№ 4’2024

НАУКА і ОБОРОНА

Щоквартальний науково-теоретичний та науково-практичний журнал

Передплатний індекс 74303

ISSN 2618-1614 (Print)
ISSN 2618-1622 (Online)

Видається з 1994 р.

Зміст

Актуальні питання національної безпеки та оборони

Komarov V. S., Oleksiiuk V. V., Shcherban K. A. Key elements of Russian Federation's strategic adaptation for sustaining a prolonged war of attrition against 3

Драпатий М. В., Дзюба Т. М., Костенко А. М., Самарський О. О. Аналіз заходів інформаційної боротьби збройних сил Російської Федерації в районах ведення бойових дій 13

Волотівський П. Б., Стешенко П. М., Богославець С. О., Корепанов В. В. Щодо обрису перспективної системи боротьби з безпілотними авіаційними комплексами 24

Розвиток теорії та методології

Коваль М. В., Косевцов В. О., Телелим В. М., Захаржевський А. Г. Методичний підхід до прогнозування узагальненого конфліктогенного індексу можливого воєнного конфлікту 33

Сніцаренко П. М. Кібероборона України як складова оборони держави 40

Сафронов О. В., Семон Б. Й., Неділько О. М. Математична модель оцінки розташування стрибків ущільнення на поверхні аеродинамічного профілю 49

Національна безпека та оборона: методичний аспект

Загорка О. М., Поліщук С. В., Загорка І. О. Обґрунтування вимог до ефективності застосування сил протидії повітряному противнику в оборонній операції 54

Summaries.....60

Contents

Topical issues of national security and defence

V. S. Komarov, V. V. Oleksiiuk, K. A. Shcherban. Key elements of Russian Federation's strategic adaptation for sustaining a prolonged war of attrition against 3

M. V. Drapatyi, T. M. Dziuba, A. M. Kostenko, O. O. Samarskyi. Analysis of information warfare activities of the armed forces of the Russian Federation in areas of combat operations 13

P. B. Volotivskyi, P. M. Steshenko, S. O. Bohoslavets, V. V. Korepanov. Regarding the outline of a prospective system for combating unmanned aerial systems 24

Development of theory and methodology

M. V. Koval, V. O. Kosevtsov, V. M. Telelym, A. H. Zakharzhevskyi. Methodological approach to predicting the generalized conflict-generating index of a possible military conflict.....33

P. M. Snitsarenko. Cyber defence of Ukraine as a component of state defence 40

O. V. Safronov, B. Y. Semon, O. M. Nedilko. Mathematical model for estimating the location of shock waves on the surface of an aerofoil 49

National security and defence: methodical aspect

O. M. Zahorka, S. V. Polishchuk, I. O. Zahorka. Substantiation of the requirements for the effectiveness of the use of air defence forces in defensive operations 54

Summaries.....60

DOI 10.33099/2618-1614-2024-27-4-3-12
UDK 355.5

V. S. Komarov,
Doctor of Military Sciences, Professor,
Defence Intelligence Research Institute,
V. V. Oleksiiuk,
Candidate of Military Sciences, Senior Researcher,
Defence Intelligence Research Institute,
K. A. Shcherban,
Defence Intelligence Research Institute

Key elements of Russian Federation's strategic adaptation for sustaining a prolonged war of attrition against Ukraine

This article analyses the key elements of the Russian Federation's strategic adaptations for sustaining a prolonged war of attrition against Ukraine. The objective is to identify critical vulnerabilities susceptible to asymmetric impact, which could establish conditions that compel the Russian Federation to abandon its military and political objectives in its armed aggression against Ukraine.

Keywords: asymmetric impact, critical vulnerabilities, DIME means, scenarios, strategic adaptation, war of attrition.

Formulation of the Problem. In both Western and Ukrainian information spaces, discussions are increasingly focusing on possible scenarios for the end of the Russian-Ukrainian war. However, regardless of the predictions [1–2], the Russian Federation's (RF) continued pursuit of its military and political objectives into the third year of full-scale aggression against Ukraine indicates one clear reality: the war is far from over and has evolved into a prolonged war of attrition. This phase is characterized by significant personnel losses, extensive destruction of weapons and specialized military equipment, massive resource expenditures, and minimal shifts in the front line [3–8].

Nevertheless, the RF's willingness to commit substantial resources has prompted a re-evaluation of the initial invasion strategies, leading to strategic adaptations in four key areas: military, political, economic, and informational. A thorough study and comprehensive analysis of actions and measures in these areas will enable us to assess the RF's capacity to sustain a prolonged war of attrition and to identify critical vulnerabilities across various sectors and institutions.

These vulnerabilities must be systematically and comprehensively targeted through DIME (Diplomatic, Information, Military, and Economic) means [9], which, in turn, could compel the RF to cease its armed aggression and bring an end to the Russian-Ukrainian war.

An analysis of recent studies and publications [3–8] reveals that think tanks and researchers have begun examining how the RF has implemented adaptation measures to build the necessary capabilities for a prolonged war of attrition against Ukraine. Specifically, these studies highlight Russia's ability to transition its national economy to a wartime footing, expand and enhance its defence industry's production and technological capabilities, incorporate lessons learned and combat experience, and adapt swiftly to dynamic situations. However, these studies primarily provide an overview of Russia's capacity for sustained warfare and, unfortunately, do not propose any mechanisms for counteracting it.

Therefore, **the purpose and main focus of this article** are to identify the key components of the RF's strategic adaptations that restore and strengthen its capacity for a prolonged war of attrition against Ukraine.

Summary of Main Research Material

An analysis of the Russian-Ukrainian war and the lessons learned reveals that the RF is continuously seeking to enhance the effectiveness of its armed forces by increasing troop numbers and equipment, altering military leadership, and adjusting tactics and methods of

deployment. According to the authors, RF's strategic adaptation to a prolonged war of attrition involves four key elements: military, political, economic, and informational (*Fig. 1*). Military reforms are being implemented; the defence industry is undergoing modernization; significant financial resources are invested in raising the technological capabilities of the RF's armed forces; the configuration of RF's international partnerships (including alliances with China, Iran, North Korea, and the Global South) is evolving; and there is an escalating militarization of Russian society, among other developments.

Fig. 1. Four key elements of the RF's strategic adaptation

A detailed analysis of each of the elements above will enable us to identify critical vulnerabilities and leverage asymmetric impacts that could compel the RF to halt its armed aggression by diminishing its relevant capabilities.

Military Element

Changes in Command and Control Systems and Organizational Structure of Troops. Following the unsuccessful blitzkrieg attempt under the slogan «Kyiv in Three Days,» Russia adapted its command and control structure to the new realities of warfare. In April 2022, a single commander was appointed to coordinate the full-scale invasion, leading the Russian armed forces to abandon the decentralized and fragmented command system initially employed. This resulted in a consolidation and unification of efforts, shifting the Russian invasion from multiple disjointed campaigns across northern, eastern, and southern Ukraine to more concentrated operations in defined areas in eastern and southern Ukraine.

At the outset of the full-scale invasion, the RF deployed battalion and company tactical groups, which ultimately proved insufficient in strength and limited in their ability to achieve strategic objectives. After a year of war, the Russian armed forces moved away from these tactical groups, reverting to a regimental and divisional structure within the ground forces. Essentially, above the battalion level, Russian forces have returned to the traditional Soviet-style combat organization of regiments, divisions, and combined arms armies. Meanwhile, the structure below the regiment has been significantly modified, with battalions now restructured to perform specifically in classical and assault operations.

As the organizational structure of the RF's armed forces has changed, the forms and methods of their deployment have also evolved, refining existing tactics and fostering the development of new warfare strategies.

The tactics for conducting assault operations have shifted to the so-called «meat assaults». This tactical adjustment arose from military necessity, particularly due to insufficient time to train mobilized personnel to a high level of combat readiness. The leadership of PMC Wagner championed this «meat tactics» approach, using convicts to breach our troop positions, which ultimately led to the capture and occupation of Lysychansk, Soledar, and Bakhmut.

The RF's manpower can likely be maintained at current levels for the next five to seven years, though the same cannot be said for weapons, military, and specialized equipment. The enemy is attempting to offset shortages in armoured vehicles by deploying light, mobile vehicles such as buggies, ATVs, and motorcycles. This adaptation aims to «conserve» armoured vehicles during assaults and relies on ground personnel as a substitute. Despite significant losses, the Russian armed forces continue to meet personnel demands without initiating a second wave of mobilization. In September 2024, a presidential decree increased the Russian army's personnel by 180,000, bringing the number of active-duty military personnel to 1.5 million [10].

The Russian authorities aim to recruit approximately 225,000 contract soldiers annually by 2027, with relevant funding allocated in the draft federal budget of the RF. Additionally, Russian legislation has been amended to dismiss criminal charges against individuals who sign military contracts that involve participation in the war against Ukraine. The Russian army's personnel in the occupied territories of Ukraine is estimated at around 600,000. This figure represents nearly half of Russia's total active military force and is almost equivalent to the official count of contract soldiers reported by RF [11].

If enemy losses continue at the current rate of approximately 30,000 personnel per month, RF's operational reserves are expected to be depleted by 2025. However, its full mobilization reserves could potentially

last until 2032 [12]. Additionally, the RF is raising the conscription age to increase the number of conscripts who will join the operational reserve after completing their military service. In total, annual conscription in RF could reach up to 400,000. The primary constraints on the size of the Russian army are the financial strain on the budget, the impact on the Russian economy, and the willingness of Russian citizens to participate directly in the war.

Offensive Capabilities

The Russian armed forces are bolstering their offensive capabilities by expanding the volume, forms, and methods of employing ground- and air-based strike systems. The extensive use of reconnaissance UAVs has significantly shortened the time between target detection and strike initiation, enabling the creation of reconnaissance-strike channels with varied firepower and minimal intelligence cycle times.

The Russian aerospace forces have adapted their tactics and methods of operation. The enemy now conducts airstrikes in grouped, massive, or combined assaults on Ukrainian territory, deploying attack drones, land-, sea-, and air-launched cruise missiles, ballistic and aerial ballistic missiles, guided and FAB-series aerial bombs equipped with UPMK kits. These strikes are executed in multiple waves, utilizing a broad range of precision weaponry. Post-strike reconnaissance assesses the impact, informs future attacks, and identifies vulnerabilities in Ukraine's air defence system.

During these strikes, the use of cruise and ballistic missiles in concentrated attacks has decreased, with a shift toward a coordinated approach involving diverse aerial systems. «Star raids» are employed, in which a localized group of closely positioned targets is attacked from multiple directions nearly simultaneously by air defence systems. The enemy also conducts simulated launches and deploys decoys (booby traps) to mislead defences, aiming to achieve surprise in SAM usage and reduce flight time. Launches are carried out under limited visibility and at low or extremely low altitudes, with some targets receiving multiple SAM hits, among other tactics.

The shortage of precise missile weaponry for striking critical infrastructure, industrial, and military facilities in Ukraine has compelled the RF to begin mass production of aerial bombs of various calibres. The introduction of the UMPK kit has enhanced both the accuracy and range of these bombs. Additionally, the enemy has adapted to transition from targeting a single direction to executing sequential strikes from multiple directions within the same flight. Airstrikes are accompanied by intensive jamming and the use of anti-radar missiles targeting Ukraine's anti-aircraft and radio engineering troops, all while avoiding the line of contact and staying outside the range of Ukraine's air defence systems.

Defence Capabilities

Relevant adaptive changes have also impacted the defensive organization of Russian troops in the temporarily occupied territories of southern Ukraine. In the second half of 2023, the Ukrainian Defence Forces encountered an enemy markedly different from that of 2022. Following initial efforts to fortify vulnerable positions at the start of the war, by late 2022 and early 2023, the Russian armed forces had established deeply entrenched defensive lines, reinforced with multi-layered minefields, across the temporarily occupied territories.

The effective use of attack UAVs (FPV drones) by the Ukrainian Defence Forces has compelled the Russian armed forces to seek protective measures against them. Significant attention has been given to shielding armoured combat vehicles from FPV drones and anti-tank missile systems, aiming to enhance the physical security of these vehicles and boost crew confidence in high-risk areas. Protective structures, so-called «mangals», are now being produced on an industrial scale, not only for armoured vehicles but also for trucks, self-propelled artillery systems, pickup trucks, and high-mobility bikes.

The enemy has also significantly enhanced its strike drone capabilities, shifting previous dynamics. Early in the war, Ukraine pioneered innovative UAV applications for reconnaissance, artillery adjustment, precision strikes, and direct engagement, giving the Ukrainian Defence Forces a significant advantage. Although the Russian armed forces were slower to adopt UAV tactics, they now surpass Ukraine in UAV production and loitering munitions, with this gap likely to widen further.

The Russian armed forces have adapted to the Ukrainian Defence Forces' use of precision weapons equipped with advanced global navigation satellite systems for accurate targeting (including HIMARS and precision artillery ammunition). They have managed to reduce the effectiveness of these weapons through the use of electronic warfare (EW) systems and counter-measures.

Electronic warfare (EW), traditionally a strong suit of the Russian armed forces, appeared to play a minor role in the early phase of the full-scale invasion of Ukraine. However, after RF regrouped following its initial setbacks, EW was once again actively employed. The enemy has since intensified efforts to develop, produce, and deploy new mobile EW systems, enhancing existing ones – including the so-called «trench» EW to counterattack UAVs and FPV drones – and introducing new roles within the organizational structure of the forces.

Thus, an analysis of the RF's military adaptations for a prolonged war of attrition against Ukraine reveals that enhancements to its command and control structure, organizational framework, mobilization resources, and defence capabilities – along with the restoration of offensive potential through the development, modernization, and production of advanced combat systems and the use of reconnaissance-strike circuits – position the RF to pursue its offensive and aggressive plans in the long perspective.

Economic Component

RF continues to take steady measures to adapt its economy and defence industry to sustain a prolonged war of attrition. Trends in the GDP of the RF indicate that economic sanctions imposed by the collective West have not achieved the intended impact, with the RF managing to increase its GDP following a decline in 2023 (*Fig. 2*).

The dynamics of total military spending shows that RF does not intend to end the war against Ukraine in the near future, but rather is adapting to a long war by increasing the amount of this spending (*Fig. 3*).

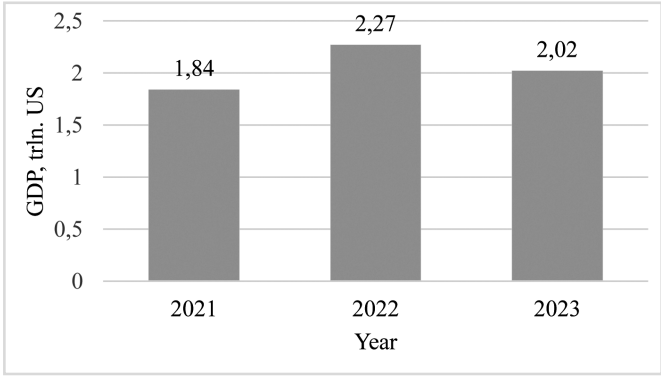

Fig. 2. The dynamics of changes GDP of the RF in 2021–2023 [13]

The analysis indicates a tendency for the Russian government to conceal and inflate the amount of classified military expenditures related to the Russian-Ukrainian war.

A significant factor influencing the economic aspect of the RF's strategic adaptation to the war of attrition is the volume of hydrocarbon production. Despite Western sanctions imposed due to the war in Ukraine, the RF's revenues from fossil fuel production increased by 41% in the first half of 2024 alone [18]. To ensure sustainable financing of military expenditures related to its war against Ukraine, the RF was compelled to increase production volumes, violating certain agreements with OPEC+.

A drop in oil prices by 20 US dollars at the current exchange rate in September 2024 would result in RF losing 1.8 trillion roubles (20 billion US dollars), which is about 1% of its GDP. This would force RF to either reduce funding for the war, which is unlikely, or accept rising inflation and higher interest rates [18] amid already galloping inflation in RF. The inflation target of 4% set by the Central Bank of the RF will not be achieved by the end of the year. At the end of 2024, inflation is expected to remain high (7% on average), with a tendency to slow down in November and December amid the tight monetary policy of the Russian state regulator.

In the summer of 2022, a number of laws and government decrees were adopted, which effectively put Russian defence industries under martial law, increasing the number of shifts and working days per week. This significantly mobilized the defence industry, in particular, by expanding production lines at existing enterprises, as well as returning to work at previously mothballed ones.

In addition to increasing its own military production, RF is purchasing weapons, ammunition, and special equipment from authoritarian states such as North Korea, Iran, and China. RF has also strengthened its position by

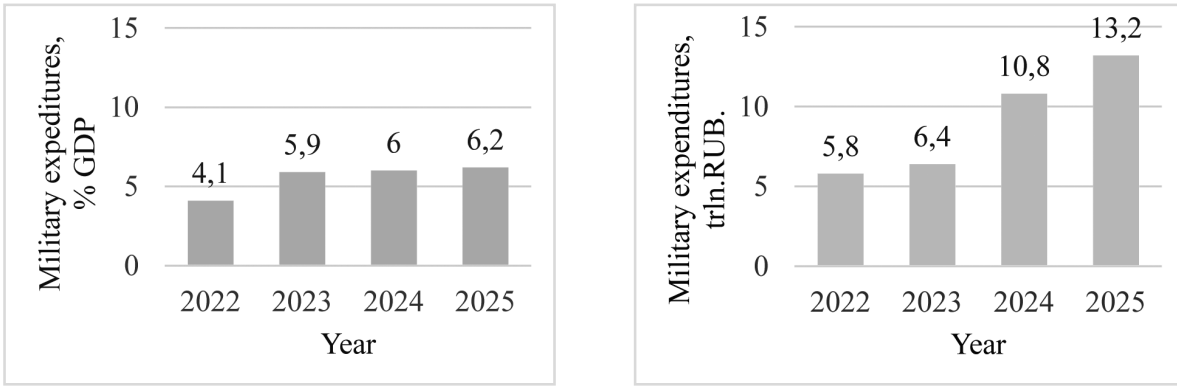

Fig. 3. Dynamics of total expenditures on military needs of the RF and their percentage of GDP in 2022–2025 [14–17]

purchasing equipment and critical electronic components through third countries that it cannot buy in the West due to sanctions. About 70% of machine tools and 90% of microelectronics imported by RF come from China and Hong Kong, which helps it produce missiles, armoured vehicles and ammunition for its war of attrition against Ukraine [19]. Chinese companies supply RF with specially designed military UAVs for testing and use by the Russian armed forces on the battlefield in Ukraine, a relevant agreement on which was signed last year [20].

Russia compensates North Korea and Iran for the arms and ammunition supplied through contracts for the sale of modern aircraft, the transfer of critical missile and nuclear weapons components, and space production technologies, as well as through the provision of food and other resources.

Russia's military-technical cooperation with China, India, Iran, and other countries in Asia, Africa, and South America is being developed and strengthened. This cooperation aims to participate in joint projects for the development of weapons, military, and special equipment in exchange for the material resources needed by Russia to sustain its war of attrition against Ukraine.

The Russian defence industry continues to produce missile weapons despite tough international sanctions. The monthly production rates are as follows: cruise missiles Kh-101 and ballistic missiles «Iskander-M» – 40 to 50; sea-based missiles «Kalibr» – 30 to 40; cruise missiles «Iskander-K» – 10 to 15; anti-ship missiles «Onyx» – up to 10; and aeroballistic missiles Kh-47M2 «Kinzhal» – 2 to 6. The production rate of «Shahed-136» attack drones exceeds 500 per month, with an upward trend.

According to estimates [21], the production of missiles on this scale costs the RF approximately 1.1 billion US dollars per month, while the production of attack drones costs about 100 million US dollars. As of the end of August and the beginning of September 2024, the RF had approximately 1,220 cruise missiles and 245 ballistic missiles in its stockpile [21]. The development of strike UAVs, aerial bombs with UMPK, and samples of robotic ground strike and reconnaissance systems is ongoing, and new facilities are being established for the development, production, and repair of armaments. The weapons, military and special equipment, strike UAVs, interceptor UAVs, FPV drones, and surface combat unmanned aerial vehicles used by the Ukrainian Defence Forces – produced by the national defence industry or provided as military and technical assistance by partner countries – are being replicated.

The production of armoured combat vehicles in the RF relies on existing military stocks from storage facilities and repair centres. Approximately 80% of tanks and other armoured vehicles are not new but have been repaired and modernized. The volume of these stocks allows the RF to maintain a stable level of production until the end of 2024. However, by 2025, it will begin to face the need for more extensive modernization of its equipment, and by 2026, most of its existing stocks are expected to be exhausted.

As the availability of repaired equipment decreases, industrial capabilities may shift toward the creation of new combat platforms. This transition will likely result in a significant reduction in the number of vehicles supplied to the Russian armed forces in the near term. In 2022, the RF restored approximately 60 tanks per month from its reserves, with plans to increase that number to 90 per month in 2023 [22]. Additionally, RF produces about 20 new tanks per month, primarily the T-90 and T-80 models [22].

If the current trend of restoration and production continues, and the rate of losses for Russian battle tanks remains consistent with that of 2024, the Russian armed forces will be adequately supplied with tanks at least until the end of 2026. Should the losses of battle tanks remain below 150 per month, the recovery resource could last until 2028.

Thus, it can be asserted that the Russian defence industry has developed an extended and continually improving cycle of adaptation that integrates lessons learned from combat operations with Russian industrial capabilities and strategies for utilizing existing and future military resources. Given this dynamic, the Russian armed forces could achieve a significant military advantage, which, if not countered in a timely manner by targeting specific «critical vulnerabilities», may evolve into a strategic advantage in a prolonged war of attrition.

Political Element

RF's strategic adaptation to the war of attrition is also evident in the political sphere, where it is reconfiguring its international network of partners. This shift involves strengthening cooperation with autocracies such as China, Iran, and North Korea. Within this coalition, RF is actively working to establish a unified anti-Western stance, aiming to position itself as a potential global centre of power.

Despite being significantly supported by China – the world's second-largest economy and a key global power – in light of the sanctions imposed by the «collective West», Iran has been reluctant to formalize a comprehensive friendship agreement with RF since 2022, even under immense pressure. On the other hand, the RF seeks to position itself as a key player in a strong and united Global South, particularly by expanding the BRICS interstate coalition. RF's efforts are directed at transforming BRICS into a geopolitical and economic rival to the G7 bloc. At the beginning of this year, at the initiative of the Russian Federation, Egypt, Ethiopia,

Iran, the United Arab Emirates, and Argentina were invited to join BRICS; however, Argentina declined the invitation. Between August and October of this year, several additional countries submitted applications to join BRICS, including Cuba as a «partner country», Azerbaijan, Turkey, Malaysia, and Sri Lanka, which formally applied for membership during the summit in Kazan. The BRICS summit in Kazan demonstrated that none of Putin's «global ideas» garnered support among the participants, as none of the attendees expressed any intention of «fighting the West» or transforming the bloc into an anti-Western platform. The summit concluded with a conditional signing of the declaration.

RF actively supports China's «peace initiative», promoting it as a project that positions China as a peacemaker. However, there are significant doubts about China's neutrality, particularly given the backing of the Chinese plan by the RF, which serves as an alternative to the Ukraine's Peace Formula. This formula is grounded in the norms and principles of the UN Charter. Additionally, China continues to provide a wide range of products, including dual-use and military goods, to the RF.

The new six-point Chinese-Brazilian «peace initiative» calls for an immediate cessation of hostilities, de-escalation of tensions, and the commencement of peace talks between Kyiv and Moscow, without requiring the Russian Federation to withdraw its troops from the occupied Ukrainian territories. Previously, China had proposed a 12-point plan, but notably, the provision regarding respect for the territorial integrity of «all countries» was omitted from the latest initiative. In this context, the RF has indicated that it will conduct negotiations solely based on the current situation at the front, meaning that it considers the line of combat contact at this moment and asserts that the territories captured during the conflict should remain with RF. Brazil and China are aware of this but have refrained from condemning the aggressive stance of the Russian Federation, which violates the UN Charter. China, Brazil, and several other countries in the Global South – such as Colombia, Egypt, Indonesia, Mexico, Saudi Arabia, South Africa, and the United Arab Emirates – have agreed to establish the «Friends of Peace» platform. Within this framework, they plan to promote a peaceful resolution to what China refers to as the «Ukrainian crisis» (as China calls the Russian war against Ukraine). Thus, through the Sino-Brazilian plan, the RF is attempting to de jure «legalize» its occupation of part of Ukrainian territory, potentially setting a precedent for future illegal territorial annexations around the world through military force.

Particular attention should be given to the outcome of the successful pressure exerted by the RF on Germany. This pressure has led Germany, one of Ukraine's key military allies and the primary supplier of assistance from the EU, to change its rhetoric. Germany now intends to postpone the delivery of the planned volume of heavy equipment to the Armed Forces of Ukraine, citing a lack of belief in a successful offensive to liberate the occupied territories. Meanwhile, the RF is demonstrating a steady pace of advancement into Ukrainian territory in 2024, despite significant losses. Additionally, the number of combat engagements in September has increased by nearly 20% compared to August (see *Fig. 4*).

In October this year, Russia captured 490 square kilometres, marking the largest territorial gain for 2024 and for the RF forces' counteroffensive, ongoing since October 2023 [23].

Of particular concern is the successful deepening of ties and «comprehensive» cooperation with North Korea, which not only produces and supplies weapons and ammunition to the RF, but has also begun to implement

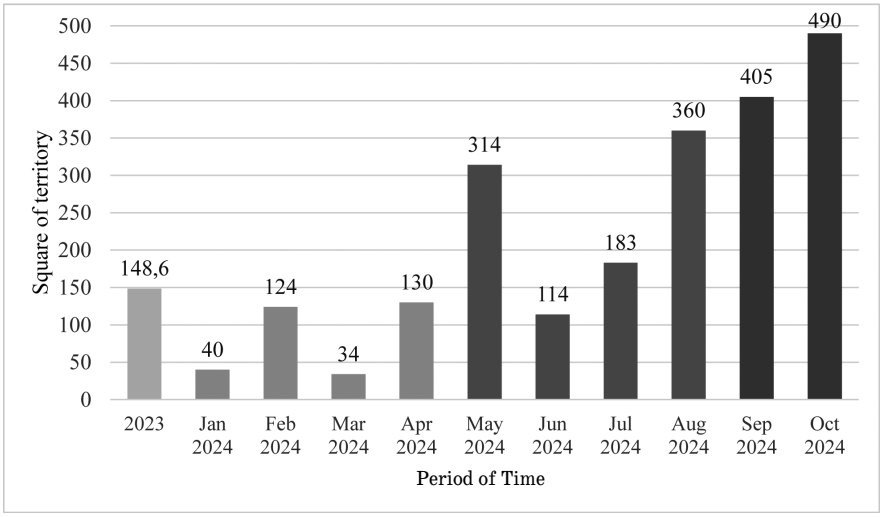

Fig. 4. Ukraine occupied territory by the RF in 2023 and monthly during 2024

concrete steps to transfer a contingent of its troops to the territory of the RF, as well as to the Kursk region. North Korea can organize, at the request of the Russian Federation, the production of weapons and military equipment, ammunition of the required nomenclature on its own territory, as well as provide significant human resources that are vital for the Russian Federation in continuing the war against Ukraine.

In exchange, RF supplies North Korea with modern military technologies to upgrade its weaponry, has agreed to test specific models in real combat conditions in Ukraine, and may even be transferring technology for nuclear weapon production.

The RF's implementation of strategic adaptation measures in the political sphere points to its efforts to restore former geopolitical influence and forge coalitions with countries that share an anti-Western stance. Additionally, Russia aims to align with coalitions within the Global South.

These actions are intended to create favourable conditions for Russia to exert pressure, potentially suspending active hostilities in the Russia-Ukraine war, re-establishing relations with the collective West, and positioning itself as a key player in shaping a new global order.

Informational element

The informational aspect of the RF's strategic adaptation to a war of attrition has evolved into a targeted information war against Ukraine. Through an effective propaganda apparatus that leverages media and internet platforms, the RF imposes Kremlin narratives on a global audience in multiple languages. Following the Goebbels principle – «the bigger the lie, the more it will be believed» – this mechanism uses bias, manipulation, and fact distortion to shape perceptions worldwide.

The full-scale invasion of the RF in Ukraine, launched on February 24, 2022, gave new momentum to Russian media operations, reinforcing their ongoing practice of creating fake news and disinformation – a tactic they have employed since 2014. This disinformation includes fabricated stories purportedly from residents of «liberated» territories, staged reports from occupied areas of Ukraine, as well as short propaganda films and videos.

Representatives of the Russian leadership and its diplomatic corps disseminate false information about Ukraine in their speeches, including those at the UN, and unfortunately, their efforts often achieve their intended goals. A key element of Russian disinformation is the accusation of the Ukrainian authorities of Nazism, portraying Ukraine as a Nazi state, despite the fact that the Verkhovna Rada of Ukraine has enacted a law condemning the National Socialist regime. Additionally, Russian propaganda propagates the fiction of an exclusive right to Ukrainian territory based on its history as a former part of the Russian empire.

Below are the significant areas of the informational component of the RF's strategic adaptation to a war of attrition, which, in the opinion of the authors of the article, have seen certain successes.

Activities of the Russian Orthodox Church

The Russian Orthodox Church, a Kremlin-controlled organization and a tool in RF's hybrid warfare strategy, convened the so-called World Russian People's Council in Moscow on March 27–28, 2024. During this event, it approved an ideological and political document that synthesized several Kremlin narratives, seemingly aimed at further establishing a nationalist and ideological foundation for the war in Ukraine and RF's expansionist ambitions in the foreseeable future. The invasion of Ukraine was described as a jihadist-style «existential and civilizational holy war,» with the assertion that the entire territory of modern Ukraine should be included in the zone of exclusive influence of the RF [24].

Furthermore, the leadership of the Russian Orthodox Church actively lobbies at the state level for the endorsement and promotion of the ideology of the «trinity doctrine.» This concept, rooted in the Russian tsarist era, denies the existence of Ukrainians and Belarusians as separate, self-sufficient nations [24].

In its religious activities, the Russian Orthodox Church employs a «double» rhetoric, simultaneously promoting peacekeeping messages alongside military ones. This approach manipulates the perceptions of its parishioners, allowing the Church to maintain its image as a «peaceful» institution. An analysis of the frequency of peacekeeping versus military rhetoric from January 01, 2022, to August 18, 2024, reveals that military language is nearly five times more prevalent than peacekeeping language.

Since the early days of RF's full-scale invasion of Ukraine, priests of the Russian Orthodox Church have actively recruited from among their congregants and Russian society at large, targeting individuals willing to go to war in Ukraine with promises of financial benefits. Their goal of establishing the first private military company under the Church's protection is being realized with some success. Currently, clergy are mobilizing both fellow clergymen and believers on a contractual basis to recruit new volunteers prepared to die in Ukraine for the ideals of nationalism and the «Russian world.» The first private «church army» – essentially a military company – was organized by priests of the Kronstadt St. Nicholas Cathedral in St. Petersburg, with the initial volunteer battalions named the St. Andrew's Cross.

Thus, the Russian Orthodox Church continues to serve as a key tool for militarizing Russian society, legitimizing

and justifying military actions, particularly acts of aggression and violence against Ukraine. Its role in the context of this aggressive war extends beyond spiritual support, becoming an integral part of state policy that ideologically justifies military actions to the unwitting Russian public as a «righteous» endeavour to defend the fatherland. Emphasizing the «sacred» nature of these actions, the Church frames them as necessary to eliminate the «oppression of Orthodox believers» in Ukraine.

Changes in the nuclear doctrine of the RF in view of its withdrawal from the Treaty on the Reduction and Limitation of Strategic Offensive Arms

On September 25 of this year, the president of the RF announced new principles for the use of nuclear weapons and the commencement of work on amending the document «Fundamentals of State Policy in the Field of Nuclear Deterrence.» Since the outset of RF's invasion of Ukraine, the president has repeatedly referenced nuclear weapons in his public rhetoric as a means of threatening the «collective West» and as a «red line» in response to the provision of high-tech weapons to Ukraine as part of military and technical assistance. In February 2023, RF suspended its participation in the Strategic Offensive Arms Treaty, and in March 2023, a decision was made to deploy tactical nuclear weapons in Belarus. At the end of May 2024, the RF conducted an exercise involving the relocation and deployment of tactical nuclear weapons. Each time, Putin's statements regarding the use of nuclear weapons have resonated with the international community and influenced the level of support for Ukraine from its partners.

The RF views the amendments to its nuclear doctrine as «a certain signal to unfriendly countries» that they should heed [25]. Simultaneously, the six-point Sino-Brazilian «peace initiative,» announced on the «Friends of Peace» platform, clearly outlines key principles against the irresponsible use of nuclear weapons. These principles include: countering the use of nuclear, biological, and chemical weapons; preventing the proliferation of nuclear weapons; avoiding nuclear crises; and countering armed attacks on peaceful nuclear facilities. This was emphasized at a joint press conference in New York on September 28, 2024, by the head of the Chinese Ministry of Foreign Affairs and the Special Representative of Brazil. Following this, on September 30, 2024, the RF issued an official statement clarifying that the adjustment of its nuclear doctrine was not a response to recent events in the Russian-Ukrainian war. Additionally, a former deputy foreign minister of India warned that if the RF were to be the first to use nuclear weapons, it would lose the support of the Global South.

Thus, the RF's attempts to modify its nuclear doctrine stem from its current weaknesses and inability to adequately respond to the potential authorization for Ukraine to use long-range Western weapons against targets deep within Russian territory. The clause in the nuclear doctrine stating that RF may use nuclear weapons in response to the alleged «aggression» of non-nuclear countries supported by nuclear countries effectively serves as a formal legitimization of a nuclear strike on Ukraine in the eyes of the international community.

Propaganda of Russian Narratives in the Media Space

Within RF's information space, public opinion has been shaped to support the need for military action in neighbouring countries. New narratives have emerged, portraying RF as a victorious nation in World War II, as a protector of the «Russian world» and Russian-speaking populations. This has fostered a distorted worldview and mindset, with intense suppression of dissent and rampant censorship. These narratives have laid the ideological groundwork for Russians to accept and justify plans to restore elements of the former Soviet Union, particularly by bringing Belarus and Ukraine back into RF's sphere of geopolitical influence. They have also fuelled the perception of a new enemy in the «collective West,» portrayed as a threat to RF. Unfortunately, this ideological framework has been effectively implemented.

Currently, the Kremlin's narratives and deliberately distorted facts about global events, elite relationships, and assessments of certain international and regional issues – particularly the Russian-Ukrainian war and related relations – are systematically presented to Western audiences through a network of online publications, television channels, and other media outlets.

Today, the RF makes extensive and largely uncontrolled use of digital propaganda, leveraging AI technology and its powerful capabilities to generate images, memes, videos, and news. Rather than engaging rationally with audiences, Russia employs these tools to overwhelm people with a flood of false information. For individuals easily influenced by propaganda, this barrage embeds itself at a subconscious level, shaping a distorted perspective on the events in Ukraine. Russian propaganda aims not only to persuade its target audience but also to undermine trust in other countries. In other words, the effectiveness of Russian propaganda is not solely based on fostering belief in specific false narratives, but rather in eroding the target audience's trust in their own democratic systems and leaders. Furthermore, Russian propaganda intertwines numerous parallel narratives in a systematic, coordinated manner to enhance its impact.

The economic sanctions, international political pressure, and substantial losses of personnel, weaponry, and military equipment sustained by the Russian armed forces in the third year of the war against Ukraine have led to notable shifts in the information and media landscape

surrounding the aggression against Ukraine. As a result, the Federal Service for Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor) in RF strictly monitors the presence of any «inaccurate information regarding the special military operation of the Russian armed forces to protect Donbas.» Media control in Russia, including online platforms, is nearly absolute, with coverage of the war and other foreign news on major Russian sites closely mirroring state narratives. This extensive censorship aims to prevent the dissemination of factual information about the current state of the Russia-Ukraine war to ordinary Russian citizens, thereby creating an artificial information vacuum around this issue. The lack of truthful information about the nature and consequences of the conflict has contributed to the indifference of the Russian public toward the war, as well as an increase in the number of individuals willing to join the occupation forces.

The RF persistently makes successful attempts to destabilize the situation in EU member states through coordinated disinformation campaigns, foreign information manipulation, and malicious actions in cyberspace. The result of these activities is the rise of pro-Russian politicians and parties that shift the vector of political support for Ukraine in Europe. Notable examples include the ascent to power of pro-Russian parties with openly anti-Ukrainian rhetoric in Austria, the Czech Republic, and Slovakia.

Thus, the analysis of the aforementioned elements and the measures taken by the RF provides insight into its ongoing strategic adaptation to a prolonged war of attrition against Ukraine. Consequently, it is essential to identify «critical vulnerabilities» within this strategy, as exploiting these vulnerabilities could undermine the RF's capacity to sustain a long-term war of attrition – not only in Ukraine but also in future armed conflicts.

Conclusion

Thus, RF's strategic adaptation to the war of attrition is taking place across military, political, economic, and informational elements, as analysed in detail above. It can be concluded that RF has significantly enhanced its capacity to adapt and learn, which suggests that the longer the Russia-Ukraine war endures, the more effectively RF will improve its strategic adaptability.

This will enable it to develop more effective armed forces, progressively assimilate new insights from analysing its own military operations, and adjust its tactics, forms, and methods of troop deployment. Over time, this will have adverse consequences for Ukraine's Defence Forces. Such improvements have been facilitated by synthesizing the experiences of countering Ukraine's Defence Forces in combat and developing specific methodological recommendations for conducting assault operations in urban areas, forested zones, open terrain, countering modern armoured vehicles, and responding to drones, among other scenarios.

RF has made substantial progress in the economic aspect of its strategic adaptation, gradually transitioning its economy to a wartime footing, mobilizing its defence industry, and securing a range of critical Western components despite U.S. and EU sanctions. However, these sanctions have proven ineffective not only in curbing RF's economy but also in diminishing its capability and willingness to persist in the war.

Recognizing the extent of RF's media influence network in Europe and globally, democratic nations should focus not only on military, technical, and financial assistance to Ukraine and imposing economic sanctions on RF but also on «cleansing» their internal political, economic, scientific, informational, and other systems of RF influence, which has created – and will continue to create – obstacles to peace in Ukraine.

The Russian-Ukrainian war is unique in the sense that the use of modern technologies mitigates some of the traditional advantage that larger armed forces have over smaller ones. However, the importance of conventional military strength and traditional forms of its application cannot be overlooked.

Therefore, identifying «critical vulnerabilities» in all sectors of life in the Russian Federation and its armed forces will help restrict its strategic adaptation to the new wartime conditions. Targeting these «critical points» will considerably limit its capacity to conduct military operations.

Implementing asymmetric measures against these «critical vulnerabilities» will not only disrupt RF's military plans but also provide Ukraine's Defence Forces with valuable time to stabilize their preparations to gain qualitative superiority over the Russian armed forces. This will weaken RF's capacity for prolonged attritional war and lay the groundwork for Ukraine to conduct not only defensive but also offensive operations.

The prospects for further research involve identifying mechanisms to influence the «critical vulnerabilities» within RF's strategic adaptation components using DIME (Diplomatic, Information, Military, and Economic means). The goal is to create conditions compelling Russia to abandon continued armed aggression against Ukraine.

References

1. Possible scenarios for the end of the Russo-Ukrainian war. The role and place of Ukraine in the post-war system at the global and regional levels [Електронний ресурс] / K. O. Budanov, V. V. Zaitsev, O. M. Romanov, V. S. Komarov // Science and Defence. – 2023. – No. 3. – P. 3–10. – Режим доступу : https://doi.org/10.33099/2618-1614-2023-22-3-3-10.

2. *Larsen H.* Political and military realities in the Russia-Ukraine war [Електронний ресурс] : policy brief / H. Larsen // The Institute for Peace & Diplomacy. – Режим доступу : https://peacediplomacy.org/2024/02/14/political-and-military-realities-in-the-russia-ukraine-war.

3. *Michel У.* Equipment losses in Russia's war on Ukraine mount [Електронний ресурс] / У. Michel, M. Gjerstad // IISS. – Режим доступу : https://www.iiss.org/online-analysis/military-balance/2024/02/equipment-losses-in-russias-war-on-ukraine-mount.

4. *Danylyuk O. V.* How to Build Ukraine's Military Effectiveness and Avoid a War of Attrition [Електронний ресурс] / O. V. Danylyuk // RUSI. – Режим доступу : https://www.rusi.org/explore-our-research/publications/commentary/how-build-ukraines-military-effectiveness-and-avoid-war-attrition.

5. *Jones S. G.* Ukrainian Innovation in a War of Attrition [Електронний ресурс] / S. G. Jones, R. McCabe, A. Palmer // CSIS. – Режим доступу : https://www.csis.org/analysis/ukrainian-innovation-war-attrition.

6. *Vershinin A.* The Attritional Art of War: Lessons from the Russian War on Ukraine [Електронний ресурс] / A. Vershinin // RUSI. – Режим доступу : https://www.rusi.org/explore-our-research/publications/commentary/attritional-art-war-lessons-russian-war-ukraine.

7. *Gady F.-S.* Making Attrition Work: A Viable Theory of Victory for Ukraine [Електронний ресурс] / F.-S. Gady // IISS. – Режим доступу : https://www.iiss.org/online-analysis/survival-online/2024/01/making-attrition-work-a-viable-theory-of-victory-for-ukraine.

8. *Watling J.* Russian military objectives and capacity in Ukraine through 2024 [Електронний ресурс] / J. Watling, N. Reynolds // RUSI. – Режим доступу : https://www.rusi.org/explore-our-research/publications/commentary/russian-military-objectives-and-capacity-ukraine-through-2024.

9. A National Security Strategy Primer [Електронний ресурс] / ed. by S. Heffington, A. Oler, David Tretler. – Washington, D. C. : National Defense University Press, 2019. – XX, 67 p. – Режим доступу : https://nwc.ndu.edu/Portals/71/Documents/Publications/NWC-Primer-FINAL_for%20Web.pdf.

10. Russia to expand armed forces to 2.3 million, with 1.5 million active soldiers [Електронний ресурс] // NV. – Режим доступу : https://english.nv.ua/nation/putin-increases-russian-military-to-over-2-3-million-troops-including-1-5-million-active-personnel-50451290.html.

11. Путін оцінив чисельність військ РФ в Україні у 600 тисяч осіб [Електронний ресурс] // Радіо Свобода. – Режим доступу : https://www.radiosvoboda.org/a/news-putin-viyska-rf-ukraina/32793460.html.

12. *Даценко В.* У Росії скоро закінчаться солдати і техніка – дуже хибна думка. Скільки насправді РФ може підтримувати війну в Україні. Розбір Forbes [Електронний ресурс] / В. Даценко // Forbes. – Режим доступу : https://forbes.ua/war-in-ukraine/viyskovi-resursi-voroga-skilki-rosiya-mozhe-pidtrimuvati-viynu-v-ukraini-rozbir-forbes-17082023-15466.

13. Russian Federation [Електронний ресурс] // World Bank Group. Data. – Режим доступу : https://data.worldbank.org/country/russian-federation.

14. Trends in world military expenditure, 2022 [Електронний ресурс] : SIPRI Fact Sheet : April 2023 // SIPRI. – Режим доступу : https://www.sipri.org/sites/default/files/2023-04/2304_fs_milex_2022.pdf.

15. Global military spending surges amid war, rising tensions and insecurity [Електронний ресурс] // SIPRI. – Режим доступу : https://www.sipri.org/media/press-release/2024/global-military-spending-surges-amid-war-rising-tensions-and-insecurity.

16. Russia Plans Huge Defense Spending Hike in 2024 as War Drags [Електронний ресурс] // Bloomberg. – Режим доступу : https://www.bloomberg.com/news/articles/2023-09-22/russia-plans-huge-defense-spending-hike-in-2024-as-war-drags-on.

17. Russia Keeps the Money Rolling in for Putin's War in Ukraine [Електронний ресурс] // Bloomberg. – Режим доступу : https://www.bloomberg.com/news/articles/2024-09-23/russia-budget-plans-show-no-let-up-in-putin-s-war-on-ukraine.

18. *Gavin G.* Putin's war economy faces pain if Saudis sink global oil prices [Електронний ресурс] / G. Gavin, E. Hartog, G. Smith // Politico. – Режим доступу : https://www.politico.eu/article/vladimir-putin-war-economy-pain-saudi-arabia-sink-global-oil-prices-energy-russia-opec.

19. *Pamuk H.* After China meeting, Blinken says Beijing's talk of Ukraine peace 'doesn't add up' [Електронний ресурс] / H. Pamuk, S. Lewis, D. Brunnstrom // Reuters. – Режим доступу : https://www.reuters.com/world/blinken-chinas-wang-meet-un-sidelines-2024-09-27.

20. *Brown L.* 'Clear evidence' China supplied weapons to Russia for Ukraine war. [Електронний ресурс] / L. Brown // The Times. – Режим доступу : https://www.thetimes.com/world/russia-ukraine-war/article/china-supplied-weapons-to-russia-ukraine-war-lk7j2jb8v.

21. *Сировой М.* Росія виготовляє від 130 далекобійних ракет та понад 500 дронів на місяць. Найбільше – Х-101, «Іскандери» та «Шахеди» [Електронний ресурс] / М. Сировой // Forbes. – Режим доступу : https://forbes.ua/news/rosiya-vigotovlyae-vid-130-dalekobiynikh-raket-ta-ponad-500-droniv-na-misyats-naybilshe-kh-101-iskanderi-ta-shakhedi-18092024-23693.

22. How quickly can Russia rebuild its tank fleet? [Електронний ресурс] // The Economist. – Режим доступу : https://www.economist.com/the-economist-explains/2023/02/27/how-quickly-can-russia-rebuild-its-tank-fleet.

23. DeepStateMAP. Мапа війни в Україні [Електронний ресурс] // Deep State. – Режим доступу : https://deepstatemap.live.

24. The Russian Orthodox Church declares «holy war» against Ukraine and articulates tenets of Russia's emerging official nationalist ideology [Електронний ресурс] / R. Bailey, C. Harward, A. Evans, G. Barros // ISW. – Режим доступу : https://www.understandingwar.org/backgrounder/russian-orthodox-church-declares-«holy-war»-against-ukraine-and-articulates-tenets.

25. Богданьок О. Зміни до ядерної доктрини РФ потрібно вважати «певним сигналом недружнім країнам» – Пєсков [Електронний ресурс] / О. Богданьок // Суспільне. Новини. – Режим доступу : https://suspilne.media/845055-zmini-do-adernoi-doktrini-rf-potribno-vvazati-pevnim-signalom-nedruznim-krainam-peskov.

DOI 10.33099/2618-1614-2024-27-4-13-23
УДК 355.4:004.056.5

М. В. Драпатий,
Генеральний штаб Збройних Сил України,
Т. М. Дзюба,
кандидат технічних наук, доцент,
Збройні Сили України,
А. М. Костенко,
Національний університет оборони України,
О. О. Самарський,
Збройні Сили України

Аналіз заходів інформаційної боротьби збройних сил Російської Федерації в районах ведення бойових дій

Попри значну кількість наукових досліджень різних аспектів російської інформаційної боротьби проти України і світу такі питання, як узгодження інформаційних операцій противника на різних рівнях – від стратегічного й до тактичного – системність його дій в інформаційному просторі, вплив заходів інформаційної боротьби противника на ефективність його військових операцій проти України, досліджені недостатньо. Метою статті є аналіз форм і способів інформаційної боротьби Російської Федерації проти України, які безпосередньо супроводжують дії російських військ, та визначення взаємозв'язку між інформаційними операціями противника тактичного, оперативного і стратегічного рівнів. Матеріали статті грунтуються на особистому практичному досвіді авторів щодо організації заходів стратегічних комунікацій сил оборони України, зокрема протидії інформаційним операціям противника в операціях оперативно-стратегічного угруповання військ «Одеса», оперативних угруповань військ «Херсон» і «Таврія», оперативно-тактичного угруповання «Харків».

Ключові слова: інформаційна боротьба, інформаційні операції, інформаційно-психологічний вплив, моніторинг інформаційного простору, форми та способи інформаційної боротьби, суб'єкти інформаційної боротьби, інформаційні ресурси.

У сучасному світі інформаційна боротьба є повноцінним інструментом реалізації національних інтересів, впливу на геополітичні процеси, невід'ємною складовою забезпечення національної безпеки для кожної країни та міжнародної безпеки у світі загалом. Причому сьогодні межі між інформаційними операціями стратегічного, оперативного і тактичного рівнів фактично стираються, особливо якщо розглядати їх за очікуваними ефектами й рівнем інформаційного впливу на визначені цільові аудиторії. Часто результати, досягнуті в інформаційній боротьбі на тактичному рівні, впливають на стратегічні цілі й навпаки, ефекти, сформовані інформаційною боротьбою на стратегічному рівні, створюють такий фон в інформаційному просторі, який безпосередньо визначає успіх на тактичному рівні.

Мета інформаційної боротьби Російської Федерації проти України і світу невіддільна від мети російської геополітичної стратегії: скориставшись слабкістю існуючої системи міжнародної безпеки та небажанням більшості провідних країн (часто – не лише небажанням, а й неготовністю) вирішувати конфлікти воєнним шляхом, змінити воєнний, політичний та економічний баланс у світі на свою користь (на користь держав – партнерів Російської Федерації, економічних і воєнно-політичних блоків та організацій, до яких входить Російська Федерація). Україна була визначена російським керівництвом як локальна мета своєї агресивної політики і водночас як жертва, дії щодо якої демонструють міжнародній спільноті можливі загрози та наслідки несприйняття цілей російської політики і способів досягнення цих цілей.

Сутність сучасної інформаційної боротьби Російської Федерації розкривається в низці досліджень таких установ, як Atlantic Council [1], RAND Corporation [2], NATO Strategic Communications Centre of Excellence [3], East StratCom Task Force [4].

В Україні системними дослідженнями різних аспектів російської інформаційної боротьби займаються Національний інститут стратегічних досліджень, Центр протидії дезінформації Ради національної безпеки і оборони України [5], Центр стратегічних комунікацій та інформаційної безпеки, створений при Міністерстві культури та інформаційної політики України [6], Інститут стратегічних комунікацій Національного університету оборони України [7, 8], недержавні аналітичні центри та проєкти: Інститут масової інформації, Український інститут майбутнього, громадська організація «Детектор медіа», група «Інформаційний спротив», міжнародна волонтерська спільнота «Інформ Напалм», авторський проєкт Оксани Мороз «Як не стати овочем» тощо.

Однак такі питання, як узгодження інформаційних операцій противника на різних рівнях: від стратегічного

й до тактичного, системність його дій в інформаційному просторі, вплив заходів інформаційної боротьби противника на ефективність його військових операцій проти України, досліджені недостатньо.

Метою статті є аналіз форм і способів інформаційної боротьби Російської Федерації проти України, які безпосередньо супроводжують дії російських військ, та визначення взаємозв'язку між інформаційними операціями противника тактичного, оперативного і стратегічного рівнів.

Матеріали статті ґрунтуються на особистому практичному досвіді авторів щодо організації заходів стратегічних комунікацій сил оборони України, зокрема протидії інформаційним операціям противника, в операціях оперативно-стратегічного угруповання військ «Одеса», оперативних угруповань військ «Херсон» і «Таврія», оперативно-тактичного угруповання «Харків».

Виклад основного матеріалу

Нині актуальними цілями інформаційної боротьби Російської Федерації проти України є:

• дискредитація української влади в очах міжнародної спільноти і населення України, зокрема особового складу сил оборони України (*очікувані противником ефекти*: суттєве зменшення підтримки України від міжнародної спільноти; формування в міжнародної спільноти й населення України запиту на переобрання влади з можливістю заміни чинних керівників на лояльніших до Російської Федерації; формування недовіри до влади в українського населення, зокрема в особового складу сил оборони України);

• дестабілізація суспільно-політичної обстановки в Україні (*очікувані противником ефекти*: конфлікти між різними соціальними групами населення; несприйняття населенням державної політики; зменшення підтримки і довіри населення України до сил оборони України; відволікання ресурсів держави на вирішення проблемних питань, не пов'язаних зі сферою оборони);

• доведення неспроможності України, навіть за умови підтримки країн-партнерів та союзників України, перемогти Російську Федерацію (*очікувані противником ефекти*: формування думки про безрезультатність і недоцільність продовження підтримки України; збільшення «втоми» від теми війни в новинах; збільшення критики урядів країн-партнерів та союзників України населенням цих країн за «безрезультатне» витрачання ресурсів на допомогу Україні замість розв'язання внутрішніх проблем);

• примушення української влади, населення та міжнародної спільноти прийняти умови російських ультиматумів (*очікувані противником ефекти*: переконання міжнародної спільноти й населення України в можливості завершення війни лише на умовах Російської Федерації; демонстрація впевненості в досягненні цілей «спеціальної воєнної операції» проти України; залякування міжнародної спільноти переростанням російської збройної агресії проти України в третю світову війну; залякування міжнародної спільноти й населення України можливістю застосування зброї масового ураження; переконання міжнародної спільноти в загостренні таких проблемних питань, як збільшення збройних конфліктів і тероризму, неконтрольованої міграції, продовольчих криз в окремих регіонах унаслідок небажання та зволікання з прийняттям вимог Російської Федерації; формування суспільної думки (в Україні та світі) щодо незворотності перемоги Російської Федерації на полі бою);

• дискредитація сил оборони України, особливо Збройних Сил України, в очах міжнародної спільноти та населення України (*очікувані противником ефекти*: формування думки про наявність значних порушень вимог міжнародного гуманітарного права в діях сил оборони України; провокування внутрішніх конфліктів між українською владою та різними структурами (окремими представниками) сил оборони України, між командирами та підлеглими; зрив заходів мобілізації; зменшення довіри населення України до сил оборони України).

Регулярна та системна діяльність, спрямована на досягнення цілей інформаційної боротьби, визначених противником, забезпечує постійну присутність в інформаційному просторі інформаційних матеріалів, потрібних противнику, та зумовлює формування необхідних йому ефектів.

Формами дій противника в інформаційному просторі можна визначити такі:

• системну інформаційну діяльність (стратегічні комунікації, хоча такий термін в офіційних російських документах не вживається);

• окремі довгострокові інформаційні кампанії (наприклад «Майдан-3», спрямовану на перезавантаження української влади й дестабілізацію суспільно-політичної обстановки в Україні; «Нелегітимний», спрямовану на дискредитацію Президента України; «Тотальна корупція», спрямовану на дискредитацію української влади в очах міжнародної спільноти й населення України; «Ухилянт», спрямовану на зрив мобілізаційних заходів в Україні; «Війна до останнього українця», спрямовану на створення контрасту між «миротворчими» ініціативами противника і повною залежністю української влади від країн-партнерів та олігархічного оточення, яким «вигідне продовження війни»);

• інформаційні операції, котрі являють собою систему інформаційних акцій та окремих інформаційних

заходів та проводяться як окремо (на визначені цільові аудиторії), так і разом з діями військ противника, підтримуючи ці дії та водночас використовуючи результати дій військ для досягнення своїх цілей інформаційної боротьби;

• окремі інформаційні акції та заходи, які проводяться поза межами інформаційних кампаній та операцій, в основному щодо реагування на ті чи інші події, які відбуваються в Україні, самій Російській Федерації чи у світі;

• комплекс заходів щодо захисту власного інформаційного простору і протидії інформаційним кампаніям та операціям України.

Постійно здійснюється моніторинг інформаційного простору, завданнями якого є виявлення інформаційних загроз та їхніх джерел, оцінювання настроїв і поведінки визначених цільових аудиторій, пошук інформації, яка може бути використана на користь противнику, визначення ефективності проведених інформаційних заходів.

Для досягнення цілей інформаційної боротьби противник створив:

• систему органів, призначену для ведення інформаційної боротьби;

• систему інформаційних ресурсів, здатних доносити інформацію до цільових аудиторій, визначених противником для інформування та впливу;

• систему заходів інформаційної боротьби, безумовність і регулярність проведення яких створює для противника необхідні ефекти в інформаційному просторі.

Система органів інформаційної боротьби противника координується та керується безпосередньо з адміністрації президента РФ.

Так, у російській адміністрації президента питаннями інформаційної боротьби опікуються заступник керівника адміністрації президента – прес-секретар президента РФ та заступник керівника адміністрації президента РФ, відповідальний за український напрямок. Крім того, цими питаннями займаються управління президента РФ із громадських зв'язків і комунікацій та управління президента РФ з питань моніторингу та аналізу соціальних процесів (*рис. 1*).

У російському уряді головними суб'єктами інформаційної боротьби проти України можна визначити:

• міністерство закордонних справ РФ;

• міністерство оборони РФ (зокрема головне воєнно-політичне управління збройних сил РФ, департамент інформації та масових комунікацій міністерства оборони РФ, головне оперативне управління генерального штабу збройних сил РФ, головне управління (раніше – головне розвідувальне управління) генерального штабу збройних сил РФ);

• міністерство цифрового розвитку, зв'язку та масових комунікацій РФ і підпорядкована цьому міністерству федеральна служба з нагляду у сфері зв'язку, інформаційних технологій і масових комунікацій («Роскомнадзор»), призначена для розвитку медіасфери та Інтернет у РФ, а також для забезпечення інформаційної безпеки в РФ.

Окремими суб'єктами інформаційної боротьби Російської Федерації проти України є:

• федеральна служба безпеки РФ;

• служба зовнішньої розвідки РФ;

• фонд «Русский мир» – російська державна некомерційна організація, призначена для реалізації комплексу міжнародних навчальних та просвітницьких програм гуманітарної спрямованості з метою популяризації вивчення російської мови, культури, історії; залучення до співробітництва та взаємодії компетентних, активних, з творчим мисленням та проросійськи налаштованих громадян з різних країн світу. Працює шляхом надання грантів. Має 82 постійні представництва («русскиє центры») у 38 країнах світу та невизнаній Південній Осетії; реалізує 124 цільові програми в 55 країнах світу та невизнаній Південній Осетії (засновниками фонду є міністерство закордонних справ РФ та міністерство науки і вищої освіти РФ, голова опікунської ради фонду – міністр закордонних справ РФ, до опікунської ради фонду входять: міністр освіти РФ, міністр культури РФ, міністр науки та вищої освіти РФ).

У генеральному штабі збройних сил РФ головним суб'єктом інформаційної боротьби проти України є головне управління (в минулому – головне розвідувальне управління). Безпосередньо за інформаційну боротьбу відповідає управління 12-біс цього головного управління.

З офіційної інформації щодо розслідування діяльності російських хакерів та пропагандистів, які перебувають на військовій службі в збройних силах РФ, відомо, що місцями їхньої служби були:

• центр оперативної координації органів військового управління «Вежа» (військова частина 74455, Хімкі, Московська область);

• 85-й (головний) центр спеціальної служби (військова частина 26165, Москва);

• 72-й центр спеціальної служби (військова частина 54777, Москва);

• 64-й центр спеціальної служби (військова частина 45055, Москва).

• військова частина (центр спеціальної служби) 20697, Санкт-Петербург;

• військова частина (центр спеціальної служби) 03126, Сертолово;

• військова частина (центр спеціальної служби) 03138, Єкатеринбург;

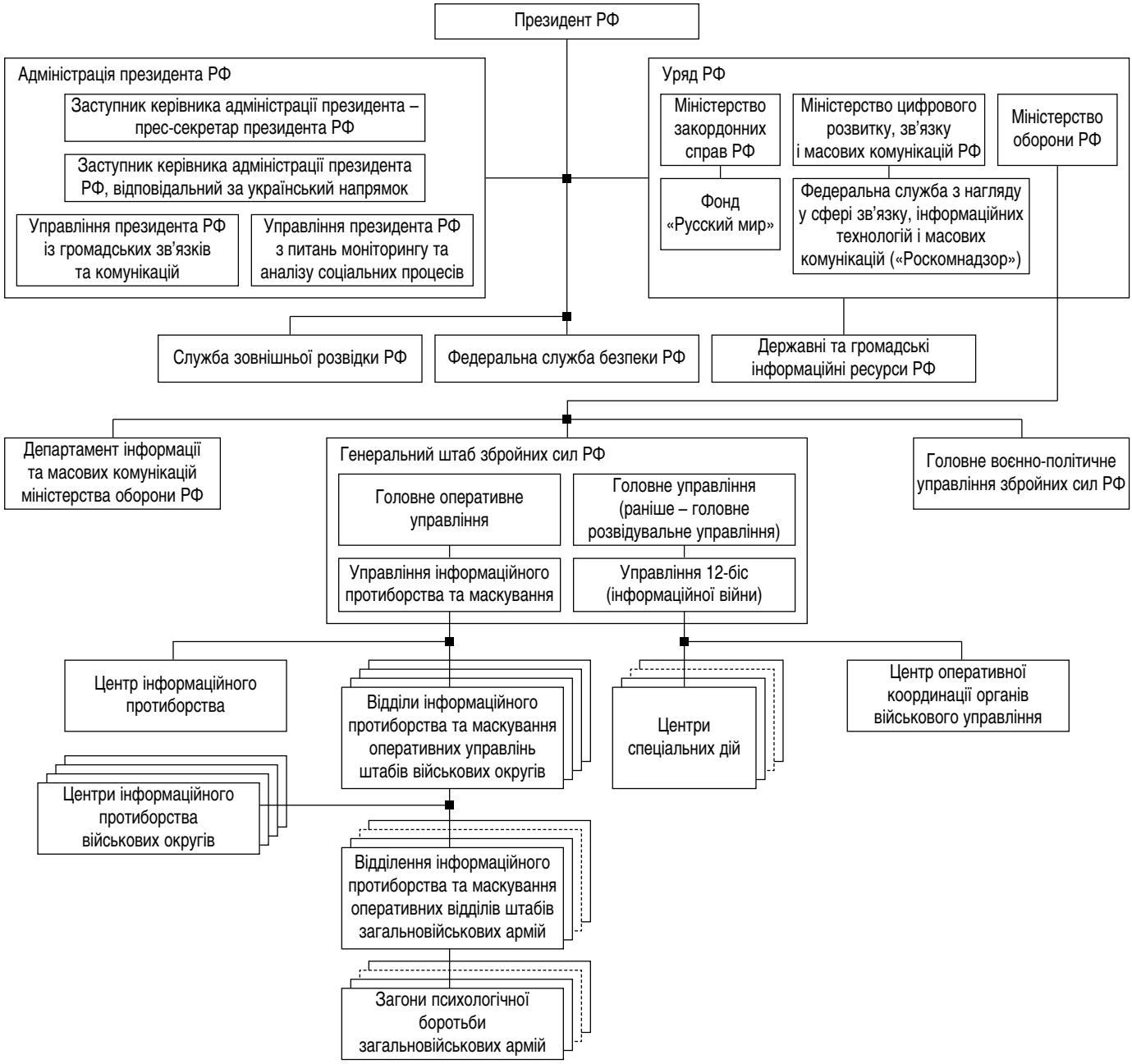

Рис. 1. Система органів інформаційної боротьби Російської Федерації

• військова частина (центр спеціальної служби) 03134, Хабаровськ;

• військова частина (центр спеціальної служби) 03128, Ростов на Дону.

Для безпосередньої підтримки дій військ противника у військових операціях задіяна система органів інформаційного протиборства та маскування, підпорядкована головному оперативному управлінню генерального штабу збройних сил РФ.

Постановку завдань, координацію та контроль проведених заходів здійснює управління інформаційного протиборства та маскування головного оперативного управління генерального штабу збройних сил РФ. Йому щодо виконання завдань інформаційної боротьби підпорядковані відділи інформаційного протиборства та оперативного маскування оперативних управлінь штабів Московського, Ленінградського, Південного, Центрального та Східного військових округів.

Частиною безпосереднього підпорядкування управління інформаційного протиборства та маскування головного оперативного управління генерального штабу збройних сил РФ є центр інформаційного протиборства, який виконує завдання моніторингу інформаційного простору (збирання даних з військових округів)

та підготовки інформаційної довідки за добу (станом на 06:00 щодня) для доповіді старшому начальнику; захисту власних об'єктів (керівництва, особового складу, інформаційної інфраструктури) від негативного впливу противника.

Відділи інформаційного протиборства та оперативного маскування оперативних управлінь штабів військових округів РФ виконують завдання:

- управління, контролю та координації діяльності відділень інформаційного протиборства та оперативного маскування загальновійськових армій;
- організації моніторингу інформаційного простору з метою забезпечення старшого начальника (командувача військовим округом) актуальною інформацією щодо суспільно-політичної обстановки в зоні відповідальності за добу;
- захисту власних об'єктів (керівництва, особового складу, інформаційної інфраструктури) від негативного впливу противника.

Цим відділам підпорядковані відділення інформаційного протиборства та оперативного маскування загальновійськових армій, центри інформаційного протиборства військових округів (з основним завданням цілодобового моніторингу інформаційного простору та підготовки на основі одержаної з відкритих джерел інформації добової довідки для забезпечення актуальною інформацією щодо суспільно-політичної обстановки в зоні відповідальності старшого начальника – командувача військовим округом).

Відділення інформаційного протиборства та оперативного маскування входять до складу оперативних відділів загальновійськових армій противника і виконують завдання моніторингу інформаційного простору зони відповідальності з метою забезпечення старшого начальника (командувача армією) актуальною інформацією щодо суспільно-політичної обстановки в зоні відповідальності за добу; захисту власних об'єктів (керівництва, особового складу, інформаційної інфраструктури армії) від негативного впливу противника.

Відділенням інформаційного протиборства та оперативного маскування загальновійськових армій підпорядковані загони психологічної боротьби, котрі, у свою чергу, входять до складу визначених розвідувальних бригад та бригад спеціального призначення.

Так, відомо, що загони психологічної боротьби входять до складу:

- 100-ї окремої розвідувальної бригади Південного військового округу (в/ч 23511);
- 127-ї окремої розвідувальної бригади Чорноморського флоту Південного військового округу (в/ч 67606);
- 45-ї бригади спеціального призначення повітряно-десантних військ Московського військового округу (в/ч 28337);
- 96-ї окремої розвідувальної бригади 1-ї танкової армії Московського військового округу (в/ч 52634).

Основними завданнями загонів психологічної боротьби визначені такі:

- розробка аналітичних документів за встановленими темами;
- розробка матеріалів інформаційно-психологічного впливу;
- проведення заходів інформаційно-психологічного впливу в мережі Інтернет з використанням звукомовних засобів, поширення друкованої продукції та використання комплексів радіоелектронної боротьби (РЕБ).

Розробка аналітичних документів охоплює детальні збирання, обробку й аналіз інформації та виготовлення на їхній основі якісного аналітичного матеріалу.

Розробка матеріалів інформаційно-психологічного впливу здійснюється черговою зміною. Чергова зміна складається з 30 військовослужбовців, які розробляють за добу 30 матеріалів. За типами матеріали поділяються на статті, дописи та графічні матеріали (демотиватори).

Усі розроблені матеріали інформаційно-психологічного впливу в обов'язковому порядку погоджуються представниками управління 12-біс головного управління генерального штабу збройних сил РФ. Таке погодження дає змогу пов'язати інформацію, яка доноситься до цільових аудиторій на тактичному рівні, зі стратегічними наративами.

В угрупуваннях російських військ, які здійснюють збройну агресію проти України («Центр», «Север», «Восток», «Юг», «Запад», «Днєпр») структура органів інформаційної боротьби ідентична структурі цих органів у військових округах РФ, а особовий склад оперативно призначається зі складу відповідного військового округу, який комплектує те чи інше угруповання військ противника.

Основними підрозділами, які здійснюють інформаційно-психологічний вплив на населення на тимчасово окупованих територіях України є оперативні групи федеральної служби безпеки РФ. Основним завданням цих оперативних груп є зниження рівня спротиву місцевого населення та легітимізація окупаційних військ. Основними каналами поширення інформації є телеграм-канали та місцеве телебачення.

Ці групи постійно взаємодіють з відділеннями інформаційного протиборства та оперативного маскування оперативних відділів штабів загальновійськових армій, які організовують виконання завдань з підготовки фото- й відеоматеріалів з метою дискредитації сил оборони України, легітимізації окупаційних військ і підвищення іміджу російської влади. Такі

завдання виконуються у взаємодії з воєнними кореспондентами (перебувають у підпорядкування командувача угрупованням російських військ).

Система інформаційних ресурсів, які безпосередньо беруть участь в інформаційній боротьбі РФ проти України і світу (*рис. 2*), керується, фінансується та забезпечується урядом РФ.

Основними серед цих інформаційних ресурсів є:

1. Всеросійська державна телевізійна та радіомовна компанія (ВГТРК), яка є державним підприємством, підпорядкованим міністерству цифрового розвитку, зв'язку і масових комунікацій РФ. ВГТРК здійснює ефірне телевізійне мовлення по 20 програмах, 16 з яких призначені для віддалених районів Росії. Ефірні канали доступні також у пакетах усіх операторів супутникового та кабельного мовлення, а також у першому мультиплексі цифрового телебачення Росії (обов'язкового для розповсюдження). Крім того, ВГТРК керує державним російським Інтернет-каналом «Россия», який концентрує Інтернет-ресурси всіх центральних і регіональних телерадіокомпаній ВГТРК; інформаційним Інтернет-порталом «Вести.ру», онлайн-платформою для стрімінгу ефірного мовлення та перегляду відеоконтенту «Смотрим»; єдиною платформою для трансляції контенту федеральних російських телевізійних каналів в Інтернет «Витрина ТВ».

2. Федеральне державне унітарне підприємство «Международное информационное агентство «Россия сегодня», підпорядковане російському уряду. Координує телевізійне та радіомовлення, новинні стрічки російською, англійською, іспанською, арабською, китайською та фарсі мовами, інформаційні портали, мультимедійні міжнародні прес-центри, виробництво і поширення фотоконтенту й інфографіки, інформаційні продукти для соціальних мереж, виробництво контенту для мобільних додатків. Російською мовою розвиває такі ресурси, як інформаційне агентство «РИА Новости», портал матеріалів, перекладених з інших мов, закордонних ЗМІ «ИноСМИ.ру». За кордоном РФ медіагрупа представлена міжнародним новинним агентством і радіостанцією з мультимедійними інформаційними центрами Sputnik. «Россия сегодня» відповідає за реалізацію таких інформаційних проектів, як «Украина.ру» і «Baltnews», призначених для публікації думок, інтерв'ю та коментарів експертів щодо ситуації в Україні та країнах Балтії, відповідно.

3. Медіакомпанія «Газпром Медиа», яка входить до складу російського державного концерну «Газпром». Медіакомпанія охоплює мережі: інформаційних і тематичних телевізійних каналів НТВ; розважальних телевізійних каналів ТНТ; розважальних телевізійних каналів РТВ; спортивних телевізійних каналів «Матч»; телекомпанії «Ред Медиа»; радіостанцій «Авторадио», «Relax FM», «Like FM», та інших; компаній з виробництва контенту «Comedy Club Production», «Централ Партнершип», «Good Story Media», «Киностудия КИТ», «1-2-3 Production», «ПодкастБар», «Студия ЯРКО»; друкованих ЗМІ; Інтернет-порталів і сайтів.

4. Загальноросійський федеральний телевізійний канал «Первый канал» та його міжнародна версія «Первый канал. Всемирная сеть».

5. Російський федеральний суспільно-патріотичний канал «Звезда», який входить до однойменної медіагрупи та належить міністерству оборони РФ.

6. Державне інформаційне агентство РФ «ТАСС».

7. Офіційний друкований орган уряду РФ «Российская газета» та однойменний Інтернет-портал новин.

8. Інтернет-газета, телевізійний канал та радіостанція «Комсомольская правда».

Усі перелічені телевізійні канали, радіостанції та друковані ЗМІ представлені в Інтернет і соціальних мережах, більшість із них має свої канали в Телеграм.

Крім ЗМІ, до ресурсів, задіяних Російською Федерацією в інформаційній боротьбі проти України, можна віднести особисті блоги, канали і веб-сторінки популярних російських політиків, державних діячів, журналістів, представників культури та шоу-бізнесу: Дмітрія Мєдвєдєва, Рамзана Кадирова, Владіміра Соловьйова, Ольги Скабєєвої, Маргаріти Сімоньян, Івана Охлобистіна та багатьох інших. Достатньо повну базу російських лідерів громадської думки, які беруть активну участь в інформаційній боротьбі проти України, можна знайти в дослідженні Оксани Мороз [9].

Зі зростанням популярності та, відповідно, збільшенням кількості користувачів багатоплатформового месенджера Телеграм, до інформаційної боротьби проти України були залучені телеграм-канали: «Топор Live», «Прямой эфир. Новости», «Mash», «Readovka», «Россия сейчас», «АРХАНГЕЛ СПЕЦНАЗА Z_{RU}», «Два майора», «WarGonzo», «Повёрнутые на войне», «Поздняков 3.0», «Kotsnews», «Военный осведомитель», «Старше Эдды» та багато інших.

Серед усіх телеграм-каналів, які працюють на противника, доцільно виділити ті, які мімікрують під проукраїнські, опозиційні до чинної влади та державної політики України. Найбільшими з них є «Резидент», «Сплетница», «Картель», «MediaKiller».

Ураховуючи те, що переважна більшість зазначених телеграм-каналів пов'язана з діяльністю воєнних блогерів, з 2022 р. проводяться регулярні зустрічі президента РФ з військовими кореспондентами та блогерами. Так, на останній зустрічі, яка відбулася 13 червня 2023 р. у Кремлі, з-поміж воєнних блогерів були присутні Сємьон Пєгов, Алєксандр Сладков, Іріна Куксєнкова, Дмітрій Стєшін, Андрєй Руденко, Максім Долгов, Євгєній Поддубний, Алєксандр Коц та ін. Кожен з них є лідером громадської думки для своїх читачів і тому цікавий для керівництва РФ.

Крім інформативної, телеграм-канали противника виконують розвідувальну функцію, збираючи інформацію від підписників через боти, призначені для зворотного зв'язку.

Починаючи з 2014 р. противник витрачає на розвиток власних інформаційних ресурсів не менше 1 млрд євро на рік.

З переліченими інформаційними ресурсами з погляду обміну інформаційними матеріалами та взаємної «розкрутки» в інформаційному просторі безпосередньо пов'язані інформаційні ресурси, які створюються російськими підрозділами інформаційної боротьби під конкретні інформаційні кампанії, операції та акції.

Заходи інформаційної боротьби проводяться противником на всіх рівнях: від стратегічного до тактичного, причому між цими рівнями існує взаємозв'язок.

Так, на стратегічному (державному) рівні визначаються наративи, аргументаційні тематики та лінії переконання, розробляються основні меседжі, створюються відповідні інформаційні матеріали, забезпечується постійна присутність власних інформаційних матеріалів у світовому інформаційному просторі.

Зі стратегічного рівня всі ці розробки доводяться до оперативного та оперативно-тактичного рівнів, тобто до рівнів застосування угруповань військ противника в його збройній агресії проти України.

Крім того, на стратегічному рівні забезпечується можливість телевізійного та радіомовлення на райони ведення бойових дій. Для цього збільшується кількість і потужність передавачів телевізійного та радіосигналу на підконтрольній противнику території. Присутність телевізійних каналів і радіостанцій противника відмічається на всій тимчасово окупованій території України та в прифронтовій зоні. Часто канали противника можна приймати на відстані 30–40 км від лінії бойового зіткнення.

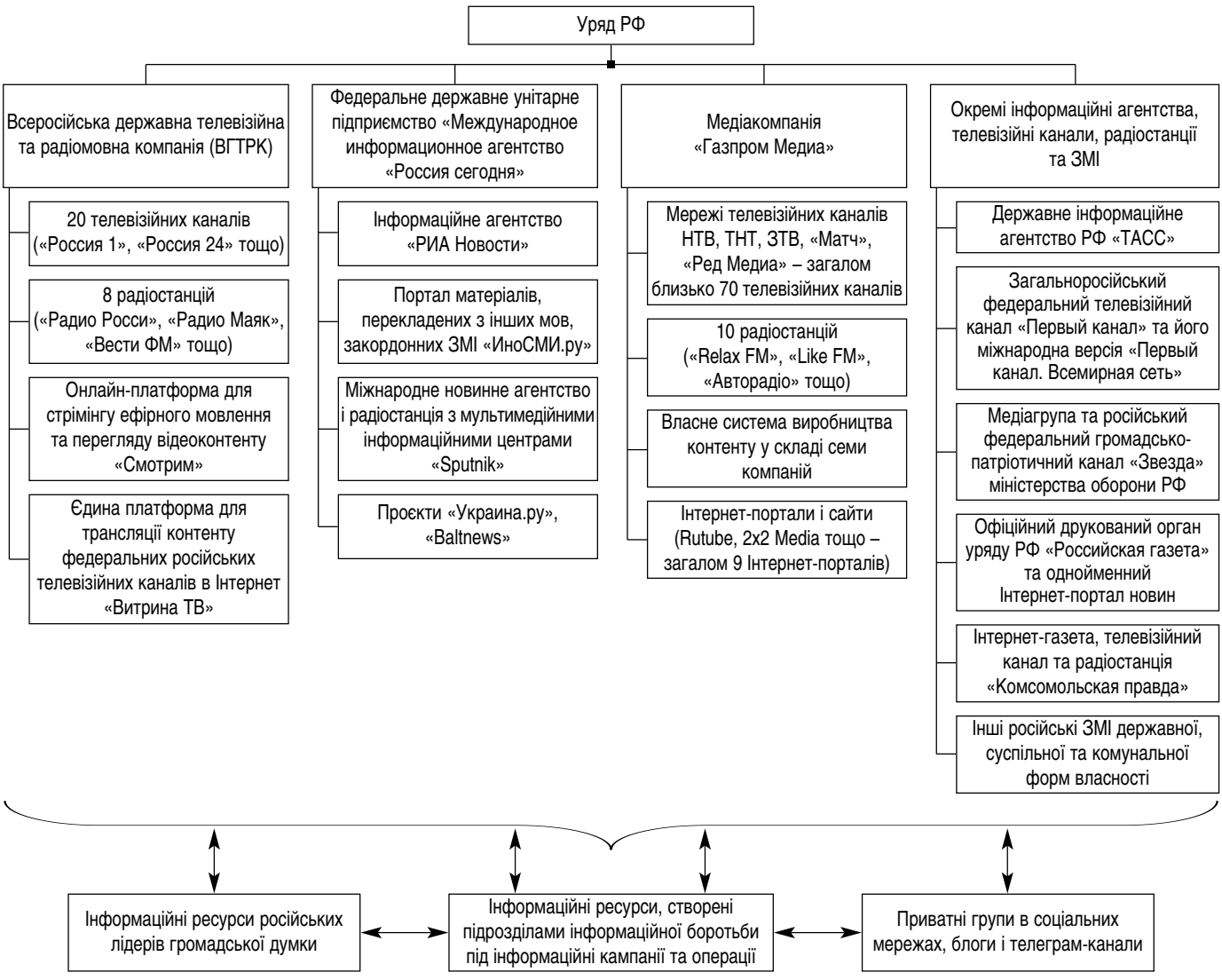

Рис. 2. Система інформаційних ресурсів РФ, залучених до інформаційної боротьби

На стратегічному рівні створюється інформаційна перевага за рахунок збільшення (порівняно з нами) кількості інформаційних ресурсів, доступних визначеним цільовим аудиторіям, та наповнення цих ресурсів відповідними інформаційними матеріалами.

З оперативного, оперативно-тактичного і тактичного рівнів на стратегічний надходить інформація, необхідна для досягнення цілей інформаційної боротьби, а також результати заходів інформаційної боротьби, проведених в операціях угруповань військ противника.

Такий взаємозв'язок зумовлює форми інформаційної боротьби, які противник використовує на оперативному (оперативно-тактичному) рівні, тобто в операціях своїх угруповань військ:

- участь в інформаційних кампаніях стратегічного рівня;
- інформаційні операції в районах проведення операцій угруповань військ, спрямовані на досягнення мети цих операцій і висвітлення результатів бойових дій відповідно до стратегічного наративу (наративів);
- інформаційні акції, спрямовані на зміну поведінки та прийняття рішень, вигідних противнику, визначеними цільовими аудиторіями (наприклад здача наших військовослужбовців у полон, відмова від участі в бойових діях, залишення позицій тощо);
- окремі інформаційні заходи (в основному – заходи інформаційного реагування на наші інформаційні (психологічні) операції, різкі зміни обстановки, негативну інформацію тощо).

В операціях своїх угруповань військ противник здійснює інформаційний вплив на:

- керівництво (командування) наших угруповань з метою спонукання до прийняття рішень, вигідних противнику;
- особовий склад наших військ (сил) з метою його деморалізації, спонукання до здачі в полон, формування недовіри до командирів;
- цивільне населення в районах бойових дій з метою поширення паніки, формування зневіри в перемозі, зменшення підтримки сил оборони України;
- міжнародну спільноту (опосередковано, через виготовлення, розміщення та коментування інформаційних матеріалів) з метою переконання в успішності власних дій та поразці сил оборони України, дискредитації сил оборони України;
- особовий склад своїх військ із метою підтримки необхідного рівня морально-психологічного стану і формування впевненості у власній перемозі.

Основними способами інформаційної боротьби противника в операціях його угруповань військ можна визначити:

- створення інформаційних ресурсів, достатніх для донесення інформації для визначених цільових аудиторій;
- кроспостинг (поширення одних і тих самих інформаційних матеріалів різними інформаційними ресурсами);
- регулярне (систематичне) інформування цільових аудиторій щодо ситуації в операційній зоні;
- залякування визначених цільових аудиторій (невідворотністю ракетних, авіаційних та артилерійських ударів, новими бойовими можливостями власної зброї тощо);
- поширення листівок з метою спонукання нашого особового складу до відмови від участі в бойових діях, залишення позицій, здачі в полон;
- розсилання СМС-повідомлень та повідомлень на особисті месенджери військовослужбовців сил оборони України та цивільного населення в районах бойових дій;
- використання наших військовополонених для власної пропаганди.

Система заходів інформаційної боротьби в операціях угруповань військ противника охоплює такі основні елементи (*рис. 3*):

- розгортання і створення мережі інформаційних ресурсів, необхідних для гарантованого донесення інформації до всіх визначених цільових аудиторій;
- оцінювання інформаційного середовища та аналіз цільових аудиторій з метою визначення найефективніших способів роботи, формування аргументаційних тематик, ліній переконання та меседжів;
- організацію постійного моніторингу інформаційного простору щодо операційної зони угруповання військ противника;
- регулярне інформування на всіх розгорнутих і створених інформаційних ресурсах про перебіг та результати бойових дій (про власні успіхи та поразки і втрати наших військ);
- дестабілізацію суспільно-політичної обстановки в частині операційної зони, яка контролюється силами оборони України;
- деморалізацію наших військ;
- залякування цивільного населення в частині операційної зони, яка контролюється силами оборони України, формування панічних настроїв, недовіри та засудження дій сил оборони України.

В операціях угруповань військ противника обов'язково створюються інформаційні ресурси трьох типів:

- перший (рівня угруповання військ противника) – для висвітлення ситуації в усій операційній зоні;
- другий (рівня загальновійськової армії) – для висвітлення ситуації на кожному з напрямків операції;
- третій (від імені лідера громадської думки або «незалежної сторони») – для висвітлення ситуації в операційній зоні від нібито стороннього (незалежного) джерела.

Рис. 3. Система заходів інформаційної боротьби в операціях угруповань військ противника

Так, в операційній зоні ОСУВ «Одеса», проти якого противник проводив операцію силами свого стратегічного угруповання «Днепр» і частково силами стратегічного угруповання «Юг», на Херсонському напрямку ним були створені та використовувалися телеграм-канали:

- «Крылатые» (рівня угруповання військ, оскільки основу угруповання противника «Дніпро» становлять військові частини повітряно-десантних військ збройних сил РФ);
- «Днепровский Рубеж» (рівня групи російських військ, яка діяла безпосередньо на Херсонщині);
- «Позывной «Осетин» (від імені контрактника збройних сил РФ, який має свою думку, відмінну від офіційних російських джерел);
- «ВДВ за Честность и Справедливость» (від імені старшого офіцера повітряно-десантних військ збройних сил РФ, який, беручи безпосередню участь у російській збройній агресії проти України, критикує командування угруповання російських військ «Днепр» за недбале керівництво, недолугі рішення та недостатнє забезпечення військ).

В операційній зоні оперативно-тактичного угруповання «Харків», проти якого противник проводив операцію силами свого стратегічного угруповання «Север», ним були створені та використовувалися телеграм-канали:

- «Северний ветер» (рівня угруповання військ);
- «Казачья Лопань Z» (рівня групи російських військ, яка діяла безпосередньо на Харківщині);
- «Адекватный Харьковчанин» (від імені екс-мешканця Харкова, полковника запасу Геннадія Альохіна).

Крім того, силами оперативних груп федеральної служби безпеки РФ у взаємодії з колабораціоністами на тимчасово окупованих територіях створювались інформаційні ресурси (Інтернет-сайти, сторінки та групи в соціальних мережах, телеграм-канали), які викликали ілюзію контролю ситуації на цих територіях російською владою [10].

Зазначені інформаційні ресурси, разом з розгорнутими в прикордонних з Україною районах РФ (на тимчасово окупованих територіях) передавачами і ретрансляторами російських телевізійних каналів і радіостанцій, забезпечували постійну присутність російського контенту, власної оцінки обстановки в операційній зоні і регулярність здійснення інформаційного впливу на визначені противником цільові аудиторії.

Інколи матеріали з інформаційних ресурсів противника, створених для проведення заходів інформаційної боротьби в операціях угруповань військ, через ресурси аналітичних центрів, таких як ISW (Інститут вивчення війни), потрапляли до українських і закордонних ЗМІ. Пояснення таких випадків доволі просте: Інститут вивчення війни публікує свої аналітичні матеріали з обов'язковим посиланням на джерела одержання інформації. Однак окремі журналісти інколи беруть для своїх публікацій сам текст аналітики ISW, без вивчення джерел інформації та, відповідно, без посилання на них. Тобто в публікаціях цих журналістів дезінформація противника подається вже як факт.

Аналіз змісту інформаційних матеріалів, які регулярно публікуються телеграм-каналами противника, дає змогу визначити основні теми інформування та впливу:

- успіхи військ противника та поразки (невдачі) наших військ;

• великі втрати нашого особового складу, озброєння та військової техніки (власні втрати замовчуються);

• неефективність нашої системи протиповітряної оборони (нездатність уражати засоби повітряного нападу, загрози для цивільного населення від застосування засобів протиповітряної оборони в населених пунктах);

• корупція в Україні, зокрема у сфері оборони;

• нарощування противником спроможностей та бойових можливостей;

• «насильницька» мобілізація в Україні та небажання громадян України брати участь у бойових діях;

• іноземні найманці у складі сил оборони України;

• скорочення підтримки України з боку країн-партнерів та союзників.

Основними характеристиками зазначених телеграм-каналів є:

• висока оперативність розміщення інформації щодо ситуації в операційній зоні;

• різноманітність інформаційних матеріалів (текстові, фото-, відеоматеріали);

• відповідність інформаційних матеріалів стратегічному наративу (наративам);

• високий рівень штабної культури авторів матеріалів щодо аналізу бойових дій в операційній зоні.

Водночас неодноразово відмічалися значні затримки в роботі цих каналів у разі різких змін обстановки, реагування на наші заходи інформаційних та психологічних операцій, появи інформації негативного характеру про дії військ противника.

Також часто інформація щодо обстановки в операційній зоні угруповання військ противника не збігалася, інколи – суперечила інформації в офіційних зведеннях міністерства оборони РФ.

Періодично публікувалися фейки та дезінформаційні матеріали, які достатньо легко виявлялися та спростовувалися.

Типовими прикладами залякування особового складу наших військ та цивільного населення в районі бойових дій є демонстрація противником збільшення загроз для життя визначених цільових аудиторій за рахунок застосування потужнішої зброї, нарощування інтенсивності ракетних, авіаційних та артилерійських ударів, низької ефективності наших засобів протиповітряної оборони та фортифікаційних систем. Так, в операційній зоні оперативно-тактичного угруповання «Харків» противник регулярно поширював інформацію про готовність застосовувати осколочно-фугасні бомби з універсальним модулем планування та корекції (який дає змогу суттєво збільшити дальність авіаційних ударів) вагою 3 тони (в окремих фейках вага бомби зростала до 10 тон). Також використовувалася ситуація в районі населеного пункту Сотницький Козачок, де більше місяця поспіль тривали позиційні бої. Противник повідомляв про захоплення цього населеного пункту і розміщення в ньому своєї реактивної та ствольної артилерії, що створювало загрозу артилерійських обстрілів для Золочівського району Харківської області.

Достатньо часто противник намагається закидати листівками позиції сил оборони України, використовуючи агітаційні боєприпаси (снаряди та міни) та безпілотні літальні апарати. Зміст листівок повністю повторює наративи та меседжі російської пропаганди: «насильницька» мобілізація, залежність української влади від країн Заходу, зв'язок нашого керівництва з олігархами, сумна ситуація в Україні тощо (*рис. 4*). У своїх листівках противник закликає наш особовий

Рисунок 4. Типова листівка противника на Харківському напрямку

склад не брати участі в бойових діях, повертатися додому або здаватись у полон російським військам.

Однією з найпоширеніших інформаційних акцій російських військ щодо пропагування здачі в полон є поширення інформації щодо такої можливості через радіозвернення на частоті 149.2 МГц «Викликай Волгу». Інформація про таку можливість поширюється в листівках, СМС-повідомленнях, усіх без винятку російських телеграм-каналах, які висвітлюють бойові дії проти України, соціальних мережах і на Інтернет-сайтах, транслюється російськими телевізійними каналами та радіостанціями. Періодично противник поширює інформацію про велику кількість військовослужбовців сил оборони України (понад 10 тисяч), які здались у полон після звернення на вказаній частоті.

Крім пропозицій щодо здачі в полон противник використовує власні засоби радіоелектронної боротьби (станція РЕБ «Леер-3») для розсилання СМС-повідомлень на стільникові телефони. У цих повідомленнях містяться заклики до співпраці з противником за матеріальну винагороду, повідомляється про загрози обстрілів населених пунктів, поширюється інформація про евакуацію тощо, що сприяє зростанню панічних настроїв.

Підрозділами кібервійськ противника регулярно проводяться заходи фішингу з метою одержання доступу до особистих електронних пристроїв та облікових записів наших військовослужбовців і представників цивільного населення. У разі одержання такого доступу у противника з'являється можливість використання персональних даних, особистої, а інколи службової, інформації, здійснення спамових розсилок власних інформаційних матеріалів за всіма адресами зі зламаних пристроїв та облікових записів.

Військовополонених зі складу сил оборони України змушують повторювати (від себе) меседжі російської пропаганди («насильницька» мобілізація, великі втрати наших військ, недостатня бойова підготовка, неефективне командування). Відповідні відео, фото і текстові матеріали одразу використовуються противником у своїх заходах інформаційної боротьби.

Висновки

1. Заходи інформаційної боротьби є невіддільною складовою військових операцій противника.

2. Інформаційні операції, акції та окремі інформаційні заходи, які проводяться угрупованнями військ противника, безумовно, пов'язані з інформаційними кампаніями та операціями стратегічного рівня.

3. Ефективність заходів інформаційної боротьби противника залежить від наших заходів протидії, наших інформаційних та психологічних операцій.

4. Попри перевагу противника в інформаційних ресурсах, залучених до інформаційної боротьби проти України, його чітку ієрархічну систему проведення інформаційних заходів, ми можемо перемагати в інформаційній боротьбі за рахунок проактивності в проведенні наших інформаційних заходів, оперативності інформування щодо ситуації на полі бою, об'єктивності наших інформаційних матеріалів (відсутності явних фейків та сумнівної інформації, яку легко перевірити), креативності і незвичності для противника наших інформаційних матеріалів, неочікуваності противником наших інформаційних заходів і матеріалів.

Перелік літератури

1. Undermining Ukraine: How Russia widened its global information war in 2023 [Електронний ресурс] / Digital Forensic Research Lab // Atlantic Council. – Режим доступу : https://www.atlanticcouncil.org/in-depth-research-reports/report/undermining-ukraine-how-russia-widened-its-global-information-war-in-2023.

2. *Helmus T. C.* Ukrainian Resistance to Russian Disinformation. Lessons for Future Conflict [Електронний ресурс] / T. C. Helmus, K. Holynska // RAND. – Режим доступу : https://www.rand.org/pubs/research_reports/ RRA2771-1.html.

3. Kremlin Communication Strategy for Russian Audiences Before and After the Full-Scale Invasion of Ukraine [Електронний ресурс] / N. Bolt, V. M. Shapir, O. Fridman et al. // NATO Strategic Communications Centre of Excellence. – Режим доступу : https://stratcomcoe.org/publications/ kremlin-communication-strategy-for-russian-audiences-before-and-after-the-full-scale-invasion-of-ukraine/293.

4. The Kremlin's multipolar order of disinformation [Електронний ресурс] // EUvsDisinfo. – Режим доступу : https://euvsdisinfo.eu/the-kremlins-multipolar-order-of-disinformation.

5. Чого Росія очікує від чергового раунду дезінформаційної кампанії щодо України [Електронний ресурс] // Центр протидії дезінформації. – Режим доступу : https://cpd.gov.ua/main/chogo-rosiya-ochikuye-vid-chergovogo-raundu-dezinformaczijnoyi-kampaniyi-shhodo-ukrayiny.

6. Спам, реклама, фейки. Як російська пропаганда атакує українців у соцмережах [Електронний ресурс] // SPRAVDI. – Режим доступу : https://spravdi.gov.ua/spam-reklama-fejky-yak-rosijska-propaganda-atakuye-ukrayinciv-u-soczmerezhah.

7. *Подибайло М. Т.* Деякі висновки щодо методів та засобів інформаційних операцій: уроки російсько-української війни [Електронний ресурс] / М. Т. Подибайло, В. А. Федорієнко // Наука і оборона. – 2024. – № 2. – С. 48–57. – Режим доступу : https://doi.org/10.33099/2618-1614-2024-25-2-48-57.

8. *Наместнік В. В.* Інформаційні операції Росії проти України у 2022–2023 роках: висновки, рекомендації, засвоєні уроки [Електронний ресурс] / В. В. Наместнік, М. С. Клунник // Наука і оборона. – 2024. – № 2. – С. 58–64. – Режим доступу : https://doi.org/10.33099/2618-1614-2024-25-2-58-64.

9. База російських пропагандистів [Електронний ресурс] // Як не стати овочем. – Режим доступу : https://www.inforules.com.ua/propagandists.

10. Як діє кремлівська пропаганда на окупованих територіях України [Електронний ресурс] // Центр протидії дезінформації. – Режим доступу : https://cpd.gov.ua/articles/yak-diye-kremlivska-propaganda-na-okupovanyh-terytoriyah.

DOI 10.33099/2618-1614-2024-27-4-24-32
УДК 355.469.5

П. Б. Волотівський,
кандидат військових наук,
старший науковий співробітник,
Державний науково-дослідний інститут авіації,
П. М. Стешенко,
кандидат технічних наук, старший дослідник,
Державний науково-дослідний інститут авіації,
С. О. Богославець,
кандидат технічних наук,
старший науковий співробітник,
Державний науково-дослідний інститут авіації,
В. В. Корепанов,
Харківський національний університет Повітряних Сил імені Івана Кожедуба

Щодо обрису перспективної системи боротьби з безпілотними авіаційними комплексами

Необхідність протидії безпілотним авіаційним комплексам (системам) збройних сил РФ, які нині входять до основних засобів для нанесення ударів по важливих державних і військових об'єктах України, вимагає створення ефективної системи боротьби із цими засобами повітряного нападу. Основним джерелом створення такої системи є сформульовані цілі й завдання, які мають вирішуватися системою, а також досягнення науки і техніки у відповідних галузях. Важливим питанням на початковому етапі створення (проєктування) такої складної бойової системи, як система протибезпілотної оборони, є окреслення її загального обрису (задум створення, вибір основних концептуальних ознак, концепція створення і застосування). Автори статті пропонують варіант загального обрису системи протибезпілотної оборони у складі вищої системи – ППО України, одержаний у результаті проведених раніше наукових досліджень.

Ключові слова: протиповітряна оборона, обрис системи протибезпілотної оборони, вимоги до системи, безпілотний авіаційний комплекс.

Постановка проблеми. Аналіз бойового досвіду сил оборони України, набутого в процесі відбиття агресії РФ, свідчить, що, враховуючи зростаючу кількість безпілотних літальних апаратів (БпЛА) противника та значну небезпеку від їхніх дій, актуальним є питання нарощування спроможностей щодо боротьби з БпЛА за рахунок формування нової підсистеми протибезпілотної оборони (ПБО) у складі системи протиповітряної/протиракетної оборони (ППО/ПРО) України [1]. Це підтверджується зробленим у роботах [1, 2] висновком про те, що БпЛА є одним з ключових видів сучасного озброєння, формується нова тактика застосування БпЛА, що призводить до зміни характеру війни, боротьба з БпЛА противника на цей час стала завданням стратегічного рівня для Повітряних Сил Збройних Сил України на рівні з протиракетною обороною.

Першим кроком побудови ПБО є формування обрису цієї системи конкретного призначення. Глибше опрацювання варіантів системи та її структури передбачає проведення досить складних системних досліджень щодо визначення оптимального варіанта системи, її структури й системи озброєння. Вирішення цього питання можливе шляхом створення відповідного науково-методичного підґрунтя.

Основною **метою** досліджень, результати яких наведені в статті, є формування варіанта загального обрису системи протибезпілотної оборони як складової частини стратегічної системи ППО/ПРО України на підставі врахування нестачі спроможностей ППО/ПРО України за напрямом боротьби з БпЛА противника.

Аналіз останніх досліджень і публікацій. Останніми роками з'явилася низка публікацій [1–6] з питань розвитку теорії протиповітряної оборони, розгляду проблем в управлінні цією сферою в Збройних Силах України та шляхів їх розв'язання. Водночас слід відмітити, що значущих робіт щодо необхідності створення бойової системи протибезпілотної оборони та окреслення її обрису, крім роботи [1], немає. Однак проблема протидії БпЛА, особливо малим БпЛА, досі залишається ефективно не розв'язаною, є надзвичайно складною та багатогранною і потребує невідкладного розв'язання.

Виклад основного матеріалу

Основною ознакою перспективної системи ПБО є те, що вона за своїм складом і структурою належить до складних систем, а за характером причинно-наслідкових зв'язків, об'єктивно наявних у системі, є дуже складною ймовірнісною системою, котра, у свою чергу, є складовою ППО/ПРО України.

Загалом для такої складної системи, як система ПБО, характерні такі особливості:

- складність структури системи, яка має велику кількість різнорідних взаємопов'язаних підсистем;

• наявність як загальних цілей системи, так і локальних цілей її складових частин;

• ієрархія в управлінні, коли централізоване управління підсистемами поєднується з їхньою автономністю;

• багатофункціональність, зумовлена різноманітністю цілей системи та окремих підсистем і вимог до них, що призводить до необхідності оцінювання системи за багатьма критеріями;

• високі вимоги до обсягів вирішуваних завдань;

• наявність множини перехресних зв'язків;

• складність поведінки системи;

• високий рівень автоматизації окремих процесів і складових елементів;

• поєднання матеріальних підсистем та елементів зі способами, правилами і теоретичними положеннями щодо їхнього застосування;

• різноманітність фізичної природи підсистем та окремих елементів;

• велика кількість зовнішніх впливів;

• наявність у середовищі змагальних відносин та інші особливості.

Зважаючи на зазначене, можемо стверджувати, що розв'язання проблеми організації та функціонування такої складної системи, як ПБО, не мислиме без застосування основних положень системного підходу, в основі якого лежить метод дослідження об'єктів як систем.

Здійснення системного підходу у військовій сфері вимагає застосування (введення) відповідних понять і термінів. Нині в практиці наукових досліджень, пов'язаних з будівництвом збалансованих збройних сил, їх реформуванням, підвищенням ефективності застосування угруповань військ (сил), з'єднань, тактичних одиниць використовується термін «*бойова система*». Під цим терміном розуміють *цілісне утворення – сукупність військ (сил) і технічних систем, об'єднаних у єдине ціле для виконання бойових завдань*.

Залежно від рівня й масштабів бойові системи можуть бути стратегічного, оперативного і тактичного призначення: система протиповітряної оборони України, угруповання збройних сил, об'єднання, з'єднання, тактична група, літак тощо. Виходячи з важливості завдань, які покладаються на систему ПБО у складі системи ППО України вже сьогодні та значно ускладняться в недалекій перспективі, вона має належати до систем стратегічного призначення.

Чинники та умови, які спонукають до створення системи протибезпілотної оборони. На третьому році російсько-української війни можна спостерігати багаторазове зростання кількості застосувань БпЛА різних класів за призначенням і масштабом вирішуваних завдань з обох сторін як у зоні бойових дій, так і далеко за її межами. БпЛА сьогодні виявились одним з основних видів сучасного озброєння.

У РФ на цей час відмічається збільшення кількості розробок БпЛА, що виконуються державними та приватними підприємствами – від найбільших літакових та вертолітних фірм до невеликих конструкторських груп. Розроблення та виробництво БпЛА здійснюється в основному за рахунок державного бюджету. За конструктивним виконанням з усіх відомих типів російських БпЛА 70% складають літаки, 30% – вертольоти, з яких значна доля є ударними мультикоптерами. При цьому з технічним удосконаленням БпЛА та збільшенням їхніх бойових можливостей зростає кількість, складність та обсяги завдань, до виконання яких вони залучаються.

Отже, об'єктивні умови збройної боротьби в російсько-українській війні висунули в ролі ударної сили БпАК, які набули значення одного з найважливіших стратегічних чинників. Вони здатні шляхом прямого впливу на угруповання військ і життєво важливі військові та важливі для держави інфраструктурні об'єкти здійснювати значний, а іноді й вирішальний вплив на перебіг воєнних дій. Нині боротьба з БпЛА противника в повітряному просторі над полем бою, в глибині оборони наших військ, у повітряному просторі поза зоною активних бойових дій стає найбільш актуальною частковою *стратегічною ціллю протиповітряної оборони держави* [1, 4].

Типові об'єкти дії (впливу) системи ПБО. Одними з основних БпЛА, які РФ постійно застосовує у війні з Україною на оперативному рівні, є разові ударні БпЛА типу «Shahed 131», «Shahed 136» іранського розроблення (російські назви «Герань-1», «Герань-2») та БпЛА типу «Гербера», «Пародія» як хибні цілі. Цілями ударного БпЛА «Shahed 136» є стаціонарні об'єкти критичної інфраструктури, промислові й житлові будівлі, елементи ППО, нерухома важкоброньована техніка, ракетні системи залпового вогню типу HIMARS та інші подібні об'єкти. Застосовуються ці БпЛА групами або парами по визначених цілях з метою підвищення імовірності їх знищення або виведення з ладу з урахуванням протидії системи протиповітряної оборони. На тактичному рівні застосовуються разові ударні БпЛА типу «Ланцет» з різними модифікаціями та радіусами дії 40–70 км та 40–65 км відповідно. Також на сьогодні противником масово використовуються разові ударні БпАК І класу мікро з БпЛА, які мають систему керування типу FPV і дальність дії до 15–20 км. Зазначені вище БпАК у недалекій перспективі застосовуватимуться масовано – у складі груп, системи наведення яких побудовані на основі алгоритмів штучного інтелекту.

Окрім наведених вище ударних разових БпЛА агресор використовує проти сил оборони України також

інші типи БпЛА у складі комплексів різного призначення, наприклад:

- комплекс безпілотної повітряної розвідки та спостереження з БпЛА «Орлан-10» («Орлан-30»);
- комплекс повітряної розвідки малої дальності «Суперкам С350»;
- комплекс оптико-електронної повітряної розвідки та ретрансляції інформації з БпЛА «Тахион»;
- комплекс «Леер-3» для ведення радіорозвідки, виявлення джерел випромінювання в радіодіапазоні, постановки завад і придушення радіоелектронних засобів;
- комплекс ведення радіомоніторингу стільникового зв'язку, постановки завад і придушення радіоелектронних засобів, ведення повітряної розвідки та спостереження за допомогою фото-, відео- та інфрачервоних камер з БпЛА «Гранат-4»;
- комплекс безпілотної повітряної розвідки та видачі цілевказівок ударним (вогневим) засобам з БпЛА «Застава».

Тому для протидії БпЛА противника, здатних виконувати бойові завдання на всіх рівнях від тактичного до стратегічного, необхідне проведення сукупності заходів, *спрямованих на недопущення їх проникнення (прольоту) в повітряний простір над полем бою та над рештою території нашої країни*. Для виконання цього складного завдання має бути створена відповідна система боротьби із цим видом зброї, складова системи ППО України.

Основні характеристики загального обрису системи ПБО. Зазначимо, що визначення загального обрису системи означає формулювання задуму на її створення. Водночас обґрунтування обрису цієї системи є складнішим завданням, адже більш повно мають бути враховані її особливості, певні ознаки та показники. Тобто під обрисом системи ПБО слід розуміти певну сукупність основних характеристик системи загалом та характеристик її ключових підсистем, співвідношення засобів повітряної розвідки, вогневого впливу, радіоелектронної боротьби (РЕБ), організаційну побудову тощо.

Важливо брати до уваги, що під час створення загального обрису мають ураховуватися можливі варіанти сценаріїв (оперативних моделей) бойових дій щодо відбиття атак БпЛА в рамках дій вищої системи, а саме системи ППО/ПРО держави.

До сукупності основних характеристик загального обрису системи ПБО (замислу її створення) автори за результатами досліджень пропонують включити такі характеристики:

- призначення системи;
- її часткова стратегічна ціль у рамках системи ППО держави;
- завдання системи, реалізацією яких досягається мета функціонування системи;
- оперативно-стратегічні вимоги до системи;
- спосіб побудови ПБО в рамках вищої системи – системи ППО;
- функціональна структура системи ПБО та її загальна структура з указуванням підпорядкованості за рівнями управління;
- підсистеми (елементи) ПБО, що утворюються для виконання завдань системою;
- основні угруповання військ (сил), створюваних для протидії БпЛА, в оперативній побудові відповідно до задуму операції (бойових дій);
- оперативно-стратегічні вимоги до перспективної системи озброєння ПБО;
- показники ефективності системи, часткові показники та значення критеріїв ефективності *i*-х складових підсистем.

Розгляньмо коротко зміст цих основних характеристик загального обрису перспективної системи ПБО.

Призначення системи ПБО логічно випливає з мети функціонування вищої системи, якою є система ППО/ПРО держави. Природно, вона призначена для недопущення перетину державного кордону України всіма типами БпЛА противника, їх проникнення в повітряний простір нашої країни та для зриву ведення ними розвідки, нанесення ударів по військах, об'єктах держави на всю глибину їхніх можливих дій шляхом послідовного та комплексного вогневого впливу, впливу радіозавадами на їхні радіоелектронні засоби (РЕЗ), руйнування (пошкодження) елементів РЕЗ засобами функціонального ураження надвисокочастотним та лазерним випромінюванням.

Частковою стратегічною метою системи ПБО, як зазначено в [1, с. 41], слід вважати «недопущення прориву БпЛА противника через державний кордон України, лінію зіткнення протиборчих сторін та їхніх дій щодо ведення розвідки, нанесення ударів по військах, об'єктах держави на всю глибину можливого їх застосування».

Основні завдання системи ПБО, реалізація яких дає змогу досягти мети її функціонування [1, с. 41], є такі:

- своєчасне виявлення БпЛА в усьому діапазоні висот їхнього польоту з урахуванням малої радіолокаційної помітності;
- оповіщення в установлені нормативні строки органів державної влади, органів військового управління, населення, військ про загрозу ударів безпілотної авіації;
- знищення (придушення) на визначених рубежах зони (поясу) ППО/ПРО/ПБО всіх типів БпЛА противника при намаганні перетину державного кордону та проникнення в повітряний простір України (у тому числі через лінію зіткнення військ) для недопущення

їхнього прориву (проникнення) в райони виконання завдань на всю глибину їхніх можливих дій;

• об'єктове прикриття великих населених пунктів, найбільш значущих для держави інфраструктурних та інших об'єктів від ударів БпЛА, що прорвалися через кордон у повітряний простір України;

• надійне прикриття угруповань військ (сил), елементів логістики в зоні бойових дій від ударів ударних і розвідувально-ударних БпЛА, у тому числі з FPV-керуванням;

• забезпечення стійкості (живучості) системи ПБО в складних умовах обстановки, атак в інформаційному та кіберпросторі, масованих авіаційно-бомбових і ракетних ударів, застосування сил і засобів РЕБ, протирадіолокаційних ракет та інших засобів;

• набуття спільних спроможностей із силами оборони щодо знищення на території противника об'єктів промисловості з виробництва БпАК, місць їхнього зберігання, ремонту та обслуговування тощо.

Оперативно-стратегічні вимоги, які висуваються до системи протибезпілотної оборони, визначаються насамперед її місцем і роллю в системі більш високого ієрархічного рівня, тобто в системі ППО держави. Система ПБО має входити як невід'ємний функціональний елемент вищої системи, виконувати завдання як у рамках цієї системи, так і автономно (самостійно).

Призначення системи боротьби з БпАК противника в перспективній інтегрованій системі ППО/ПРО/ПБО України, часткова стратегічна мета функціонування системи та її завдання, реалізацією яких досягається ця ціль, погляди інших дослідників у сфері ППО держави [1–6], військово-технічні чинники, що вносять кардинальні зміни у зміст збройної боротьби (нове озброєння та військова техніка, їхній технологічний рівень, розвиток технологій подвійного призначення тощо), можливі сценарії (оперативні моделі) бойових дій сил протибезпілотної оборони в системі інтегрованої ППО/ПРО/ПБО держави, логічні міркування та практика відбиття засобів повітряного нападу в процесі війни з РФ дають підстави сформулювати варіант основних загальних оперативно-стратегічних вимог до системи протибезпілотної оборони з урахуванням [1]. Це такі окремі показники вимог:

1. Система ПБО має входити як невід'ємний функціональний елемент вищої системи, системи ППО України, виконувати завдання як у рамках цієї системи, так і автономно (самостійно).

2. Система ПБО має забезпечити своєчасне виявлення БпЛА в усьому діапазоні висот їхнього польоту з урахуванням малої радіолокаційної помітності.

3. Система ПБО повинна мати спроможність знищення *не менше 90%* БпЛА, які намагатимуться прорватися через державний кордон України для виконання визначених завдань у глибині території.

4. Система ПБО повинна мати ієрархічну організацію, загальну керівну (командну) підсистему, підсистеми різного рівня зі своїми органами управління з певним пріоритетом у прийнятті рішень між підсистемами.

5. Розвиток озброєння системи ПБО має відбуватись у рамках створення багатофункціональної бойової системи, яка об'єднуватиме в єдине ціле засоби виявлення, знищення та придушення на базі автоматизованої системи управління.

6. Перспективна система ПБО повинна бути оснащена високотехнологічними зразками озброєння та військової техніки, котрі мають необхідні бойові спроможності та об'єднані інноваційними технологіями управління, застосування яких дає суттєве збільшення бойового потенціалу та можливість здобуття переваги над противником.

7. Упровадження для боротьби з БпАК озброєння та військової техніки на основі нових фізичних принципів, технологій у сфері штучного інтелекту, використання лазерів, електромагнітної зброї, мережних гармат.

8. Забезпечення стійкості (живучості) системи ПБО в складних умовах обстановки, атак в інформаційному та кіберпросторі, масованих авіаційно-бомбових та ракетних ударів, застосування сил і засобів РЕБ, протирадіолокаційних ракет та інших засобів.

9. Набуття спільних спроможностей із силами оборони щодо знищення на території противника об'єктів промисловості з виробництва БпАК, місць їхнього зберігання, ремонту та обслуговування тощо.

10. Система ПБО повинна мати високу працездатність і надійність.

Спосіб побудови протибезпілотної оборони. Досвід відбиття агресії проти України, досвід побудови системи ППО в державі Ізраїль, КНР, США, наукові дослідження, проведені впродовж останнього десятиліття, дають підстави зробити висновок, що для сучасних умов та на довгострокову перспективу найдоцільнішим способом побудови протиповітряної оборони України від засобів повітряного нападу противника в загрозливий період та під час війни є організація зонально-об'єктової протиповітряної оборони [6, с. 48]. Тому спосіб побудови протибезпілотної оборони має відповідати способові побудови протиповітряної оборони України та полягає в організації зональної та об'єктової ПБО в рамках інтегрованої ППО/ПРО/ПБО України з організацією ударної, забезпечувальної, керівної та обслуговувальної підсистем, у створенні угруповань військ (сил) на певних напрямках у їхній оперативній побудові (бойовому порядку). У зонах ППО/ПРО/ПБО угруповання (підрозділи) ПБО розгортаються в бойові порядки та знищують виявлені БпЛА противника.

Функціональна схема системи ПБО відображає задум її побудови. Саме в цій схемі в символічній формі знаходять відображення основні варіанти ідей побудови системи ПБО. Вони, у свою чергу, надалі відображаються в структурі системи. Опис функціональної схеми має на меті створення алгоритмів функціонування підсистем і ПБО загалом. Структура системи ПБО, що відображає її організаційну форму, розробляється відповідно до бойових завдань, покладених на систему. Вона створюється за принципом ієрархії підпорядкованості (угруповання військ (сил), з'єднання, частини, підрозділи й інші елементи, які, у свою чергу, складатимуть функціональні підсистеми).

Як зазначалося вище, система ПБО є багатофункціональною бойовою системою, що об'єднує в єдине ціле засоби: ведення розвідки, спостереження, видання цілевказання (*забезпечувальна підсистема*); знищення та придушення (*ударна підсистема*); енергетичні й інші системи, призначені для забезпечення бойової діяльності (*обслуговувальна підсистема*); органи та пункти управління, автоматизації, зв'язку тощо, які утворюють *керівну підсистему* та забезпечують єдність управління силами й засобами (*рис. 1*).

Особлива роль у системі ПБО, як і в будь-якій іншій бойовій системі, належить керівній підсистемі, яка організує процес функціонування решти підсистем. Адже її руйнування або дезорганізація призводить, як правило, до розбалансування всієї системи загалом.

Рівню системи ПБО мають відповідати масштаби і розмірність її елементів. При цьому кожна підсистема містить притаманні тільки їй підсистеми (елементи) другого рівня (*рис. 2*).

Для виконання системою ПБО завдань боротьби з БпЛА мають утворюватися відповідні підсистеми в рамках функціональної структури системи ПБО у складі ударної, забезпечувальної, керівної та обслуговувальної підсистем. Виходячи з практичного досвіду, це такі підсистеми:

- розвідки та попередження (оповіщення) про перебування в повітрі БпЛА;
- управління силами та засобами ПБО в єдиній системі ППО/ПРО/ПБО території держави, об'єктів та угруповань військ;
- зенітного ракетно-артилерійського прикриття;
- винищувального авіаційного прикриття;
- прикриття військ від ударів безпілотних засобів повітряного нападу під час вогневого протиборства сторін у зоні бойових дій;
- підсистеми об'єктової ПБО для прикриття найбільш значущих для держави об'єктів та інфраструктури від дій ударних БпЛА.

Угруповання військ (сил). З метою виконання завдань системою ПБО з'єднання, частини, окремі підрозділи, призначені для протидії безпілотним системам (комплексам), зводяться в доцільно розгорнуті угруповання військ (сил) на оперативно-стратегічних та окремих оперативних напрямках. Кожне із цих угруповань також становить єдину систему.

Це можуть бути угруповання військ (сил) для недопущення проникнення БпЛА противника через

Рис. 1. Функціональна структура бойової системи ПБО

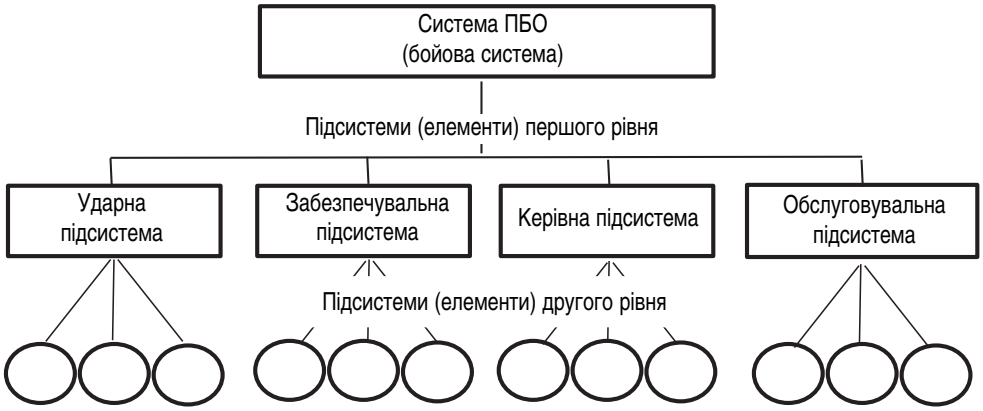

Рис. 2. Склад бойової системи ПБО

державний кордон у повітряний простір держави (у тому числі з боку моря); у повітряний простір над районами бойових дій; угруповання військ (сил) для протиповітряного прикриття важливих державних об'єктів; угруповання військ (сил) для протиповітряного прикриття угруповань військ, що ведуть бойові дії на окремих оперативних напрямках, а також для прикриття системи логістики сил оборони. Природно, ці угруповання поділяються на угруповання за функціональним призначенням: вогневого ураження (ударні), засоби розвідки, РЕБ тощо (забезпечувальні), сил і засобів логістики (обслуговувальні).

Кількісно-якісний склад угруповань військ (сил) визначається відповідно до заданих рівнів ефективності виконання визначених завдань. Це завдання, як правило, вирішується під час проведення складних наукових досліджень науково-дослідними установами збройних сил.

Оперативно-стратегічні вимоги до системи озброєння протибезпілотної оборони. Без створення перспективного озброєння протиповітряної оборони, зокрема озброєння протибезпілотної оборони з підвищеними бойовими спроможностями, говорити про воєнну безпеку держави безпредметно. Адже зброя завжди була і залишається матеріальною основою бойових спроможностей кожної організаційної структури збройних сил від підрозділу до стратегічного об'єднання.

Оперативно стратегічні вимоги до системи озброєння ПБО – це вимоги до складу та якісних характеристик озброєння і військової техніки ПБО, до його кількості та бойових спроможностей, які забезпечать ефективне виконання основних завдань для досягнення визначеної для системи ПБО оперативно-стратегічної мети.

Питанню формування оперативно-стратегічних вимог до перспективних систем озброєння приділяла увагу у своїх працях значна кількість учених, наприклад [7–10].

Оперативно-стратегічні, тактичні й технічні вимоги до перспективної системи озброєння ПБО мають формуватися на основі аналізу:

- основної оперативно-стратегічної мети і часткових завдань системи ПБО;
- загальних оперативно-стратегічних вимог до системи ПБО;
- тенденцій розвитку БпЛА (БпАК) в інших країнах, зокрема в РФ, способів їх бойового застосування;
- особливостей прикриття території держави, окремих об'єктів держави, угруповань військ Збройних Сил України від ударів БпЛА-камікадзе, зокрема із системою керування типу FPV;
- способу побудови ПБО в рамках інтегрованої ППО/ПРО/ПБО держави та складу її основних елементів;
- необхідних спроможностей перспективних зразків (комплексів) зброї системи озброєння ПБО, призначених для виконання визначених завдань цією системою;
- оперативно-тактичних нормативів для угруповань військ (сил), організаційних структур ПБО, що залучаються до виконання завдань боротьби з БпЛА противника;
- досягнень науки й техніки та можливостей їх реалізації під час розроблення озброєння системи ПБО.

На підставі викладеного маємо визнати, що *розвиток перспективної системи боротьби з БпАК РФ залежить і може бути зведений передусім до побудови перспективної, якісно нової системи озброєння протибезпілотної оборони*.

Результати аналізу пропозицій, викладених у зазначених вище наукових працях, вимоги Стратегії воєнної безпеки України [11], досвід протидії БпЛА в процесі відбиття широкомасштабної агресії РФ, результати аналізу оперативно-стратегічної мети і часткових завдань системи ПБО, загальні оперативно-стратегічні вимоги до цієї системи, спосіб її побудови,

тенденції розвитку засобів повітряного нападу, можливі сценарії збройного нападу та ведення операцій, результати аналізу найперспективніших напрямів розвитку озброєння протидії безпілотним авіаційним системам та оцінка можливості їх реалізації під час розроблення та виробництва озброєння й інші дані дають можливість сформувати *узагальнені* та *конкретні* оперативно-стратегічні вимоги до перспективної системи озброєння ПБО [8].

На підставі проведених досліджень до **узагальнених оперативно-стратегічних вимог** перспективної системи озброєння ПБО можемо віднести:

- створення в зональній та об'єктовій системах ПБО єдиного суцільного радіолокаційного поля спостереження за рахунок раціонального типажу засобів стратегічної, оперативної та тактичної повітряної розвідок системи ППО/ПРО/ПБО з базуванням їх на землі, в повітрі та в морській зоні;
- підсистема виявлення БпЛА повинна мати спроможності виявлення БпЛА відповідно I, II, III класів на відстанях, що забезпечують своєчасне їх ураження (придушення) та зрив виконання поставлених завдань;
- перспективне озброєння ПБО має забезпечити створення в Україні глибокоешелонованої ПБО на всю глибину дії існуючих і перспективних БпЛА, для чого потрібно мати: зенітні ракетні комплекси (ЗРК), зенітні артилерійські комплекси (ЗАК), авіаційні ракетні комплекси перехоплення (знищення) БпЛА на всіх висотах їхнього застосування, засоби радіоелектронної протидії (РЕП) для радіоелектронного придушення сигналів навігації, управління (телеметрії) та передачі даних, комплекси радіоелектронної розвідки (РЕР), засоби функціонального ураження БпЛА лазерним та надвисокочастотним випромінюванням, інші засоби протидії БпЛА;
- озброєння ПБО має забезпечувати боротьбу з усіма типами БпЛА без значного розширення типажу та номенклатури зразків озброєння ПБО;
- перспективні (модернізовані) системи зброї для протидії ворожим БпЛА, FPV-БпЛА та «баражуючим боєприпасам» мають створюватися на основі комплексування ЗРК і ЗАК з комплексами радіо- та радіотехнічної розвідки (РРТР), РЕП з їх подальшим використанням як єдиної функціональної системи;
- досягнення відповідності системи ПБО та систем її зброї за технологією побудови, технічними й тактичними характеристиками стандартам НАТО;
- забезпечення мінімальних строків створення перспективної ПБО на основі швидкого налагодження виробництва високотехнологічних засобів боротьби з БпЛА противника всіх типів, у тому числі основаних на передових цивільних технологіях;
- оснащення системи ПБО сучасними радарами, високотехнологічними засобами радіотехнічної розвідки, іншими засобами для забезпечення якісної повітряної, наземної та морської складової розвідки в інтересах системи ПБО;
- відповідно до ієрархічної структури побудови угруповань військ, які прикриваються системою ППО/ПРО/ПБО, система вогневих засобів, засобів РЕБ ПБО має поділятися на підсистеми оперативно-стратегічних та оперативно-тактичних об'єднань, бригадних і батальйонних ланок тощо;
- система управління силами й засобами ПБО має бути інтегрована в єдину систему управління силами й засобами ППО/ПРО/ПБО;
- упровадження сучасних інформаційних технологій, які забезпечать поєднання в єдиній інформаційній мережі джерел інформації (розвідки), органів управління та засобів ураження географічно розосереджених військових частин і підрозділів підсистеми ПБО;
- забезпечення мобільності й захисту озброєння системи ПБО від засобів РЕБ, вогневого ураження протирадіолокаційних ракет (снарядів) противника в місцях розташування, під час здійснення маневру військ (сил) з одного напрямку на інший. Для цього зразки (комплекси) озброєння мають базуватися на уніфікованих за бойовою масою (легка, проміжна, середня категорії) засобах пересування з високими швидкісними характеристиками, високою прохідністю і транспортабельністю, бути захищеними від атак в інформаційному та кіберпросторі, забезпечуватися уніфікованими комплектами маскування;
- система озброєння для протидії безпілотним авіаційним комплексам (системам) має бути збалансованою та уніфікованою;
- для забезпечення підготовки особового складу мають бути розроблені, виготовлені та поставлені у війська навчально-тренувальні засоби, комплексні, спеціалізовані й універсальні тренажери-імітатори, макети і моделі, які повинні в повному обсязі імітувати повітряну обстановку, а також дії сил і засобів ПБО щодо відбиття нальоту та ударів БпЛА противника.

Крім загальних вимог до перспективної системи озброєння ПБО висуваються конкретні вимоги.

Конкретні вимоги до перспективної системи озброєння ПБО – це конкретні вимоги до систем озброєння складових підсистем системи ПБО, призначених для боротьби з БпАК противника, а саме до:

- підсистеми управління силами та засобами ПБО в єдиній системі ППО держави, об'єктів та угруповань військ (сил);
- підсистеми виявлення та ідентифікації БпЛА противника;
- підсистеми оповіщення військ (сил) про появу в повітрі БпЛА противника;
- підсистеми вогневого ураження БпЛА противника;

• підсистеми протидії бортовим системам розвідки БпЛА;

• підсистеми виявлення майданчиків (місць) підготовки БпАК до застосування та здійснення пусків БпЛА;

• підсистеми ураження наземної складової системи виробництва, складування БпЛА противника, майданчиків їх підготовки та здійснення пусків.

Показники ефективності системи. Кожне із завдань системи ПБО виконується певною функціональною підсистемою у складі відповідних угруповань. Значущість системи ПБО визначається сумарною величиною збитків, що завдаються підсистемами ПБО безпілотній авіації противника під час вирішення кожного поставленого завдання. При цьому різноманітність завдань, вирішуваних системою ПБО, різнорідність властивостей її підсистем та елементів, широкий діапазон змін параметрів системи і середовища не дають змоги мати один узагальнений показник ефективності. Це означає, що мета функціонування системи досягається спільним вирішенням завдань різними підсистемами.

Ефективність вирішення кожного із завдань різного рівня ієрархії та змісту оцінюється відповідним частковим показником – показником ефективності *i*-ї підсистеми. Тому, вибираючи показники ефективності під час обґрунтування вимог до системи ПБО, виходять з того, що вони мають об'єктивно характеризувати як складові частини ПБО, так і всю систему загалом, відображати її цільове призначення, бути чутливими до змін її основних параметрів.

Загалом вважатимемо, що ефективність системи боротьби з БпАК на всіх напрямках полягає в забезпеченні збереження об'єктів, що прикриваються. Допустимі втрати не повинні бути більшими за 10%: ПБО успішна – більше 90% збережених об'єктів; стійкість ПБО порушена – 70–90% збережених об'єктів; ПБО прорвана – менше 70% збережених об'єктів.

Перспективи розвитку системи ПБО. Командування повітряно-космічних сил РФ має сподівання, що застосування в ударах декількох ешелонів груп малих і відносно дешевих ударних БпЛА може паралізувати ППО України. Уже сьогодні групове застосування БпЛА стає серйозним чинником для досягнення воєнної переваги малими затратами. Отже, подальший розвиток тактики й технології групового застосування БпЛА суттєво ускладнить умови функціонування комплексів ППО та потребуватиме кардинального перегляду ідеології створення і застосування систем ППО. Тому маємо визнати, що ефективна боротьба з БпЛА РФ може бути забезпечена насамперед на основі побудови перспективної, якісно нової системи ПБО.

Перспективна система ПБО має бути оснащена високотехнологічними зразками озброєння та військової техніки, об'єднаними інноваційними технологіями управління. Це надасть можливість суттєвого збільшення бойового потенціалу сил оборони України і здобуття переваги над противником. Нарощування спроможностей системи ПБО має здійснюватися на передових технологіях. При цьому залучення для масового виробництва озброєння та військової техніки елементної бази, комплектувальних вузлів та іншої цивільної продукції здатне значно розширити можливості промисловості і скоротити строки виробництва озброєння і військової техніки.

Уже сьогодні є актуальним завдання створення безпілотних винищувачів (перехоплювачів) літакового та коптерного типу, а також розвитку технологій їх групового застосування.

Ефективна боротьба з БпЛА противника і закриття українського неба для його безпілотної авіації можуть бути забезпечені необхідною інтеграцією, уніфікацією та збалансованістю вогневих засобів, засобів радіо- та радіотехнічної розвідки й радіоелектронного придушення в рамках інтегрованої ППО/ПРО/ПБО України.

Таким чином, система ПБО як складова системи ППО України має створюватися з науковим обґрунтуванням основних характеристик цієї системи, в основу яких покладаються оперативно-стратегічні та оперативно-тактичні вимоги до системи озброєння та систем зброї протибезпілотної оборони.

Наведений варіант загального обрису системи ПБО дає уявлення про її призначення, завдання, склад, функціональну структуру, принцип упорядкування елементів (підсистем) і взаємодію між ними. Одержана в результаті формування загального обрису інформація є необхідними вихідними даними для подальших складних системних досліджень системи ПБО.

Висновки

1. Створення (проєктування) такої складної бойової системи, як система протибезпілотної оборони, має розпочинатися з окреслення її загального обрису.

2. Система ППО України, яка діє нині, у протистоянні масованим атакам ударних БпЛА має дефіцит спроможностей щодо захисту як окремих об'єктів, так і території України загалом від цього виду озброєння. Саме потреба в посиленні спроможностей системи ППО щодо боротьби з БпЛА зумовлює необхідність та визначає напрями розбудови системи протибезпілотної оборони.

3. Розвиток перспективної системи боротьби з безпілотною авіацією зводиться передусім до побудови якісно нової системи її озброєння. Система ПБО як підсистема стратегічної системи ППО держави повинна мати необхідні оперативні спроможності для боротьби з БпЛА ймовірного противника згідно з науково обґрунтованими оперативно-стратегічними вимогами до неї та її системи озброєння.

Перелік літератури

1. *Волотівський П. Б.* Погляди і перспективи створення системи протибезпілотної оборони, її роль та місце в системі протиповітряної оборони України [Електронний ресурс] / П. Б. Волотівський, О. В. Самойленко, П. М. Стешенко, П. А. Глущенко // Наука і оборона. – 2024. – № 3. – С. 37–44. – Режим доступу : https://doi.org/10.33099/2618-1614-2024-26-3-37-44.

2. *Коршець О. А.* Уроки застосування безпілотних літальних апаратів у російсько-українській війні [Електронний ресурс] / О. А. Коршець, В. М. Горбенко // Повітряна міць України. – 2023. – № 1 (4). – С. 9–17. – Режим доступу : https://doi.org/10.33099/2786-7714-2023-1-4-9-17.

3. *Ткачов В. В.* Проблеми в управлінні протиповітряною обороною та шляхи їх розв'язання [Електронний ресурс] / В. В. Ткачов, Ю. О. Горобець, В. В. Камінський, Г. С. Степанов // Наука і оборона. – 2020. – № 3. – С. 15–19. – Режим доступу : https://doi.org/10.33099/2618-1614-2020-12-3-15-19.

4. *Крикун П. М.* Система протиповітряної оборони України в умовах збройної агресії [Електронний ресурс] / П. М. Крикун, В. І. Павленко, В. С. Корендович // Наука і оборона. – 2022. – №3/4. – С. 17–21. – Режим доступу : https://doi.org/10.33099/2618-1614-2022-20-3-4-17-21.

5. *Дроздов С. С.* Аналіз операційного середовища та ймовірні сценарії застосування Повітряних Сил Збройних Сил України [Електронний ресурс] / С. С. Дроздов, В. В. Тюрін, О. А. Коршець, В. М. Горбенко // Наука і оборона. – 2019. – № 3. – С. 25–30. – Режим доступу : https://doi.org/10.33099/2618-1614-2019-8-3-25-30.

6. *Лосєв І. Ф.* Тенденції розвитку теорії протиповітряної оборони Повітряних Сил Збройних Сил України / І. Ф. Лосєв, В. В. Антонець // Наука і оборона. – 2006. – № 2. – С. 46–52.

7. *Антонець В. В.* Концептуальні підходи до створення перспективних систем озброєння протиповітряної оборони / В. В. Антонець, В. І. Білетов, М. Ю. Голобородько // Наука і оборона. – 2006. – № 1. – С. 38–43.

8. *Стеценко О. О.* Методологічні аспекти формування оперативно-стратегічних та оперативно-тактичних вимог до перспективних систем озброєння Збройних Сил України / О. О. Стеценко, О. П. Ковтуненко, І. С. Цибулько // Наука і оборона. – 2001. – № 4. – С. 46–54.

9. *Антонець В. В.* Методологічні аспекти формування вимог до систем озброєння Збройних Сил України / В. В. Антонець, В. М. Миронович, О. В. Сафронов, С. Л. Луцик // Наука і оборона. – 2002. – № 4. – С. 52–55.

10. Большие технические системы: проектирование и управление : монография / Л. М. Артюшин, Ю. К. Зиатдинов, И. А. Попов, А. В. Харченко; под ред. И. А. Попова. – Х. : Факт, 1997. – 400 с.

11. Стратегія воєнної безпеки України [Електронний ресурс] : затверджена Указом Президента України № 121/2021 від 25 березня 2021 р. // Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show//121/2021#Text.

DOI 10.33099/2618-1614-2024-27-4-33-39
УДК 355.013

М. В. Коваль,
доктор військових наук,
Національний університет оборони України,
В. О. Косевцов,
доктор військових наук, професор,
Національний університет оборони України,
В. М. Телелим,
доктор військових наук, професор,
Національний університет оборони України,
А. Г. Захаржевський,
кандидат технічних наук,
Національний університет оборони України

Методичний підхід до прогнозування узагальненого конфліктогенного індексу можливого воєнного конфлікту

У статті надано авторське бачення вирішення проблемних питань моніторингу воєнно-політичної обстановки на основі визначення узагальненого конфліктогенного індексу у взаємовідносинах з будь-якою країною для своєчасного запровадження заходів запобігання, стримування або відбиття можливого нападу противника.

Ключові слова: воєнний конфлікт, узагальнений конфліктогенний індекс конфлікту, конфліктогенні чинники, методи багатовимірного порівняльного аналізу, коефіцієнти важливості конфліктогенних чинників, фази та етапи розвитку воєнного конфлікту.

Постановка проблеми. Попри прагнення світової спільноти до спільного забезпечення стратегічної стабільності, формування багатополярної структури міждержавного співробітництва на регіональному рівні, світова політика залишається сферою неприхованого панування «кулачного права». «Кулачне право» як інструмент міжнародних відносин, на жаль, і у XXI столітті продовжує використовуватися під час розв'язання існуючих політичних, економічних, територіальних, етнічних, релігійних протиріч. Тому своєчасне виявлення моменту підготовки й нападу агресора залишається однією з найважливіших проблем для кожної країни. У зв'язку із цим постійний моніторинг зміни рівня напруженості між країнами є дуже актуальним завданням, для вирішення якого пропонується технологія визначення узагальненого конфліктогенного індексу можливого воєнного конфлікту.

Аналіз останніх досліджень і публікацій. Ідея методу кількісного багатовимірного оцінювання воєнно-політичної обстановки на основі визначення рівня воєнної небезпеки з боку будь-якої держави з використанням методів таксономії була визначена в науковій роботі [1]. У подальшому ця ідея була перекладена на метод аналізу ієрархій [2]. У статті [3] був представлений алгоритм поетапної процедури проведення розрахунків. Ідея оцінювання воєнно-політичної обстановки на основі методів таксономії була модифікована із заміною переліку показників, які загалом характеризують ступінь загострення воєнно-політичної обстановки вже на останньому етапі розгортання військ противника на кордоні у статті [4]. У статті [5] запропонований узагальнений алгоритм оцінювання стану воєнно-політичної обстановки на основі методів теорії експертного оцінювання. У роботі [6] наведена векторна модель воєнно-політичної обстановки на основі напруженості для трьох ситуацій: спокійна, загострена, кризова.

Але всі наведені роботи загалом спираються або на показники військового характеру приготування противника до розв'язання воєнного конфлікту, або на окремих етапах (ситуаціях) зростання напруженості, що, у свою чергу, унеможливлює прогнозування зародження напруженості у взаємовідносинах сторін з урахуванням глибинних цивілізаційних політичних, культурних, історичних, ідеологічних, духовних та інших відмінностей. Ці роботи не враховують особливості національного менталітету, закономірності виникнення воєнних конфліктів, наміри досягнення привілеїв, реалізації особистих національних інтересів тощо.

Отже, виникла необхідність розроблення сучаснішої технології визначення узагальненого конфліктогенного індексу (УКІ) зародження антагоністичних воєнно-політичних відносин між державами на основі закономірностей виникнення воєнних конфліктів, що вже

відбулися. Такий підхід стане «лакмусовим папірцем» оцінювання зародження і зростання напруженості між державами як на окремому етапі, так і в динаміці.

Метою статті є надання методичного підходу оцінювання, прогнозування і визначення рівня напруженості у взаємовідносинах між країнами (коаліціями) як на початковому етапі, так і критичного рівня цієї напруженості для своєчасної підготовки й ефективного реагування на воєнну загрозу та агресію.

Виклад основного матеріалу

Характерною рисою кінця XX і початку XXI століття на посткомуністичному просторі є розбудова незалежних держав. В умовах відсутності відповідної правової бази, обґрунтованої політики та стратегії національної безпеки це призвело до всеосяжних кардинальних змін у всіх сферах їхнього політичного та суспільного життя. На жаль, багато в чому в негативному плані.

Насамперед різко загострилися протиріччя всередині країн, активізувалися сепаратистські рухи, посилилася боротьба між конфліктуючими елітними угрупованнями за владу, власність, установлення впливу, контролю, здобуття привілеїв тощо.

У відносинах між державами також посилилася боротьба за стратегічні сировинні ресурси, ринки збуту своєї продукції та технологій, дешеву кваліфіковану робочу силу, поширилися територіально-прикордонні суперечки з метою перегляду існуючих кордонів.

Перелічені «вибухонебезпечні» події в молодих незалежних державах, а також дестабілізаційні дії лідерів національних меншин дедалі частіше в нових геополітичних умовах стають детонаторами збройних конфліктів і локальних війн.

Як свідчать події останнього часу, стають мало контрольованими процеси не лише уникнення регіональних конфліктів, а й вирішення конфліктно-кризових ситуацій політичними, економічними і дипломатичними засобами. Безумовно, все це є дуже тривожним симптомом і дестабілізуючим чинником воєнно-політичної обстановки не лише на регіональному, а й на глобальному рівні, загрозою зниження рівня стратегічної стабільності у світі.

У зв'язку із цим розроблення сучасної технології визначення узагальненого конфліктогенного індексу розвитку будь-якого конфлікту в теоретичному плані набуває особливої важливості. Це дасть змогу своєчасно й ефективно запровадити заходи з недопущення кризи, мирного врегулювання існуючих гострих протиріч і запобігання воєнним конфліктам.

У світовій практиці конфліктні відносини, криза, воєнний конфлікт розглядаються у вигляді окремих фаз та етапів [7].

Основні фази й етапи розвитку воєнного конфлікту зображені на *рисунку 1*.

Як бачимо, в кожному воєнному конфлікті наявні три фази [7]:

- латентна передконфліктна фаза, на якій конфлікт зароджується і має прихований характер;
- відкрита фаза, коли учасники конфлікту починають реалізовувати свої цілі силовими методами;
- латентна (батальна) фаза (післяконфліктна), яка зовні не проявляється, але на якій відбувається мирне врегулювання кризи й завершення конфлікту.

З латентною передконфліктною фазою пов'язана наявність у супротивних сторін протиріч у потребах, інтересах або цінностях. Наявність цих протиріч і ступінь їхньої важливості можуть бути визначені конфліктогенним індексом можливого конфлікту. З наростанням напруженості між супротивними сторонами цей індекс зростає, і в разі досягнення певного його значення (рівня) починається безпосередньо збройна боротьба – фаза відкритого воєнного конфлікту.

Теоретично і практично всі конфлікти відрізняються один від одного масштабом, інтенсивністю загострення відносин, часом перебігу тощо, але всім їм притаманні характерні особливості й тенденції розвитку.

Розвиток конфлікту може відбуватись як за рахунок його поширення по горизонталі (втягування нових учасників, виникнення нових проблемних суперечок або поглиблення, диференціація старих), так і за рахунок ескалації (загострення конфліктних відносин) – розвиток по вертикалі.

Дуже небезпечним є те, що частіше ці два процеси перебігають одночасно, і в основі воєнних конфліктів сучасної епохи лежать головним чином політичні, територіальні, етнічні, соціальні, економічні, технологічні та культурні протиріччя і зіткнення національних інтересів.

Загалом воєнні конфлікти характеризуються за змістом:

- *воєнно-політичним* – визначається:
  - склад протиборчих сторін (коаліцій);
  - їхні політичні цілі, причини і джерела воєнних конфліктів;
  - ставлення до них народів і армій сторін, а також форми і способи ведення ідеологічної, психологічної та дипломатичної боротьби;
- *воєнно-економічним* – цілі сторін в економічному протиборстві:
  - засоби, вживані для економічної боротьби;
  - форми і способи її ведення;
- *воєнно-стратегічним* – визначаються:
  - стратегічні цілі й завдання сторін;
  - причини і способи розв'язування воєнного конфлікту;

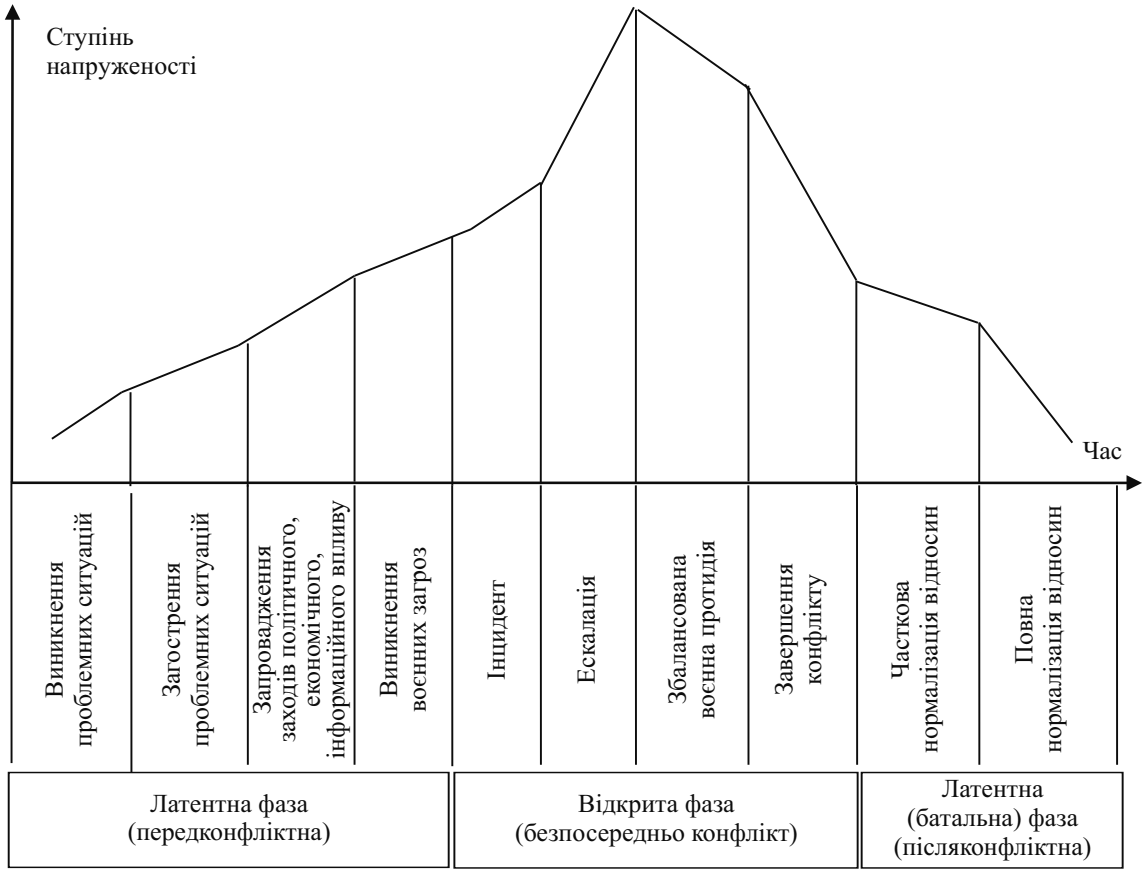

Рис. 1. Основні фази й етапи розвитку воєнного конфлікту

– види застосовуваної зброї, масштаб і розмах воєнних дій;
– особливості, форми і способи ведення воєнних дій;
– імовірна тривалість воєнного конфлікту, його періодизація.

Як свідчить досвід воєнних конфліктів, воєнні дії переважно переміщуються в повітряно-космічний простір з використанням безпілотних високоточних літальних апаратів, активно використовуються засоби радіоелектронної боротьби, активізуються заходи гібридної характеру. Це підтверджують приклади з досвіду підготовки і проведення операцій «Буря в пустелі» в зоні Перської затоки та «Союзницька сила» в Югославії [8–10] та повномасштабна війна Російської Федерації проти України.

Таким чином, можна стверджувати, що в основі виникнення й ескалації воєнних конфліктів лежать характерні особливості і спроможності сторін, специфічні причини (конфліктогенні чинники), які загострюються.

Динаміку розвитку воєнних конфліктів доцільно розглядати на підставі змін значень конфліктогенних чинників, які повною мірою характеризують розвиток воєнно-політичних відносин протиборчих сторін.

До таких найсуттєвіших конфліктогенних чинників, що характеризують наявність глибинних цивілізаційних відмінностей і проблемних ситуацій, можна віднести:

1. Наявність історичного конфліктогенного коріння (анексія території, акваторії, елементів інфраструктури, колонізація, окупація, кривда стосовно етносу, національної меншини, різного роду гноблення).

2. Наявність конфліктуючих елітних угруповань (захоплення влади, власності, встановлення впливу, контролю, привілеїв).

3. Різниця в потенціалах сторін конфлікту (людському, фінансовому, військово-технічному, організаційному, духовному тощо), що стимулює конфлікт.

4. Зіткнення ідеологій, наявність спірних конфронтаційних питань, перетин інтересів країн, релігій, етносів, меншин, політичних еліт тощо.

5. Наявність конфліктогенних зовнішніх впливів різного характеру (економічного, політичного, морального, психологічного, релігійного, воєнного, технічного тощо).

6. Порушення прав і свобод громадян, що викликає втручання третьої сторони.

7. Геноцид стосовно національних меншин або нелегітимне обмеження їхнього розвитку (економічного, політичного, культурного, соціального тощо).

8. Ксенофобія в міжнаціональних відносинах.

9. Прагнення до самовизначення.

10. Природні катаклізми, техногенні катастрофи, епідемії, які слугують каталізаторами соціальних суперечностей.

11. Посилення кризових явищ, перманентне падіння життєвого рівня населення, безробіття тощо.

12. Посилення загроз життєво важливим національним інтересам.

13. Криміналізація суспільства, зростання злочинності на соціально-побутовому та державному рівнях, недосконаліть нормативно-правової бази.

14. Ініціація конфлікту ззовні.

15. Організовані масові акції протесту (демонстрації, мітинги, поховання видатних осіб, жертв соціальних заворушень тощо), викликані національно-культурними суперечностями.

16. Особливості національного менталітету, які стимулюють початок конфлікту.

На підставі оцінювання інтегрального впливу всіх перелічених конфліктогенних чинників можна визначити узагальнений конфліктогенний індекс як будь-якого воєнного конфлікту, так і спрогнозувати тенденції розвитку конфліктних ситуацій, що зароджуються.

Для вирішення цього завдання доцільно розглянути конфліктогенні чинники воєнних конфліктів, що відбулись і ґрунтовно описані [8–10], тоді ця одержана база знань може бути використана для прогнозування ступеня розвитку будь-якого можливого воєнного конфлікту.

Були розглянуті такі воєнні конфлікти:

I. Карабаський конфлікт (між Азербайджаном і Вірменією).

II. Російсько-чеченський.

III. Напад Іраку на Кувейт і «Буря в пустелі».

IV. Придністровський.

V. Російсько-грузинський.

VI. Конфлікт між НАТО та Югославією «Союзницька сила».

VII. Війна СРСР в Афганістані.

VIII. Повномасштабна війна РФ проти України.

У *таблиці 1* наведені значення конфліктогенних чинників для розглядуваних воєнних конфліктів. Ці дані були одержані на основі аналізу фаз та етапів розвитку воєнних конфліктів, результатів експертного опитування, а також деяких джерел [8–10]. На підставі цих даних, використовуючи методи багатовимірного порівняльного аналізу, можна одержати коефіцієнти важливості конфліктогенних чинників і розрахувати критичні узагальнені конфліктогенні індекси конфліктів, що розглядаються.

Таблиця 1

Результати кількісного оцінювання конфліктогенних чинників та узагальнених конфліктогенних індексів розглядуваних воєнних конфліктів

Конфліктогенні чинники	Значення конфліктогенних чинників воєнних конфліктах								$K_{важлив}$
	I	II	III	IV	V	VI	VII	VIII	
1	0,80	0,85	0,90	0,50	0,68	0,45	0,10	0,8	**0,75**
2	0,70	0,70	0,70	0,67	0,8	0,70	0,90	0,8	**0,50**
3	0,25	0,88	1,00	0,40	0,6	0,90	0,75	0,8	**0,62**
4	0,85	0,80	0,85	0,75	0,5	0,90	0,80	0,8	**1,00**
5	0,90	0,75	0,70	0,90	0,55	1,00	1,00	0,8	**0,89**
6	0,60	0,50	0,80	0,60	0,4	0,60	0,15	0,8	**0,73**
7	0,80	0,60	0,30	0,50	0,4	0,70	0,00	0,8	**0,69**
8	0,70	0,50	0,60	0,30	0,2	0,20	0,00	0,8	**0,65**
9	0,80	1,00	0,70	0,80	0,9	0,90	0,50	0,8	**0,94**
10	0,30	0,00	0,00	0,00	0,3	0,00	0,10	0,8	**0,11**
11	0,90	0,70	0,80	0,70	0,8	0,35	0,70	0,8	**0,83**
12	0,80	0,70	0,60	0,70	0,8	0,60	0,75	0,8	**0,92**
13	0,40	0,85	0,00	0,50	0,5	0,70	0,60	0,8	**0,59**
14	0,30	0,25	0,10	0,50	0,25	0,40	1,00	0,8	**0,70**
15	0,35	0,60	0,10	0,40	0,5	0,60	0,00	0,8	**0,33**
16	0,50	1,00	0,40	0,30	0,6	0,40	0,90	0,8	**0,72**
УКІ	**0,81**	**0,78**	**0,75**	**0,76**	**0,8**	**0,76**	**0,71**	**0,83**	

Після визначення вихідних даних і проведення розрахунків результати кількісного оцінювання коефіцієнтів важливості конфліктогенних чинників та узагальнених конфліктогенних індексів розглядуваних конфліктів, зведені у *таблиці 1*.

На підставі цих даних, використовуючи методи багатовимірного порівняльного аналізу, можна одержати коефіцієнти важливості конфліктогенних чинників і розрахувати критичні узагальнені конфліктогенні індекси розглядуваних конфліктів.

Найкориснішими в цьому плані є методи таксономії [1, 11, 12], оскільки вони позбавлені недоліків, притаманних іншим аналогічним методам, дають змогу одержувати прийнятні результати в умовах відсутності жорстких обмежень на кількість конфліктогенних чинників, обраних для оцінювання узагальнених конфліктогенних індексів конфліктів.

Узагальнений конфліктогенний індекс конфлікту в даному випадку характеризує інтегрований вплив усіх вибраних конфліктогенних чинників з урахуванням їхньої важливості на ступінь загострення конфліктної обстановки.

В окремому стовпчику *таблиці 1* (виділено жирним шрифтом) наведені коефіцієнти важливості конфліктогенних чинників ($К_{важлив}$) Значення ж узагальненого конфліктогенного індексу розглядуваних воєнних конфліктів (УКІ), показані в окремому рядку в *таблиці 1* (жирним шрифтом) і на гістограмі (*рис. 2*).

Одержані результати свідчать, що більшість конфліктогенних чинників мають значний коефіцієнт важливості. Це є свідченням правильного вибору переліку конфліктогенних чинників.

Особливістю одержаних результатів є те, що для всіх конфліктів, що вже сталися, значення кризового узагальненого конфліктогенного індексу перевищує 0,7. Цей результат наштовхує на думку, що 0,7 можна вважати мінімальним кризовим значенням узагальненого конфліктогенного індексу, який може бути розглянутий як індикатор переходу конфлікту, що зароджується, до наступних небезпечних фаз – ворожості та відкритої конфронтації (*рис. 2*).

На основі одержаної бази знань можна провести оцінювання узагальненого конфліктогенного індексу будь-яких воєнних конфліктів і процесу загострення конфліктної ситуації в часі. Так, наприклад, можливо оцінити тенденції зміни узагальненого конфліктогенного індексу Російської Федерації відносно України від розпаду СРСР до повномасштабного її вторгнення на територію України, які наведені на *рисунку 3*.

На основі проведених розрахунків, а також [1], можна стверджувати, що конфліктогенна ситуація в Україні загострювалася, починаючи вже з набуття незалежності. Особливе занепокоєння викликають і, найімовірніше, викликатимуть у подальшому проблеми, пов'язані з взаємовідносинами України з РФ, яка окупувала Крим і продовжує окуповувати території півдня України.

Як свідчать результати розрахунків, у взаємовідносинах України з Російською Федерацією найбільший сумарний потенціал конфліктогенних чинників на даний час зосереджений в ідеологічній, політичній, економічній і воєнній сферах. По-перше, Російська Федерація не бажає визнавати демократичний розвиток України і прагнення її до євроатлантичної інтеграції, по-друге, Російська Федерація помилково переоцінила свій воєнний потенціал і, по-третє, в неї знижується життєвий рівень населення, загострюється економічна криза за рахунок накладених санкцій і, відповідно, зменшення доходів у виробничому секторі та від торгівлі паливно-енергетичними ресурсами.

Відомо [13–15], що для протидії будь-якій ескалації на різних етапах воєнно-політичних взаємовідносин між країнами взагалі використовуються три основні концепції:

- концепція запобігання, яка передбачає активну співпрацю з усіма державами світу в напрямі забезпечення стратегічної стабільності і відвернення воєнних конфліктів виключно політичними, дипломатичними та економічними методами;
- концепція стримування, за якою створюється воєнний потенціал, здатний звести до мінімуму ймовірність виникнення воєнного конфлікту за рахунок потенційної можливості завдати агресору шкоди, за якої він втрачає стимули для нападу;
- концепція відсічі можливій збройній агресії, яка передбачає можливість завдання агресору поразки і примушення його до припинення воєнних дій та відмови від своїх намірів.

Імовірність застосування наведених концепцій залежить від значення узагальненого конфліктогенного індексу і визначається відповідними зонами, наведеними на *рисунку 3*.

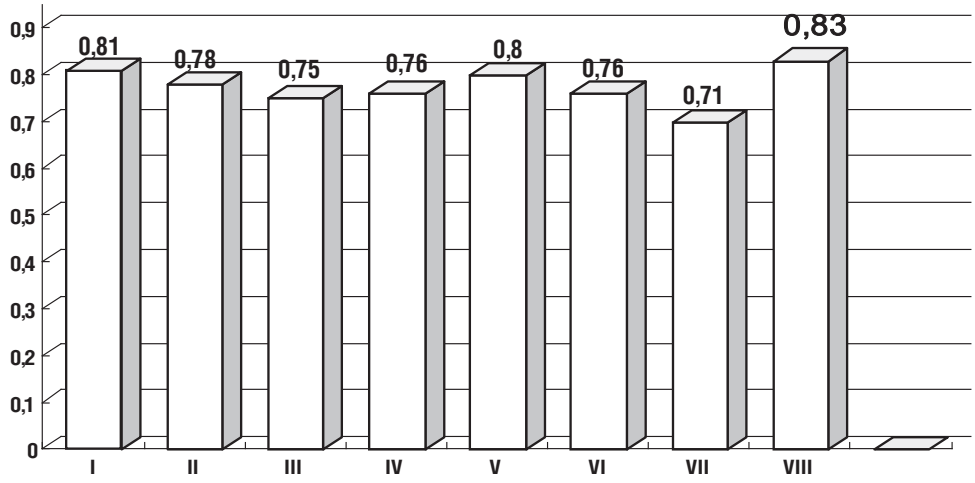

Рис. 2. Значення узагальненого конфліктогенного індексу розглядуваних воєнних конфліктів

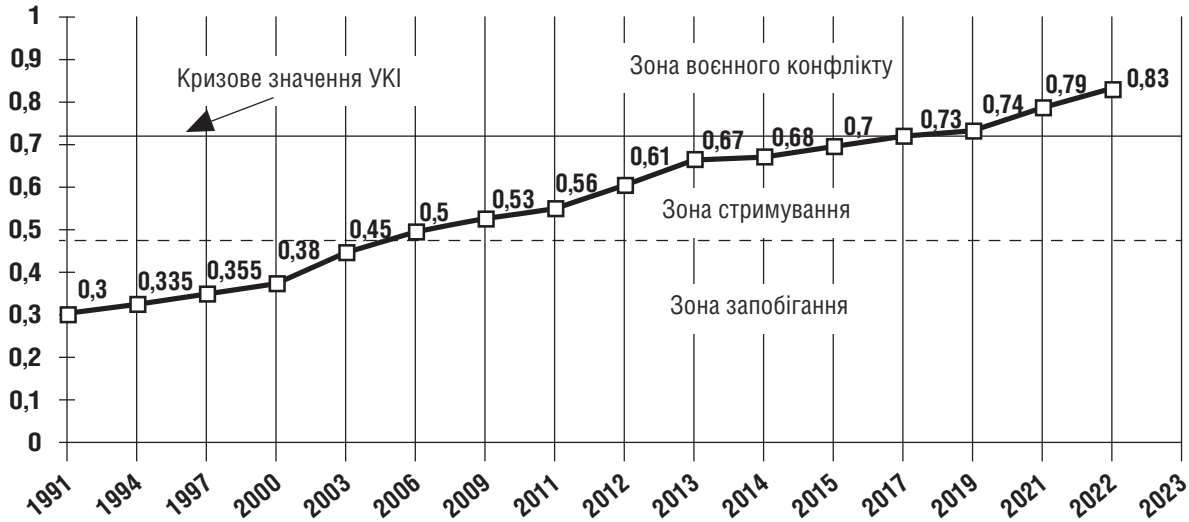

Рис. 3. Тенденції зміни узагальненого конфліктогенного індексу у взаємовідносинах Російської Федерації з Україною від розпаду СРСР до її повномасштабного вторгнення на територію України

Одержані результати розрахунків і визначені закономірності свідчать, що є можливість виявити перші фази будь-якого конфлікту і спрогнозувати деструктивний розвиток подій у різних регіонах світу. Це дає конфліктуючим сторонам змогу з метою недопущення розвитку воєнного конфлікту або швидкої його нейтралізації на початковому етапі своєчасно й ефективно реагувати на конфліктну ситуацію як самостійно, так і з втручанням третьої сторони. При цьому до значення узагальненого конфліктогенного індексу 0,4 необхідно проводити заходи із запобігання воєнному конфлікту, у діапазоні 0,4–0,7 – заходи стримування, а після 0,7 – відбиття агресії.

Таким чином, спираючись на результати розрахунків, стає можливим своєчасно організовувати процес підготовки сил безпеки та оборони, населення, території та держави загалом до захисту, а також забезпечувати медіатора (третю сторону) достовірною інформацією щодо загострення небезпечних конфліктогенних чинників розвитку конфлікту.

Необхідність усунення протиріч на початковому етапі розвитку воєнного конфлікту викликана тим, що останні збройні конфлікти хоча й були в багатьох випадках швидкоплинними, проте не лише мали для конфліктуючих сторін досить трагічні наслідки і значні матеріальні та людські втрати, а й загострювали воєнно-політичну обстановку в регіоні та знижували рівень глобальної безпеки.

Крім того, необхідно враховувати те, що головною метою воєнної безпеки будь-якої країни є відвертання воєнних конфліктів.

Тому для реалізації концепції запобігання потрібно активізувати заходи політичного, дипломатичного, юридичного й економічного характеру, насамперед поширити офіційні та неофіційні зустрічі на рівні найвищого керівництва держав, парламентських і політичних делегацій з метою нейтралізації проблемних ситуацій у міждержавних відносинах та зміцнення довіри, активувати заходи з метою укладення (продовження) довгострокових торговельно-економічних договорів на взаємовигідній основі.

У разі подальшого загострення воєнно-політичної обстановки між державами доцільно звертатися до міжнародних безпекових і правових інститутів для прийняття відповідних санкцій і судових рішень та організовувати заходи стримування агресора. Зокрема йдеться про проведення демонстраційних та організаційних заходів оперативного розгортання з'єднань і частин уздовж кордону, проведення навчань з бойовою стрільбою, перебазування і розосередження сил оборони, цілеспрямованого збирання розвідданих у прикордонних районах, а також активізацію заходів інформаційно-психологічного впливу на країну-агресора. Тобто слід продемонструвати рішучість завдати агресору шкоди, за якої він втрачає стимули для нападу.

Таким чином, можна вважати, що наведений методичний підхід до прогнозування узагальненого конфліктогенного індексу можливого воєнного конфлікту дає підстави для визначення можливої сутності та змістовного наповнення всіх етапів загострення воєнно-політичної обстановки і своєчасного й ефективного реагування на її зміни.

Перелік літератури

1. *Косевцов В. О.* Україна в системі військово-політичних відносин з сусідніми країнами: кількісний вимір / В. О. Косевцов, І. Ф. Бінько. – К. : НІСД, 1996. – 40 с.

2. *Богданович В. Ю.* Воєнна безпека України: методологія дослідження та шляхи забезпечення / В. Ю. Богданович. – К. : Дельта, 2002. – 322 с.

3. *Гогонянц С. Ю.* Загальні положення методики оцінювання рівня воєнної небезпеки на основі таксономічних методів [Електронний ресурс] / С. Ю. Гогонянц, П. М. Грицай, О. О. Шапран // Сучасні інформаційні технології у сфері безпеки та оборони. – № 34 (1). – 2019. – С. 29–36. – Режим доступу : https://doi.org/10.33099/2311-7249/2019-34-1-29-36.

4. Оцінка впливу загострення воєнно-політичної обстановки на виникнення кризової ситуації: методичний аспект [Електронний ресурс] / О. М. Загорка, С. В. Поліщук, В. В. Коваль, І. О. Загорка // Наука і оборона. – № 2. – 2021. – С. 61–65. – Режим доступу : https://doi.org/10.33099/2618-1614-2021-15-2-61-65.

5. *Рябцев В. В.* Методика оцінки воєнно-політичної обстановки в державі / В. В. Рябцев, С. С. Бучик, С. О. Соболенко // Сучасні інформаційні технології у сфері безпеки та оборони. – 2011. – № 1–2 (10–11). – С. 138–141.

6. *Бочарніков В. П.* Системні воєнно-політичні риси сучасного конфлікту на території України : монографія / В. П. Бочарніков, С. В. Свєшніков, Р. І. Тимошенко. – Харків : ХНУПС, 2019. – 206 с.

7. Конфліктологія : навчальний посібник / Л. М. Ємельяненко, В. М. Петюх, Л. В. Торгова, А. М. Гриненко ; за заг. ред. В. М. Петюха, Л. В. Торгової. – К. : КНЕУ, 2003. – 315 с.

8. Локальні війни та збройні конфлікти другої половини XX століття. Історико-філософський аспект / О. І . Гуржій, С. П. Мосов, В. Д. Макаров та ін. – К. : Знання України, 2006. – 355 с.

9. Історія війн та військового мистецтва : навчальний посібник : [В 3 ч.]. – Ч. 3. Локальні війни та збройні конфлікти кінця XX – початку XXI стст. / В. І. Жуков, В. П. Коцюба, В. В. Пугач, І. А Таран. – Харків : ХУПС, 2010. – 134 с.

10. *Толубко В. Б.* Основні закономірності сучасних локальних війн та збройних конфліктів / В. Б. Толубко, Ю. І. Бут, В. О. Косевцов. – К. : НАОУ, 2002. – 68 с.

11. *Плюта В.* Сравнительный многомерный анализ в экономическом моделировании / В. Плюта. – М. : Финансы и статистика, 1989. – 176 с.

12. Development and implementation of the target function in the decision-making process in the system of providing the military security of the state [Електронний ресурс] / V. Kosevtsov, V. Telelim, A. Lobanov, Y. Punda // Eastern-European Journal of Enterprise Technologies. – 2020. – Vol. 5, No 3 (107). – P. 17–23. – Режим доступу : https://doi.org/10.15587/1729-4061.2020.215128.

13. Стратегія воєнної безпеки України [Електронний ресурс] : затверджена Указом Президента України № 121/2021 від 25 березня 2021 р. // Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/121/2021#Text.

14. *Пелих А. О.* Концепції застосування військової сили в системі державної політики національної безпеки США [Електронний ресурс] / А. О. Пелих // Державне управління: теорія та практика. – 2013. – № 2. – С. 62–68. – Режим доступу : http://nbuv.gov.ua/UJRN/Dutp_2013_2_9.

15. Воєнна доктрина України [Електронний ресурс] : затверджена Указом Президента України № 648/2004 від 15 червня 2004 р. // Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/648/2004/ed20040615#Text.

DOI 10.33099/2618-1614-2024-27-4-40-48
УДК 355.4

П. М. Сніцаренко,
доктор технічних наук,
старший науковий співробітник,
Національний університет оборони України

Кібероборона України як складова оборони держави

Питання кібероборони України розглядається з позиції, що це складова оборони держави, а не кібербезпеки. Сьогодні законодавство України з питань оборони розглядає кібероборону обмежено – лише як вид воєнних дій у виконанні Збройних Сил України разом з іншими військовими формуваннями у фазі відбиття збройної агресії, що не вичерпує всіх можливостей захисного (оборонного) потенціалу України в кіберпросторі. При цьому, на відміну від поняття «оборона України», національним законодавством щодо оборони поняття кібероборони України не визначене, безпосередньо питання кібероборони держави не ставиться. Водночас розуміння предмету кібероборони України та його наслідки є концептуально найважливішим та актуальним теоретичним і практичним завданням, яке має бути розв'язане першочергово.
У зв'язку із цим виключно з позиції законодавства України з питань оборони на основі застосування системного підходу і структурно-логічного методу дослідження вперше обґрунтовано сутність кібероборони України як складової оборони держави, окреслено елементи відповідної загальнодержавної системи та взаємозв'язки між ними, намічено основні етапи її реалізації (здійснення).

Ключові слова: оборона, кібероборона, кібероборона як вид воєнних дій, кібероборона України, законодавство України.

Постановка проблеми. Стрімкий розвиток упродовж останніх десятиліть інформаційних технологій та інформаційних систем на їхній основі спричинив утворення потужної складової загального інформаційного простору – простору електронних інформаційних ресурсів (ЕІР), який одержав назву «кіберпростір». Це створило новий вид взаємодії – взаємодії в сигнально-електронному виді. Поряд з іншим, така взаємодія може бути реалізована і з метою шкідливого впливу шляхом кібератаки (або їх сукупності) для нанесення вразливого кіберудару технічним елементам інформаційної інфраструктури суперника (противника) або ментальності його соціального середовища через «присутність» людини в кіберпросторі. Таким чином, виникає ситуація агресії в кіберпросторі, яка, зокрема, може мати воєнний характер.

З метою виконання завдань у кіберпросторі, що мають воєнний характер, сьогодні дедалі активніше діють відповідні підрозділи збройних сил та спецслужб провідних держав світу. Зважаючи на можливість реалізації такими підрозділами різноманітних агресивних дій у кіберпросторі шляхом генерації шкідливих програмних кодів, спеціальних електронних медіапродуктів маніпулятивно-підступного змісту, а також створення різних завад для ЕІР, кіберпростір сьогодні виступає як базова платформа здійснення гібридних воєнних дій. Для України агресія в кіберпросторі проявилася надзвичайно гостро під час російсько-української війни, коли різноманітні кібератаки на елементи інформаційної інфраструктури держави стали повсякденним явищем. Тому очевидною є практична проблема кібероборони України як один з необхідних механізмів протидії гібридним воєнним загрозам через агресії в кіберпросторі. Сьогодні питання кібероборони України є новим розділом знань, що потребує належного теоретичного опрацювання та відповідних наукових досліджень.

Аналіз останніх досліджень і публікацій. Конституція України розмежовує сферу національної безпеки (отже, і кібербезпеку як її складову) та сферу оборони, а сферу оборони України відносить до компетенції Збройних Сил України (ЗСУ). Із цієї причини Законом України «Про оборону України» [1] питання кібероборони зосереджуються у сфері оборони за домінуючої ролі ЗСУ у фазі відбиття збройної агресії проти України. Тому питання кібероборони України, зокрема її теоретичних засад, може розглядатися з позиції, що це складова оборони держави. Водночас у нечисленних публікаціях, де висвітлюється тема кібероборони України, наприклад [2, 3], автори тяжіють до поняття кібероборони як складової кібербезпеки, не критикуючи при цьому відверто невдалі та взаємно суперечливі законодавчі тлумачення сутності кібероборони, що

викликає різні підходи у висвітленні цієї теми, а також у формулюванні положень підзаконних нормативних документів. Тобто питання кібероборони сьогодні, передусім з наукового погляду, є дискусійним, відповідна теорія перебуває в стані формування. Зважаючи на це, у статті автора [4] вперше започатковано розгляд теми кібероборони виключно *з позиції законодавства України з питань оборони*, що на основі застосування системного підходу та структурно-логічного методу дослідження засвідчило таке:

- законодавство України з питань оборони розглядає кібероборону як елемент відсічі (протидії, спротиву) збройній (воєнній) агресії проти України, незалежно від того, як та де така агресія вперше розпочалась – у кіберпросторі чи поза його межами, або одночасно в усіх можливих сферах життєдіяльності держави;
- у сукупності чинних положень законодавства стосовно оборони кібероборона розглядається як одна з функцій ЗСУ (сил оборони) в разі збройної агресії проти України, тобто йдеться не про кібероборону держави загалом, а лише про її складову у виконанні ЗСУ разом з іншими військовими формуваннями у фазі відбиття (відсічі) збройної агресії (ведення кібероборони) – це кібероборона у вузькому розумінні поняття «оборона», що слід розглядати як вид воєнних дій військ (сил).

Зазначене дало підстави сформулювати визначення:

кібероборона (*як вид воєнних дій*) – дії військ (сил), що застосовуються в умовах відбиття (відсічі) збройної агресії проти держави для комплексного кіберзахисту середовища електронних інформаційних ресурсів власних сил оборони, нанесення ураження (шкоди) середовищу електронних інформаційних ресурсів противника, а також прикриття критичних об'єктів інформаційної діяльності держави від ударів засобами традиційної зброї, з метою досягнення інформаційної переваги над противником у кіберпросторі в процесі збройної боротьби.

Це визначення дає підстави окреслити структурно-логічну схему організації виконання завдання кібероборони зусиллями переважно ЗСУ (сил оборони) безпосередньо *в процесі відбиття збройної агресії проти України*. Тобто сьогодні законодавство України з питань оборони, де йдеться про кібероборону (Закон України «Про оборону України» [1], Стратегія воєнної безпеки України [5], Указ Президента України «Про невідкладні заходи з кібероборони держави» [6]), розглядає кібероборону обмежено – лише як вид воєнних дій. Іншими словами, на відміну від поняття «оборона України», законодавством України щодо оборони поняття *кібероборони України* не визначене, безпосередньо *питання кібероборони держави не ставиться*.

Але з точки зору оборони держави кібероборона як вид воєнних дій у виконанні ЗСУ (сил оборони) не вичерпує всіх можливостей захисного (оборонного) потенціалу держави в кіберпросторі, й до того ж такі дії сил оборони не можуть бути реалізовані без використання можливостей держави, що висуває потребу розуміння загальної сутності кібероборони України. Це розуміння та його наслідки концептуально є найважливішим та актуальним теоретичним і практичним завданням, яке має виконуватись у пріоритетному порядку.

У зв'язку із зазначеним **метою статті** є обґрунтування сутності кібероборони України як складової оборони держави та окреслення основних елементів загальнодержавної системи її реалізації.

Викладення основного матеріалу. Для досягнення поставленої мети першочергово підкреслимо, що як і у випадку інформаційної інфраструктури ЗСУ, яка в різноманітті реалізацій мереж комп'ютеризованих об'єктів інформаційної діяльності (ОІД) утворює кіберпростір (середовище EIP) для інформаційного забезпечення процесів управління військами (силами) та зброєю в цифровому (автоматизованому) режимі [4], так і інформаційна інфраструктура держави аналогічно утворює національний кіберпростір, але в більших масштабах, в інтересах забезпечення інформаційних потреб у різних галузях життєдіяльності.

Питання кібероборони України пов'язане з усім кіберпростором держави, але на відміну від кібероборони як виду воєнних дій має розглядатись у широкому розумінні поняття «оборона», визначеному в Законі України «Про оборону України» [1] в редакції:

оборона України – система політичних, економічних, соціальних, воєнних, наукових, науково-технічних, інформаційних, правових, організаційних, інших заходів держави щодо підготовки до збройного захисту та її захист у разі збройної агресії або збройного конфлікту.

Як видно, оборона України – це комплексний процес, який охоплює сукупність різних необхідних заходів усієї держави та передбачає *дві фази – фазу підготовки* до збройного захисту держави та *фазу захисту* в разі збройної агресії або збройного конфлікту. Відповідно, це стосується і кібероборони України як складової частини загального процесу оборони держави.

При цьому неможливо уявити реалізацію кібероборони як виду воєнних дій без першої фази – попередньої підготовки сил і засобів ЗСУ (сил оборони) до рівня необхідних спроможностей. При цьому кібероборона як вид воєнних дій реалізується впродовж другої фази – шляхом умілого застосування набутих спроможностей за призначенням у процесі кібероперацій (кіберакцій) під час відбиття збройної агресії. Важливо зазначити, що всі необхідні умови та інструменти для реалізації обох фаз надає (забезпечує) держава. Отже, в цьому випадку маємо розглядати поєднаний процес в інтересах оборони України. Тому цілком очевидно, що *кібероборона як вид воєнних дій ЗСУ (сил оборони)* –

складова кібероборони України, що потребує цього доповнення до визначення, наведеного в [4].

Щодо інших складових кібероборони України зазначимо таке.

По-перше, згідно із Законом України «Про оборону України» [1] у разі збройної (воєнної) агресії проти України виключне право на ведення воєнних (бойових) дій у кіберпросторі у формі проведення кібероперацій (кіберакцій) надається лише ЗСУ (силам оборони). Це означає, що всі решта суб'єктів в Україні, котрі мають у своєму підпорядкуванні (розпорядженні) ОІД або їхні мережі (середовища ЕІР), такими повноваженнями не наділені. Тому вони в інтересах кібероборони України здійснюють лише доступні їм заходи *комплексного кіберзахисту*, який, поряд із прикриттям силами та засобами ЗСУ критичних ОІД національної інформаційної інфраструктури від механічних (кінетичних) ударів під час кібероборони як виду воєнних дій, як уже зазначалося в [4], також охоплює:

- радіоелектронний захист технічних елементів у складі мереж ОІД (середовищ ЕІР, що утворюють національний кіберпростір);
- захист наявних ЕІР від кібератак противника шляхом його скритного проникнення через комунікаційні мережі (мережевий кіберзахист);
- захист від негативного інформаційно-психологічного впливу, ворожої пропаганди на різні соціальні групи України через широкодоступні кіберпросторові платформи на основі Інтернет.

Пояснюючи ці елементи комплексного кіберзахисту, зазначаємо таке.

Радіоелектронний захист, незалежно від форми власності середовищ ЕІР, в умовах воєнної (збройної) агресії здійснюється відповідно до технічних регламентів застосування режимів роботи технічних елементів у складі мереж ОІД, тобто впроваджених заздалегідь на етапі їх створення, передбачених для умов експлуатації, – забезпечується діями штатного персоналу на таких засобах.

Захист наявних ЕІР на критичних ОІД держави від кібератак противника (мережевий кіберзахист) здійснюється шляхом обов'язкового впровадження стандартизованих для всієї держави інструментів мережевого кіберзахисту в межах запровадження організаційно-технічної моделі кіберзахисту відповідно до постанови Кабінету Міністрів України № 1426 від 29 грудня 2021 р. [7] – забезпечується кожною юридичною особою – утримувачем мережі (мереж) ОІД самостійно.

Захист від негативного інформаційно-психологічного впливу, ворожої пропаганди на різні соціальні групи України, включно з військовою аудиторією, реалізуються в системі загальнодержавних профілактичних заходів (заборона деяких мереж, посилення кібергігієни, медіакомпетентності тощо).

Наведені елементи комплексного кіберзахисту є захисними інструментами неагресивного (невоєнного) характеру, але вони мають принципове значення для будь-якого ОІД у державі на випадок збройної (воєнної) агресії проти України. Як правило, ці заходи плануються та запроваджуються у фазі підготовки кібероборони України і можуть бути застосовані ще в мирний час та продовжуються (посилюються) у фазі захисту держави в разі збройної агресії проти неї.

Отже, *невоєнні інструменти комплексного кіберзахисту*, насамперед критичних ОІД – носіїв ЕІР (критичних об'єктів інформаційної інфраструктури держави) незалежно від їхньої форми власності, поряд з інструментом кібероборони як виду воєнних дій, у своїй сукупності є *іншою складовою кібероборони України*. Це означає, що як у фазі підготовки кібероборони, так і у фазі ведення кібероборони в частині комплексного кіберзахисту залучаються всі суб'єкти – утримувачі критичних ОІД (носіїв ЕІР) держави, тобто відповідні структурні одиниці критичних об'єктів інформаційної інфраструктури сил оборони, всіх органів державної влади, органів місцевого самоврядування, а також визначені юридичні і фізичні особи, віднесені до таких, що провадять важливу для України діяльність, пов'язану з ЕІР та їхнім захистом.

По-друге, якщо уявити, що в державі відсутнє середовище ЕІР (національний кіберпростір), тоді буде відсутня й необхідність використовувати ЕІР за призначенням, а також їх усебічно захищати (ЕІР немає!), отже, відпадає саме питання кібероборони. Але сьогодні ЕІР є стратегічним ресурсом, без якого вже неможливо уявити життєдіяльність будь-якої держави, як і України. Чим більший потенціал ЕІР держави, тим ефективніше реалізуються процеси управління в багатьох сферах, у тому числі у сфері оборони. Лише створення чи вдосконалення різноманітних комп'ютеризованих інформаційних систем і за їхньою допомогою одержання необхідних інформаційних продуктів може забезпечити необхідний та достатній обсяг ЕІР, зокрема в інтересах підвищення інформаційних можливостей сил оборони України. Це дає змогу реалізувати надійне інформаційне забезпечення управління військами та зброєю в цифровому (автоматизованому) режимі в єдиному інформаційному просторі (кіберпросторі воєнної сфери), зокрема за мережоцентричним принципом ведення воєнних (бойових) дій, а також здійснювати різноманітний електронно-інформаційний вплив на противника для реалізації управління його діями на свою користь. Зазначене означає першочергову потребу наявності розвиненого кіберпростору України (національного середовища ЕІР), причому з необхідністю досягнення (забезпечення) можливостей у формуванні та використанні ЕІР на рівні, достатньому для успішного виконання завдань оборони держави. Саме

тому таке середовище ЕІР має створюватися та постійно розвиватися, зокрема в цілях оборони України. При цьому національне середовище ЕІР є водночас об'єктом як забезпечення власних конструктивних дій через кіберпростір, так і об'єктом захисту від негативного впливу. Отже, за фактом, національне середовище ЕІР, поряд з іншим, являє собою інформаційну платформу реалізації через кіберпростір заходів кібероборони держави. Із цієї причини *формування й подальше розширення національного кіберпростору для збільшення обсягу ЕІР у ньому є невід'ємною складовою кібероборони України*, при цьому є також найбільшим завданням у фазі підготовки кібероборони держави, про що в такому контексті, на жаль, зовсім не йдеться у відомих публікаціях.

Зважаючи на окреслені особливості, ґрунтуючись на положеннях національного законодавства з питань оборони, підходимо до розуміння узагальненої сутності кібероборони України в такій редакції:

кібероборона України – це складова оборони держави як сукупність загальнодержавних заходів, спрямованих на розвиток (розширення) національного кіберпростору, підготовку комплексного кіберзахисту критичних ОІД національної інформаційної інфраструктури та набуття спроможностей ЗСУ (сил оборони) для кібероборони як виду воєнних (бойових) дій, а також використання досягнутих сукупних спроможностей в інтересах захисту України в разі здійснення проти неї збройної (воєнної) агресії.

За цими базовими ознаками кібероборона України як невід'ємна складова оборони держави є фактично справою всього українського народу, що потребує єдиної політики організації та координації на загальнодержавному рівні. Отже, має діяти відповідна система. Допускаючи, як уже зазначено тут, а також у [4], що положення законодавства України з питань оборони, які потребують зміни в інтересах кібероборони, встановленим порядком доповнені, то йтиметься про *перспективну систему кібероборони держави*.

Окреслити обриси цієї системи означає вказати її суб'єктів, сформулювати їхні рольові завдання та означити взаємозв'язки між ними. Кібероборона України, як зазначено, є загальнодержавною справою, тому система, яка її впроваджує в практику, має поширюватися на широке коло інституцій, які, відповідно, стають суб'єктами системи кібероборони держави.

У роботі [4] кібероборона була розглянута як вид воєнних дій, що є складовою кібероборони України, на підставі чого визначені її основні суб'єкти у фазі відсічі збройній агресії проти України: Головнокомандувач ЗСУ, підпорядковані йому Генеральний штаб ЗСУ, загалом Збройні Сили України (сили оборони), а також розвідувальний орган Міністерства оборони України; показані їхня рольова місія та взаємозалежність у процесі спільних дій. Тому вони є серед основних суб'єктів системи кібероборони України, а їхні місії у фазі підготовки кібероборони України будуть розкриті нижче. Стосовно інших задіяних у цій загальнодержавній системі основних суб'єктів зазначаємо таке.

Верховна Рада України здійснює законодавче регулювання питань кібероборони України.

Президент України здійснює загальне керівництво кібероборoною держави з організацією координації шляхом видання указів і розпоряджень, а як *Верховний Головнокомандувач ЗСУ* – наказів та директив з питань оборони. Основою для керівництва кібероборoною держави є затверджений Президентом України План кібероборони України як складова Плану оборони України.

Рада національної безпеки і оборони України (РНБОУ) здійснює координацію діяльності щодо кіберборони держави відповідно до закону, указів та розпоряджень Президента України. Слід зазначити, що законодавством України не розкривається сутність цього процесу, тому на підставі положень низки нормативно-правових актів це буде пояснено згодом.

Міністерство оборони України (МОУ) – відповідно до Закону України «Про національну безпеку України» [8] до його повноважень належить, поряд з іншим, здійснення в установленому порядку координації діяльності державних органів та органів місцевого самоврядування щодо *підготовки держави до кібероборони* як однієї зі складових оборони держави. При цьому, згідно з Положенням про МОУ [9], воно «взаємодіє з іншими державними органами, допоміжними органами і службами, утвореними Президентом України, та тимчасовими консультативними, дорадчими та іншими допоміжними органами, утвореними Кабінетом Міністрів України, органами місцевого самоврядування, об'єднаннями громадян, громадськими спілками, профспілками та організаціями роботодавців, відповідними органами іноземних держав і міжнародних організацій, а також підприємствами, установами і організаціями». Отже, на перший погляд, виникає ефект дублювання з РНБОУ, що небажано.

У зв'язку із цим звернімося за уточненням до пункту 8 цього Положення, де визначено: «...накази Міноборони, видані в межах повноважень, передбачених законом, є обов'язковими для виконання центральними органами виконавчої влади, їхніми територіальними органами, місцевими держадміністраціями, органами влади Автономної Республіки Крим, органами місцевого самоврядування, підприємствами, установами і організаціями незалежно від форми власності і громадянами». Тобто МОУ має повноваження координувати та взаємодіяти лише в межах переліку цих суб'єктів, причому виключно з питань підготовки оборони держави, отже, поряд з іншим, і з *підготовки*

кібероборони. Це обмежений рівень повноважень, оскільки до цього переліку не входять окремі суб'єкти сектору безпеки та оборони України, які підпорядковані Президенту України та мають залучатися до процесів кібероборони відповідно до законодавства.

Зважаючи на вказане, повертаючись до координаційної ролі РНБОУ, логічно вважати, що на основі її рішень, затверджених указом Президента України, в питаннях підготовки кібероборони вона безпосередньо координує як МОУ, так і державні органи, підпорядковані Президенту України, у тому числі шляхом надання доручень Голови РНБОУ її членам для забезпечення взаємодії та гармонійної інтеграції зусиль щодо кібероборони, та встановленим порядком здійснює контроль виконання обраних заходів.

Крім цього додамо: потреба проведення загальнодержавних профілактичних заходів, які протидіють негативному інформаційно-психологічному впливу, ворожій пропаганді через кіберпростір на різні соціальні групи України та є складовими комплексного кіберзахисту в процесі кібероборони України, зумовлює необхідність як у першій фазі (підготовки кібероборони), так і у фазі другій (ведення кібероборони) реалізації єдиної державної політики та належної координації за цим напрямом діяльності. Загальнодержавна значущість проведення в життя такої політики вимагає координації зусиль на найвищому рівні. Із цієї причини цю координацію в обох фазах кібероборони також має здійснювати РНБОУ відповідно до її повноважень.

У зв'язку із зазначеним МОУ, за координаційної ролі з боку РНБОУ, маючи повноваження, визначені законодавством, шляхом відповідних наказів міністерства та безпосередньої взаємодії координує діяльність державних органів (крім підпорядкованих Президентові України) та органів місцевого самоврядування щодо підготовки держави до кібероборони. У цій діяльності основні зусилля МОУ мають зосереджуватися на:

- формуванні та розвитку національного кіберпростору України шляхом удосконалення інформаційної інфраструктури держави в інтересах формування дружнього середовища ЕІР для потреб оборони;
- створенні умов забезпечення комплексного кіберзахисту середовища ЕІР критичних ОІД інформаційної інфраструктури України;
- упровадженні та реалізації в державі заходів захисту соціальної свідомості суспільства, насамперед особового складу сил оборони, від негативного інформаційно-психологічного впливу в кіберпросторі зі змістом, спрямованим на підрив суверенітету, територіальної цілісності й недоторканності України.

Поза цим, відповідно до Закону України «Про національну безпеку України» [8], у підпорядкуванні МОУ перебувають ЗСУ, якими Міністр оборони України здійснює військово-політичне та адміністративне керівництво (безпосередньо або через своїх заступників та Головнокомандувача ЗСУ). Тому МОУ, забезпечуючи всебічно життєдіяльність ЗСУ згідно з потребами, визначеними Генеральним штабом ЗСУ [10], шляхом видання наказів і директив та безпосередньо також координує і спрямовує діяльність ЗСУ, інших складових сил оборони щодо підготовки кібероборони за напрямами:

- формування та розвитку кіберпростору воєнної сфери шляхом удосконалення цифрової інформаційної інфраструктури сил оборони як основи інтегрованого інформаційного середовища ЕІР для задоволення інформаційних потреб військових споживачів та забезпечення оперативної електронної комунікації;
- створення умов забезпечення комплексного кіберзахисту середовища ЕІР критичних ОІД інформаційної інфраструктури сил оборони;
- забезпечення формування і підготовки спроможностей сил та засобів ЗСУ, інших складових сил оборони для кібероборони як виду воєнних дій у разі відбиття збройної (воєнної) агресії проти України.

Маючи повноваження з питань оборони держави, МОУ з метою організації кібероборони держави та запровадження механізму координації у фазі підготовки кібероборони розробляє структуру і порядок розроблення Плану кібероборони України (як частини Плану оборони України) та організовує розроблення його складових. У Плані кібероборони України мають бути складові, які відображають рольові функції всіх суб'єктів системи кібероборони держави, за типом тих їхніх функцій, які вже були означені вище.

Після затвердження Президентом України Плану кібероборони України як частини Плану оборони України МОУ здійснює координацію передбачених заходів підготовки кібероборони.

Генеральний штаб ЗСУ в питаннях підготовки кібероборони діє під координацією МОУ. Для цього Генеральний штаб ЗСУ:

- розробляє пропозиції до Плану кібероборони України (як частини Плану оборони України);
- визначає вимоги щодо ЕІР ЗСУ, інших складових сил оборони, а також відомчих ЕІР для потреб оборони держави, а спільно з *Державною службою спеціального зв'язку та захисту інформації України* (ДССЗЗІУ) – щодо забезпечення комплексного кіберзахисту середовища ЕІР критичних ОІД інформаційної інфраструктури України, у тому числі інформаційної інфраструктури сил оборони;
- здійснює планування кібероборони з питань удосконалення інформаційної інфраструктури ЗСУ та інших складових сил оборони як основи інтегрованого інформаційного середовища ЕІР (кіберпростору воєнної сфери) для задоволення інформаційних потреб

військових споживачів ЕІР, здійснення оперативної електронної комунікації;

• здійснює планування заходів забезпечення комплексного кіберзахисту середовища ЕІР критичних ОІД інформаційної інфраструктури сил оборони;

• організовує та здійснює заходи щодо формування і підготовки спроможностей сил та засобів ЗСУ та інших складових сил оборони для кібероборони як виду воєнних дій у разі відбиття збройної (воєнної) агресії проти України;

• організовує взаємодію та здійснює контроль складових сил оборони щодо набуття ними необхідних об'єднаних спроможностей з питань кібероборони.

Збройні Сили України (сили оборони) з питань підготовки кібероборони координуються МОУ (через Генеральний штаб ЗСУ) та здійснюють заходи щодо набуття ними необхідних об'єднаних спроможностей з питань кібероборони як виду воєнних (бойових) дій.

Слід зауважити, що в мирний час ЗСУ (сили оборони) можуть використовувати набуті в процесі підготовки кібероборони спроможності, зокрема кібервійськ (мають бути у складі ЗСУ [4]), в інтересах моніторингу кіберпростору (розвідувальної діяльності) та кіберзахисту власних ЕІР.

Головні рольові функції Генерального штабу ЗСУ, а також ЗСУ з питань ведення кібероборони в умовах воєнного часу та відбиття збройної агресії проти України окреслені в роботі [4] під час розгляду кібероборони як виду воєнних дій.

Крім зазначених, суб'єктами системи кібероборони України є також *інші державні органи, органи місцевого самоврядування, підприємства, установи та організації, віднесені до критичних об'єктів інфраструктури, а також суб'єкти господарювання, громадяни України та об'єднання громадян, особи, які провадять діяльність та/або надають послуги, пов'язані з національними ЕІР, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями та кіберзахистом* незалежно від їхньої форми власності, які діють в інтересах кібероборони.

Основні завдання інших суб'єктів системи кібероборони України з питань підготовки кібероборони полягають у вдосконаленні їхнього власного цифрового комунікативного середовища (середовища ЕІР – власного кіберпростору), в тому числі в інтересах оборони держави, та проведенні заходів щодо забезпечення його комплексного кіберзахисту. Координація їхньої діяльності та взаємодія у фазі підготовки кібероборони проводиться відповідно до наказів МОУ, за винятком суб'єктів, підпорядкованих Президентові України, які мають залучатися до процесів кібероборони держави (такі суб'єкти координуються на основі рішень РНБОУ або через доручення Голови РНБОУ її членам).

Слід окремо зауважити, що серед суб'єктів системи кібероборони України в питанні підготовки кібероборони держави особливі місце та роль належать ДССЗЗІУ, котра згідно із Законом [11] здійснює формування та реалізацію державної політики, зокрема щодо захисту державних ЕІР та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту критичних об'єктів інформаційної інфраструктури тощо. Із цією метою ДССЗЗІУ забезпечує впровадження організаційно-технічної моделі кіберзахисту (у наведеному вище розумінні мережевого кіберзахисту). Положення про таку модель затверджене урядовою постановою [7], де викладені загальні рекомендації щодо організації кіберзахисту об'єктів інформаційної діяльності на національному, галузевому (регіональному, місцевому) та об'єктовому (підприємства, установи, організації) рівнях. При цьому відповідно до концепції моделі заходи кіберзахисту на кожному рівні покладаються на спеціалізовані органи (підрозділи, команди) – сили кіберзахисту. У цих заходах сили кіберзахисту мають застосовувати засоби кіберзахисту, перелічені в Положенні в сенсі їхнього функціонального призначення, зокрема:

• системи виявлення вразливостей та реагування на кіберінциденти і кібератаки;

• інформаційні технології, технічні і програмні засоби (пристрої, обладнання, комплекси), які використовуються в інтересах забезпечення кіберзахисту національних ЕІР, комунікаційних і технологічних систем, а також критичних об'єктів інформаційної інфраструктури.

Як рекомендація загального характеру цей перелік засобів кіберзахисту не викликає сумніву. Але реалізація цього положення без додаткових пояснень неодмінно призводить до різноманітних підходів до практики кіберзахисту ЕІР конкретних ОІД («на місцях»), причому на кожному із зазначених рівнів, та, відповідно, нерівномірності в ефективності кіберзахисту ЕІР різних ОІД. Такий наслідок є небажаним, зокрема з погляду кібероборони України. Із цієї причини в інтересах рівної міцності кібероборони доцільно стандартизувати набори засобів кіберзахисту для кожного рівня організаційно-технічної моделі кіберзахисту.

Ініціатива щодо розроблення таких стандартів і методичних рекомендацій щодо їх впровадження, на наш погляд, має належати ДССЗЗІУ, що стало б чи не найголовнішим елементом реалізації всієї організаційно-технічної моделі кіберзахисту та спростило б завдання кіберзахисту ЕІР усіх суб'єктів системи кібероборони України.

Координацію щодо впровадження цих стандартів в інтересах кібероборони України відповідно до компетенції мають здійснювати РНБОУ та МОУ.

В умовах воєнного часу та відбиття збройної агресії проти України *суб'єкти системи кібероборони України* в процесі реалізації заходів кібероборони як виду воєнних (бойових) дій координуються Генеральним штабом ЗСУ – робочим органом Ставки Верховного Головнокомандувача, згідно з наказами і директивами Верховного Головнокомандувача ЗСУ з питань оборони та діють відповідно до компетенції та набутих спроможностей.

Кабінет Міністрів України в обох фазах оборони держави забезпечує здійснення державної політики щодо кібероборони України у спосіб організації та забезпечення необхідними силами, засобами і ресурсами заходи кібероборони шляхом:

- формування, розміщення, фінансування та виконання відповідного державного оборонного замовлення на поставку (закупівлю) продукції, виконання робіт, надання послуг для потреб ЗСУ та інших складових сил оборони, а також програм (планів) з питань кібероборони інших державних суб'єктів системи кібероборони України в межах коштів, виділених на фінансування цих заходів у затвердженому Верховною Радою України Державному бюджеті України;
- створення сприятливих умов для впровадження заходів комплексного кіберзахисту власного середовища ЕІР суб'єктами системи кібероборони України недержавної форми власності, які провадять діяльність та/або надають послуги, пов'язані з національними ЕІР, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями та кіберзахистом.

Наведений вище перелік суб'єктів системи кібероборони України, з'ясування їхнього функціонального призначення у фазах підготовки кібероборони та ведення кібероборони, виходячи з положень чинного законодавства держави з питань оборони, уточнення взаємозв'язків між ними та особливостей координації в цій системі дає змогу зобразити перспективний варіант її структурно-логічної схеми, як представлено на *рисунку 1*, що відображає сутність концептуальної архітектури системи кібероборони України (її перспективний структурний обрис).

З урахуванням викладеного стає можливим пропонувати перелік основних етапів створення перспективної системи кібероборони України відповідно до положень національного законодавства з питань оборони.

Етап 1. *Сформувати належну правову основу організації кібероборони України шляхом внесення необхідних змін до національного законодавства з питань оборони*, виходячи при цьому з понять кібероборони як у широкому, так і у вузькому розумінні процесу оборони, а також того, що кібероборона передбачає наявність двох фаз – підготовка кібероборони та ведення кібероборони, до яких залучається широкий перелік суб'єктів держави відповідно до їхньої компетенції, котрі при цьому утворюють систему кібероборони України.

Деталізація шляхів організації кібероборони держави може бути зосереджена в окремій Стратегії кібероборони України, але після попереднього внесення необхідних змін щодо кібероборони до Законів України «Про оборону України», «Про розвідку», «Про Збройні Сили України» та до Стратегії національної безпеки України і Стратегії воєнної безпеки України.

Етап 2. *Створити у ЗСУ кібервійська* з повноваженнями протиборства в кіберпросторі шляхом розвідки в кіберпросторі, кіберзахисту ЕІР на ОІД ЗСУ (сил оборони), нанесення поразки агресору в кіберпросторі або через кіберпростір у разі збройної (воєнної) агресії проти України, забезпечивши створені війська належними фінансовими, кадровими і технічними ресурсами.

Етап 3. *Створити в Україні єдину мережу галузевих, регіональних, місцевих ситуаційних центрів з питань кіберзахисту*, здатну забезпечити оперативне реагування на кіберзагрози на рівні, що відповідає потребам кібероборони держави.

Етап 4. *Уточнити План кібероборони України* як керівництво щодо підготовки кібероборони держави та її здійснення в разі воєнної (збройної) агресії проти України, зокрема з такими складовими:

- розвиток національного середовища ЕІР (розширення національного кіберпростору України), зокрема в інтересах активного функціонування єдиного цифрового інформаційного середовища сил оборони;
- когнітивна безпека України в кіберпросторі (безпека соціальної свідомості суспільства під час використання кіберпростору);
- комплексний кіберзахист у національному кіберпросторі України (захист критичних ОІД держави від традиційної зброї, впровадження організаційно-технічної моделі кіберзахисту на основі стандартизованих процедур);
- набуття спроможностей і кібероперації (кібердії) ЗСУ та інших складових сил оборони, у тому числі дії кібервійськ у кіберпросторі (мережевий кіберзахист ЕІР, мережеві акції, радіоелектронна боротьба);
- ресурсне забезпечення системи кібероборони України (кадрове, матеріально-технічне, фінансове);
- механізми керівництва, координації та контролю в системі кібероборони України.

Етап 5. *Забезпечити реалізацію заходів уточненого Плану кібероборони України* в перспективній системі кібероборони України.

Цими етапами означено, на наш погляд, найбільш принципові особливості в системному розумінні шля-

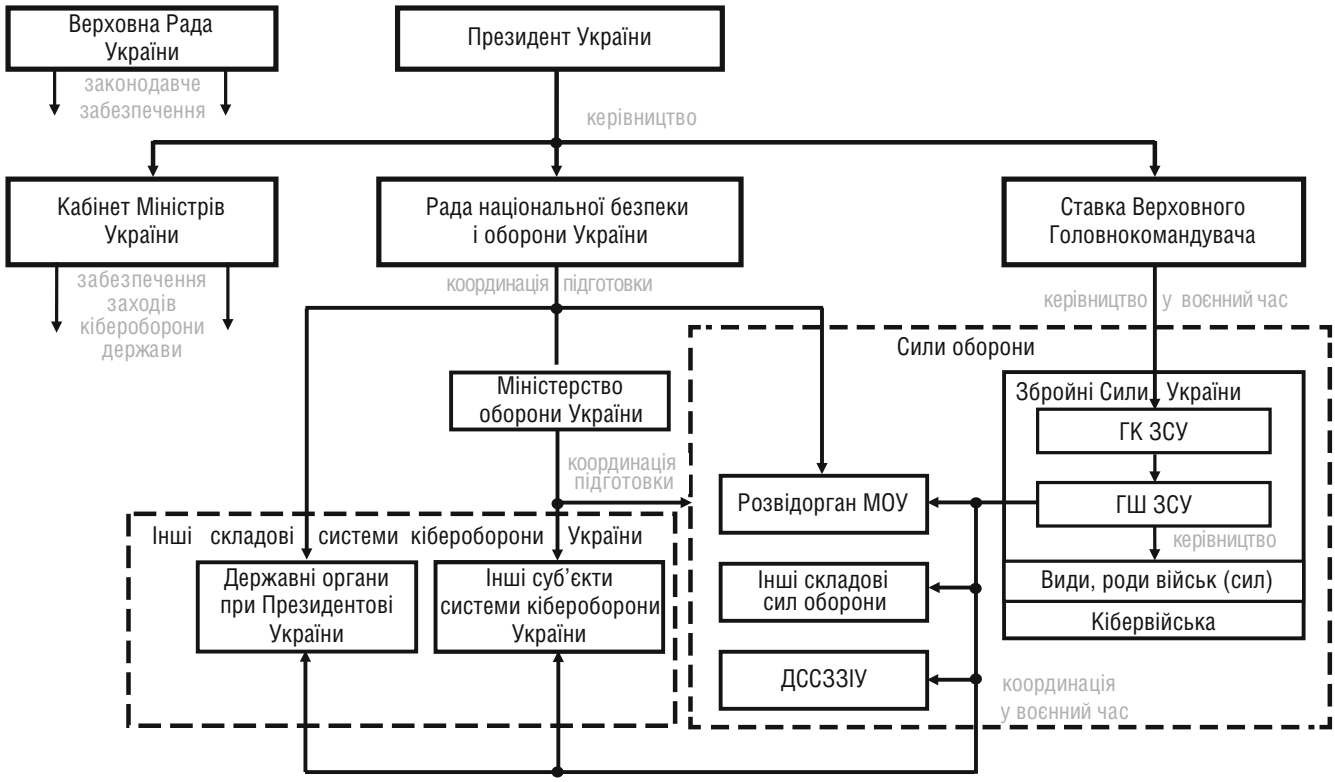

Рис. 1. Структурно-функціональна схема перспективної системи кібероборони України

хів практичної реалізації наміченого обрису перспективної системи кібероборони України, що слід вважати головними орієнтирами розвитку цієї системи.

Висновки

1. Оскільки Конституція України розмежовує сферу національної безпеки (включно зі складовою кібербезпеки) і сферу оборони, а сферу оборони України відносить до компетенції ЗСУ, то питання кібероборони України може розглядатися з позиції, що це складова оборони держави, а не кібербезпеки. Водночас сьогодні законодавство України з питань оборони розглядає кібероборону обмежено – лише як вид воєнних дій у виконанні ЗСУ разом з іншими військовими формуваннями у фазі відбиття збройної агресії. При цьому, на відміну від поняття «оборона України», законодавством України щодо оборони поняття кібероборони України не визначене, безпосередньо питання кібероборони держави не ставиться.

2. З погляду оборони держави кібероборона як вид воєнних дій у виконанні ЗСУ (сил оборони) не вичерпує всіх можливостей захисного (оборонного) потенціалу України в кіберпросторі і, до того ж, такі дії сил оборони не можуть бути реалізовані без використання можливостей держави, що зумовлює потребу розуміння загальної сутності кібероборони України. Це розуміння та його наслідки концептуально є найважливішим та актуальним теоретичним і практичним завданням, яке має бути розв'язане в пріоритетному порядку. У зв'язку із цим, виключно з позиції законодавства України з питань оборони на основі застосування системного підходу і структурно-логічного методу дослідження вперше обгрунтовано сутність кібероборони України як складової оборони держави, окреслено складові відповідної загальнодержавної системи та взаємозв'язки між ними, намічено основні етапи її реалізації.

Подальші дослідження можуть бути зосереджені на формуванні та розвитку теоретичних засад кібероборони України як складової оборони держави, виходячи з її сутності та особливостей реалізації, а також на обґрунтуванні пропозицій щодо вдосконалення національного законодавства з питань оборони в частині положень про кібероборону держави.

Перелік літератури

1. Про оборону України [Електронний ресурс] : Закон України № 1932-XII від 6 грудня 1991 р. // Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/1932-12#Text.

2. *Даник Ю. Г.* Основи кібербезпеки та кібероборони : підручник / Ю. Г. Даник, П. П. Воробієнко, В. М. Чернега. – Вид. 2-ге. – Одеса : ОНАЗ ім. О. С. Попова, 2019. – 320 с.

3. *Савченко В. А.* Забезпечення стійкості кібероборони держави в умовах збройного конфлікту [Електронний ресурс] / В. А. Савченко // Сучасний захист інформації. – 2023. – № 3 (55). – С. 6–11. – Режим доступу : https://doi.org/10.31673/2409-7292.2023.030001.

4. *Сніцаренко П. М.* Про сутність кібероборони як виду воєнних дій [Електронний ресурс] / П. М.Сніцаренко // Наука і оборона. – 2024. – № 3. – С. 45–54. – Режим доступу : https://doi.org/10.33099/2618-1614-2024-26-3-45-54.

5. Стратегія воєнної безпеки України [Електронний ресурс] : затверджена Указом Президента України № 121/2021 від 25 березня 2021 р. // Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/121/2021#Text.

6. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про невідкладні заходи з кібероборони держави» [Електронний ресурс] : Указ Президента України № 446/2021 від 26 серпня 2021 р. // Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/446/2021#n5.

7. Положення про організаційно-технічну модель кіберзахисту [Електронний ресурс] : затверджене постановою Кабінету Міністрів України № 1426 від 29 грудня 2021 р. // Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/1426-2021-п#Text.

8. Про національну безпеку України [Електронний ресурс] : Закон України № 2469-VIII від 21 червня 2018 р. // Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/2469-19#Text.

9. Положення про Міністерство оборони України [Електронний ресурс] : затверджене постановою Кабінету Міністрів України № 671 від 26 листопада 2014 р. (у редакції постанови Кабінету Міністрів України № 730 від 19 жовтня 2016 р.) // Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/671-2014-п#Text.

10. Положення про Генеральний штаб Збройних Сил України [Електронний ресурс] : затверджене Указом Президента України № 23/2019 від 30 січня 2019 р. // Верховна Рада України. Законодавство України. – Режим доступу :

DOI 10.33099/2618-1614-2024-27-4-49-53
УДК 629.7.015.4:533.6.011.3

О. В. Сафронов,
доктор технічних наук, професор,
Національний університет оборони України,
Б. Й. Семон,
доктор технічних наук, професор,
Національний університет оборони України,
О. М. Неділько,
кандидат технічних наук, доцент,
Національний університет оборони України

Математична модель оцінювання розташування стрибків ущільнення на поверхні аеродинамічного профілю

У статті на базі аналізу закономірностей адіабатичного розширення місцевого надзвукового потоку повітря на поверхні аеродинамічного профілю в навколозвуковому діапазоні чисел М польоту представлені результати дослідження залежності розташування стрибків ущільнення від геометричних характеристик профілю, числа М незбудженого потоку повітря та від критичного числа М аеродинамічного профілю. Адекватність одержаних результатів підтверджується шляхом порівняння результатів оцінювання розташування стрибків ущільнення на поверхні аеродинамічного профілю, одержаних за допомогою розрахунків, з результатами, одержаними в експериментальних дослідженнях.

Ключові слова: авіаційна техніка, літак, адіабатичне розширення, аеродинамічна поверхня, математична модель, місцевий надзвуковий потік, число М польоту, критичне число М аеродинамічного профілю, розташування стрибків ущільнення

Постановка проблеми. Оцінювання характеристик аеродинамічних поверхонь надзвукових літаків у трансзвуковому потоці повітря теоретичними методами залишається актуальною науковою та прикладною проблемою, яку необхідно розв'язувати під час досліджень аеропружних характеристик.

Одним з етапів створення нових зразків літаків є етап досліджень з використанням теоретичних методів, які дають змогу визначити оптимальні напрями поліпшення характеристик літаків, прогнозувати зміну характеристик у різноманітних умовах експлуатації літаків, зокрема в умовах, реалізація яких у натурному експерименті небезпечна або неможлива.

Аналіз основних досліджень і публікацій. Автори статті в наукових роботах за даною проблемою відзначають низку публікацій, які базуються як на результатах лабораторних досліджень, так і на результатах теоретичних досліджень [1–9]. Для обґрунтування сутності проблеми та аналізу одержаних результатів попередніми дослідниками, а також єдності змісту статті наведемо основні з них.

У роботі [1] запропонований теоретичний метод оцінювання максимального числа M місцевого надзвукового потоку на поверхні аеродинамічного профілю NACA 64A010, але порівняння одержаного результату з результатами лабораторних досліджень не наведене.

У роботі [2] запропонований чисельний метод оцінювання розташування стрибків ущільнення на поверхні аеродинамічного профілю, але порівняння одержаного результату з результатами лабораторних досліджень також не наведене.

У роботах [3–5] наведені результати продувок моделей крила з поверхнею керування в аеродинамічних трубах у трансзвуковому діапазоні чисел M. Результати цих досліджень можуть бути використані для обґрунтування можливості оцінювання деяких характеристик аеродинамічних поверхонь за допомогою наближених теоретичних методів.

Труднощі розв'язання проблеми зумовлені необхідністю врахування впливу стисненості повітря на зміну характеристик аеродинамічних профілів надзвукових літаків у трансзвуковому діапазоні швидкостей польоту. У деяких працях вплив стисненості повітря на зміну характеристик аеродинамічних профілів здійснюється за допомогою різноманітних поправок.

Додаткові труднощі під час оцінювання характеристик аеродинамічних поверхонь надзвукових літаків на трансзвукових числах M польоту теоретичними методами виникають у разі формування стрибків ущільнення на поверхні аеродинамічного профілю, вплив яких на зміну характеристик аеродинамічних поверхонь поправками не може бути визначений.

Із цього приводу в роботі [5] відмічено, що «теорія переміщення стрибків ущільнення по поверхні профілю досі не розроблена».

Слід також додати, що в роботі [6] відмічено, що в діапазоні чисел $M = 0{,}95–1{,}1$ чисельні методи рішення втрачають стійкість, тому до результатів досліджень, одержаних цими методами, слід ставитися з обережністю.

Мета статті. У даній статті оцінювання залежності розташування стрибків ущільнення за хордою профілю аеродинамічної поверхні від геометричних характеристик профілю, від числа M незбудженого потоку повітря та від критичного числа M аеродинамічного профілю визначається на базі аналізу закономірностей адіабатичного розширення місцевого надзвукового потоку на поверхні аеродинамічного профілю літаків на трансзвукових швидкостях польоту.

Виклад основного матеріалу

У статтях [7, 8] автори запропонували математичну модель оцінювання залежності розташування стрибків ущільнення за хордою профілю аеродинамічної поверхні від його геометричних характеристик та від числа M незбудженого потоку повітря.

Для визначення залежності розташування стрибків ущільнення від геометричних характеристик профілю, числа M незбудженого потоку повітря та від критичного числа M аеродинамічного профілю наведемо основні положення та залежності запропонованої моделі.

Математична модель адіабатичного розширення місцевого надзвукового потоку на поверхні аеродинамічного профілю визначена рівнянням [7, 8]:

$$M_1 - 1 \approx 2\left(M_\infty - M_{кр}\right), \qquad (1)$$

де M_1 – число M місцевого надзвукового потоку на поверхні аеродинамічного профілю;

M_∞ – число M незбудженого потоку повітря;

$M_{кр}$ – критичне число M аеродинамічного профілю.

Число M місцевого надзвукового потоку на поверхні аеродинамічного профілю в рівнянні (1) визначається залежністю, запропонованою в роботі [7]:

$$M_1 \approx \sqrt[3]{1 + 11{,}5\varphi(x)}, \qquad (2)$$

де $\varphi(x)$ – кут відхилення надзвукового потоку в дифузорній частині аеродинамічного профілю.

Для кількісного оцінювання залежності розташування стрибків ущільнення за хордою профілю аеродинамічної поверхні в рівнянні (2) нагадаємо, що, згідно з даними роботи [5], для типових аеродинамічних симетричних профілів зміну кута нахилу дотичної до поверхні дифузорної частини профілю можна подати наближеною лінійною залежністю

$$\varphi(x) \approx \varphi_0 \frac{x}{b - b_\tau}, \qquad (3)$$

де φ_0 – максимальний кут нахилу дотичної до поверхні дифузорної частини профілю або максимальний кут відхилення місцевого надзвукового потоку в дифузорній частині аеродинамічного профілю;

x – відстань перетину дифузорної частини хорди аеродинамічного профілю від перетину максимальної товщини профілю;

b – хорда профілю;

b_τ – відстань перетину максимальної товщини профілю від його носка.

Згідно з тією самою роботою [5], для наближених інженерних оцінок характеристик аеродинамічних профілів можна прийняти

$$\varphi_o \approx 0{,}85\bar{\tau}\ . \qquad (4)$$

З урахуванням залежностей (3) і (4) залежність (2) можна подати таким чином:

$$M_1 \approx \sqrt[3]{1 + 9{,}8\frac{x\bar{\tau}}{b - b_\tau}}\ . \qquad (5)$$

Критичне число M у залежності (1) для тонких аеродинамічних профілів, розташованих у потоці повітря під нульовим кутом атаки, можна приблизно визначити на підставі результатів лабораторних досліджень [3, 5] або з рівняння, запропонованого в роботі [9],

$$M_{кр} \approx 1 - 0{,}7\sqrt{\bar{\tau}}\ , \qquad (6)$$

де $\bar{\tau}$ – відносна товщина аеродинамічного профілю, тобто відношення максимальної товщини профілю до його хорди.

За визначеної величини критичного числа M аеродинамічного профілю з рівняння (6) та числа M місцевого надзвукового потоку на поверхні аеродинамічного профілю з рівняння (5) число M незбудженого потоку повітря визначається з рівняння (1).

Рівняння (1) визначає зв'язок числа M місцевого надзвукового потоку на поверхні аеродинамічного профілю, числа M незбудженого потоку повітря та критичного числа M аеродинамічного профілю. Тобто рівняння (1) визначає закономірності адіабатичного розширення місцевого надзвукового потоку повітря на поверхні аеродинамічного профілю в діапазоні чисел M незбудженого потоку повітря від числа $M_\infty = M_{кр}$ до числа $M_\infty = 1{,}0$.

Саме рівняння (1) визначає умови формування стрибків ущільнення на поверхні аеродинамічного профілю або умови перетворення місцевого надзвукового потоку повітря на поверхні аеродинамічного профілю в дозвуковий потік.

Відмічені закономірності адіабатичного розширення місцевого надзвукового потоку на поверхні аеродинамічного профілю дають змогу кількісно оцінити характер розташування стрибків ущільнення на поверхні аеродинамічного профілю залежно від числа M незбудженого трансзвукового потоку повітря, критичного числа M аеродинамічного профілю та геометричних характеристик аеродинамічного профілю.

Можливість оцінювання характеру розташування стрибків ущільнення на поверхні аеродинамічного профілю наближеними теоретичними методами розглянемо на прикладі оцінювання розташування стрибків ущільнення за хордою профілю аеродинамічної поверхні типових симетричних аеродинамічних профілів, для яких зміну кута нахилу дотичної до поверхні дифузорної частини профілю можна представити залежністю (3).

Оскільки рівняння (1) визначає умови формування стрибків ущільнення на поверхні аеродинамічного профілю, то, підставляючи залежність (5) у рівняння (1), після перетворення одержимо

$$x_c \approx \frac{\mathrm{b} - \mathrm{b}_\tau}{9{,}8\bar{\tau}} \left\{ \left[2\left(M_\infty - M_{кр}\right) + 1 \right]^3 - 1 \right\}, \qquad (7)$$

де x_c – відстань перетину розташування стрибків ущільнення за хордою профілю від перетину максимальної товщини аеродинамічного профілю.

Наближене рівняння (7) являє собою математичну модель оцінювання залежності розташування стрибків ущільнення за хордою аеродинамічного профілю від його геометричних характеристик, числа M незбудженого потоку повітря та критичного числа M аеродинамічного профілю в діапазоні чисел M від числа $M_\infty = M_{кр}$ до числа $M_\infty = 1{,}0$.

Можливість використання запропонованої математичної моделі попередньо доведено в роботі [8] порівнянням результатів, одержаних за допомогою моделі, і результатів, одержаних у лабораторних дослідженнях.

У цій статті оцінимо можливість використання вказаної моделі для інших експериментальних даних.

Але спочатку визначимо можливість оцінювання критичного числа M аеродинамічного профілю за допомогою рівняння (6) для оцінювання залежності розташування стрибків ущільнення за хордою аеродинамічного профілю згідно з математичною моделлю (7).

Із цією метою скористаймося даними роботи [5], у якій за результатами продувок моделі крила в аеродинамічній трубі в діапазоні трансзвукових чисел M незбуреного потоку повітря наведені залежності критичних чисел M аеродинамічного профілю від кута відхилення аеродинамічної поверхні керування.

Характеристики аеродинамічного профілю моделі крила:

- профіль моделі крила – симетричний профіль NACA 00009-0,55-40;
- відносна товщина профілю $\bar{\tau} = 0{,}096$;
- критичне число M профілю $M_{кр} = 0{,}783$;
- відносна відстань перетину максимальної товщини профілю від його носка $\frac{b_\tau}{b} = 0{,}4$;
- відносна хорда аеродинамічної поверхні керування $\frac{b_k}{b} = 0{,}2$.

Зауважмо, що при відхиленні аеродинамічної поверхні керування відносна товщина аеродинамічного профілю умовно збільшується на величину, яка дорівнює

$$\Delta\bar{\tau} = 2\bar{\mathrm{b}}_\tau \bar{b}_k \delta_k, \qquad (8)$$

де $\bar{b}_\tau$ – відносна відстань перетину максимальної товщини профілю від його носка;

$\bar{b}_\mathrm{k}$ – відносна хорда аеродинамічної поверхні керування;

δ_k – кут відхилення аеродинамічної поверхні керування.

Тобто при відхиленні аеродинамічної поверхні керування критичне число M аеродинамічного профілю, як можна бачити з рівняння (6) і залежності (8), зменшується згідно з рівнянням

$$M_{кр} \approx 1 - 0{,}7\sqrt{\bar{\tau} + 2\bar{\mathrm{b}}_\tau \bar{b}_k \delta_k}, \qquad (9)$$

Згідно з рівнянням (9) визначимо критичне число M аеродинамічного профілю залежно від кута відхилення аеродинамічної поверхні керування.

Результати цих розрахунків і результати експериментальних досліджень, наведені в роботі [5], представлені в *таблиці 1*.

Таблиця 1

	0°	2°	4°	8°
$M_{кр}$ – експеримент	0,783	0,775	0,770	0,758
$M_{кр}$ – розрахунок	0,783	0,7769	0,7708	0,759
Похибка, %	0	0,245	0,104	0,13

З *таблиці 1* бачимо, що результати розрахунків величин критичних чисел M аеродинамічного профілю залежно від кута відхилення аеродинамічної поверхні керування практично не відрізняються від результатів, одержаних в експериментальних дослідженнях.

Тобто визначення критичних чисел M згідно з рівняннями (6) та (9) можна використовувати під час оцінювання розташування стрибків ущільнення за хордою аеродинамічного профілю.

З порівняння цих результатів випливає, що величина критичного числа M аеродинамічного профілю залежить лише від відносної товщини аеродинамічного профілю, в тому числі й відносної товщини стрілоподібних профілів.

Відносна товщина стрілоподібного профілю визначається відомою залежністю [10]

$$\bar{\tau}_{\chi} = \bar{\tau}\,\mathrm{Cos}\,\chi \ . \qquad (10)$$

де $\bar{\tau}_{\chi}$ – відносна товщина стрілоподібного профілю;

χ – кут стрілоподібності аеродинамічного профілю.

Тому критичне число M стрілоподібного аеродинамічного профілю можна визначити з рівняння, аналогічного рівнянню (6), а саме:

$$M_{кр\chi} \approx 1 - 0{,}7\sqrt{\bar{\tau}\,\mathrm{Cos}\,\chi} \ , \qquad (11)$$

де $M_{кр\chi}$ – критичне число M стрілоподібного аеродинамічного профілю.

Але необхідно зауважити таке: в деяких роботах, наприклад [11], величину критичного числа M стрілоподібного профілю рекомендовано визначати згідно з рівнянням

$$M_{кр\chi} \approx \frac{M_{кр}}{\mathrm{Cos}\,\chi} \ . \qquad (12)$$

Водночас у цій роботі зазначено, що відповідно до досвіду досліджень точніше величина критичного числа M стрілоподібного аеродинамічного профілю визначається згідно з рівнянням

$$M_{кр\chi} \approx \frac{M_{кр}}{\sqrt{\mathrm{Cos}\,\chi}} \ . \qquad (13)$$

Зауважимо також, що критичне число M стрілоподібного аеродинамічного профілю в разі визначення згідно з рівняннями (12) та (13) у деяких випадках може бути $M_{кр\chi} \geq 1{,}0$, а це неможливо. Тому критичне число M стрілоподібного аеродинамічного профілю доцільно визначати згідно з рівнянням (11), у тому числі в разі оцінювання розташування стрибків ущільнення на поверхні стрілоподібного аеродинамічного профілю.

Для оцінювання залежності розташування стрибків ущільнення за хордою аеродинамічного профілю від його геометричних характеристик, числа M незбудженого потоку повітря та критичного числа M аеродинамічного профілю згідно з математичною моделлю (7) скористаймося також даними роботи [5], у якій за результатами продувок моделі крила в аеродинамічної трубі в діапазоні трансзвукових чисел M незбудженого потоку повітря наведені залежності розташування стрибків ущільнення за хордою профілю від числа M незбудженого потоку повітря з такими характеристиками аеродинамічного профілю:

- профіль моделі крила – симетричний профіль С-11с-9;
- відносна товщина профілю $\bar{\tau} = 0{,}09$;
- критичне число М профілю $M_{кр} = 0{,}79$;
- відносна відстань перетину максимальної товщини профілю від його носка $\frac{b_{\tau}}{b} = 0{,}3$;
- відносна хорда аеродинамічної поверхні керування $\frac{b_k}{b} = 0{,}3$.

Оскільки розташування стрибків ущільнення за хордою профілю роботі [5] наведені як відносна відстань перетину розташування стрибків ущільнення від носка профілю, тому математична модель (7) у даному випадку перетворимо до вигляду

$$\bar{x}_{c1} \approx \frac{1 - \bar{b}_{\tau}}{9{,}8\bar{\tau}} \left\{ \left[2\left(M_{\infty} - M_{кр}\right) + 1 \right]^3 - 1 \right\} + \bar{b}_{\tau} \ , \qquad (14)$$

де $\bar{x}_{c1}$ – відносна відстань перетину розташування стрибків ущільнення за хордою профілю від носка профілю.

Критичне число M аеродинамічного профілю у залежності (10) визначалося згідно з рівняннями (6) чи (9).

Порівняння результатів розрахунків, одержаних за допомогою математичної моделі (14), з результатами, одержаними при продувках моделі крила в роботі [5], наведені в *таблиці 2*.

Таблиця 2

$\bar{x}_{c1}$	0,3	0,425	0,5	0,55	0,6	0,7
M_{∞} – робота [5]	0,783	0,8	0,818	0,83	0,842	0,87
M_{∞} – розрахунок	0,79	0,815	0,83	0,837	0,8465	0,862
Похибка, %	0,89	1,02	1,15	0,84	0,53	0,93

З порівняння наведених у *таблиці 2* результатів випливає, що максимальне відхилення величини числа M незбудженого потоку повітря, одержаного теоретичним методом за допомогою математичної моделі (14), від величини числа M незбудженого потоку повітря, яке спостерігалося в лабораторному експерименті, не перевищує похибок обробки експериментальних даних [5]. Тому запропонована математична модель може бути рекомендована для оцінювання розташування стрибків ущільнення на поверхні аеродинамічного профілю.

З аналізу одержаної математичної моделі оцінювання розташування стрибків ущільнення по поверхні

аеродинамічного профілю та з аналізу одержаних результатів розрахунків випливає, що в разі відхилення аеродинамічної поверхні керування донизу стрибки ущільнення на верхній поверхні аеродинамічного профілю переміщуються від початкового розташування до задньої кромки аеродинамічного профілю, оскільки при цьому зростає величина критичного числа M.

Ця особливість взаємодії розташування стрибків ущільнення на поверхні аеродинамічного профілю з відхиленням аеродинамічної поверхні керування відмічена і в деяких дослідженнях. Так, у роботі [5] зазначено: «...відхилення керма донизу супроводжується переміщенням стрибка ущільнення в напрямку до керма на верхній поверхні та віддаленням його від керма на нижній поверхні».

У роботі [12] додатково відмічена ще одна особливість впливу відхилення аеродинамічної поверхні керування на стрибки ущільнення, а саме: «...відхилення керма донизу приводить до подальшого прискорення потоку і до збільшення потужності верхньої ударної хвилі».

Зауважмо, що відмічені особливості взаємодії відхилення аеродинамічної поверхні керування з розташуванням стрибків ущільнення на поверхні аеродинамічного профілю можна дуже просто пояснити за допомогою математичної моделі (14) та залежностей (5) і (9) або за допомогою *таблиць 1* та *2*.

Справді, як можна побачити з рівняння (9) і *таблиці 1*, у разі відхилення аеродинамічної поверхні керування зменшується критичне число M аеродинамічного профілю. Тому, згідно з математичною моделлю (14) і *таблицею 2*, стрибки ущільнення переміщуються до задньої кромки аеродинамічного профілю, і, згідно з рівняннями (1) та (5), зростає число M місцевого надзвукового потоку на поверхні аеродинамічного профілю та потужність ударної хвилі.

Висновок

У статті наведена модель, яка визначає зв'язок розташування стрибків ущільнення за хордою профілю аеродинамічної поверхні від числа M незбудженого потоку повітря, геометричних характеристик і критичного числа M аеродинамічного профілю та результати розрахунків за даною моделлю.

Можливість практичного використання одержаної математичної моделі підтверджена шляхом порівняння результатів оцінювання розташування стрибків ущільнення на поверхні аеродинамічного профілю, одержаних за допомогою цієї моделі, з результатами, одержаними в експериментальних дослідженнях.

Подальші дослідження доцільно присвятити розробці й удосконаленню теоретичних методів оцінювання та інших характеристик аеродинамічних профілів надзвукових літаків та аерокосмічних систем у трансзвуковому діапазоні чисел M польоту, які базуються на аналізі закономірностей адіабатичного розширення місцевого надзвукового потоку повітря на поверхні аеродинамічного профілю.

Перелік літератури

1. *Штейнберг Р. И.* Максимальная скорость на поверхности крылового профиля при околозвуковых скоростях / Р. И. Штейнберг // Труды ЦАГИ. – 1978. – Вып. 1931. – С. 3–15.

2. *Лифшиц Ю. Б.* Способ определения положения скачка уплотнения на крыловом профиле / Ю. Б. Лифшиц, Р. И. Штейнберг // Труды ЦАГИ. – 1974. – Вып. 1577. – С. 13–19.

3. *Левкин В. Ф.* Экспериментальные исследования нестационарных аэродинамических характеристик поверхностей управления при трансзвуковых скоростях / В. Ф. Левкин. – М. : ЦАГИ, 1982. – 16 с. – (Труды ЦАГИ ; вып. 2132).

4. *Агеев Ю. И.* Экспериментальное исследование установившихся колебаний элерона в околозвуковом потоке / Ю. И. Агеев, В. В. Назаренко, Т. П. Невежина // Ученые записки ЦАГИ. – 1974. – Т. V, № 8. – С. 71–80.

5. *Свищев Г. П.* Эффективность руля и шарнирные моменты его при больших скоростях / Г. П. Свищев. – М. : ЦАГИ, 1975. – 10 с. – (Труды ЦАГИ ; вып. 1722).

6. *Traci R. M.* Perturbation Method for Transonic Flows about Oscillating Airfoils [Електронний ресурс] / R. M. Traci, E. D. Albano, J. L. Farr // AIAA Journal. – 1976. – Vol. 14, No 9. – P. 1258–1265. – Режим доступу : https://doi.org/10.2514/3.61459.

7. *Сафронов А. В.* Аэродинамическое воздействие скачков уплотнения на колеблющийся в околозвуковом потоке элерон / А. В. Сафронов // Ученые записки ЦАГИ. – 1991. – Т. XX11, № 3. – С. 110–117.

8. Закономірності адіабатичного розширення місцевого надзвукового потоку повітря на поверхні аеродинамічного профілю [Електронний ресурс] / О. В. Сафронов, Б. Й. Семон, О. М. Неділько, Ю. Г. Бодрик // Наука і оборона. – № 1. – 2022. – С. 34–39. – Режим доступу : https://doi.org/10.33099/2618-1614-2022-18-1-34-39.

9. *Сафронов А. В.* Условия возникновения автоколебаний аэродинамических поверхностей управления при безотрывном обтекании околозвуковым потоком газа / А. В. Сафронов // Проблемы прочности. – 1990. – № 2. – С. 50–55.

10. *Краснов Н. Ф.* Аэродинамика : учеб. для студ. высших технических учеб. заведений. В 2 ч. Ч. 1. Основы теории. Аэродинамика профиля и крыла / Н. Ф. Краснов. – Изд. 2-е, перераб. и доп. – М. : Высшая школа, 1976. – 384 с.

11. *Гошек И.* Аэродинамика больших скоростей / И. Гошек ; пер. с чешского А. А. Дородницына, М. М. Богословского. – М. : Изд-во иностран. лит., 1954. – 547 с.

12. *Бисплингхофф Р. Л.* Аэроупругость / Р. Л. Бисплингхофф, Х. Эшли, Р. Л. Халфмэн ; пер. с англ. Г. И. Баренблатта, А. И. Смирнова, В. П. Шидловского ; под ред. Э. И. Григолюка. – М. : Изд-во иностран. лит., 1958. – 800 с.

DOI 10.33099/2618-1614-2024-27-4-54-59
УДК 355.4

О. М. Загорка,
доктор військових наук, професор,
Національний університет оборони України,
С. В. Поліщук,
кандидат військових наук,
Національний університет оборони України,
І. О. Загорка,
Національний університет оборони України

Обґрунтування вимог до ефективності застосування сил протидії повітряному противнику в оборонній операції

Протиповітряна оборона угруповання військ в оборонній операції здійснюється зенітними ракетними військами, винищувальною авіацією, військами протиповітряної оборони сухопутних військ, силами радіоелектронної боротьби, застосуванням засобів технічного маскування. Під час організації протиповітряної оборони важливим є визначення потрібних внесків зазначених сил і засобів (сил протидії повітряному противнику) в її ефективність, що дає можливість обґрунтувати їхній бойовий склад. У статті викладений методичний підхід, яким передбачається визначення вимог до ефективності застосування в оборонній операції зенітних ракетних військ, винищувальної авіації, військ протиповітряної оборони сухопутних військ, сил радіоелектронної боротьби, засобів технічного маскування.

Ключові слова: угруповання військ, ракетно-авіаційний удар, протиповітряна оборона, ефективність.

Постановка проблеми. З досвіду минулих війн бойові дії стороною, яка розв'язувала воєнний конфлікт, починалися нанесенням ракетно-авіаційних ударів (РАУ) по об'єктах країни, котра зазнала нападу, зокрема по її угрупованню військ. Тим самим створювалися сприятливі умови для дій сухопутних військ.

Прикриття угруповання військ від ударів засобів повітряного нападу (ЗПН) здійснюється зенітними ракетними військами (ЗРВ), винищувальною авіацією (ВА), військами протиповітряної оборони (ППО) сухопутних військ (СВ), силами радіоелектронної боротьби (РЕБ). Для зниження результативності застосування ЗПН використовується маскування об'єктів угруповання військ технічними засобами. Під час організації ППО угруповання військ важливим є визначення потрібних внесків сил протидії повітряному противнику в загальну ефективність відбиття РАУ, зокрема першого РАУ як найважливішого для дій наших сил. Це дасть змогу визначити потрібний склад сил протидії повітряному противнику в оборонній операції.

Аналіз останніх досліджень і публікацій. Методичні положення оцінювання ефективності застосування ЗРВ, ВА, військ ППО СВ при відбитті РАУ по військах і об'єктах розглянуті в багатьох роботах. Наприклад, у роботах [1–5] обґрунтовані показники і наведені методики оцінювання ефективності застосування сил і засобів ППО при відбитті ударів ЗПН, які ґрунтуються на використанні методів імітаційного моделювання, аналітико-стохастичних і аналітичних методів. Водночас у роботах мало уваги приділяється обґрунтуванню вимог до ефективності застосування сил і засобів ППО, зокрема в оборонній операції, не розглядається зв'язок цих вимог зі збереженням боєздатності угруповання військ на кінець оборонної операції, не враховуються можливості сил РЕБ і засобів технічного маскування (ЗТМ) щодо зниження результативності застосування ЗПН.

Метою статті є розроблення методичного підходу до визначення потрібної ефективності (вимог) застосування сил протидії повітряному противнику в оборонній операції.

Виклад основного матеріалу. Відповідно до тенденцій розвитку збройної боротьби і досвіду минулих війн можна вважати, що на початок воєнного конфлікту протиборчі сторони обмінюватимуться РАУ. Втрати угрупованню військ, яке обороняється, особливо в першому РАУ, завдаватимуться переважно ЗПН. Тому обґрунтування вимог до ефективності сил протидії повітряному противнику доцільно здійснювати з урахуванням потрібного зниження втрат угруповання військ від ЗПН у першому РАУ. Порядок визначення потрібного зниження втрат угруповання військ у першому РАУ від ЗПН наведений на *рисунку 1*.

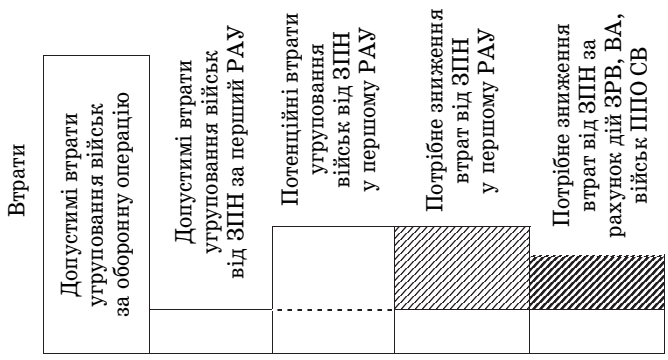

Рис. 1. Порядок визначення потрібного зниження втрат угруповання військ від ЗПН у першому РАУ

Визначення допустимих втрат угруповання військ за оборонну операцію доцільно здійснювати з урахуванням критичних втрат. За попередніми дослідженнями визначено, що в минулих війнах наступ припинявся в разі загальних втрат 30–50%. Оборона втрачала стійкість у разі загальних втрат 50–70%. Тому допустимими за оборонну операцію можна вважати втрати угруповання військ не більше 50%.

При змінюванні бойового потенціалу угруповання військ під час оборонної операції за експоненціальною залежністю математичне сподівання величини допустимих відносних загальних втрат за добами операції можна визначити за формулою

$$M_{вт}^{доп} = 1 - e^{-\gamma T_{оп}}, \qquad (1)$$

де $T_{оп}$ – доба операції;

γ – коефіцієнт, який характеризує інтенсивність змінювання втрат угруповання військ в операції.

При $M_{вт}^{доп} = 0{,}5$ (допустимі втрати за операцію 50%) можна записати

$$e^{-\gamma T_{оп}^{*}} = 0{,}5, \qquad (2)$$

де $T_{оп}^{*}$ – тривалість оборонної операції.

Звідси коефіцієнт

$$\gamma = -\frac{\ln 0{,}5}{T_{оп}^{*} \ln e} = \frac{0{,}69}{T_{оп}^{*}}. \qquad (3)$$

При тривалості операції $T_{оп}^{*}$ = 10 діб γ = 0,069, при $T_{оп}^{*}$ = 5 діб γ = 0,138.

Змінювання математичних сподівань величин допустимих відносних втрат угруповання військ під час оборонної операції різної тривалості за критичних втрат 50% показане на *рисунку 2*.

Якщо прийняти, що противник у першу добу операції здатний завдати угрупованню військ два РАУ, то

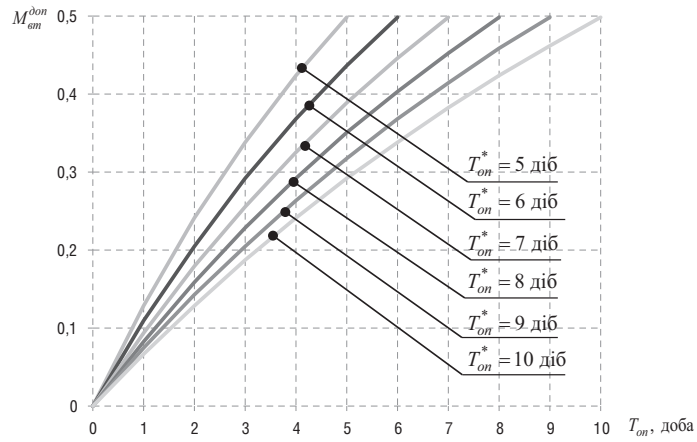

Рис. 2. Змінювання математичних сподівань величин допустимих відносних втрат угруповання військ під час оборонної операції

допустимими втратами від ЗПН у першому РАУ можна вважати втрати, які завдаються за половину першої доби операції. Це дає змогу визначити допустимі втрати угруповання військ від ЗПН у першому РАУ за формулою

$$M_{вт}^{доп*} = 1 - e^{-0{,}5\gamma}. \qquad (4)$$

Для допустимих втрат угруповання військ за операцію 50% при тривалості операції $T_{оп}^{*}$ = 10 діб $M_{вт}^{доп*}$ = 0,034, при $T_{оп}^{*}$ = 5 діб $M_{вт}^{доп*}$ = 0,067.

Для визначення математичного сподівання величини відносних потенційних втрат, які можуть бути завдані угрупованню військ у першому РАУ, доцільно застосовувати аналітичну методику на підставі використання полігонних нарядів ЗПН для ураження військових об'єктів і методу ітерацій [3–5].

Математичне сподівання величини відносних потенційних втрат $M_{вт}^{пот}$ визначається за формулою

$$M_{вт}^{пот} = \frac{\sum\limits_{z} m_z Q_z}{\sum\limits_{z} n_z Q_z}, \; z = \overline{1,L}, \qquad (5)$$

де m_z – кількість об'єктів z-го типу угруповання військ, що можуть уражатися ЗПН у першому РАУ;

n_z – кількість об'єктів z-го типу у складі угруповання військ;

Q_z – коефіцієнт важливості об'єктів z-го типу;

L – кількість типів об'єктів у складі угруповання військ.

Структурна схема методичного підходу до визначення математичного сподівання величини відносних

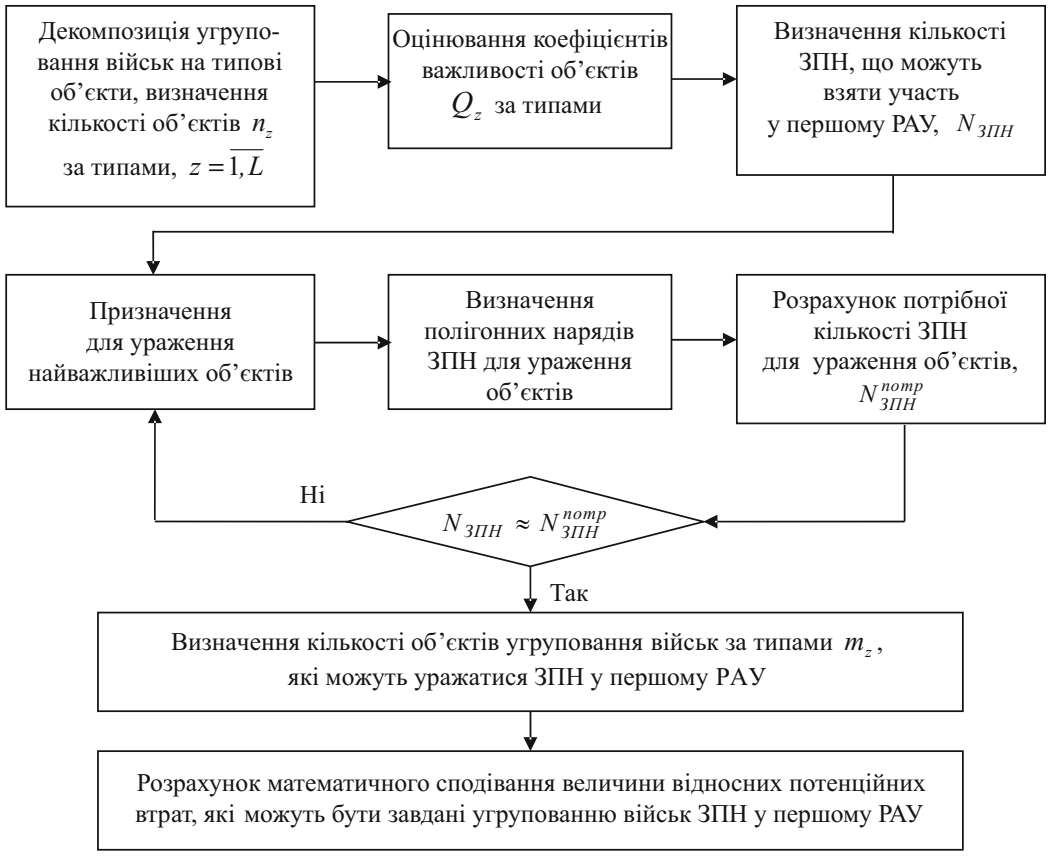

Рис. 3. Структурна схема методичного підходу до визначення математичного сподівання величини відносних потенційних втрат угруповання військ від ЗПН у першому РАУ

потенційних втрат угруповання військ від ЗПН у першому РАУ наведена на *рисунку 3*.

У роботах [4, 6] для оцінювання коефіцієнтів важливості військових об'єктів запропоновано використовувати метод аналізу ієрархій [7].

Відповідно до методичного підходу ітерації здійснюються, поки кількість ЗПН, які можуть взяти участь у РАУ, $N_{ЗПН}$ не дорівнюватиме кількості потрібних ЗПН $N_{ЗПН}^{потр}$ для ураження обраних об'єктів.

Ураховуючи, що в РАУ застосовуються літаки, крилаті ракети, безпілотні літальні апарати і балістичні ракети тактичного або оперативно-тактичного призначення, втрати від їхніх дій оцінюються окремо з подальшим підсумовуванням для одержання математичного сподівання $M_{вт}^{пот}$.

Відповідно до цього підходу можна прийняти, що математичне сподівання величини відносних потенційних втрат прямо пропорційне кількості ЗПН у РАУ.

Потрібне зниження втрат угруповання військ від ЗПН у першому РАУ відповідно до схеми на *рисунку 1* визначається за формулою

$$\Delta M_{вт} = M_{вт}^{пот} - M_{вт}^{доп*}. \qquad (6)$$

Потрібні рівні зниження втрат угруповання військ застосуванням ЗРВ, ВА, військ ППО СВ, сил РЕБ, ЗТМ визначаються з урахуванням відповідних внесків $C_{ЗРВ}$, $C_{ВА}$, $C_{вППО}$, $C_{РЕБ}$, $C_{ЗТМ}$ цих сил і засобів в ефективність протидії повітряному противнику таким чином:

$$\Delta M_{вт}^{ЗРВ} = C_{ЗРВ}\Delta M_{вт}; \quad \Delta M_{вт}^{ВА} = C_{ВА}\Delta M_{вт};$$
$$\Delta M_{вт}^{вППО} = C_{вППО}\Delta M_{вт}; \quad \Delta M_{вт}^{РЕБ} = C_{РЕБ}\Delta M_{вт};$$
$$\Delta M_{вт}^{ЗТМ} = C_{ЗТМ}\Delta M_{вт}. \qquad (7)$$

Математичне сподівання відносної кількості ЗПН, яка повинна знищуватися при відбитті першого РАУ, визначається за формулою

$$N_{зн} = \frac{\Delta M_{вт} - \Delta M_{вт}^{РЕБ} - \Delta M_{вт}^{ЗТМ}}{M_{вт}^{пот}} =$$
$$= 1 - \frac{M_{вт}^{доп*}}{M_{вт}^{пот}} - \frac{\Delta M_{вт}^{РЕБ} + \Delta M_{вт}^{ЗТМ}}{M_{вт}^{пот}}. \qquad (8)$$

Потрібні рівні математичних сподівань відносної кількості знищення засобів повітряного нападу ЗРВ, ВА, військ ППО СВ визначаються за формулами:

$$N_{зн}^{ЗРВ} = D_{ЗРВ} N_{зн}; \quad N_{зн}^{ВА} = D_{ВА} N_{зн};$$

$$N_{зн}^{вППО} = D_{вППО} N_{зн}, \qquad (9)$$

де $D_{ЗРВ}$, $D_{ВА}$, $D_{вППО}$ – внески ЗРВ, ВА, військ ППО СВ у знищення ЗПН відповідно.

Вважається, що за умови виконання цих вимог забезпечуватиметься зрив першого РАУ і збереження боєздатності військ від ударів ЗПН за весь період оборонної операції.

Для обґрунтування вимог до ефективності застосування сил протидії повітряному противнику здійснюється прогнозування завдання першого РАУ по об'єктах угруповання військ, що обороняється. При прогнозуванні доцільно формувати декілька варіантів РАУ, якими визначаються їхній склад, способи застосування засобів, об'єкти ураження угруповання військ тощо.

Знищення потрібної кількості ЗПН під час відбиття РАУ може забезпечуватися при різних внесках ЗРВ, ВА, військ ППО СВ в ефективність відбиття РАУ, що визначається бойовим складом цих сил. Таким чином, під час обґрунтування вимог також потрібно формувати декілька або безліч варіантів бойового складу сил протидії повітряному противнику, як показано на *рисунку 4*, та обирати з них раціональний варіант. Формування варіантів першого РАУ $A_i \left(i = \overline{1,R}\right)$ та сил протидії $B_j \left(j = \overline{1,K}\right)$ здійснюється з використанням евристичного методу.

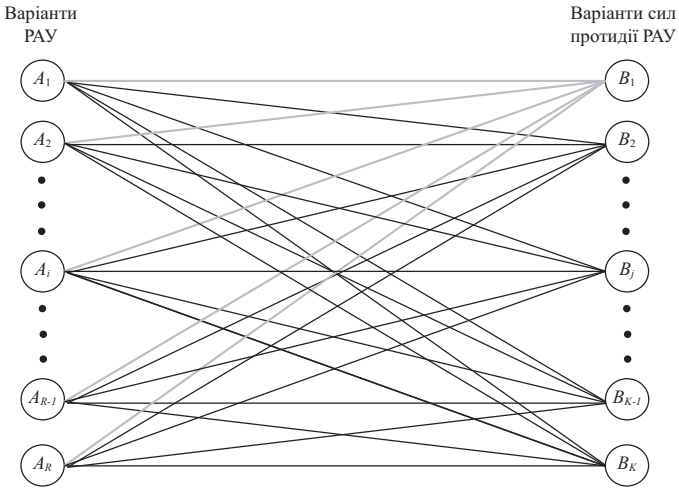

Рис. 4. Сполучення варіантів РАУ та варіантів сил протидії РАУ

При формуванні варіантів складу сил протидії можна прийняти, що силами РЕБ і ЗТМ забезпечується визначене зниження втрат угруповання військ $\Delta M_{вт}^{РЕБ}$, $\Delta M_{вт}^{ЗТМ}$.

Формування варіантів бойового складу ЗРВ, ВА, військ ППО СВ здійснюється за умовою забезпечення відносної кількості ураження ЗПН, яке при протидії i-му варіанту першого РАУ, дорівнює $N_{зні}$ та визначається з використанням формули (8).

Водночас математичне сподівання відносної кількості ЗПН, яка може бути знищена j-м варіантом бойового складу ЗРВ, ВА, військ ППО СВ при відбиті i-го варіанта першого РАУ

$$N_{знji}^{*} = N_{знji}^{ЗРВ} + N_{знji}^{ВА} + N_{знji}^{вППО}. \qquad (10)$$

Математичне сподівання відносної кількості ЗПН, яка може знищуватися ЗРВ, ВА, військами ППО СВ $N_{знji}^{ЗРВ}$, $N_{знji}^{ВА}$, $N_{знji}^{вППО}$ залежно від їхнього бойового складу, доцільно визначати з використанням аналітико-стохастичних моделей [1–3].

Порядок формування варіантів складу сил протидії (ЗРВ, ВА, військ ППО СВ) РАУ наведений на *рисунку 5*. Кожний варіант бойового складу сил протидії $B_j \left(j = \overline{1,K}\right)$ розглядається для всіх варіантів РАУ $A_i \left(i = \overline{1,R}\right)$.

Ураховуючи, що застосування кожного варіанта бойового складу сил протидії повинне забезпечувати потрібне знищення ЗПН при відбитті кожного варіанта РАУ, раціональним доцільно вважати варіант, якому відповідає мінімальна вартість бойових засобів.

Загальними вимогами до сил протидії повітряному противнику, які визначаються з використанням запропонованого підходу, є потрібне зниження втрат угруповання від ЗПН у першому РАУ і знищення потрібної кількості ЗПН при його відбитті. Ці вимоги визначаються максимальними значеннями для всіх варіантів РАУ $\left(\Delta M_{вт} = \max\limits_{i} \Delta M_{вті}, \ N_{зн} = \max\limits_{i} N_{зні}\right)$.

Раціональним варіантом сил протидії визначаються вимоги до внесків $D_{ЗРВ}$, $D_{ВА}$, $D_{вППО}$ у знищення ЗПН при відбитті першого РАУ, а також вимоги до внесків $C_{РЕБ}$, $C_{ЗТМ}$ у зниження втрат угруповання військ від ЗПН. Таким вимогам відповідає раціональний бойовий склад сил протидії повітряному противнику.

Висновки. Запропоновано методичний підхід до визначення потрібної ефективності (вимог) застосування сил протидії повітряному противнику (ЗРВ, ВА, військ

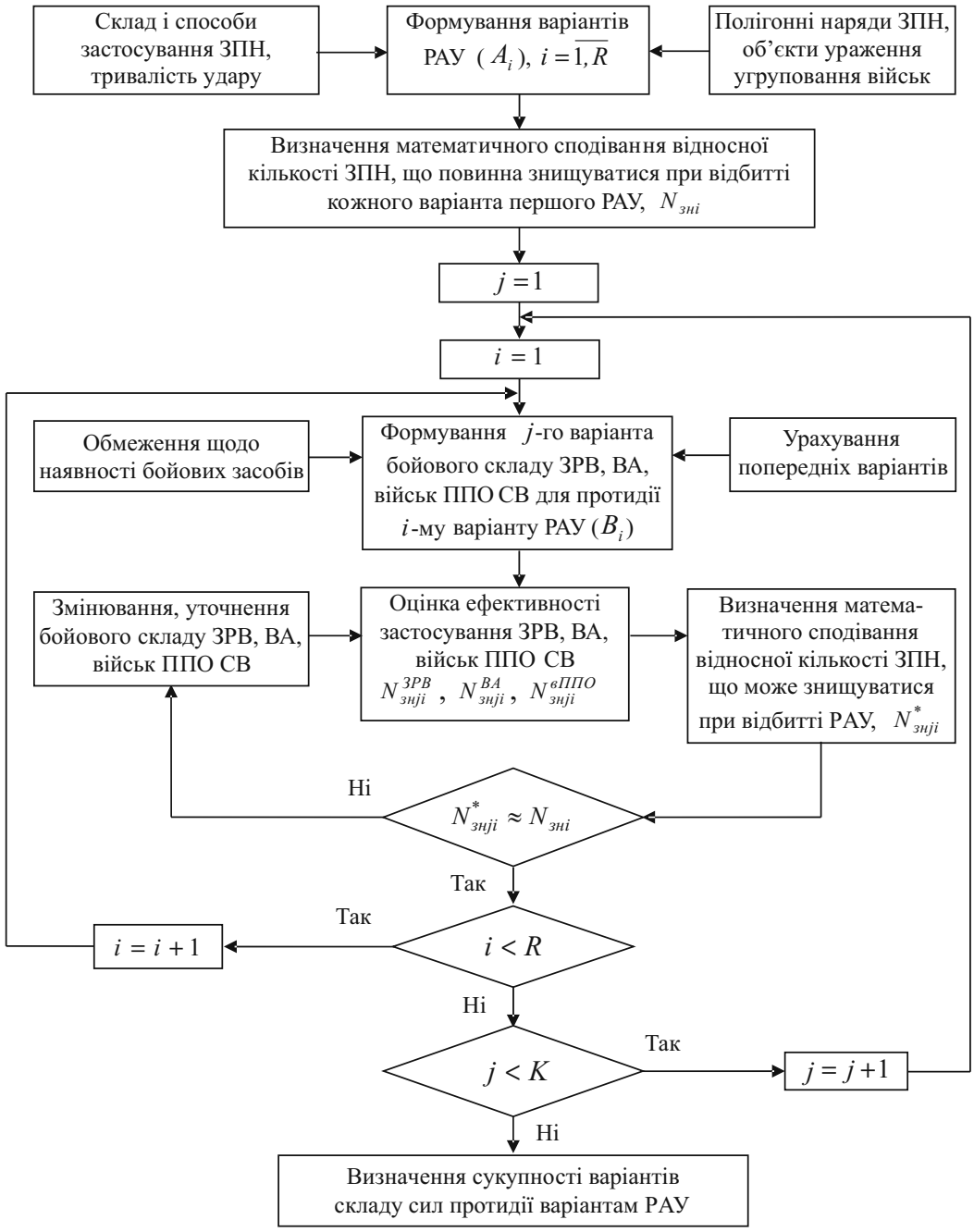

Рис. 5. Порядок формування варіантів складу сил протидії (ЗРВ, ВА, військ ППО СВ) РАУ

ППО СВ, РЕБ, ЗТМ) в оборонній операції, який ґрунтується на урахуванні допустимих втрат угруповання військ від ЗПН у першому РАУ. Вимоги до ефективності застосування сил протидії повітряному противнику визначаються з урахуванням можливих варіантів завдання першого РАУ по угрупованню військ, яке обороняється, і відповідних варіантів застосування визначеного складу сил протидії.

Методичним підходом передбачається визначення: потрібного зниження втрат угруповання військ від ЗПН у першому РАУ; потрібної кількості знищених ЗПН та внесків ЗРВ, ВА, військ ППО СВ у відбиття першого РАУ; внесків сил РЕБ, ЗТМ у зниження втрат угруповання військ від дій ЗПН. Внески ЗРВ, ВА, військ ППО СВ у знищення ЗПН визначають раціональний склад цих сил ППО за вартістю бойових засобів.

У подальшому доцільно на підставі наведеного методичного підходу розробити методику визначення вимог до ефективності застосування сил протидії повітряному противнику в оборонній операції.

Перелік літератури

1. Моделювання бойових дій військ (сил) протиповітряної оборони та інформаційне забезпечення процесів управління ними (теорія, практика, історія розвитку) : монографія / В. П. Городнов, Г. А. Дробаха, М. О. Єрмошин та ін. – Х. : ХВУ, 2004. – 409 с.

2. *Єрмошин М. О.* Оцінка ефективності бойових дій зенітних ракетних військ : навч. посіб. / М. О. Єрмошин, Г. А. Дробаха. – Х. : ХВУ, 2004. – 259 с.

3. *Городнов В. П.* Методика прогноза эффективности группировок родов войск ПВО / В. П. Городнов. – Х. : ХВУ, 1999. – 32 с.

4. Прогнозування втрат військ і об'єктів від авіаційних ударів противника / С. І. Онищенко, О. М. Загорка, В. В. Коваль, В. В. Тюрін // Системи озброєння і військова техніка. – 2011 – № 2 (26). – С. 2–8.

5. Теоретичні основи управління угрупованням військ (сил) у сучасних умовах збройної боротьби : монографія / О. М. Загорка, А. К. Павліковський, А. А. Корецький та ін. ; за заг. ред. І. С. Руснака. – К. : НУОУ, 2020. – 248 с.

6. *Тарасов В. М.* Розвідувально-ударні, розвідувально-вогневі комплекси (принципи побудови в умовах реалізації концепції мережоцентричних війн, оцінка ефективності бойового застосування) : монографія / В. М. Тарасов, Р. І. Тимошенко, О. М. Загорка ; за заг. ред. В. М. Телелима. – К. : НУОУ, 2015. – 183 с.

7. *Saaty T. L.* Analytical planning: the organization of systems / T. L. Saaty, K. P. Kearns. – Oxford : Pergamon Press, 1985. – VII, 208 p. – (International series in modern applied mathematics and computer science ; vol. 7).

Комаров В. С., *доктор військових наук, професор, Науково-дослідний інститут воєнної розвідки,*

Олексіюк В. В., *кандидат військових наук, старший дослідник, Науково-дослідний інститут воєнної розвідки,*

Щербань К. А., *Науково-дослідний інститут воєнної розвідки*

Складові стратегічної адаптації Російської Федерації до спроможності ведення довготривалої війни на виснаження проти України

Авторами проведено аналіз складових стратегічної адаптації російської федерації до спроможності ведення довготривалої війни на виснаження проти України з метою визначення «критичних точок», асиметричний вплив на які дасть змогу створити передумови до примусу Російської Федерації відмовитись від реалізації її воєнно-політичних загарбницьких цілей.

Ключові слова: асиметричний вплив, «критичні точки», засоби DIME, сценарії, стратегічна адаптація, війна на виснаження.

Drapatyi M. V., *General Staff of the Armed Forces of Ukraine,*

Dziuba T. M., *Candidate of Technical Sciences, Associate Professor, Armed Forces of Ukraine,*

Kostenko A. M., *National Defence University of Ukraine,*

Samarskyi O. O., *Armed Forces of Ukraine*

Analysis of information warfare activities of the armed forces of the Russian Federation in areas of combat operations

Despite a significant number of scientific studies of various aspects of the Russian information warfare against Ukraine and the world, such issues as coordination of the enemy's information operations at different levels (from strategic and tactical), the systematic way of its actions in the information space, the impact of the enemy's information warfare on the effectiveness of its military operations against Ukraine has not been studied enough.

The purpose of the article is to analyse the forms and methods of the information warfare of the Russian Federation against Ukraine, which directly accompany the actions of the Russian troops, and to determine the relationship between the information operations of the enemy at the tactical, operational, and strategic levels.

The materials of the article are based on the personal practical experience of the authors regarding the organization of strategic communications activities of the Defence Forces of Ukraine, in particular countering information operations of the enemy in the operations of the operational-strategic group «Odesa», the operational groups «Kherson» and «Tavria», the operational-tactical task force «Kharkiv».

Key words: information warfare, information operations, informational and psychological influence, monitoring of the information space, forms and methods of information warfare, actors of information warfare, information resources.

Volotivskyi P. B., *Candidate of Military Sciences, Senior Researcher, State Research Institute of Aviation,*

Steshenko P. M., *Candidate of Technical Sciences, Senior Researcher, State Research Institute of Aviation,*

Bohoslavets S. O., *Candidate of Technical Sciences, Senior Researcher, State Research Institute of Aviation,*

Korepanov V. V., *Ivan Kozhedub Kharkiv National Air Force University*

Regarding the outline of a prospective system for combating unmanned aerial systems

The need to counter unmanned aerial systems of the Armed Forces of the Russian Federation, which are currently among the main means of striking important state and military facilities of Ukraine, requires the creation of an effective system for combating these means of air attack. The main source of the creation of such a system is the formulated goals and objectives that must be attained by the system, as well as the achievements of science and technology in the relevant areas.

An important issue at the initial stage of the creation (design) of such a complex combat system as an anti-drone defence system is the delineation of its general outline (the conception, the choice of the main conceptual features, the concept of creation and application).

The authors of the article proposed a variant of the general outline of the anti-drone defence system as part of the higher system – the Air Defence of Ukraine, which was obtained as a result of previously conducted research.

Key words: air defence, outline of the anti-drone defence system, system requirements, unmanned aerial system.

Koval M. V., *Doctor of Military Sciences, National Defence University of Ukraine,*

Kosevtsov V. O., *Doctor of Military Sciences, Professor, National Defence University of Ukraine,*

Telelym V. M., *Doctor of Military Sciences, Professor, National Defence University of Ukraine,*

Zakharzhevskyi A. H., *Candidate of Technical Sciences, National Defence University of Ukraine*

Methodological approach to predicting the generalized conflict-generating index of a possible military conflict

The article provides the author's vision of solving the problematic issues of monitoring the military-political situation based on determining the generalized conflict-generating index in relations with any country for the timely introduction of measures to prevent, deter, or repel a possible enemy attack.

Key words: military conflict, generalized conflict-generating index of conflict, conflict-generating factors, methods of multidimensional comparative analysis, coefficients of importance of conflict-generating factors, phases and stages of development of a military conflict.

Snitsarenko P. M., *Doctor of Technical Sciences, Senior Researcher, National Defence University of Ukraine*

Cyber defence of Ukraine as a component of state defence

The issue of cyber defence of Ukraine is considered from the position that it is a component of state defence, not cyber security. Today, Ukrainian defence legislation considers cyber defence in a limited way – only as a type of military action performed by the Armed Forces of Ukraine together with other military formations in the phase of repelling armed aggression, which does not utilize all the capabilities of Ukraine's defensive potential in cyberspace. At the same time, unlike the concept of «defence of Ukraine», the national defence legislation does not define the concept of cyber defence of Ukraine, and the issue of cyber defence of the state is not directly raised. Meanwhile, understanding the subject of cyber defence of Ukraine and its consequences is conceptually the most important and relevant theoretical and practical task that must be solved as a matter of priority. In this regard, exclusively from the position of the legislation of Ukraine on defence issues, based on the application of the system approach and the structural-logical research method, the essence of the cyber defence of Ukraine as a component of the state defence is substantiated for the first time, the elements of the corresponding nationwide system and the relationships between them are delineated, and the main stages of its implementation are outlined.

Key words: defence, cyber defence, cyber defence as a type of military action, cyber defence of Ukraine, legislation of Ukraine.

Safronov O. V., *Doctor of Technical Sciences, Professor, National Defence University of Ukraine,*

Semon B. Y., *Doctor of Technical Sciences, Professor, National Defence University of Ukraine,*

Nedilko O. M., *Candidate of Technical Sciences, Associate Professor, National Defence University of Ukraine*

Mathematical model for estimating the location of shock waves on the surface of an aerofoil

The article, based on the analysis of the consistent patterns of adiabatic expansion of local supersonic airflow over an aerofoil surface in the subsonic range of Mach numbers, presents the results of a study of the dependence of the location of shock waves on the geometric characteristics of the aerofoil, the Mach number of undisturbed airflow and the critical Mach number of the aerofoil.

The credibility of the obtained findings is confirmed by comparing the calculated results of estimation of the location of shock waves on the aerofoil surface with the results obtained in experimental studies.

Key words: aviation equipment, aircraft, adiabatic expansion, aerodynamic surface, mathematical model, local supersonic flow, Mach number, critical Mach number of the aerofoil, location of shock waves.

Zahorka O. M., *Doctor of Military Sciences, Professor, National Defence University of Ukraine,*

Polishchuk S. V., *Candidate of Military Sciences, National Defence University of Ukraine,*

Zahorka I. O., *National Defence University of Ukraine*

Substantiation of the requirements for the effectiveness of the use of air defence forces in defensive operations

Air defence of a joint task force in defensive operations is carried out by anti-aircraft missile forces, fighter aircraft, air defence troops of the ground forces, electronic warfare units and by means of camouflage. When organizing air defence, it is important to determine the necessary contributions of the specified forces and means (air defence forces) to its effectiveness, which makes it possible to substantiate their combat composition.

The article presents a methodological approach that provides for the determination of the requirements for the effectiveness of the use of anti-aircraft missile forces, fighter aircraft, air defence troops of the ground forces, electronic warfare units and camouflage means in defensive operations.

Key words: joint task force, missile and air strike, air defence, effectiveness.

Основні вимоги до оформлення статей, які подаються до журналу «Наука і оборона»

Журнал приймає для опублікування статті українською або англійською мовами. Анотації статей подаються українською та англійською мовами.

Журнал «Наука і оборона» включений до категорії «Б» наукових фахових видань України (наказ Міністерства освіти і науки України № 409 від 17 березня 2020 р.).

Спеціальності, за якими видання публікує наукові праці:

253 – Військове управління (за видами збройних сил);

254 – Забезпечення військ (сил);

255 – Озброєння та військова техніка;

256 – Національна безпека (за окремими сферами забезпечення і видами діяльності);

263 – Цивільна безпека.

Подані авторами статті повинні за змістом відповідати тематиці журналу та вимогам щодо опублікування наукових статей. Передусім приймаються матеріали, в яких викладені результати наукових досліджень, спрямованих на розв'язання проблем, що мають важливе оборонне значення, статті, які містять нові теоретичні ідеї, принципи, концепції, моделі, спрямовані на пояснення певних явищ і процесів у галузі національної безпеки і оборони та прогнозування їх розвитку. Також приймаються до опублікування статті практичного змісту, які висвітлюють актуальні питання національної безпеки і оборони, науково-методичні та оглядові статті, інформаційні повідомлення про наукові новини і події.

Рукопис статті повинен бути підготовлений з використанням комп'ютера і подається до редакції в електронному вигляді. Для цього автори можуть скористатися своїми обліковими записами, попередньо зареєструвавшись на сайті журналу (http://nio.nuou.org.ua), або надіслати статтю на електронну пошту редакції журналу (nio2017@ukr.net).

Загальний обсяг рукопису разом з графічними матеріалами не повинен перевищувати 20 сторінок у форматі паперу А4. Поля сторінок, мм: зліва – 30, справа – 10, зверху та знизу – 20. Сторінки мають бути пронумеровані.

Основний текст статті друкується шрифтом Times New Roman чорного кольору прямого накреслення через півтора міжрядкові інтервали кеглем 14. Допускається авторські акценти виділяти напівжирним шрифтом або курсивом.

На першій сторінці рукопису розміщуються індекс УДК, назва статті, анотація, перелік ключових слів і далі текст статті. Обсяг анотації – у межах 120–150 слів, включаючи ключові слова.

У кінці статті наводиться перелік джерел, на які є посилання у тексті статті. Бібліографічні описи джерел у переліку оформлюються згідно з ГОСТ 7.1:2006. Нумерація джерел – відповідно до порядку появи їх у тексті статті.

Рисунки, таблиці, формули, посилання оформлюються відповідно до ДСТУ 3008:2015.

Ілюстрації, виконані в окремих графічних редакторах, подаються як у середині тексту, так і в окремих файлах, створених цими редакторами.

Для забезпечення гарантій сліпого рецензування відомості про авторів у файлі статті не наводяться. У разі подання статті на сайті журналу ці відомості необхідно занести у відповідні поля форми подання. Якщо стаття надсилається до редакції електронною поштою, їх необхідно розмістити в окремому файлі. Відомості про авторів надаються за формою: прізвище, ім'я та по батькові, науковий ступінь та вчене звання, найменування посади та місце роботи, військове звання, почесні звання, ідентифікатор ORCID, інформація для зворотного зв'язку (телефонні номери, адреса електронної пошти).

Про журнал «Наука і оборона»

Науково-теоретичне та науково-практичне видання «Наука і оборона» було започатковане з огляду на нагальну потребу суспільства, державних діячів, політиків, учених, військових – усіх, хто опікується питаннями національної безпеки та оборони і професійно працює в цій сфері, – у друкованому засобі масової інформації, на сторінках якого обговорювалися б актуальні проблеми воєнної політики й реформування оборонної галузі держави та публікувалися б результати наукових досліджень з питань воєнної безпеки України, з воєнно-теоретичних і військово-технічних питань.

Часопис видається на громадських засадах. Найміцнішою його опорою в нелегкий час становлення були читачі та автори. Редакційна колегія сподівається на Вашу подальшу, шановні друзі, підтримку діяльності журналу «Наука і оборона», яка має на меті:

- сприяння створенню необхідного науково-теоретичного підґрунтя для постановки та розв'язання завдань військового будівництва шляхом опублікування інформації щодо результатів основних напрямів наукових досліджень, які стосуються оборонної сфери;
- сприяння обговоренню нагальних питань реформування оборонної сфери всіма, хто опікується питаннями національної безпеки та оборони і професійно працює в цій галузі;
- поширення воєнно-наукових знань;
- сприяння підвищенню професійного рівня військовослужбовців Збройних Сил України та інших військових формувань, утворених згідно із чинним законодавством України.

Статті до друку відбираються з урахуванням результатів рецензування членами редакційної колегії або зовнішніми фахівцями. Передусім приймаються матеріали, в яких на підставі виконаних авторами досліджень розв'язано проблему, що має важливе оборонне значення.

Видання розповсюджується за передплатою.

Редакційна колегія може мати точку зору, відмінну від поглядів авторів.

Видання розповсюджується за передплатою.
Передплата здійснюється у поштових відділеннях.
Передплатний індекс 74303.

Поточні та попередні номери журналу можна замовити у видавництві за адресою:
stylos.publish@gmail.com

Електронні версії попередніх випусків журналу «Наука і оборона»
можна знайти на веб-сторінці журналу: http://nio.nuou.org.ua,
а також на сайті Національної бібліотеки України ім. В. І. Вернадського: www.nbuv.gov.ua

Адреса редакції:
03049 Київ, проспект Повітряних Сил, 28.

Тел.: (044) 271-08-91, (067) 790-23-22, (066) 362-79-50.
E-mail: nio2017@ukr.net.
http://nio.nuou.org.ua.
Ідентифікатор медіа R30-01599.

Підп. до друку 07.01.2025 р.
Формат 60x90/8. Папір офс. Друк офсет.
Ум. друк. арк. 8,0. Обл.-вид. арк. 8,8.

Видавничий дім «Стилос».
04080, Київ, вул. Оленівська, 8, к. 2.
Тел.: (050) 331-85-03.
E-mail: stylos.publish@gmail.com .
http://www.stylos.com.ua .
Свідоцтво про внесення
до Державного реєстру суб'єктів видавничої справи
України ДК № 1465 від 13.08.2003 р.