis of the legal framework and does not disclose practical instruments for implementing these mechanisms in the sphere of military activity. H. P. Sytnyk [8] analyzes the organizational and legal foundations of ensuring Ukraine's military security and identifies areas for improving the interaction of the defense forces. However, the study hardly addresses modern information-psychological and cyber threats, which are now key challenges for the defense sector.

The philosophical and ethical dimension is also important. V. H. Dykun, V. M. Moroz, and V. V. Stasiuk [9] substantiate methodological approaches to assessing the moral and psychological state of servicemen. The authors argue that psychological resilience and moral orientations significantly influence the effectiveness of military activity. However, the work does not propose systematic practical mechanisms for enhancing such resilience under martial law. I. Sevruk and Yu. Sokolovska [10] focus on the moral and ethical aspects of the activities of military and civilian persons/structures in countries subjected to aggression. The study underscores the importance of the humanitarian dimension in the military sphere, but does not consider specific means of integrating ethical principles into the security management system.

Despite existing developments, scholarly research predominantly highlights individual components of the problem—legal foundations, organizational mechanisms, or moral and psychological aspects. At the same time, there is a lack of a comprehensive approach that would integrate regulatory and legal solutions, risk management, cybersecurity, and psychological support for servicemen into a unified security system. This gap determines the relevance of the present study and defines its aim: to identify ways to enhance the level of security of military activities during the legal regime of martial law.

The purpose of the article is to identify ways to enhance the level of security of military activities under the legal regime of martial law by integrating legal norms, ethical principles, and practical measures. This involves analyzing applicable regulatory legal acts, assessing the moral and ethical foundations of servicemen's conduct, and substantiating managerial decisions aimed at reducing risks and strengthening the state's defense capability.

Presentation of the main material. To ensure the effective functioning of the state and maintain an appropriate level of defense capability under martial law, security plays a vital role, encompassing all spheres of life—military, informational, economic, and humanitarian. Security under martial law presupposes the implementation of comprehensive measures aimed at protecting personnel of the security and defense forces, the civilian population, strategic facilities, and state information resources. One of the key tasks is to ensure the stable functioning of the defense sector and critical infrastructure, which makes it possible to minimize risks associated with potential sabotage, cyberattacks, and the destruction of transport and energy communications. In addition, an important element is the establishment of an effective coordination system among the military, law enforcement bodies, and civilian institutions in order to maintain public order and prevent internal threats.

An analysis of regulatory legal acts governing the concept of security makes it possible to assert that under martial law, the security of military activities acquires special significance, going beyond generally accepted definitions [4].

The Law of Ukraine "On National Security of Ukraine" defines military security as the protection of state sovereignty, territorial integrity, the democratic constitutional order, and other vital national interests from military threats [11]. In addition to military security, the Law of Ukraine "On National Security of Ukraine" also defines the concept of state security, which encompasses a much broader set of measures for protecting national interests. State security provides for a комплекс (comprehensive set) of measures aimed at ensuring the stable functioning of state institutions, protecting the constitutional order, territorial integrity, and citizens' rights and freedoms from both internal and external threats. It includes counterterrorism efforts, counterintelligence measures, protection of the information space, economic security, and preventing attempts to destabilize the situation within the country. In this context, military security is a component of state security; however, it focuses exclusively on protection against armed aggression and maintaining the country's defense capability.

The main difference between these concepts lies in the scope of their implementation and the nature of the threats they address. While military security primarily concerns the armed defense of the state against external aggression, state security is a more

complex phenomenon that also includes internal threats such as political instability, economic crises, sabotage activity, and information attacks. Under martial law, these two areas of security are closely intertwined, since ensuring the resilience of state institutions and public order is no less important than the direct military defense of the territory. This underscores the importance of a comprehensive approach to security that combines legal, organizational, and technical measures.

In the context of military operations, security is a multifaceted phenomenon that includes minimizing unacceptable risk associated with the possibility of harm to the life and health of servicemen and the civilian population, as well as damage to military equipment and infrastructure. It covers not only the physical protection of personnel and equipment, but also cybersecurity, information security, and psychological resilience. Under martial law, regulatory legal acts establish clear procedures and protocols to minimize risks and prevent losses, and they also expand the concept of security by including protection against non-traditional forms of aggression. This requires a comprehensive approach and continuous improvement of security strategies, taking into account the changing operational environment and the emergence of new threats [12].

External threats consist of aggressive actions by the adversary aimed at violating the state's territorial integrity and sovereignty [6]. They include direct military invasions, artillery, missile, and drone strikes, sabotage acts, and cyberattacks intended to undermine the country's defense capability.

Internal threats pose a serious challenge to national security because they can destabilize not only the military sphere but society as a whole. Sabotage and terrorist acts are aimed at undermining the state's defense potential, creating chaos and panic among the population, which complicates coordination between military and law enforcement bodies.

Information attacks – particularly the dissemination of disinformation and cyberattacks – can undermine trust in state institutions and demoralize both servicemen and the civilian population. In such circumstances, maintaining the combat readiness of military units requires not only physical and technical preparedness, but also information resilience, psychological training, and an effective management system.

Only a comprehensive approach that combines enhanced protection of critical infrastructure, cybersecurity, and coordinated work of all security structures will make it possible to effectively counter internal threats and ensure stability in the country [4]. This presupposes providing servicemen with the necessary resources, maintaining a high level of discipline, and ensuring compliance with safety requirements in handling weapons and equipment.

Special attention is paid to minimizing harm to the civilian population and the environment. Military operations should be conducted with due regard to the need to protect civilians from the adverse consequences of hostilities and to prevent environmental disasters. Under martial law, priority tasks include ensuring the security of critical infrastructure, protecting the information space, and preventing technogenic and natural emergencies [3, 13]. Thus, the security of military activities during martial law is a complex and multifaceted phenomenon encompassing a wide range of measures aimed at ensuring the state's defense capability, preserving the life and health of servicemen, and maintaining societal resilience in the face of external and internal threats.

It includes legal, organizational, technical, informational, and psychological support, which requires coordinated efforts by various state institutions, the armed forces, security structures, and the civilian population. This includes improving the regulatory framework governing the actions of military units under extraordinary conditions and developing modern management mechanisms that allow rapid responses to changes in the operational situation. An important aspect is information security, which includes countering enemy propaganda, cyberattacks, and psychological operations aimed at demoralizing servicemen and society. Technical modernization also plays a special role, including equipping military units with modern weapons, communications, and reconnaissance capabilities, which increases their effectiveness in combat conditions.

Psychological training of servicemen and support of their morale are no less important, since stress resilience and motivation directly affect their ability to perform combat missions. Thus, the security of military activities in wartime is not only a matter of protecting territory, but also a comprehensive system of measures that requires flexibility, adaptability, and continuous improvement in response to new challenges and threats [12].

Legal regulation of military activity is the foundation for ensuring security under martial law.

Yu. O. Zahumenna and V. V. Sokurenko emphasize the need to adapt legislation to modern challenges through the integration of international standards and the development of specialized regulatory legal acts [1]. This will contribute to a clearer delineation of the powers of military formations and their interaction with public authorities and local self-government bodies. We believe that harmonization of national legislation with international humanitarian law – particularly the Geneva Conventions and additional protocols – plays a significant role in the legal regulation of military activity. This not only ensures the legality of the actions of military formations, but also strengthens the protection of the rights of civilians and servicemen in armed conflict. In addition, improving mechanisms for monitoring compliance with legality in the military sphere helps raise the level of accountability of command personnel and personnel of the security and defense forces.

An important aspect is the introduction of effective legal instruments to regulate relations between the military and state institutions, which makes it possible to avoid legal conflicts and abuses. Special attention should be given to developing regulatory legal acts governing the activities of reservists and volunteer formations, since their participation in military operations requires clearly defined legal frameworks. Thus, a comprehensive approach to the legal regulation of military activity is a prerequisite for the effective functioning of the defense sector under modern threats.

The legal regulation of military activity should take into account not only the general principles of national security but also specific challenges arising under martial law. One of the key areas for improvement is the development of legislative initiatives aimed at increasing the speed of decision-making in the military sphere. The introduction of flexible legal mechanisms that allow rapid responses to changes in the combat situation is necessary to ensure the effectiveness of military governance. In addition, strengthening legal oversight of the activities of military administrations plays a special role by ensuring an appropriate level of accountability and responsibility for decisions taken. An important task is to establish effective procedures regulating interaction between military structures and civilian authorities, particularly with regard to the use of material and human resources for defense needs.

Another important aspect of the legal regulation of military activity is the harmonization of national legislation with international security standards and international humanitarian law. Taking into account the provisions of the Geneva Conventions and other international agreements makes it possible not only to ensure the legality of the actions of military formations, but also to strengthen international support and cooperation in the security sphere. In particular, aligning Ukrainian legislation with NATO and European Union standards will enhance interoperability with international partners, increase the effectiveness of defense planning, and promote the development of the defense-industrial complex.

The issue of legal support for cybersecurity in the military sphere requires special attention. Modern conflicts are characterized by the extensive use of information technologies in warfare, which creates new challenges for legal regulation. The absence of clear legal norms on liability for cybercrime and mechanisms for its prevention may lead to significant threats to national security. In this regard, it is necessary to improve legislation on the protection of critical information infrastructure, develop provisions establishing liability for cyberattacks on military facilities, and ensure effective mechanisms for cooperation between state authorities and international partners in the field of cyber defense. A comprehensive approach to the legal regulation of cyber protection will not only minimize the risks of attacks but also strengthen the state's information resilience under martial law.

As D. Korniienko and D. Tolstonosov note, during martial law the state faces substantial information-related threats, including the spread of disinformation, cyberattacks, and interference with the functioning of information systems within the defense sector [3]. Building on their findings, it may be assumed that under martial law the state encounters an escalation of information threats, including the dissemination of disinformation, cyberattacks, and interference with critical information systems of the defense sector. These threats are aimed at destabilizing society, undermining trust in state institutions, and disrupting the functioning of critical infrastructure. Of particular concern is the use of social networks and messaging applications for the rapid spread of disinformation and manipulation.

Cybersecurity is acquiring special importance in contemporary conflicts. T. Kovalova emphasizes the need to establish effective mechanisms for protecting critical information infrastructure, to develop regulatory acts governing liability for cybercrimes, and to counter the adversary's

information and psychological operations [2]. In addition, an important aspect is the development of a national cybersecurity strategy that would cover both the military and civilian sectors, ensuring a comprehensive approach to protecting state information resources. Research points to the need to expand cooperation with international partners, in particular within the EU and NATO cyber policy frameworks, in order to exchange experience and develop common security standards. The training of qualified specialists in cyber defense is also highly relevant, as the rapid development of technology requires continuous improvement of the skills of professionals working in the field of information security. Finally, the implementation of modern artificial intelligence systems for analyzing cyberattacks and responding to them оперативно (promptly) can significantly enhance the state's level of cyber protection.

Psychological training of servicemen is an important factor for the successful fulfillment of combat missions. V. I. Fedorchuk-Moroz and L. F. Bondarchuk emphasize the need for psychological support and rehabilitation programs to reduce stress levels and strengthen personnel morale [6]. In our view, effective methods of psychological training include the simulation of combat situations, psychological training sessions, and the use of cognitive-behavioral therapy techniques. It is also important to ensure access to qualified psychological assistance both in the combat zone and after servicemen return to civilian life, which facilitates their social adaptation. Finally, a systematic approach to psychological training helps increase unit cohesion and creates conditions for effective performance of combat missions in difficult circumstances. It should also be noted that it is important to integrate ethical principles, in particular compliance with international humanitarian law and the protection of the rights of servicemen and their family members [12].

Effective management of military risks involves identifying threats, assessing them, and developing mitigation strategies. The use of mathematical models, including Lanchester differential equations, makes it possible to forecast the development of hostilities and make evidence-based decisions regarding the allocation of forces and means [5]. Historical sources indicate that in 1916, during World War I, the British engineer Frederick William Lanchester developed a system of differential equations to model the interaction of opposing forces. These equations describe the dynamics of troop strength of two opposing sides during a battle, taking into account the intensity of inflicting losses on the adversary and one's own losses. The principal models are Lanchester's linear law, applied to the analysis of ancient warfare, and Lanchester's square law, which models modern conflicts involving long-range weapons.

Applying these models makes it possible not only to forecast the outcomes of direct combat engagements, but also to assess the effectiveness of strategic decisions such as resource allocation, operational planning, and the selection of optimal tactics. In today's military context, where hybrid warfare and cyber threats are becoming increasingly prevalent, risk analysis must take into account not only physical but also informational dimensions. This requires integrating mathematical models with data analysis on cybersecurity and information operations, enabling the prediction and prevention of potential threats in the information domain.

Protecting critical infrastructure and the information space is an integral component of the security of military activity. Researchers emphasize the need to develop a national cybersecurity strategy that takes into account the specifics of martial law and provides measures to counter disinformation and propaganda [13].

Based on the analysis of available information, we can outline the following ways to enhance the level of security of military activity:

1. Development of specialized training programs covering legal aspects, cybersecurity, and psychological training. To respond effectively to modern challenges, it is necessary to create comprehensive training courses for servicemen that include legal aspects of conducting hostilities, protection of the information space, and countering cyber threats. Particular attention should be given to psychological training, as stress resilience directly affects combat capability.

2. Modernization of technical equipment of security and defense units to minimize risks. The introduction of modern technologies such as automated command-and-control systems, reconnaissance unmanned aerial vehicles, and electronic warfare capabilities will increase the effectiveness of military operations. In addition, the system of individual protection for servicemen should be improved, including body armor, helmets, and tactical communication equipment.

3. Establishment of an effective information-sharing system between units. Under martial law, the speed and accuracy of information transmission play a critical role in operational decision-making. For this purpose, it is necessary to develop secure communication channels that prevent the adversary from intercepting data. Unified standards of interaction among different security structures should also be introduced to improve coordination.

4. Continuous monitoring and risk analysis to identify threats and develop countermeasures. Military analytical centers should regularly assess current and potential threats using modern data analysis and forecasting methods. This will enable timely identification of hazards, adaptation of military strategies, and development of new tactical solutions aimed at mitigating risks.

The identified ways to enhance the level of security of military activity demonstrate that it requires a systemic approach combining legal, organizational, and technological measures. Integrating modern solutions into military governance, developing information protection, upgrading technical equipment, and supporting the moral and psychological state of personnel are key factors for the effectiveness of defense strategies. Special attention should be given to interaction between military structures and state institutions and international partners, which will contribute to strengthening Ukraine's defense capability and national security.

Conclusions and prospects for further research. The article provides a comprehensive analysis of the security of military activity under martial law. Regulatory legal acts were examined, and the main external and internal threats – including hybrid forms of warfare – were identified. The study also analyzed the state of cybersecurity protection and the psychological preparedness of servicemen, and considered risk-management practice using modern approaches.

The findings indicate that the key problems remain: fragmented legal regulation, insufficient protection of critical information infrastructure, limited mechanisms for managing military risks, and a low level of systematic psychological support for personnel. On this basis, the study proposes ways to enhance the security of military activity, including improvement of the legislative framework, development of interagency coordination, strengthening of cyber defense, modernization of technical equipment, and the introduction of psychological support programs.

Further research should focus on developing specialized mechanisms for the legal regulation of military administrations, creating new strategies for cybersecurity protection and countering information aggression, and adapting command-and-control methods to the conditions of hybrid warfare. A promising area is the integration of artificial intelligence technologies into military governance and the development of innovative approaches to training servicemen, which would increase their resilience and readiness for the dynamic conditions of modern conflicts.

References

1. Hlushchenko O. (2023). *Funktsiia zabezpechennia bezpeky derzhavy v umovakh voiennoho stanu* [The function of ensuring the security of the state in conditions of martial law]. *Chasopys Kyivskoho universytetu prava*, no. 1, pp. 53–56. DOI: https://doi.org/10.36695/2219-5521.1.2023.10 [in Ukrainian].

1. Dykun V., Moroz V., Stasiuk V. (2023). *Metodolohiia doslidzhennia moralno-psykholohichnoho stanu osobovoho skladu viisk (syl)* [Methodology for researching the moral and psychological state of military personnel (forces)]. Kyiv : 7BTs. Retrieved from: https://surl.lt/pypwdf (accessed 25 August 2025) [in Ukrainian].

2. Zahumenna Yu., Sokurenko V. (2024). *Natsionalna bezpeka Ukrainy v umovakh voiennoho stanu: teoretyko-pravovyi analiz* [National security of ukraine under martial law: theoretical and legal analysis]. *Visnyk Natsionalnoi akademii pravovykh nauk Ukrainy*, no. 31 (2), pp. 114–138. DOI: https://doi.org/10.31359/1993-0909-2024-31-2-114 [in Ukrainian].

3. *Zakon Ukrainy "Pro Natsionalnu hvardiiu Ukrainy" № 876-VII* [Law of Ukraine about the National Guard of Ukraine activity no. 876-VII]. (2014, March 13). Retrieved from: https://zakon.rada.gov.ua/laws/show/876-18#Text (accessed 25 August 2025) [in Ukrainian].

4. Kovalova T. (2024). *Normatyvno-pravove zabezpechennia antykoruptsiinoho zakonodavstva pid chas dii voiennoho stanu v sektori bezpeky ta oborony* [Current issues of regulatory and legal security of anti-corruption legislation during the effect of martial status in the sector of security and defense]. *Naukovyi visnyk KI NHU*, no. 2, pp. 103–107. DOI: https://doi.org/10.59226/2786-6920.2.2023.103-107 [in Ukrainian].

5. Korniienko D., Tolstonosov D. (2020). *Udoskonalennia orhanizatsiino-pravovykh zasad diialnosti Natsionalnoi hvardii Ukrainy po zabezpechenniu hromadskoi bezpeky* [Improvement of the organizational and legal framework of the National Guard's of Ukraine activities to ensure public security]. *Pravo i suspilstvo*, no. 6, pp. 208–213. DOI: https://doi.org/10.32842/2078-3736/2020.6.2.1.31 [in Ukrainian].

6. Medvid L. P., Symchukevych Yu. V. (2024). *Pravovi aspekty zastosuvannia syl oborony pid chas voiennoho stanu* [Legal aspects of the application of the defense forces during the state of martial]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia: pravo*, vol. 2 (82), pp. 216–221. DOI: https://doi.org/10.24144/2307-3322.2024.82.2.34 [in Ukrainian].

7. *Postanova Kabinetu Ministriv Ukrainy "Pro zabezpechennia nadiinosti y bezpechnoi ekspluatatsii budivel, sporud ta inzhenernykh merezh" № 409* [Resolution of the Cabinet of Ministers of Ukraine "On ensuring the reliability and safe operation of buildings, structures and engineering networks" activity no. 409]. (1997, May 5). Retrieved from: https://surl.li/qnrhhc (accessed 25 August 2025) [in Ukrainian].

8. *Zakon Ukrainy "Pro natsionalnu bezpeku Ukrainy" № 2469-VIII* [Law of Ukraine about the National Security of Ukraine activity no. 2469-VIII]. (2018, June 21). Retrieved from: https://zakon.rada.gov.ua/laws/show/2469-19#Text (accessed 25 August 2025) [in Ukrainian].

9. Sevruk I., Sokolovska Yu. (2022). *Moralno-etychni aspekty diialnosti tsyvilnykh ta viiskovykh na terytorii krainy, shcho zaznala viiskovoi ahresii: ukrainskyi dosvid* [Moral and ethical aspects of civil and military activities on the territory of a country subjected to military aggression: Ukrainian experience]. *Visnyk Lvivskoho universytetu. Seriia: filosofsko-politolohichni studii*, vol. 41, pp. 78–87. DOI: https://doi.org/10.30970/PPS.2022.41.11 [in Ukrainian].

10. Sytnyk H. (2023). *Orhanizatsiino-pravovi zasady zabezpechennia voiennoi bezpeky Ukrainy* [Organizational and legal principles of ensuring military security of Ukraine]. Kyiv : SAK Ltd. Retrieved from: https://surl.li/abzlmw (accessed 25 August 2025) [in Ukrainian].

11. Fedorchuk-Moroz V., Bondarchuk L. (2023). *Bezpeka pratsi v konteksti vplyvu okremykh chynnykiv psykhichnoho zdorovia pratsivnykiv v umovakh voiennoho stanu* [Occupational safety in the context of the impact of individual factors on mental health of workers in times of war]. *Naukovyi visnyk DonNTU*, vol. 2 (11), pp. 161–169. DOI: https://doi.org/10.31474/2415-7902-2023-2-11-161-169 [in Ukrainian].

12. Fivkin P. (2024). *Teoretyko-prykladni problemy diialnosti viiskovykh administratsii v Ukraini* [Theoretical and applied problems of the military administration in Ukraine]. *Yurydychnyi naukovyi elektronnyi zhurnal,* no. 5, pp. 355–360. DOI: https://doi.org/10.32782/2524-0374/2024-5/88 [in Ukrainian].

Received / Стаття надійшла до редакції: 10.09.2025
Revised / Прорецензовано: 23.09.2025
Accepted / Схвалено до друку: 30.09.2025

РОМАШКО ОЛЕГ МИКОЛАЙОВИЧ
старший викладач кафедри забезпечення державної безпеки,
Київський інститут Національної гвардії України
https://orcid.org/0000-0003-1601-1591

ROMASHKO Oleh
Senior Lecturer, Department of State Security,
Kyiv Institute of the National Guard of Ukraine
https://orcid.org/0000-0003-1601-1591

WAYS TO ENHANCE THE SECURITY OF MILITARY ACTIVITIES UNDER THE LEGAL REGIME OF MARTIAL LAW

The article examines the key problems of ensuring the security of military activities under the legal regime of martial law. Based on the analysis of current regulatory acts and scientific publications, it is established that legislative regulation remains fragmented, the level of cybersecurity of critical infrastructure is insufficient, risk management lacks a comprehensive approach, and the psychological training of military personnel requires systematic improvement. External and internal threats are identified, including hybrid forms of warfare, information and psychological operations, and cyberattacks that significantly affect the state's defense capability. As a result of the study, the following ways to enhance the security of military activities have been identified: improvement of the regulatory framework in line with international standards, development of interagency coordination, strengthening of cyber defense, modernization of technical equipment, and expansion of psychological support programs for personnel. The obtained results are important for strengthening Ukraine's defense capacity, ensuring the resilience of critical infrastructure, and reducing risks in the modern context of hybrid warfare. Prospects for further research are related to the development of models for assessing military risks and the integration of artificial intelligence technologies into the field of security.

Keywords: *martial law; military activity; risks; threats; military personnel; regulatory acts; information and psychological operations; security; cybersecurity.*

UDC 323.22/.28 DOI 10.59226/2786-6920.2.2025.149-158

TKACHENKO OLEKSANDR
Candidate of Juridical Sciences, Senior Researcher,
Scientific Secretary of the Secretariat of the Academic Council,
Kyiv Institute of the National Guard of Ukraine

ZOLOTAROVA NATALIIA
Doctor of Law, Professor,
Professor of the Department of Police Activities,
National Academy of Internal Affairs
https://orcid.org/0000-0002-3614-8328

PROSPECTIVE DIRECTIONS OF CHANGE IN STATE POLICY IN THE CONTEXT OF TRANSFORMATION OF THREATS IN THE FIELD OF NATIONAL SECURITY

This scientific article is devoted to the study of threats in specific areas of national security. Using analysis and empirical scientific research methods, the circumstances and conditions that influenced the transformation of threats in specific areas of national security since Ukraine's declaration of independence have been identified. The author's vision of the intensification of threats to specific areas of Ukraine's national security in connection with the consequences of the ongoing armed aggression of the Russian Federation is modeled. The author concludes that internal and external factors influence the change in threats to national security in different historical periods, in particular the state's ability to fulfill its constitutional obligations, which stem from its responsibility to its citizens for its activities, as well as international politics, the global economy, global and regional globalization processes, and technological developments, including artificial intelligence.

Threats to national security and the factors that influence them are constantly relevant for study in order to develop scientifically sound forecasts regarding the security environment and state policy on the implementation of measures to counteract possible negative consequences in the areas of national security.

***Keywords**: national security, threats to national security; areas of national security; state security; globalization.*

Statement of the problem. The current state of the global security environment is volatile and unpredictable. For Ukraine, such unpredictability is primarily driven by the war unleashed by the Russian Federation, as a result of which the international security system established after World War II has been nearly dismantled.

Ukraine's domestic long-term planning documents defining the main directions of state policy in the field of national security were adopted before the onset of the armed aggression of the Russian Federation. Their content indicates that a substantial share of threats to Ukraine stemmed precisely from the aggressive policy of the Russian Federation. In the pre-war period, such threats

included: encroachments on Ukraine's sovereignty and territorial integrity; attempts to block Ukraine's movement toward full membership in the EU and NATO; the possibility of further escalation of the Russian Federation's armed aggression and the large-scale use of military force against Ukraine; provocation of an armed conflict along Ukraine's state border; intelligence and subversive activities conducted by the special services of the Russian Federation against Ukraine; information and psychological special operations, etc.

Today, in the context of repelling the armed aggression of the Russian Federation, state policy on ensuring national security has undergone significant changes. This was influenced, in particular, by the ineffectiveness of the international security system combined with the failure of the security assurances provided to Ukraine upon its accession to the Treaty on the Non-Proliferation of Nuclear Weapons (the Budapest Memorandum). The Russian Federation, despite being a guarantor state under the Budapest Memorandum, did not refrain from annexing part of Ukraine's territory and waging hybrid warfare, including through controlled puppet quasi-entities in Donetsk and Luhansk regions. In addition, the shortcomings of international law together with the ineffectiveness of international organizations responsible for peace and security worldwide; the dependence of European countries artificially created by the Russian Federation through hydrocarbon supplies; and other factors of the Russian Federation's aggressive policy affecting the global economy and international security, created conditions for the tacit reaction of a significant number of states to the beginning of open armed aggression against Ukraine in February 2022. Consequently, uncertainty regarding the ability of the international community to compel the aggressor to comply with international law and to uphold the security guaranteed to Ukraine in the conditions of the Russian Federation's armed aggression prompted Ukraine's leadership to revise national security policy, strengthen national defense capability, and improve the national resilience system.

Beyond its aggressive intent to undermine Ukraine's statehood and sovereignty, the Russian Federation is also testing the civilized international community, military-political alliances, and international security organizations – institutions that are expected to be responsible for global security – for their ability to enforce compliance and implement policies aimed at maintaining peace and stability. The current state of globalizing processes, which increasingly affect Ukraine's security, generates the need to search for new, theoretically grounded approaches and practical response measures to existing and potential threats, with a view to improving mechanisms for ensuring Ukraine's national security in general and across its specific domains.

Analysis of recent researchs and publications.

Issues related to ensuring Ukraine's national security and its components have been addressed in the scholarly works of Ukrainian researchers, including V. O. Antonov, P. P. Bohutskyi, O. S. Vlasiuk, N. P. Hedikova, V. P. Horbulin, O. P. Dzoban, V. A. Lipkan, O. P. Kosevtsov, A. B. Kachynskyi, O. O. Reznikova, H. P. Sytnyk, and others.

Despite the substantial number of studies devoted to the theoretical foundations of national security, research on threats to the domains of national security remains continuously relevant and will require further reconsideration in view of processes shaping the security environment (international politics, the global economy, global and regional globalization, migration, the development of weapons systems and technologies, including artificial intelligence, etc.) and other factors.

Accordingly, the **purpose of the article** is to examine the process of transformation of threats in the field of Ukraine's national security in order to identify promising directions for the development of state policy in ensuring national security domains under changing globalization processes and the разрушение (erosion) of the international security architecture.

Presentation of the main material. n scholarly and expert discourse, threats to national security are typically classified according to the following criteria: by the location of the source of danger (external and internal threats); by the scale of

possible consequences (nationwide, regional, local, isolated); by the degree of threat formation (potential, real); by the degree of subjective perception (overstated, understated, minimal, adequate); and by spheres of societal life (threats in the economic, political, defense, international, social, informational, scientific and technological, environmental, cultural, and spiritual domains) [1, p. 204]. The capacity to identify existing and potential threats to national security directly affects the ability and effectiveness of developing means to neutralize them and prevent their emergence. Therefore, timely identification of probable threats to national security domains, determination of their sources, forecasting the scale of their impact and possible consequences in the context of the globalizing security environment, and assessing countering capabilities – while preserving fundamental national interests – constitute a prerequisite for the existence and development of the Ukrainian state.

Pursuant to the Law of Ukraine "On National Security of Ukraine" of June 21, 2018 No. 2469-VIII (as amended), threats to the national security of Ukraine are defined as phenomena, trends, and factors that make it impossible or difficult, or may make it impossible or difficult, to realize national interests and preserve Ukraine's national values [2]. The National Security Strategy of Ukraine, approved by Decree of the President of Ukraine of September 14, 2020 No. 392/2020, identifies current and projected threats to national security and national interests of Ukraine, taking into account external political and domestic conditions, as well as the main directions of the state's foreign and domestic policy aimed at ensuring its national interests and security [3].

The national security system is multi-level and comprises a significant number of interconnected and interdependent components. According to V. O. Antonov, when studying the structure of a complex system, several levels of analysis are typically distinguished, including its subsystems, depending on its design, functional purpose, organizational tier, place within a higher-level system, stages of creation, formation and operation, the management and support system, the system-technical level, and others [4, p. 108]. D. I. Dzvynchuk points to a dynamic state that constantly changes as a characteristic feature of national security, which depends on many factors such as the geopolitical situation, the level of economic and technological development, social cohesion, and others. In turn, governance in the field of national security is a dynamic process that continuously adapts to new challenges and threats [5, pp. 61–65]. Professor H. P. Sytnyk notes that managerial decisions on ensuring the security of social systems should be made on the basis of the results of an analysis of the dynamics of their development, the results of philosophical and political-science, legal, value-based and ethical aspects of the problem of security provision, as well as the laws of the evolution of living matter in the biosphere [6]. In the context of state policy on national security, we share the view that public policy is an instrument that helps the state achieve certain goals in a particular area by using various methods of influence based on available resources [7, p. 63].

The effectiveness of state policy in ensuring national security and national interests can be achieved by combining scientific achievements and practical experience when examining the results of applying the above-mentioned methods of influence. In this regard, it is advisable to consider the experience of the United States, where developments by scholars at leading universities and research centers are based on practical material and measures that the state has taken and continues to take to overcome existing threats to national security and to forecast such threats [8, p. 32].

Therefore, in the author's view, studying the conditions for the transformation of threats across the domains of national security over time and within a historical period – as a component of a subsystem of a complex system – constitutes a prerequisite for forming theoretical foundations that will facilitate the development of new theories to explain phenomena and forecast future events, and will become a basis for future doctrinal documents and regulatory legal acts in the relevant sphere, thereby directly influencing state policy on ensuring national security.

The ability to withstand existing and potential threats in the domains of national security is

influenced by mechanisms that ensure resilience and the capacity to resist and recover in the event of adverse impact. In particular, Ukraine's National Security Strategy defines resilience as one of the core principles underpinning the Strategy, and the introduction of a national resilience system is included among the main directions of the state's foreign and domestic policy aimed at ensuring its national interests and security. In turn, pursuant to the Concept for Ensuring the National Resilience System, approved by Decree of the President of Ukraine of September 27, 2021 No. 479/2021, the source of internal threats is usually vulnerabilities that indicate the existence of problems, defects, and shortcomings that generate or increase susceptibility to disruption of functionality, systemic damage, and/or vulnerability to negative effects of risks and threats [9].

Security environment analysis is intended to identify processes, phenomena, factors, conditions, circumstances, events, results of activity and interaction among subjects of social relations, as well as trends in their development that affect the level of protection of the state, society, and the environment within a certain territory from existing and projected threats. Changes in the security environment – deviations from its normal equilibrium state – entail risks that require further analysis. Understanding a threat as a potential cause of an undesirable incident that may harm individuals, assets, a system or organization, the environment, or society, it can be concluded that threats to national security may be created by certain actions, phenomena, processes, events, or situations directly aimed at undermining state sovereignty and territorial integrity and/or capable of harming citizens' life, health, and property; disrupting the uninterrupted provision of critically important state functions; causing physical or economic damage to enterprises, organizations, and critical infrastructure facilities; or preventing the realization of national interests, etc. In doing so, the source of a threat may be the policy of a state or group of states; individual persons, groups of persons, or organizations; the natural environment or outer space – changes in the activity, implementation, functioning, or existence of which give rise to certain threats and determine their general character. More than one threat may originate from a single source [10].

Ukrainian scholars and experts, in different periods of the country's historical development, identified key phenomena and factors influencing the security environment and the state's development in different ways. Consider the first years of independence, when the core threats were determined as those arising from the Chornobyl nuclear power plant disaster and related to ensuring its further functioning. During the first decade of Ukraine's independence, significant threats were considered those caused by the economic crisis and, as a result, by the emergence and growing influence of organized crime on various spheres of state processes. Threats to territorial integrity stemming from the Russian Federation's aggressive policy became explicit for Ukraine in 2014. Since then, dangerous trends of various kinds directed by Russia toward the comprehensive weakening of our state have only intensified. In the years preceding the full-scale invasion, Ukraine experienced a pandemic and efforts to prevent the spread of uncontrolled processes caused by a poorly studied disease known as COVID-19, which affected citizens' security, societal security, and, above all, the state's economic security due to imposed restrictions.

With the onset of the armed aggression of the Russian Federation, Ukraine found itself in a situation where phenomena, trends, and factors that complicate or make impossible the realization of national interests and the preservation of national values emerged across all domains of national security.

Domains of national security related to the security of socio-economic development have faced significant threats. The human factor is one of the main drivers of economic and social development. The individual has always been and remains at the center of transformations of social life, the formation of the economic system, and the structure of the state [11].

The war has caused a shortage of labor, as a large number of working-age citizens left Ukraine, while many men and women were mobilized into the armed forces. Ukraine's demographic losses in

recent years have exceeded all pessimistic forecasts. Due to declining living standards and the war, people have been leaving the country en masse, and it is unknown whether they will return. Over the last 30 years, Ukraine has lost about 10 million citizens for various reasons, and after the beginning of the full-scale war—approximately another 6 million. Today, Ukraine has the highest intensity of natural population decline in the world. The demographic crisis began long before the invasion, and the war has only accelerated it [12]. In Ukraine, during the years of the full-scale war, male life expectancy has decreased from 65 to 57 years. If previously this figure was already extremely low, the situation is now critical. At the same time, Ukraine has one of the worst indicators in terms of birth rates [13].

Unfortunately, the war results in losses, including irreversible ones. In addition, it is necessary to note the outflow of researchers and academics from Ukraine, which negatively affects education, scientific and technological development, and related areas.

It should also be stated that there is no clear vision of the country's future. Sociologists currently note a rise in pessimistic sentiments, primarily regarding the country's economic situation. The share of those who believe that in ten years Ukraine will be a country with a ruined economy and a significant outflow of people has increased from 5% to 19% [14]. Clearly, the key factor of uncertainty is the war, which is now in its fourth year.

All of this negatively affects the demographic situation and influences Ukraine's labor potential and its ability to sustain the economy at the required level.

Existing threats target objects essential for ensuring state security, including defense, economic, and scientific-and-technological potential, as well as critical infrastructure facilities. Today, due to continuous missile strikes and UAV attacks by Russian forces on the territory of our country, there are risks of further destruction and loss of energy facilities. Cases in which Ukraine's critical infrastructure has been disabled as a result of Russia's missile strikes, as well as the reduction of its capacity, have had a negative impact on the life of society and on the state of the security environment. The destruction of the Kakhovka Hydroelectric Power Plant dam has consequences not only for the natural environment. In addition to ecological damage, there are also no less serious consequences for the agricultural sector, the energy sector, the population, and Ukraine's nuclear safety. The Zaporizhzhia Nuclear Power Plant, seized by the Russians, remains at risk; improper handling of it may lead not only to infrastructure-security consequences, but also to consequences of a much broader scale.

Special attention should be paid to the contamination of the state's territory with mines, which poses a danger to the infrastructure necessary for the normal functioning of the economy and for sustaining societal life. Thus, according to the State Emergency Service of Ukraine, 174,000 sq. km of Ukraine is contaminated with remnants of Russian mines and unexploded ordnance, which constitutes about 30% of the entire territory of the country; full demining may require about thirty years [15].

A war conducted in the context of rapidly developing communication technologies and globalization processes affects the information environment, which is a separate domain of national security and also an object of ensuring state security as a sphere of national security. With the beginning of hostilities in Ukraine, insufficient measures were taken to prevent the dissemination of unreliable information or any other information that causes harm and threatens the security environment. This led to the mass spread of false narratives regarding Ukrainians' attitudes toward the aggressor and the "absorption" of Ukraine by Russia, which affected the capacity to resist, etc.

Modern means of communication, available to almost every citizen, create virtually unlimited opportunities to obtain and disseminate almost any information. The free dissemination of information by citizens in the online space gives the enemy the ability to adjust its actions both on the battlefield and in the information domain. Using "information tools," the enemy seeks to reduce our ability to mount armed resistance and to undermine the authority of the state, its leadership, and military command in the eyes of the international

community in order to induce partners to reduce or even discontinue assistance.

It should be acknowledged that with the onset of military aggression, information and psychological influences intensified, aimed at denigrating the Ukrainian language and culture, falsifying facts of Ukrainian history, and provoking artificial disputes on religious issues – particularly regarding a church that is administratively subordinated to Russia. Countless narratives are aimed at distorting truthful historical information about crimes against Ukraine and Ukrainians and at forming, through Russian mass communication media, a distorted and false informational picture of the world regarding Ukraine and Ukrainians.

In this context, a fundamental task of state policy is the formation of national identity and a national idea on the basis of historical memory, which should become a state policy for the coming decades. The systematic and purposeful lack of a national idea, ideology, and worldview in Ukraine's state-building strategies after 1991 led to Ukraine's weakening and its transformation into a multipolar oligarchic neocolony, which nearly became prey to Russia's imperialist ambitions [16, p. 5]. Ukrainian scholars justifiably emphasize the need to intensify the state's humanitarian policy, especially in the fields of science, education, and culture. The main task is to restore historical memory through objective research and to acquaint the public with its results. It is important to overcome the crisis of national and cultural identity, which in a multi-ethnic society may lead to social tension and the spread of anti-Ukrainian sentiments. The process of overcoming the Soviet mentality requires a consistent and principled approach. At the same time, it is important to consider regional linguistic, religious, ethnic, and other characteristics, avoiding manipulation. To form national identity, it is necessary to expand the spheres of use of the Ukrainian language, ensure access to truthful information, and develop critical thinking. The cultivation of national dignity should contribute to overcoming an inferiority complex [17].

The above list of real and potential threats to the domains of national security is not exhaustive. It depends on the historical stage of development and on the conditions, factors, and drivers influencing these processes. The set of real and potential threats is not static (permanent): threats may appear and disappear, intensify and diminish, and their significance for security will also change. When assessing the nature of real and potential threats and the probability of their materialization, it should be borne in mind that in some cases public perception of a particular phenomenon as a threat may differ substantially [18]. At the current stage of development, Ukraine has faced threats and challenges that require immediate solutions – based not on the past, but taking into account forecasts of the development of human civilization, technologies, global geopolitical processes, and other factors that may affect the domains of our state's national security.

In our view, the end of the war should lead to changes in international security and peace-maintenance policies. However, it is clear that under the impact of the war, the security environment in which our state exists, as well as policy for ensuring national security domains and national interests, will be transformed.

Given the above conditions shaping Ukraine's contemporary security environment, it is possible to project likely sources of the main threats to Ukraine's national security in the near future. In this regard, we share the view of O. O. Reznikova, Head of the Department for National Security Issues at the Center for Security Studies of the National Institute for Strategic Studies, that the Russian Federation will remain the main source of threats to Ukraine's national security for many years. Although the worst forecasts regarding the expansion of Russia's aggression against Ukraine have already materialized, after the war ends one should not expect Russia's leadership (even in the event of a change of its leaders) to abandon aggressive plans to continue an expansionist policy toward Ukraine. Russia will seek to recover primarily by seizing new Ukrainian territories during the war and gaining access to our state's resources. After the war, it is unlikely that Russia will abandon attempts – by various means – to harm Ukraine's interests and to interfere in the internal affairs of our state [10].

In the future, the russian federation will attempt to establish control over Ukraine by exploiting existing internal linguistic, religious, political, and other contradictions, which constitutes a major threat to Ukraine. In addition, there remains a high probability that Russia will resort to armed aggression as well as hybrid forms of aggression to achieve its aims of destroying Ukrainian statehood and sovereignty. There is also a significant likelihood that all available capabilities of the Republic of Belarus will be involved in implementing the above intentions, which expands the threat sector for Ukraine.

As for hybrid threats from the Russian Federation, in addition to armed aggression, the use of information and propaganda campaigns is likely both domestically and internationally in order to cast doubt on Ukraine's statehood and identity, its capacity to develop as an independent state, the professionalism and legitimacy of the authorities in Ukraine, etc. In addition, the energy factor and special intelligence and subversive measures will be employed. These efforts will be aimed at weakening the system of public governance, comprehensively destabilizing the internal situation in Ukraine, and creating preconditions for disrupting the process of European and Euro-Atlantic integration, as well as for the fragmentation of the Ukrainian state.

Conclusions and prospects for further research. The study of the theoretical aspects of threats to the domains of national security is driven by the need for continuous analysis of risks and potential threats in an unstable security environment, the identification of vulnerable points in the national security system and the "levers of influence" on it, the development of prevention and response mechanisms to possible challenges, and the forecasting of their effectiveness. From a practical standpoint, examining the conditions under which threats transform across the domains of national security is necessary for shaping and implementing state policy to protect national interests by developing – on the basis of scientific findings and proposals – strategies, concepts, programs, and development plans for security and defense sector actors, as well as for resource management and their effective allocation, and for improving Ukraine's legislation, etc. In turn, the above will contribute to the proper training of highly qualified specialists for the state's security sector.

Russia's armed aggression has led to enormous losses and has caused socio-economic, demographic, and energy crises, thereby bringing Ukraine closer to recognizing the need for modernization as a state that is a fully sovereign and influential subject of international relations. Taking into account the lessons of the russian–ukrainian war, the state's security policy should be oriented toward improving the system for ensuring the domains of national security, creating an effective security and defense sector and a defense-industrial complex capable of providing continuous protection of Ukraine's national interests from threats to territorial integrity, the constitutional order, and other national interests of Ukraine, which in turn will become a foundation for Ukraine's development.

State policy on ensuring national security should be implemented with due regard to the international security situation, as well as the military-political situation around Ukraine and in the world, and forecasts of their changes in view of globalizing processes, the state's real capabilities, and other factors that affect and will continue to affect the sustainable development of Ukraine in the near and long term. It is necessary to take into account that threats to national security and its domains are not permanent or rigidly defined and may change qualitatively within a short period of time. Under conditions of transforming threats across the domains of national security, state policy on ensuring national security and its domains must be flexible, capable of effectively responding to projected threats, and prepared to address the emergence of complex multi-level challenges and dangers that could not have been foreseen. At the same time, Ukraine's security should not depend on the unpredictability of globalizing processes, the policies of neighboring states, or on partner states and potential assistance from them.

One of the directions for achieving the above task should be the ability to promptly amend legislation and regulatory acts governing the components of the security and defense sector, as

well as planning documents in the field of national security, when the security situation changes; to determine a set of political, military, economic, social, informational, and other necessary measures to prevent the emergence of threats to the domains of national security or to eliminate them, and – if that is not possible – to adapt to new realities.

References

1. Sytnyk H. P. (2014). *Pidkhody shchodo vyznachennia rivnia zahroz natsionalnii bezpetsi v politychnii sferi* [Approaches to determining the level of threats to national security in the political sphere]. Kyiv : NADU [in Ukrainian].

2. *Zakon Ukrainy "Pro natsionalnu bezpeku" № 2469-VIII* [Law of Ukraine about the national security of Ukraine activity no. 1932-XII]. (2018, June 21). *Vidomosti Verkhovnoi Rady Ukrainy*. Retrieved from: https://surl.li/qekwxj (accessed 12 September 2025) [in Ukrainian].

3. *Ukaz Prezydenta Ukrainy Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 veresnia 2020 roku "Pro Stratehiiu natsionalnoi bezpeky Ukrainy" № 392/2020* [Decree of the President of Ukraine on the decision of the National Security and Defense Council of Ukraine dated September 14, 2020, "On the National Security Strategy of Ukraine" activity no. 392/2020]. (2020, September 14). *Vidomosti Verkhovnoi Rady Ukrainy*. Retrieved from: https://surl.lu/apbdxd (accessed 12 September 2025) [in Ukrainian].

4. Antonov V. O. (2017). *Konstytutsiino-pravovi zasady natsionalnoi bezpeky Ukrainy* [Constitutional and legal foundations of Ukraine's national security]. Kyiv : TALKOM [in Ukrainian].

5. Dzvinchuk D. I. (2024). *Natsionalna bezpeka Ukrainy: sutnist, tsili, zavdannia* [National security of Ukraine: essence, goals, objectives]. Proceedings of the All-Ukrainian scientific and pedagogical advanced training course *"Natsionalna bezpeka: zahrozy ta vyklyky"* (Lviv – Torun, April 1– May 12, 2024). Lviv–Torun : Liha-Pres, pp. 61–65 [in Ukrainian].

6. Sytnyk H. P. (2019). *Vzaiemozumovlenist sotsialnykh yavyshch, yaki vyznachaiut kontseptamy "nebezpeka" i "bezpeka", ta yii vrakhuvannia v teorii publichnoho upravlinnia* [The interdependence of social phenomena defined by the concepts of "danger" and "safety" and its consideration in public administration theory]. *Investytsii: practyka ta dosvid*, no. 16, pp. 61–67 [in Ukrainian].

7. Kniaziev V. M., Bakumenko V. D. (2002). *Derzhavne upravlinnia* [Public Administration]. Kyiv : UADU [in Ukrainian].

8. Bohutskyi P. P. (2020). *Kontseptualni zasady prava natsionalnoi bezpeky Ukrainy* [Conceptual Foundations of Ukraine's National Security Law]. Kyiv : NDI informatsii i prava NAPrN Ukrainy. Odesa : Feniks [in Ukrainian].

9. *Ukaz Prezydenta Ukrainy Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 20 serpnia 2021 roku "Pro zaprovadzhennia natsionalnoi systemy stiikosti" № 479/2021* [Decree of the President of Ukraine on the decision of the National Security and Defense Council of Ukraine dated August 20, 2021, "On the introduction of a national resilience system" activity no. 479/2021]. (2021, September 27). *Vidomosti Verkhovnoi Rady Ukrainy*. Retrieved from: https://surl.li/txowpe (accessed 12 September 2025) [in Ukrainian].

10. Reznikova O. O. (2022). *Stratehichnyi analiz bezpekovoho seredovyshcha Ukrainy* [Strategic analysis of Ukraine's security environment]. *Natsionalnyi instytut stratehichnykh doslidzhen*. Retrieved from: https://surl.li/ulhgtt (accessed 12 September 2025) [in Ukrainian].

11. Vlasiuk O. S., Pyrozhkov S. I., Bielov O. F. (2016). *Kontseptualni pidkhody do formuvannia systemy natsionalnoi bezpeky Ukrainy* [Conceptual approaches to the formation of Ukraine's national security system]. *Natsionalna bezpeka Ukrainy: evoliutsiia problem vnutrishnoi polityky* [Ukraine's national security: the evolution of domestic policy issues: Selected scientific works]. Kyiv : NISD, pp. 23–50 [in Ukrainian].

12. Opryshchenko A. (2023). *Vse bilshe ukraintsiv mihruiut za kordon (i, ymovirno, navriad chy povernutsia pislia viiny). Chy spravdi Ukrainu chekaie demohrafichna kryza?* [More and more Ukrainians are migrating abroad (and are unlikely to return after the war). Is Ukraine really facing a demographic crisis?]. *Zaborona Media.* Retrieved

from: https://surl.li/piqaua (accessed 10 September 2025) [in Ukrainian].

13. Lytvyn O. (2025) *V Ukraini choloviky u serednomu zhyvut do 57 rokiv, a riven narodzhuvanosti naihirshyi u sviti: skilky zalyshytsia ukraintsiv ta do yakykh dvokh stsenariiv hotuvatys* [In Ukraine, men live to an average age of 57, and the birth rate is the worst in the world: how many Ukrainians will remain and what two scenarios should we prepare for?]. *OBOZ.UA.* Retrieved from: https://surl.lt/wscwwb (accessed 12 September 2025) [in Ukrainian].

14. Hrushetskyi A. (2022). *Yakym ukraintsi bachat maibutnie Ukrainy cherez 10 rokiv i hotovnist terpity materialni trudnoshchi* [How Ukrainians see Ukraine's future in 10 years, and willingness to endure material hardship]. *KMIS.* Retrieved from: https://surl.lt/fwplrg (accessed 12 September 2024) [in Ukrainian].

15. Amelina K. (2023). *Vidkryta mapa zaminovanykh terytorii avtomatychno stane mapoiu skarbiv. Yak v Minekonomiky bachat pidkhid do ochyshchennia terytorii* [An open map of mined territories will automatically become a treasure map. How the Ministry of Economy sees the approach to clearing territories]. *LB.ua.* Retrieved from: https://is.gd/ErMnsO (accessed 9 September 2024) [in Ukrainian].

16. Ivanyshyn P. V. (2022). *Ideolohiia i derzhava: natsiosofska interpretatsiia* [Ideology and the State: A Nationalist Interpretation]. Ternopil : Kryla [in Ukrainian].

17. Mosiienko O., Hordiichuk O., Klymenko I., Kondratiuk Yu. (2024). *Natsionalna bezpeka Ukrainy: analiz ryzykiv ta vyklykiv* [National security of Ukraine: analysis of risks and challenges]. *Suspilstvo ta bezpeka,* no. 2–3 (3), pp. 98–105. Retrieved from: https://sas.ztu.edu.ua/issue/view/18349 (accessed 11 September 2025) [in Ukrainian].

18. Pavlenko V. S. (2022). *Natsionalni interesy ta zahrozy derzhavnii bezpetsi Ukrainy* [National interests and threats to the state security of Ukraine]. *Naukovi zapysky Lvivskoho universytetu. Seriia ekonomichna. Seriia yurydychna,* vol. 34, pp. 84–92. Retrieved from: https://surl.li/zgiegk (accessed 11 September 2025) [in Ukrainian].

Received / Стаття надійшла до редакції: 16.09.2025
Revised / Прорецензовано: 29.09.2025
Accepted / Схвалено до друку: 07.10.2025

ТКАЧЕНКО ОЛЕКСАНДР ВІКТОРОВИЧ
кандидат юридичних наук, старший дослідник,
вчений секретар секретаріату вченої ради,
Київський інститут Національної гвардії України
https://orcid.org/0000-0002-3485-6603

ЗОЛОТАРЬОВА НАТАЛІЯ ІВАНІВНА
доктор юридичних наук, професор,
професор кафедри поліцейської діяльності,
Національна академія внутрішніх справ
https://orcid.org/0000-0002-3614-8328

ПЕРСПЕКТИВНІ НАПРЯМИ ЗМІН У ПОЛІТИЦІ ДЕРЖАВИ В УМОВАХ ТРАНСФОРМАЦІЇ ЗАГРОЗ У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Досліджено еволюцію загроз національній безпеці за її окремими сферами. З'ясовано обставини й умови, що впливали на трансформацію загроз національній безпеці України з часу проголошення незалежності. Запропоновано авторське бачення процесу посилення загроз в окремих сферах національної безпеки України внаслідок триваючої збройної агресії російської федерації.

Зроблено висновки, що в різні історичні періоди зміну загроз у сфері національної безпеки зумовлювали внутрішні й зовнішні чинники, зокрема спроможність держави забезпечити виконання своїх конституційних обов'язків щодо відповідальності перед громадянами за свою діяльність, а також міжнародна політика, світова економіка, світові й регіональні глобалізаційні процеси, розвиток технологій, штучного інтелекту включно.

Загрози сферам національної безпеки та чинники, які на них впливають, актуалізовані постійно і тому є об'єктом вивчення задля розроблення науково обґрунтованих прогнозів стосовно змін безпекового середовища і політики держави щодо впровадження заходів протидії ймовірним негативним наслідкам у сферах національної безпеки.

Ключові слова: *національна безпека; загрози національній безпеці; сфери національної безпеки; державна безпека; глобалізація.*

UDC 355.58:378.147:159.954 DOI 10.59226/2786-6920.2.2025.159-169

KHATSAIUK OLEKSANDR
Honored coach of Ukraine, Head of the Department of Physical Education, Special Physical Training and Sports – Head of Physical Training and Sports, Kyiv Institute of the National Guard of Ukraine
https://orcid.org/0000-0002-4166-9099

PURNAK VIKTOR
PhD, Associate Professor of the Department of Fire Training, Kyiv Institute of the National Guard of Ukraine
https://orcid.org/0009-0002-2214-9351

VOLIANSKYI VOLODYMYR
Senior Lecturer at the Department of Physical Education, Special Physical Training and Sports, Kyiv Institute of the National Guard of Ukraine
https://orcid.org/0000-0001-6528-3783

FORMATION OF CRITICAL THINKING IN FUTURE OFFICERS OF THE NATIONAL GUARD OF UKRAINE: THEORETICAL AND METHODOLOGICAL ASPECT

The article presents the results of a scientific and theoretical substantiation and methodological elaboration of approaches to the development of critical thinking in future officers during the study of subjects within the «combat training» block, namely: «Firearms Training» and «Physical Education and Special Physical Training». The relevance of cultivating critical thinking is substantiated in the context of ongoing transformations in the system of higher military education, as well as growing demands for the analytical, reflective, and prognostic components of officers' professional competence in conditions of uncertainty and combat-related risk.

Through the use of systemic, comparative, and logical-gnoseological analysis, the study identifies the specific features of these disciplines as an integrative environment conducive to the development of intellectual competencies that foster effective decision-making, adaptability, and self-reflection among future officers. The article specifies pedagogical conditions and methodological techniques that enhance cadets' cognitive engagement in the educational process, including situational modeling, heuristic questioning, combat case analysis, reflective exercises, and psychophysical training.

The conceptual foundations of pedagogical modeling of content and organization of educational and training tasks are disclosed, focusing on the integration of critical thinking development with physical and applied combat skills. Key pedagogical principles to be implemented within relevant training courses are identified: conscious action, intellectual intensity, contextualization, variability, and reflexivity.

The results of the study may be applied to the modernization of educational programs, the development of methodological guidelines for instructors in the field of combat training, and the design of training scenarios that integrate physical, tactical, and cognitive components of officer preparation.

Keywords: *combat training, firearms training, critical thinking, future officers, methodological approaches, educational process, professional training, special physical training, physical education*

Statement of the problem. At the present stage of development of the system of higher military education of Ukraine, the task of forming critical thinking in future officers of the National Guard of Ukraine acquires particular significance as a leading intellectual and cognitive quality that ensures a high quality of assessment, comprehension, and decision-making under conditions of uncertainty, risk, and combat stress (extreme conditions of service and combat activity). Taking into account the new realities of conducting combat operations, the specifics of hybrid warfare, information influences, and the need to adapt to a rapidly changing operational environment, the ability of higher education applicants (cadets of higher military educational institutions) to think rationally, engage in reflection, identify cause-and-effect relationships, and make balanced decisions is not merely important – it constitutes an essential and necessary condition for the professional effectiveness of a future officer.

At the same time, an analysis of scientific and methodological literature and practical experience in the professional training of representatives of the security and defense sector institutions of Ukraine indicates fragmentation, methodological inconsistency, and limited application of targeted technologies for the formation of critical thinking specifically within the study of disciplines of the "combat training" block—such as "Fire Training" and "Physical Education and Special Physical Training." The dominance of modern teaching methods focused on automatism in performing exercises, along with a lack of cognitive load in training situations, leads to a decrease in the intellectual activity of cadets, limiting the development of their analytical, prognostic, and reflective competencies.

On the other hand, modern requirements for a military specialist necessitate the integration of cognitive and physical components of professional training. It is precisely the disciplines of the "fire" and "physical" blocks that, provided appropriate methodological support, can become an effective tool not only for physical improvement but also for the development of critical thinking as a means of conscious control of one's own actions, making non-standard decisions, instant situation analysis, and risk assessment during the execution of assigned tasks.

Thus, an urgent scientific and pedagogical problem arises – the theoretical substantiation and methodological elaboration of effective approaches to the formation of critical thinking in future officers of the National Guard of Ukraine in the process of mastering the basic disciplines of "combat training." Solving this problem involves an interdisciplinary analysis, a reconsideration of the goals and content of higher military education, and the creation of comprehensive methodological tools and pedagogical conditions that will ensure a harmonious integration of physical, tactical, and cognitive components of officer training for the needs of the National Guard of Ukraine (NGU) and other institutions of the security and defense sector of Ukraine.

The research activity was carried out within the framework of the implementation of the initiative research project "Creativity of Future NGU Officers" (code "C.F.O. NGU"), which is implemented with the direct participation of academic and pedagogical staff of the Department of Fire Training of the Faculty of Service and Combat Activities and the Department of Physical Education, Special Physical Training, and Sports of the Kyiv Institute of the National Guard of Ukraine. The project is focused on identifying effective pedagogical approaches to the development of the intellectual and creative potential of higher education applicants within the system of long-term training.

Analysis of recent research and publications. The problem of forming critical thinking in the context of professional training of servicemen of the institutions of the security and defense sector of Ukraine (SDSU) has gained particular relevance in light of the transformations taking place in the system of higher military education of Ukraine in accordance with NATO standards and the demands of the realities of "hybrid warfare." In the scientific discourse, this problem is addressed in the works of such Ukrainian researchers as O. Rybchuk [1], V. Mirnenko, V. Artamoshchenko, S. Paldūnas [2], V. Hrydchyna [3], V. Antoniuk [4], C. Briggs, Y. Danyk, T. Maliarchuk [5], T. Kovalchuk, O. Korystin, N. Sviridyuk [6], A. Bratko, D. Zaharchuk, V. Zolka [7], who emphasize the importance of critical thinking as a component of the professional competence of an officer capable of operational decision-making in complex conditions accompanied by uncertainty and risk (extreme conditions of service and combat activity).

In particular, the works of S. Melnychenko, V. Ovchynnyk, S. Hudal, M. Kulyk [8], V. Rudynskyi [9], K. Horiacheva [10], A. Syrotenko, V. Artamoshchenko [11],

Y. Sergienko, A. Lavrentiev, S. Antonenko [12] emphasize the need for a systemic revision of teaching methodologies of the "combat training" block disciplines toward the activation of cognitive activity of cadets of higher military educational institutions (HMEIs).

Studies by S. Nechkhaiev, O. Luhanskyi, I. Kryzhanivskyi [13], I. Dragomir, B. Niculescu, G. Obilisteanu [14], A. Kanova [15] reveal the significance of heuristic methods and problem-oriented approaches in military pedagogy as means of developing cognitive flexibility and independent thinking. In the areas of physical and fire training, publications by A. Andres, V. Kryzhanovskyi, O. Rymar [16], S. Romanchuk, V. Ozharevskyi, Ya. Pankevych, I. Kolinka, V. Pylypchak, O. Meleshenko, R. Senyk [17], O. Khatsaiuk, M. Medvid, B. Maksymchuk, O. Kurok, P. Dziuba (et al.) [18], O. Markova, Yu. Samsonova, S. Borodina, V. Shemchuk, I. Atamanenko [19], Yu. Samsonova, O. Markova, O. Zabula, O. Khatsaiuk, Ye. Harbara (et al.) [20], M. Medvid, O. Khatsaiuk, K. Sydorchenko, S. Vorok, A. Kernas, M. Borovyk [21], R. Kizian, O. Khatsaiuk, O. Biriukov [22] demonstrate the effectiveness of integrating intellectual tasks into the training process, which in turn contributes to the development of logical analysis skills, assessment of the combat situation, and the formation of prognostic thinking.

At the same time, despite the presence of certain theoretical developments, there is a lack of a holistic methodological vision regarding the formation of critical thinking specifically within the framework of the disciplines of the "combat training" block. Existing studies are generally fragmented, do not take into account the interdisciplinary potential of educational courses, and methodological recommendations are not adapted to the specifics of training officer personnel for the needs of the Security and Defense Forces of Ukraine, considering contemporary realities.

Thus, the scientific problem of forming critical thinking in the process of mastering the disciplines "Fire Training" and "Physical Education and Special Physical Training" requires a comprehensive analysis, the development of appropriate pedagogical models, methodological approaches, and means of their implementation within the educational process of a higher military educational institution.

The purpose of the article is the scientific and theoretical substantiation and methodological disclosure of approaches to forming critical thinking in future officers of the National Guard of Ukraine in the process of mastering the disciplines "Fire Training" and "Physical Education and Special Physical Training."

In the course of implementing the research and analytical stage, members of the research group employed a set of complementary methods of scientific inquiry adapted to the subject area of the study, its goals, and objectives. In particular, an in-depth analysis of scientific and methodological literature was conducted, which made it possible to outline the theoretical foundations of the problem and identify existing approaches to the formation of critical thinking in the context of military professional education. Systemic analysis allowed for a comprehensive consideration of the educational process as an integral system within which cause-and-effect relationships between its components and the development of thinking skills of higher education applicants (cadets) can be traced. The application of comparative analysis made it possible to compare the effectiveness of various pedagogical practices and educational models within the disciplines of the "combat training" block. Pedagogical modeling was used to create a theoretical construct of the process of forming critical thinking in future NGU officers, taking into account the specifics of the military profession and contemporary challenges of the security environment. Methods of abstraction and generalization ensured the identification of dominant patterns that determine the effectiveness of this process.

In addition, the study was based on an empirical foundation that includes generalized materials of real combat experience, as well as practical achievements of educational and professional training of officer personnel for the needs of the

NGU and other institutions of the security and defense sector of Ukraine. This made it possible to increase the applied value of the research and ensure its relevance to contemporary realities.

Presentation of the main material. Under the current conditions of transformation of the security environment, the hybrid nature of wars, the widespread use of information and psychological means of influence, and the high level of technological saturation of combat operations, the formation of critical thinking in future officers of the institutions of the Security and Defense Sector of Ukraine (SDSU), in particular the National Guard of Ukraine (NGU), acquires particular importance. The successful activity of a military leader capable of making well-grounded, responsible, and non-standard decisions under conditions of uncertainty largely depends on their ability to analyze, evaluate, and interpret information, engage in reflection, and make reasoned judgments—that is, on the level of formation of critical thinking.

It is generally recognized that critical thinking is an intellectual process of active and motivated analysis, synthesis, and evaluation of information, which presupposes flexibility of thinking, autonomy of judgments, the ability to self-correct, and to make balanced decisions. In the field of military education, namely in the training of officer personnel, this quality of thinking plays an important role in the organization of combat activities, unit command and control, threat assessment, and adaptation to changes in the combat environment.

This issue becomes particularly relevant in the process of mastering such disciplines as “Fire Training” and “Physical Education and Special Physical Training.” At first glance, these disciplines have an applied, utilitarian nature and are focused on the development of physical, psychophysiological, and technical qualities of servicemen (applied professional competencies). However, a deeper analysis reveals their significant potential in the sphere of cognitive development of the officer’s personality.

In particular, fire training includes processes of spatial orientation, instant analysis of the situation, assessment of the combat environment, and the application of firing tactics under dynamically changing conditions. This forms the ability to instantly analyze incoming data, take into account multiple factors, and assess risks and consequences of one’s own decisions. The pedagogical value lies in the possibility of deploying combat modeling situations, introducing methods of “tactical case analysis,” and conducting training with dynamic scenarios that develop the analytical flexibility of cadets [19, 20, 22].

Even broader opportunities for the development of critical thinking are provided by the discipline “Physical Education and Special Physical Training,” especially in the context of conducting classes under extreme conditions, with the inclusion of elements of psychological stress, sensory isolation, and time constraints. Under conditions of special physical training, critical thinking manifests itself in the ability to control one’s own physical condition, manage physical resources, and make оперативні decisions under conditions of fatigue, stress, or risk of injury [18, 21].

In order to scientifically substantiate the importance of forming critical thinking in the process of “combat training,” members of the research group organized a comparative study based at the Kyiv Institute of the National Guard of Ukraine (KI NGU, n = 65) and the National Academy of the National Guard of Ukraine (NANGU, n = 147), Table 1.

The results of the study confirm that a specially organized methodology for the development of critical thinking in the process of physical and fire training significantly increases not only cognitive but also operational indicators of effectiveness of cadets. The formation of critical thinking in future officers of the National Guard of Ukraine is an integral element of training a new-generation specialist capable of making well-grounded decisions under conditions of uncertainty, limited time, and high risk.

Table 1 – Key indicators of the level of critical thinking formation in the process of completing the disciplines "Fire Training" and "Physical Education and Special Physical Training" by higher education applicants of the Kyiv Institute of the National Guard of Ukraine (KI NGU) and the National Academy of the National Guard of Ukraine (NANGU)

Indicators	Group with targeted development of critical thinking (EG)	Control Group (CG)
Decision-making speed (average)	4.3 s	7.8 s
Accuracy of tactical situation assessment	91%	67%
Level of psycho-emotional stability in a stress test	high (78%)	medium (51%)
Number of errors when performing exercises under variable conditions	1.2	3.9

This process becomes particularly relevant during the mastering by higher education applicants of the disciplines of the "combat training" block – specifically, "Fire Training" and "Physical Education and Special Physical Training." It is within these educational components that the foundation of practical competence is laid, which must be complemented by the intellectual potential of the officer – the ability to reflect, critically analyze, interpret, and evaluate situations under combat conditions.

Analyzing the scientific works of the researchers Y. Sergienko, A. Lavrentiev, S. Antonenko [12], O. Markova, Yu. Samsonova, S. Borodina, V. Shemchuk, I. Atamanenko [19], R. Kizian, O. Khatsaiuk, O. Biriukov [22], it is appropriate to state that critical thinking in the professional dimension of a serviceman is the ability to: consciously interpret operational information; assess the adequacy of actions in a dynamic environment; identify erroneous judgments and contradictions in unit actions; select the most effective tactics among alternative options; and intellectually model risks in the process of making command decisions. In addition, under conditions of modern armed conflict, critical thinking acts not only as a cognitive component of professionalism but also as an element of survival and maintenance of the combat capability of a unit.

Taking into account the above, the members of the research group identified the following methodological approaches (see Table 2):

1) for the discipline "Fire Training": problem-based learning, the method of combat cases and decision analysis;

2) for the discipline "Physical Education and Special Physical Training": contextualization of physical tasks; tactical games and situational learning (concurrent physical training).The approaches listed above ensure the formation of critical thinking in the process of studying the disciplines of the "combat training" block by future law enforcement officers (cadets of the Kyiv Institute of the National Guard of Ukraine, as well as cadets of the National Academy of the National Guard of Ukraine).

According to the results of monitoring scientific-methodological, specialized, and reference literature (S. Melnychenko, V. Ovchynnyk, S. Hudal, M. Kulyk [8], Y. Sergienko, A. Lavrentiev, S. Antonenko [12], A. Kanova [15], S. Romanchuk, V. Ozharevskyi, Ya. Pankevych (et al.) [17], O. Khatsaiuk, M. Medvid, B. Maksymchuk (et al.) [18], Yu. Samsonov, O. Markov, O. Zabula, O. Khatsaiuk (et al.) [20], R. Kizian, O. Khatsaiuk, O. Biriukov [22]), the members of the research group established that the introduction of digital simulators, video analysis (biomechanical analysis of applied movements), personal physical load trackers, and VR platforms (technologies) opens new opportunities for the analysis of cadets' actions, namely: video analysis of fire training exercises makes it possible to assess the sequence of actions and errors; trackers allow evaluation of the distribution of physical effort, recovery, and movement rhythm; VR technologies enable the simulation of scenarios with elements of cognitive overload (multiple threats simultaneously).

Table 2 – Main methodological approaches ensuring the formation of critical thinking among representatives of the studied category

Methodological Approaches	Content Characteristics
I. Firearms Training	
1.1. Problem-based and situational learning (Problem-Based Learning):	The problem-based and situational approach involves posing tactical, logistical, or psychologically complex tasks to cadets, the solution of which requires analysis, hypothesis generation, and forecasting of consequences. For example: assigning a task to engage a target under changed weather conditions with a limited ammunition supply; analyzing the consequences of an incorrect choice of firing position; selecting a type of weapon depending on the characteristics of the enemy, available cover assets, and terrain elevation. Within this approach, the modeling of combat scenarios with an unpredictable development of events is used, which encourages cadets to flexibly rethink their actions and critically assess standard patterns.
1.2. Method of combat cases and decision analysis:	Real or simulated combat situations (cases) serve as objects for discussion, group analysis, and comparison of alternatives. For example: analysis of combat actions (operations) in urban environments (using combat experience of own troops, the enemy, and allies); assessment of the actions of a machine-gun crew under extreme conditions; consideration of situations involving unreliable communications in dense urban combat. These cases are processed using a system of evaluative questions that stimulate the identification of hidden errors, weaknesses in decisions, as well as potential options for optimization.
II. Physical Education and Special Physical Training	
2.1. Contextualization of physical tasks:	Physical exercises are presented not as isolated elements, but as components of tactical scenarios that require additional comprehension. For example: exercises involving accelerated movement in body armor over rough terrain are assessed according to such criteria as endurance, speed of situational assessment, and selection of the safest route; exercises on casualty evacuation include analysis of cover tactics and determination of priorities in combat actions.
2.2. Tactical games and situational learning (associated physical training):	Simulation modules in which physical activity is accompanied by logical and command tasks are an effective means of developing critical thinking. For example: a group commander receives new input regarding a change of mission during a foot march, and cadets must adapt to task execution without loss of time; during an input scenario (imitation of an attack on an enemy column), cadets must independently distribute functions, taking into account the physical readiness of each servicemember.
Reflective and analytical processing of results: After completing the exercises, cadets fill in reflective sheets in which they answer questions such as: what difficulties arose, what decisions were made and why, and what could have been done differently. Such actions form a habit of self-analysis, which constitutes the basis of critical thinking.	

Taking into account the above, we have constructed a graphical model of the formation of critical thinking in future officers of the National Guard of Ukraine in the process of studying the disciplines of the "combat training" block (Fig. 1), which demonstrates the interrelationship between disciplines, methodological approaches, modern tools, and the final result – the development of critical thinking among representatives of the studied category.

Based on the obtained results (Table 1), the members of the research group developed a comparative table (Table 3) that demonstrates the effectiveness of the proposed methodological approaches, which are advisable to use in the educational process of representatives of the studied category.

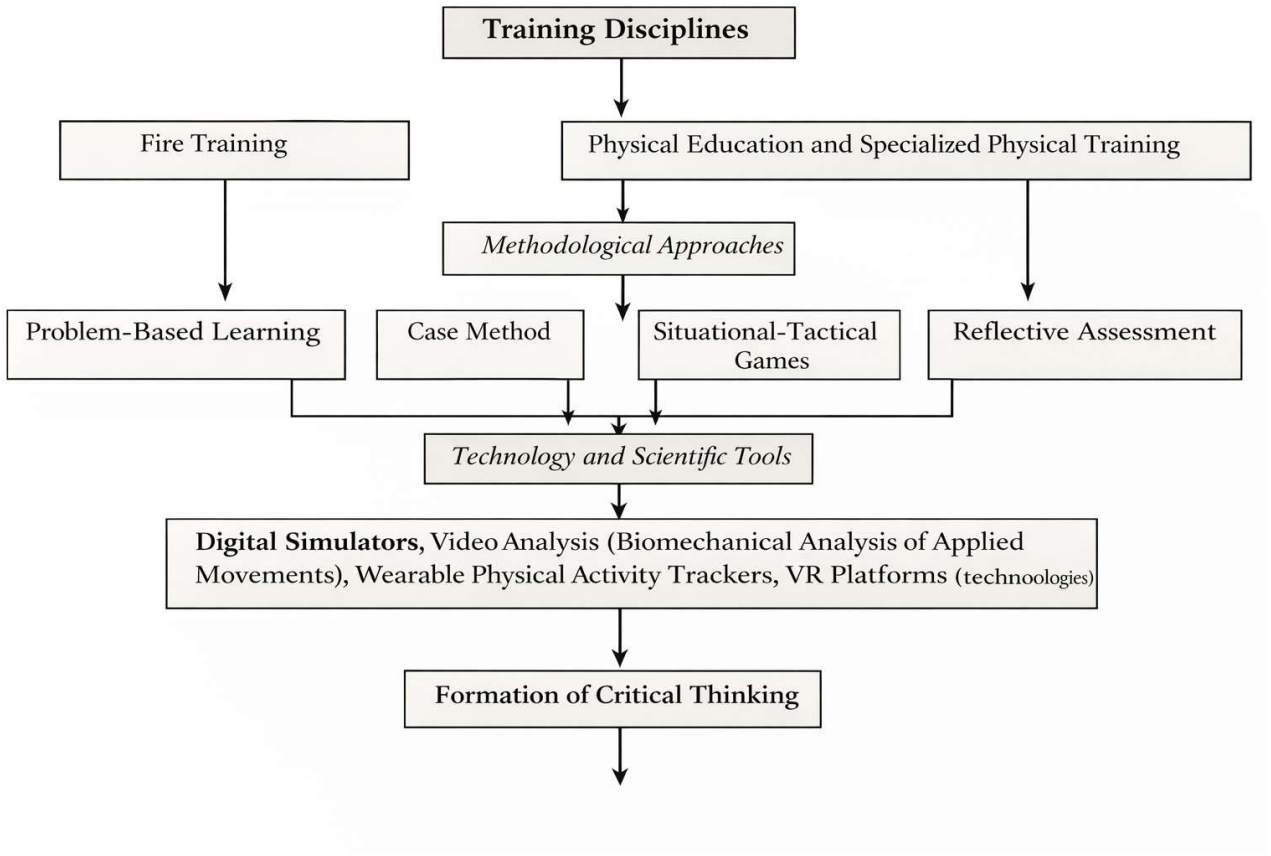


Figure 1 – Graphical model of the formation of critical thinking in future law enforcement officers in the process of studying the disciplines of the "combat training" block

Table 3 – Comparative Table of the Main Methodological Approaches

Methodological Approach	Application in Firearms Training	Application in Physical Education and Special Physical Training (SPT)	Impact on Critical Thinking
Problem-based and situational learning	Solving modified combat situations and tactical dilemmas.	Responding to changes in initial inputs during the performance of physical exercises.	Development of cognitive flexibility and the ability to respond to change.
Case method (analysis of combat actions)	Analysis of examples of unit actions (successful/unsuccessful).	Analysis of exercises containing errors or emergency situations.	Formation of analytical thinking and the ability to identify cause-and-effect relationships.
Situational and tactical games	Combat simulations with tactical command elements.	Quest-based and situational tasks; competitive methods.	Activation of dynamic decision-making and development of team thinking.
Reflective assessment	Self-analysis after live-fire exercises; evaluation of the effectiveness of decisions made.	Assessment of actions after physical loads; work with reflective sheets.	Development of self-assessment skills and the ability to recognize and correct mistakes.
Tools: VR, simulators, video	Simulators for imitation of fire contacts; video analysis of tactics.	Load trackers, video recording of physical exercises, simulators of tactical situations.	Multilevel analysis of actions and development of visual critical perception.

The development of critical thinking of cadets of higher military educational institutions of the National Guard of Ukraine in the process of studying the disciplines of the "combat training" block should be based on the integration of physical, cognitive, and moral load with simultaneous immersion in a dynamically changing tactical environment. The implementation of problem-oriented methods, contextual practices, reflective assessment, and digital technologies makes it possible not only to optimize the learning process but also to train officers capable of critical thinking, independent action, and responsible behavior under extreme conditions of service and combat activity.

Conclusions and prospects for further research. The scientific and theoretical substantiation and methodological elaboration of approaches to the formation of critical thinking in future officers of the National Guard of Ukraine in the process of mastering the disciplines "Fire Training" and "Physical Education and Special Physical Training" made it possible to formulate the following conclusions:

1. critical thinking is one of the key professionally significant cognitive competencies of an officer in the modern security environment, which is characterized by instability, unpredictability, and a high level of threats. Its development is necessary for effective analysis of the combat situation, making balanced decisions, and implementing adaptive actions under conditions of uncertainty (extreme conditions of service and combat activity);

2. the disciplines of the "combat training" block, in particular "Fire Training" and "Physical Education and Special Physical Training," possess significant potential for the integration of heuristic, problem-oriented, case-based, and reflective-activity approaches, which contributes to the activation of cognitive activity of cadets of higher military educational institutions of the National Guard of Ukraine (and other institutions of the security and defense sector of Ukraine) and to the formation of their abilities for logical analysis, prognostic thinking, and independent decision-making under stress-inducing conditions (extreme conditions of service and combat activity);

3. the experimental model for the formation of critical thinking in future officers of the National Guard of Ukraine in the process of mastering the disciplines of the "combat training" block, developed by the members of the research group, provides for the holistic integration of the following components: motivational–target, content–operational, organizational–methodological, and control–evaluation. Its implementation ensures the systemic nature and manageability of the process of critical thinking development in education;

4. the results of the theoretical analysis indicate the need to revise traditional approaches to teaching the disciplines of the "combat training" block toward reorienting from formal acquisition of knowledge to the development of the ability for flexible thinking, problem formulation, analysis of alternatives, and risk assessment. This determines the necessity of introducing innovative didactic technologies that meet the requirements of modern higher military education;

5. the scientific and methodological support for the formation of critical thinking in future officers should be based on the principles of learner-centered education, military-professional orientation, integration of physical and intellectual loads, interdisciplinarity, and the subject-oriented nature of the educational process.

Given the multifactorial and complex nature of the problem of forming critical thinking in higher military education, further research should be directed toward empirical verification of the effectiveness of the proposed methodological approaches in the conditions of educational practice of higher military educational institutions of the National Guard of Ukraine (and other institutions of the security and defense sector of Ukraine), in particular through pedagogical experimentation.

References

1. Rybchuk, O. (2024). Officer′s critical thinking in the process of operational planning. *Science and Education*, no. 4, pp. 56–61 [in Englihs].

2. Mirnenko, V., Artamoshchenko, V., Paldūnas, S. (2021). Meeting NATO standards in quality assurance: institutional audit of professional military education of Ukraine. *Civitas et Lex*, no. 4, pp. 7–21 [in Englihs].

3. Hrydchyna, V. (2024). Implementation of NATO standards in military education. *Visnyk Taras Shevchenko National University of Kyiv. Seriia: military-special sciences*, vol. 4 (60), pp. 5–9 [in Englihs].

4. Antoniuk, V. P. (2023). The war as a factor of upheavals and transformations in higher education – experience of Ukraine. *Higher Education – Reflections From the Field*, no.1, pp. 157–159 [in Englihs].

5. Briggs, C., Danyk, Yu., Maliarchuk, T. (2021). Security Aspects of Hybrid War, COVID-19 Pandemic and Cyber-Social Vulnerabilities. *Connections: The Quarterly Journal*, no. 20 (3), pp. 47–72 [in Englihs].

6. Kovalchuk, T., Korystin, O., Sviridyuk, N. (2023). Hybrid threats in the civil security sector in Ukraine. *Problems of Legality*, no. 1, pp. 122–126. DOI: https://doi.org/10.21564/2414-990x.147.180550 [in Englihs].

7. Bratko, A., Zaharchuk, D., Zolka, V. (2021). Hybrid warfare – a threat to the national security of the state. *Revista de Estudios en Seguridad Internacional*, no. 7 (1), pp. 147–160 [in Englihs].

8. Melnychenko S., Ovchynnyk V., Hudal S., Kulyk M. (2024). *Pedahohichni aspekty rozvytku liderskykh yakostei u kursantiv vyshchykh viiskovykh navchalnykh zakladiv* [Pedagogical aspects of developing leadership qualities in cadets of higher military educational institutions]. *Naukovyi visnyk Mukachivskoho derzhavnoho universytetu. Seriia: pedahohika ta psykholohiia*, vol. 10 (1), pp. 87–97 [in Ukrainian].

9. Rudynskyi, V. (2024). The Implementation of the Blended Learning Technologies at the Higher Military Educational Institution: Features of the Readiness Formation of the Future Special Purpose Specialists for Professional Activity. *Educological Discourse*, no. 1, pp. 131–137. DOI: https://doi.org/10.28925/2312-5829.2024.110 [in Englihs].

10. Horyacheva, K. (2024). Enhancing Strategic Thinking through Role-Playing Games in the Training of Cadets in Military Higher Educational Institutions (Ukrainian Case Study). *ICERI2024 Proceedings*, no. 1, pp. 4–8 [in Englihs].

11. Syrotenko A. M., Artamoshchenko, V. S. (2021). *Nabuttia sumisnosti viiskovoi osvity i pidhotovky kadriv syl oborony na zasadakh yakosti* [Acquiring compatibility of military education and training of defense forces personnel on the basis of quality]. *Nauka i oborona*, no 1, pp. 48–53 [in Ukrainian].

12. Sergienko, Yu., Lavrentiev, A., Antonenko, S. (2023). Formation of tactics of actions of cadets taking into account their cerebration during training in higher education institution. *Slobozhanskyi Herald of Science and Sport*, no. 54, pp. 94–98. DOI: https://doi.org/10.15391/snsv.2016-4.017 [in Englihs].

13. Nechaiev, S. M., Luhanskyi, O. P., Kryzhanivskyi, I. M. (2021). Group project training technology in training of operational level listeners). *Zbirnyk naukovykh prats Kharkivskoho natsionalnoho universytetu Povitrianykh Syl,* vol. 70, pp. 118–124 [in Englihs].

14. Dragomir, I., Niculescu, B., Obilisteanu, G. (2019). Problem-Based Strategies for Teaching Military English. *Knowledge-based Organization*, no. 25 (2), pp. 240–244 [in Englihs].

15. Kanova, A. Yu. (2021). Methodological Approaches of Professional Training of Ukrainian Armed Forces Officers According to NATO Standards. *Innovative Solution in Modern Science*, no. 6 (50), pp. 137–148. DOI: https://doi.org/10.26886/2414-634X.6(50)2021.5 [in Englihs].

16. Andres, A., Kryzhanovskyi, V., Rymar, O. (2021). Socio-personal aspects of psychophysical training of personnel of the National Guard of Ukraine. *Physical Education, Sports and Health Culture in Modern Society*, no. 2 (54), pp. 3–11 [in Englihs].

17. Romanchuk S., Ozharevskyi V., Pankevych Ya., Kolinko I., Pylypchak V., Meleshenko O., Senyk R. (2024). *Fizychna pidhotovlenist – yak skladova uspishnoho vykonannia zavdan za pryznachenniam (na prykladi fakhivtsiv inzhenernykh viisk)* [Physical fitness – as a component of successful performance of assigned tasks (on the example of specialists of the engineering troops)]. *Naukovyi chasopys Ukrainskoho derzhavnoho universytetu imeni Mykhaila Drahomanova. Seriia 15*, no. 7 (180), pp. 147–154. DOI: https://doi.org/10.31392/UDU-nc.series15.2024.7(180).30 [in Ukrainian].

18. Khatsaiuk, O., Medvid, M., Maksymchuk, B., Kurok, O., Dziuba, P., Tyurina, V., Chervonyi, P., Yevdokimova, O., Levko, M., Demchenko, I., Maliar, N., Maliar, E., Maksymchuk, I. (2021). Preparing Future Officers for Performing Assigned Tasks through Special Physical Training. *Revista Romaneasca pentru Educatie Multidimensionala*, no. 13 (2), pp. 457–475. DOI: https://doi.org/10.18662/%20r-rem/13.2/431 [in Englihs].

19. Markov O. V., Samsonov Yu. V., Borodin S . V., Shemchuk V. A., Atamanenko I. O. (2021). *Formuvannia profesiinykh kompetentnostei maibutnikh ofitseriv riznykh instytutsii sektoru bezpeky i oborony Ukrainy v systemi vohnevoi pidhotovky iz vykorystanniam suchasnykh tekhnichnykh zasobiv navchannia* [Formation of professional competencies of future officers of various institutions of the security and defense

sector of Ukraine in the system of fire training using modern technical training tools]. *Innovatsiina pedahohika*, no. 32 (2), pp. 60–74 [in Ukrainian].

20. Samsonov Yu. V., Markov O. V., Zabula O. Ye., Khatsaiuk O. V., Harbar Ye. O., Mahmet T. M., Zadorozhnyi K. A., Povar O. V. (2023). *Aprobatsiia pedahohichnykh umov formuvannia hotovnosti maibutnikh ofitseriv NGU do zastosuvannia PTRK "JAVELIN" iz aktsentovanym vykorystanniam zasobiv SFP* [Testing of pedagogical conditions for forming the readiness of future NGU officers to use the JAVELIN ATGM with an emphasis on the use of SFP means]. *Naukovyi chasopys Ukrainskoho derzhavnoho universytetu imeni Mykhaila Drahomanova. Seriia 15*, vol. 3 (161), pp. 136 –141 [in Ukrainian].

21. Medvid, M., Khatsaiuk, O., Sydorchenko, K., Vorok, S., Kernas, A., Borovyk, M. (2024). Sports Pedagogy: Readiness of Cadets to Apply Physical Action in Different Conditions of Service Activity. *RREM*, no. 16 (2), pp. 336–355. DOI: https://doi.org/10.18662/rrem/16.2/860 [in Englihs].

22. Kizian R. V., Khatsaiuk O. V., Biriukov O. I. (2023). *Aprobatsiia orhanizatsiino-pedahohichnykh umov formuvannia navychok strilby z avtomatychnoi striletskoi zbroi maibutnikh ofitseriv NGU* [Testing of organizational and pedagogical conditions for the formation of automatic small arms shooting skills of future NGU officers]. *Naukovyi visnyk KI NHU*, vol. 2, pp. 31–39. DOI: https://doi.org/10.59226/2786-6920.2.2023.31-39 [in Ukrainian].

Received / Стаття надійшла до редакції: 07.07.2025
Revised / Прорецензовано: 18.07.2025
Accepted / Схвалено до друку: 25.07.2025

ХАЦАЮК ОЛЕКСАНДР ВОЛОДИМИРОВИЧ
заслужений тренер України, начальник кафедри фізичного виховання, спеціальної фізичної підготовки і спорту – начальник фізичної підготовки і спорту, Київський інститут Національної гвардії України
https://orcid.org/0000-0002-4166-9099

ПУРНАК ВІКТОР ПАВЛОВИЧ
доктор філософії, доцент кафедри вогневої підготовки, Київський інститут Національної гвардії України
https://orcid.org/0009-0002-2214-9351

ВОЛЯНСЬКИЙ ВОЛОДИМИР ГЕОРГІЙОВИЧ
старший викладач кафедри фізичного виховання, спеціальної фізичної підготовки і спорту, Київський інститут Національної гвардії України
https://orcid.org/0000-0001-6528-3783

ФОРМУВАННЯ КРИТИЧНОГО МИСЛЕННЯ У МАЙБУТНІХ ОФІЦЕРІВ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ: ТЕОРЕТИКО-МЕТОДИЧНИЙ АСПЕКТ

Подано результати науково-теоретичного обґрунтування та методичного розкриття підходів до формування критичного мислення у майбутніх офіцерів у процесі опанування ними дисциплін блока бойової підготовки «Вогнева підготовка», «Фізичне виховання та спеціальна фізична підготовка».

Визначено актуальність проблеми розвитку критичного мислення в умовах трансформації системи вищої військової освіти, зростання вимог до аналітичного, рефлексивного та прогностичного складників професійної готовності майбутнього офіцера в умовах невизначеності й бойового ризику.

На основі системного, порівняльного та логіко-гносеологічного аналізу розглянуто специфіку зазначених дисциплін як інтегративного середовища для розвитку інтелектуальних компетентностей, що забезпечують ефективне прийняття рішень, адаптивність і саморефлексію майбутніх офіцерів. Уточнено педагогічні умови й методичні прийоми, що сприяють активізації когнітивної діяльності курсантів і курсанток в освітньому процесі, а саме: ситуаційне моделювання, евристичне опитування, бойове кейс-аналізування, рефлексивні вправи та психофізичне тренування.

Розкрито концептуальні засади педагогічного моделювання змісту й організації навчально-тренувальних завдань, орієнтованих на розвиток критичного мислення у поєднанні з фізичними й вогневими військово-прикладними навичками. У межах відповідних навчальних курсів доцільно реалізовувати такі педагогічні принципи: усвідомленість дії, інтелектуальна напруженість, контекстуальність, варіативність, рефлексивність.

Результати дослідження можуть бути використані в оновленні освітніх програм, підготовці методичних рекомендацій для викладачів блока бойової підготовки та розробленні тренувальних сценаріїв, що поєднують фізичний, вогневий, тактичний і когнітивний складники підготовки майбутніх офіцерів Національної гвардії України.

Ключові слова: *бойова підготовка; вогнева підготовка; критичне мислення; майбутні офіцери; методичні підходи; освітній процес; професійна підготовка; спеціальна фізична підготовка; фізичне виховання.*

UDC 351.746.1 DOI 10.59226/2786-6920.2.2025.170-178

SHEVCHUK VLADYSLAV
Senior lecturer of the Border Guard Services Department,
Bohdan Khmelnytskyi National Academy
of the State Border Guard Service of Ukraine
https://orcid.org/0000-0001-5583-2160

METHODOLOGY OF THE BORDER DEPARTMENT HEADQUARTERS REGARDING THE APPLICATION OF STATE BORDER GUARD UNITS USING SIMULATION

The author has improved the methodology of the headquarters of a border guard detachment regarding the employment of state border protection units using simulation modeling, which serves as an auxiliary tool within the decision support system. The methodology ensures a high level of planning of operational and service activities and provides an opportunity to assess the adopted decision on the employment of these units at the state border.

Keywords: *planning; operational and service activities; decision-making; modeling; employment of units; management processes; training; methodology.*

Problem of the statement. Under current conditions, the work of the command and control bodies of border guard detachments and state border protection units (hereinafter – SBPU) requires continuous improvement of the scientific and methodological framework that would ensure a high level of planning of operational and service activities (hereinafter – OSA) and the employment of these units at the state border. Existing systems for assessing the OSA of border units often have a fragmented nature, are focused on retrospective analysis of statistical indicators (data) (the number of detained offenders, an increase in passenger flow, detention of contraband goods, weapons, narcotic substances, etc.), and do not take into account the integral capability of SBPU units to adapt to rapidly changing conditions. The absence of a unified methodological basis for comprehensive assessment of the adopted decision reduces the effectiveness of the work of the command and control bodies of border guard detachments and state border protection units [1]. This gives rise to an urgent scientific task of developing a methodology that would ensure the adoption of substantiated decisions and their assessment.

Analysis of recent research and publications. Issues of national and border security, action planning, employment of units, and increasing their effectiveness have been addressed by scholars Telelym V. M. [2] and Romanchenko I. S. [3]. Monograph [4] presents general principles and the content of staff decision-making procedures in military command and control, in particular according to NATO standards. Voloshyna V. V. and Rudnytskyi A. V., in their study [5], proposed a conceptual framework based on best practices, which relies on theoretical and methodological achievements in the field of studying decision-making processes of military personnel under crisis conditions. Olenchenko V., Nemeryshchyn V., and Ihnatiev A. analyzed existing decision support systems used by the security forces of Ukraine [6]; however, in the field of state border protection, simulation modeling in the decision-making process has not yet been considered. In monograph [7], the authors developed a methodology for the comprehensive use of military and non-military forces and means of the security and defense sector. Kachynskyi A. B., together with the team of authors of monograph [8], developed scientific concepts and mathematical methods for command and control of forces and means. Issues of planning the operational and service activities of the State Border Guard Service of Ukraine were addressed in the scientific works of Bratko A. V. [9]. Existing methods, models, and methodologies of planning do not take into account new conditions of joint task execution by military formations and law enforcement agencies that arise under modern threats, nor do they consider managerial decision-making using simulation modeling systems by the

bodies and units of the State Border Guard Service of Ukraine.

The purpose of the article is to improve the methodology of the work of the headquarters of a border guard detachment regarding the employment of state border protection units using simulation modeling.

Presentation of the main material. In accordance with the conduct of Stage II of preparation for operational and service activities in the next calendar year or another period, the headquarters of a border guard detachment develops a plan of special measures for searching for offenders within the area of responsibility of the border guard detachment [15].

Preparation of the headquarters of a border guard detachment for conducting special measures to search for offenders (hereinafter – SMSO) is carried out with forecasting of threats at the state border, monitoring of the situation in the controlled border area, prevention of offenders' actions, continuity of actions of forces and means, and their timely maneuver in order to localize, neutralize, and suppress offenses.

The main stages of the improved methodology of the work of the headquarters of a border guard detachment regarding the employment of SBPU units under conditions of complication are presented in Figure 1.

1.COLLECTION, STUDY, AND PROCESSING OF SITUATIONAL DATA

- study of intelligence information from operational-search and other units;
- study of information from the headquarters of higher command, neighboring regional administrations, and bodies (units) of state border protection;
- processing of information from state institutions, public organizations, and the local population;
- study of topographic maps, photographic images, and weather forecasts.

↓

2. CLARIFICATION OF THE TASK AND ASSESSMENT OF THE SITUATION

- determination of the purpose of actions and the intent of the senior commander;
- assessment of own forces and means, attached forces, and neighboring units;
- analysis of the actions of offenders, terrain, and weather conditions;
- in units with checkpoints – analysis of cargo and passenger transportation.

3. PREPARATION OF PROPOSALS FOR DECISION-MAKING

- conclusions based on the assessment of the situation;
- determination of directions for the concentration of main efforts;
- calculation of forces and means, including reserves;
- conducting operational and tactical calculations and verification of the adopted decision using JCATS;
- preparation and issuance of preliminary orders;
- organization of command and control and communications.

4. FORMALIZATION OF THE DECISION

- formulation of the concept (intent) of actions;
- assignment of tasks to units and determination of the procedure for interaction;
- development of the border protection plan (service order);
- graphical representation on a map with an explanatory note;
- approval of the decision by the senior commander.

Figure 1 – General scheme of the improved methodology of the work of the headquarters of a border guard detachment regarding the employment of state border protection units using simulation modeling

Stage 1.

Collection, Study, and Processing of Situational Data.

The collection (acquisition), study, and processing of situational data are carried out jointly with operational-search and other units in order to provide the necessary data for decision-making within the guarded section of the state border.

The main sources of obtaining situational data include: intelligence of all types; information from the higher headquarters, neighboring regional administrations, bodies (units) of state border protection, interacting bodies of other state structures, public organizations, and the local population; reports and briefings from the headquarters of subordinate bodies (units); reports of headquarters officers seconded to subordinate structures; study of topographic and maritime charts, photographic images, and other reference documents; weather forecasts from hydrometeorological (meteorological) stations, etc.

Stage 2.

Work During Clarification of the Task and Assessment of the Situation.

As a result of clarifying the received task, it is necessary to understand: the purpose of future actions; the intent of the senior commander; the tasks, role, and place of the state border protection body (unit) in future actions; the tasks of neighboring units and the procedure for interaction with them; which tasks are performed by the forces and means of the senior commander in the interests of the state border protection body (unit); the procedure for the employment of forces and means; readiness to execute the received task.

A deep understanding of the content of the received task enables the chief of staff to purposefully organize the work of the command and control body.

When assessing the situation, the headquarters of the border guard detachment evaluates it comprehensively, by elements: the position, composition, and possible nature of actions of offenders; the position, composition, condition, and capabilities of own and attached bodies (units); the position and nature of actions of neighboring units and the conditions of interaction with them; the position and capabilities of interacting bodies; the nature of the terrain; the radiation, chemical, and bacteriological (biological) situation, possible changes therein and their impact on the actions of bodies (units); the nature of economic and production activities of enterprises and organizations in the border strip and the controlled border area and their impact on the activities of the state border protection body (unit); the state of weather, season of the year, and time of day.

In addition, in state border protection bodies (units) that include checkpoints across the state border of Ukraine, the volume and nature of transportation across the state border are assessed.

Stage 3.

Preparation of Proposals for Decision-Making.

Based on clarification of the received task and a comprehensive assessment of the situation, the headquarters of the border guard detachment prepares proposals for the commander to make a decision. The proposals, as a rule, should provide for: conclusions from the assessment of the situation; which units are to be transferred to enhanced state border protection and the content of the measures to be implemented; directions for concentrating main efforts; which forces and means are to be engaged in operational and service activities; the overall organization of state border protection (according to defined systems) and the organization of the service order; by which forces and means, on which lines, and by what time to strengthen the covering of the state border, to block (cover) areas of probable presence of offenders; tasks to be assigned to bodies (units); the procedure for guarding junctions and gaps; routes for the movement of reserves and reinforcing units; additional regime measures to be implemented; the composition of reserves, by what time and in which areas they are to be concentrated; with whom and on which issues to organize interaction; the procedure for comprehensive support of the actions of bodies (units); organization of command and control; main measures for advance preparation of state border protection bodies (units) for actions; other measures arising from the specifics of the development of the situation within the section of the state border.

In addition, it is necessary to provide for the procedure for the actions of forces and means in the event of the emergence of special measures to search for offenders.

Simultaneously with the preparation of proposals for the employment of forces and means, the headquarters prepares data and calculations related to the organization of command and control.

After clarification of the received task, assessment of the situation, and approval of the intent, in order to provide bodies (units) with more

time to prepare for future actions, preliminary orders are issued to them (under the parallel method of work).

Preliminary orders, as a rule, specify: the intent of actions; measures to be taken immediately to prepare bodies (units) for future actions and, if necessary, the movement of reserves to action areas; tasks related to obtaining necessary situational data; informing neighboring units and interacting bodies; preparation of the data necessary to complete planning; readiness time.

Preliminary orders, in order to save time, may be communicated to bodies (units) orally, personally by the commander or the chief of staff, and must necessarily be duplicated in written form (for example, by telegram) in accordance with established rules for the preparation of operational and service documents.

Operational and tactical calculations are conducted in order to determine initial data—quantitative, qualitative, as well as temporal and other normative indicators—required for the commander to make a decision, to plan operational and service activities, and to ensure command and control of subordinate bodies (units).

The initial data for conducting calculations include: the received task; the composition and capabilities of subordinate bodies and units; possible actions of offenders; and other situational data.

In all structural subdivisions of the command and control body, a list of the main operational and tactical calculations to be performed during organization and in the course of typical measures is determined; standard calculations for the most important operational and tactical tasks are carried out in advance, and methodologies for conducting and refining calculations for a specific situation are developed. Technical means, including simulation modeling, are used to prepare operational and tactical calculations.

Simulation modeling is used to verify and assess the adopted decision of commanders of state border protection bodies and units.

Modeling is conducted through the phased input of data on offenders, own forces and means, including attached and interacting forces, taking into account terrain, season, weather conditions, and time of day. The simulation is conducted until the result is achieved through continuous adjustment of tactical techniques.

Modeling is conducted in the classroom of the Simulation Modeling Center (hereinafter – SMC). Actions begin with a briefing in which the commander of the border guard detachment communicates the intent for conducting special measures to search for offenders.

Upon its completion, the officers of the headquarters and the senior elements of the service order take their places at automated workstations, and the simulation modeling system conducts the play of actions of the elements of the service order of the border guard detachment, attached reserves, and law enforcement agencies in the prepared area for conducting special measures to search for offenders.

Representatives of the Simulation Modeling Center, acting as offenders, introduce changes to the conditions of conducting special search actions, namely: they change movement routes and hiding places, conduct armed attacks on elements of the service order, introduce suddenness of actions under changing weather conditions and other factors that complicate the conduct of the search, etc.

The command headquarters continues to escalate the situation by providing inputs, controls the work and command and control of the elements of the service order of the border guard detachment, and verifies the quality of the elaboration by officials of the defined documents by stages.

Officers at automated workstations verify the expediency of the adopted decision, check operational and tactical calculations and proposals, as well as maneuver and march routes of the forces and means of the border guard detachment.

After verification of the effectiveness of the submitted proposals by the headquarters of the border guard detachment, Stage 4 begins, namely the formalization of the decision by the commander of the border guard detachment.

Stage 4.

Formalization of the Decision.

The commander of the border guard detachment makes the decision personally on the basis of clarification of the received task, assessment of the situation, and the operational and tactical

calculations and modeling of future actions conducted by the headquarters.

The decision defines: conclusions from the assessment of the situation; the intent of actions; tasks for state border protection bodies (units) and attached units; the main issues of interaction and comprehensive support; organization of command and control.

The basis of the decision is the intent of actions, which determines: the purpose of actions; directions (areas) for concentrating main efforts; the organization of border protection (operational (service) order); the procedure and methods for executing tasks; additional regime measures in controlled border areas; locations for organizing (deploying) filtration points (if necessary); areas and main measures for conducting operational search; areas of aerial reconnaissance, etc.

In the state border protection body, the intent of actions and the plan of operational and preventive measures are usually developed on a single map (scheme).

The decision of the commander of the border guard detachment on conducting operational and service activities in connection with the complication of the situation is presented graphically on a map (scheme) with an explanatory note. It is the most important planning operational and service document and is intended for reporting the decision for approval by the senior commander, assigning tasks to subordinate and attached bodies (units), organizing interaction and comprehensive support, as well as for command and control of bodies (units) during the conduct of operational and service activities. After approval by the senior commander, the decision becomes the legal basis for the development of all other operational and service documents and for the command of subordinate bodies (units) [16].

Thus, for approbation of the methodology, namely verification of the adequacy of managerial decision-making procedures within the simulation modeling system, a command-and-staff exercise (hereinafter – CSE) was conducted with trainees of the Faculty of Professional Education and Leadership of the Bohdan Khmelnytskyi National Academy of the State Border Guard Service of Ukraine (hereinafter – NASBGSU) within the discipline "Operational and Service Activities of the State Border Guard Service of Ukraine" on the topic "Organization of Operational and Service Activities within the Area of Responsibility of a Border Guard Detachment," using the JCATS simulation modeling system (at the Simulation Modeling Center of NASBGSU).

During the third stage, "Organization and Conduct of Special Measures to Search for Offenders," a situation was created that prompted the commander of the border guard detachment to plan measures for decision-making on conducting special measures to search for a group of armed persons, to conduct operational and tactical calculations, and to formalize the initial data of the elements of the service order for input into JCATS.

In addition, the issues of the stage revealed the work of the commander of the border guard detachment and officials of the detachment in assigning tasks to the elements of the service order, organizing interaction, and providing comprehensive support for the planned measures.

During the practical part of the third stage, the trainees conducted a simulation of the actions of the forces and means of the border guard detachment and reserves on the prepared JCATS theater, tested the input of calculations, determination of lines and areas of special measures, and modeled methods of action for searching for offenders (Figures 2, 3).

With the assistance of the instructor staff of the Simulation Modeling Center, at least two simulations of situational actions of offenders and actions of the forces and means of the border guard detachment were conducted with each group, involving changes in routes, suddenness of actions, under changing weather conditions and other factors complicating the conduct of the search.

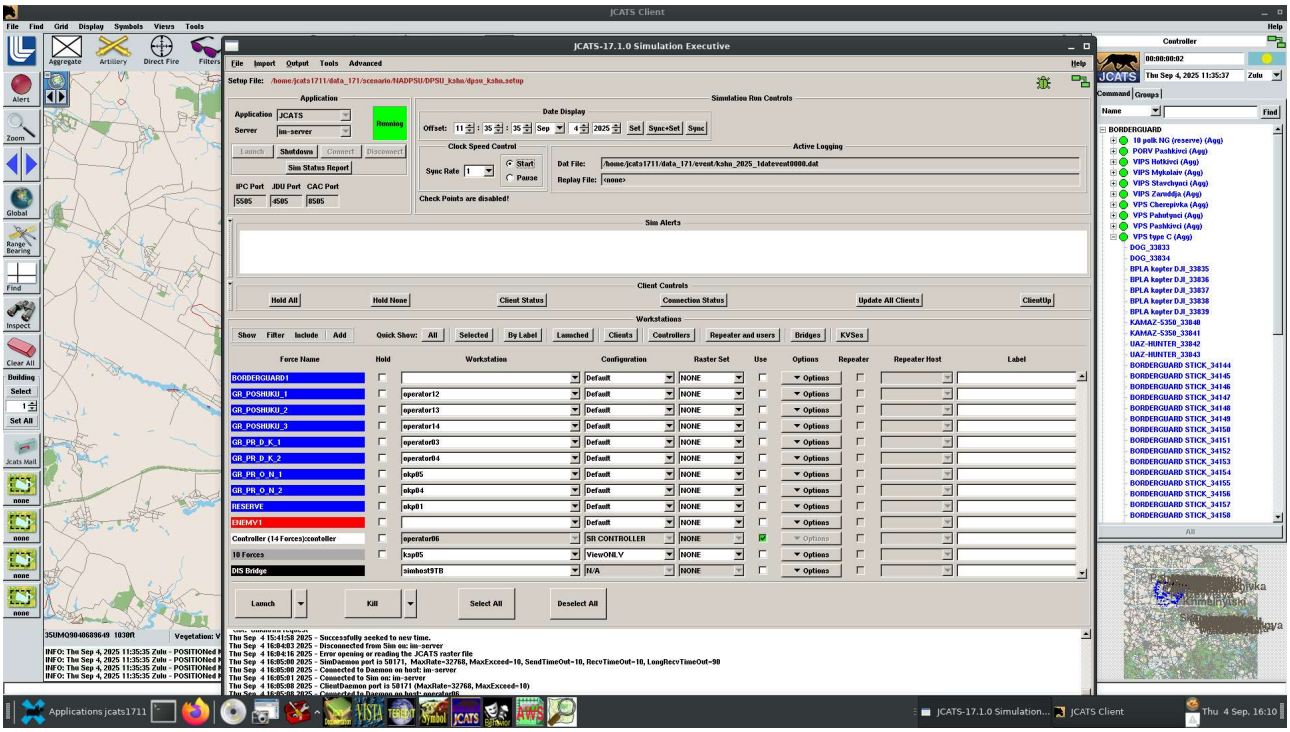


Figure 2 – Interactive panel for inputting initial data in the JCATS Simulation Modeling System

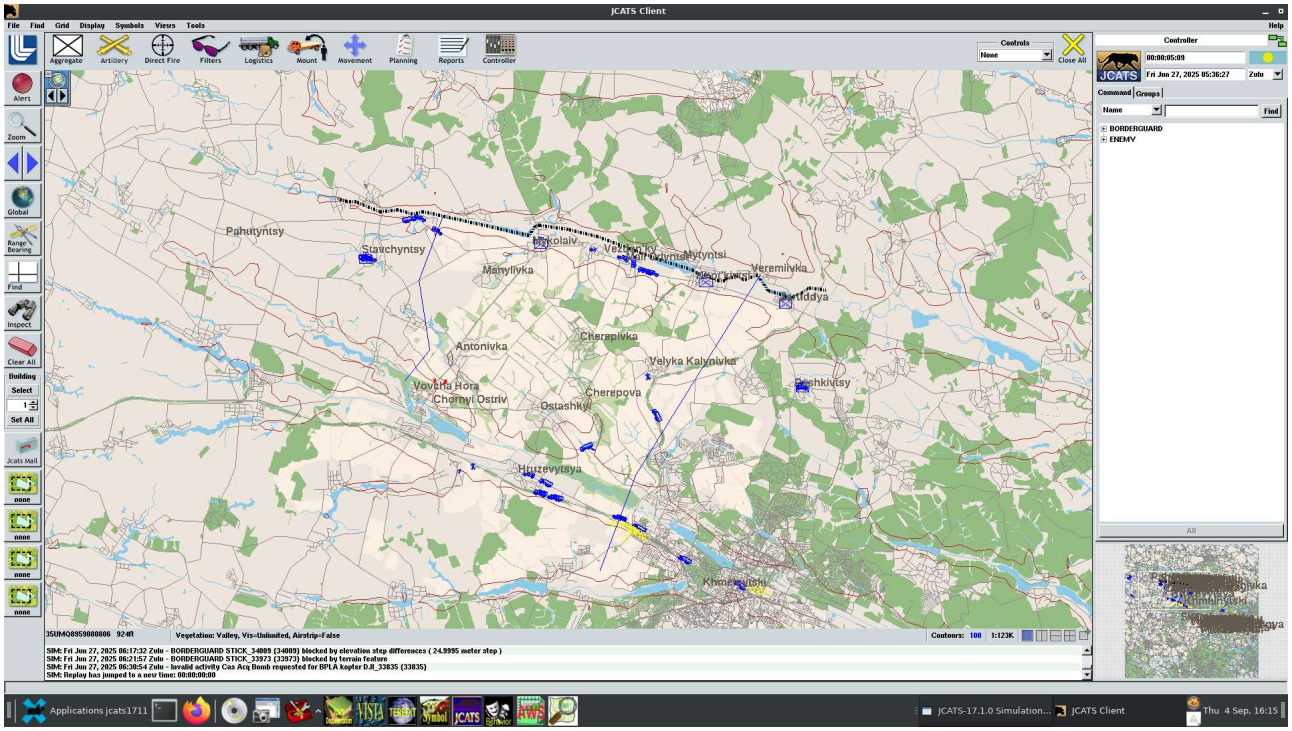


Figure 3 – Simulation of the adopted decision regarding special measures to search for offenders in the JCATS Simulation Modeling System

Thus, based on the results of the conducted command-and-staff exercise (CSE), the effectiveness of the methodology of the work of the headquarters of a border guard detachment regarding the employment of state border protection units using simulation modeling was demonstrated. The work of the commander of the border guard detachment and the staff officers in organizing operational and service activities and in decision-making on special measures to search for offenders was practiced. The methodology using simulation modeling provides the headquarters of a border guard detachment with the opportunity to increase the required level of practical skills in resolving inputs that model various elements of the situation occurring in the operational and service activities of state border protection bodies.

The application of simulation modeling made it possible to model future actions and predict their nature, as well as to carry out preventive measures against the actions of offenders in advance and to assess future decisions. The use of simulation modeling serves as an auxiliary tool in the managerial decision-making procedure.

Conclusions and prospects for further research. Thus, the developed methodology of the work of the headquarters of a border guard detachment regarding the employment of state border protection units using simulation modeling is an auxiliary tool within the decision support system. Based on the conclusions of the approbation of the methodology during the CSE, decision-making using simulation modeling made it possible to:

increase the level of coordination of the command and control bodies of a border guard detachment without involving personnel, equipment, weapons, consumption of fuel and lubricants, and communication means;

reproduce variants of changes in the situation, analyze and assess the actions of various parties under different scenarios in the shortest possible time;

carry out rapid replacement of scenarios for the development of the situation;

model special measures (actions) to search for offenders in order to practice tactical techniques, modernize and improve the organizational and staffing structure of existing units of the State Border Guard Service of Ukraine, determine forms and methods of their employment, and increase the effectiveness of operational and service activities;

verify and assess the adopted decision, which is currently difficult to achieve;

reduce the time required for making a managerial decision by 15% compared to the existing methodology.

The methodology constitutes the fourth simulation-modeling block (a modeling and approbation tool) of the concept “Model of Employment of State Border Protection Units under Conditions of Complication of the Situation.”

In further research, it is advisable to develop scenarios for the development of the situation at the state border and variants of decisions taking into account contemporary threats.

References

1. Shevchuk V. V. (2025). *Analiz naiavnoho naukovo-metodychnoho aparatu zastosuvannia pidrozdiliv Derzhavnoi prykordonnoi sluzhby Ukrainy* [Analysis of the existing scientific and methodological apparatus of the use of units of the State Border Guard Service of Ukraine]. *Natsionalni interesy Ukrainy*, no. 1 (6), pp. 171–180. DOI: https://doi.org/10.52058/3041-1793-2025-3(8)-524-538 [in Ukrainian].

2. Telelym V. M., Muzychenko D. P., Punda Yu. V. (2014). *Planuvannia syl dlia vykonannia boiovykh zavdan u "hibrydnii viini"* [Force planning for combat missions in "hybrid war"]. *Nauka i oborona*, no. 3, pp. 30–35 [in Ukrainian].

3. Romanchenko I. S., Bohdanovych V. Yu. (2012). *Kompleksna metodyka obgruntuvannia zavdan subiektam systemy zabezpechennia natsionalnoi bezpeky shchodo vidvernennia abo neitralizatsii zahroz voiennoho kharakteru dlia derzhavy* [Comprehensive methodology for substantiating tasks for subjects of the national security system regarding the prevention or neutralization of military threats to the state]. *Nauka i tekhnika Povitrianykh Syl Zbroinykh Syl Ukrainy,* no. 2 (8), pp. 120–127 [in Ukrainian].

4. Rebrii I. M., Huzchenko S. V., Teliukov S. M., Taran I. A., Zlyvka H. A. (2018). *Viiskovyi protses pryiniattia rishennia. Osnovy orhanizatsii shtabiv* [Military decision-making process. Fundamentals of headquarters organization]. Kharkiv : KHNUPS [in Ukrainian].

5. Voloshyna, V., Rudnytskyi, A. (2025). A conceptual framework for military crisis decision-making: theoretical and methodological foundations. *Visnyk Natsionalnoho universytetu oborony Ukrainy,* vol. 83 (1), pp. 59–66 [in English].

6. Olenchenko, V., Nemeryshchyn, V., Ihnatiev, A. (2024). Analysis of decision-making support systems in the performance of service and combat tasks by the security forces of Ukraine. *Bezpeka derzhavy*, no. 2 (4), pp. 58–62 [in English].

7. Bohdanovych V. Yu., Romanchenko I. S., Svyda I. Yu., Syrotenko A. M. (2019). *Metodolohiia kompleksnoho vykorystannia viiskovykh i neviiskovykh syl ta zasobiv sektoru bezpeky i oborony dlia protydii suchasnym zahrozam voiennii bezpetsi Ukrainy* [Methodology of the integrated use of military and non-military forces and means of the security and defense sector to counter modern threats to the military security of Ukraine]. Lviv : NASV [in Ukrainian].

8. Kachynskyi A. B. (2004). *Bezpeka, zahrozy i ryzyk: naukovi kontseptsii ta matematychni metody* [Security, threats and risk: scientific concepts and mathematical methods]. Kyiv : IPNB, NA SBU [in Ukrainian].

9. Bratko A. V. (2023). *Metodyka orhanizatsii roboty orhaniv upravlinnia Derzhavnoi prykordonnoi sluzhby Ukrainy shchodo planuvannia operatyvno-sluzhbovoi diialnosti* [Methodology of organizing the work of management bodies of the State Border Service of Ukraine in terms of planning operational-service activities]. *Social development and Security,* vol. 13, no. 1, pp. 29–37. DOI: https://doi.org/10.33445/sds.2023.13.1.4 [in Ukrainian].

10. Bratko A. V. (2022). *Kontseptsiia planuvannia operatyvno-sluzhbovoi diialnosti Derzhavnoi prykordonnoi sluzhby Ukrainy* [Concept of planning operational and service activities of the State Border Guard Service of Ukraine]. *Social development and Security,* vol. 12, no. 6, pp. 1–10. DOI: https://doi.org/10.33445/sds.2022.12.6.1 [in Ukrainian].

11. *Nakaz Ministerstva vnutrishnikh sprav Ukrainy "Pro zatverdzhennia Poriadku roboty orhaniv upravlinnia Derzhavnoi prykordonnoi sluzhby Ukrainy z pidhotovky do operatyvno-sluzhbovoi diialnosti v nastupnomu kalendarnomu rotsi abo inshomu periodi" № 350* [Order of the Ministry of Internal Affairs of Ukraine "About approval of the Procedure for the work of the management bodies of the State Border Service of Ukraine on preparation for operational and service activities in the next calendar year or other period" activity no. 350]. (2018, April 26). *Vidomosti Verkhovnoi Rady Ukrainy.* Retrieved from: https://surl.lu/cwzode (accessed 2 September 2025) [in Ukrainian].

12. Derzhavna prykordonna sluzhba Ukrainy (2006). *Metodychni rekomendatsii shtabam orhaniv (pidrozdiliv) okhorony kordonu z orhanizatsii roboty pid chas uskladnennia obstanovky* [Methodological recommendations to the headquarters of border guard bodies (units) on organizing work during a complicated situation]. Kyiv [in Ukrainian].

Received / Стаття надійшла до редакції: 12.09.2025
Revised / Прорецензовано: 30.09.2025
Схвалено до друку / Accepted: 06.10.2025

ШЕВЧУК ВЛАДИСЛАВ ВАЛЕРІЙОВИЧ
старший викладач кафедри прикордонної служби,
Національна академія Державної прикордонної служби України
імені Богдана Хмельницького
https://orcid.org/0000-0001-5583-2160

МЕТОДИКА РОБОТИ ШТАБУ ПРИКОРДОННОГО ЗАГОНУ ЩОДО ЗАСТОСУВАННЯ ПІДРОЗДІЛІВ ОХОРОНИ ДЕРЖАВНОГО КОРДОНУ З ВИКОРИСТАННЯМ ІМІТАЦІЙНОГО МОДЕЛЮВАННЯ

Автором розроблено методику роботи штабу прикордонного загону щодо застосування підрозділів охорони державного кордону з використанням імітаційного моделювання, що є допоміжним інструментом у системі підтримки прийняття рішень. Методологія забезпечує високий рівень планування оперативної та службової діяльності та надає можливість оцінити прийняте рішення про застосування цих підрозділів на державному кордоні. Основна робота офіцерів штабу органу охорони державного кордону в процесі прийняття рішень полягає в тому, що на основі глибокого та всебічного уточнення завдань, оцінки обстановки, проведення оперативно-тактичних розрахунків, моделювання майбутніх дій, вони готують пропозиції та тим самим допомагають керівнику органу охорони державного кордону у прийнятті обґрунтованого рішення. Прийняття рішень з використанням імітаційного моделювання дозволило: підвищити рівень координації дій органів управління прикордонного загону, без залучення витрат на особовий склад, техніку, озброєння, паливо та зв'язок; відтворити варіанти зміни обстановки, проаналізувати та оцінити дії різних сторін за різними варіантами у найкоротші терміни; провести оперативну заміну сценаріїв розвитку ситуації; моделювати спеціальні заходи (дії) з пошуку правопорушників, відпрацьовувати тактичні прийоми, модернізувати та вдосконалити організаційно-штатну структуру існуючих підрозділів Державної прикордонної служби та визначити форми та методи їх застосування, підвищити ефективність оперативно-службової діяльності; перевірити та оцінити прийняте рішення, що наразі є складним; скоротити час прийняття управлінського рішення на 15 % порівняно з існуючою методикою. Методологія є четвертим блоком моделювання (інструментом моделювання та тестування) концепції "Моделі застосування підрозділів охорони державного кордону в умовах складної обстановки".

Ключові слова: *планування; оперативно-службова діяльність; прийняття рішення; моделювання; застосування підрозділів; процеси управління; підготовка; методика.*

Наукове видання

НАУКОВИЙ ВІСНИК КИЇВСЬКОГО ІНСТИТУТУ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ

Науковий журнал (півріччник)

№ 2 (7) 2025

Відповідальний за випуск *В. О. Галай*
Редактор *Я. М. Холоденко*
Комп'ютерне складання і верстання *Ю. І. Медвідь*

Підписано до друку 26.12.2025.
Формат 60х84/8. Папір офсет. Умовн. друк. арк. 20,9.
Наклад 50 прим. Зам. 248

Видавець і виготовлювач: Київський інститут Національної гвардії України.
Адреса: вул. Оборони Києва, 7, м. Київ, 03179

Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців, виготовлювачів і розповсюджувачів
видавничої продукції Серія ДК № 7696 від 8.11.2022 р.

S c i e n t i f i c p u b l i c a t i o n

SCIENTIFIC BULLETIN
OF THE KYIV INSTITUTE OF THE NATIONAL GUARD OF UKRAINE

Scientific journal (semiannual)

No. 2 (7) 2025

Responsible for the publication *V. Halai*
Editor *Ya. Kholodenko*
Computer assembly and layout *Yu. Medvid*

Signed for publication 26.12.2025
Format 60x84/8. Offset paper. Approx. printed pages. 20.9
Edition of 50 copies. Order No 248

Founder and publisher: Kyiv Institute of the National Guard of Ukraine.
Kyiv, 7, Oborony Kyieva Str., 03179

Certificate of registration of a publishing entity to the State Register
of Publishers, Manufacturers and Distributors of Publishing
Products Series DK No 7696 dated 8.11.2022.