UDC: 355.45:004.056(477)

V. Maltsev

V. Trobiuk

I. Gerasimenko

INFORMATION SECURITY PROVISION IN THE DEFENSE SECTOR OF UKRAINE

The article focuses on determining the place of information security in the defense sector of Ukraine, as well as its importance for protecting sovereignty and democratic institutions.

The concept of cyber resilience is considered as the ability of the state, institutions and citizens to counteract threats and restore functioning after attacks. The experience of creating integrated incident response centers that combine resources from the public and private sectors, ensuring operational monitoring and coordination of actions, is analyzed.

The emphasis is on the role of training cyber defense specialists on an interdisciplinary basis, as well as increasing the level of media literacy of the population, which has a positive impact on the resistance of society to information influences.

Information security in the conditions of hybrid warfare is defined not only as a technical or organizational task, but also as a strategic component of the defense of the state, which combines political, social and technological factors.

Keywords: *information security, hybrid warfare, cyber defense, critical infrastructure, cyber resilience, media literacy.*

Statement of the problem. In the current conditions of full-scale armed aggression against Ukraine, the problem of ensuring information security has become particularly urgent. Information security is no longer perceived as a narrowly technological sphere – it has become a key strategic component of the state's defense policy and an integral component of national security.

Modern wars are characterized by hybrid methods of warfare, where cyber sabotage, information and psychological operations, propaganda and disinformation are used alongside traditional military means. In such conditions, victory is impossible without effective counteraction to these threats, in particular in cyberspace, as well as without the formation of public resilience to information influences. Therefore, there is a need to rethink the role of information security as a system-forming factor for the effective functioning of the defense sector of Ukraine, taking into account both technological and organizational and legal aspects.

Analysis of recent research and publications. The issues of national and information security have been reflected in the scientific works of such domestic researchers as V. B. Averyanov, O. F. Andriyko, Y. P. Bytyak, V. A. Lipkan, N. V. Galitsyna, O. V. Golyashkin, H. P. Yarmak, as well as specialists in the field of cyber defense and cyber resilience: P. M. Snitsarenko, Y. M. Sarychev, V. A. Gordiychuk, V. I. Hrytsyuk and S. A. Zaporozhets. The works of these scientists highlight the administrative and legal principles of national security, the role of state regulation in the field of information policy, the conceptual principles of cybersecurity as a component of protecting the state's information space, as well as approaches to the formation of cyber defense and the development of cyber resilience in the context of hybrid warfare.

However, the issues of integrating information security specifically into the defense sector of Ukraine, determining its place and role in the overall architecture of national security remain insufficiently researched. Administrative and legal mechanisms for ensuring information security in wartime and approaches to protecting critical information infrastructure in conditions of prolonged hybrid aggression need to be developed. This creates the basis for further scientific analysis and the search for optimal solutions.

The purpose of the article is to analyze the role of information security as a key element of the defense sector of Ukraine in the context of hybrid warfare and digital threats, as well as its theoretical justification. The task of the study is to determine modern technical, organizational and administrative-legal mechanisms for ensuring cyber defense in the defense sector, identify challenges associated with the protection of critical information infrastructure, and formulate proposals for increasing the effectiveness of the national information security system. Special attention is paid to improving interdepartmental interaction in the structure of the defense sector of Ukraine.

Summary of the main material. In modern conditions of globalization and the rapid development of digital technologies, the issue of information security has become one of the key problems of public administration and national security. Ukraine, being in conditions of a prolonged hybrid war, is faced with an unprecedented level of cyber threats, disinformation campaigns, attempts to influence public sentiment and disrupt the functioning of critical infrastructure. Information security has long ceased to be an exclusively technical task, but is perceived as a strategic component of the defense sector, the effectiveness of which determines the stability of the state in conditions of military and information-psychological threats.

At the same time, it should be noted that modern military conflicts are increasingly taking on the characteristics of the so-called “fifth generation wars”, where information and psychological operations, cyber sabotage and campaigns of influence on mass consciousness play a decisive role. In such conditions, even the most advanced weapons and classic defense structures may be vulnerable to powerful information strikes. That is why the integration of cyber and information security into the country’s defense architecture is a desirable and necessary prerequisite for national survival and development in the 21st century.

Protecting the state's information space requires not only technical solutions and modern equipment, but also a systematic approach to the formation of appropriate state policy, the creation of an effective regulatory framework, the development of human potential and raising public awareness of the risks of information warfare. Every year, information attacks become more complex, aimed at undermining citizens' trust in government bodies, discrediting the country's defense capabilities, manipulating public opinion and increasing internal instability. In such conditions, the state has to constantly adapt to new challenges and create mechanisms for rapid response to threats that arise in the digital environment.

Special attention needs to be paid to the coordination of actions of all state bodies involved in ensuring information and cyber security, as well as the development of interaction with civil society and international partners. An effective information security system should take into account not only the protection of state information resources and critical infrastructure, but also the improvement of the information culture of the population, the development of media literacy and the formation of the ability to resist disinformation campaigns. Modern wars are increasingly being transferred to the information-psychological plane, and that is why it is difficult to overestimate the importance of a safe and stable information space for preserving state sovereignty and national identity.

Today, information security determines not only the level of a country's defense capability, but also the level of its political stability, democracy, and capacity for sustainable development. This is a complex multidimensional category that covers issues of legislative regulation, technical solutions, management approaches, and the formation of social values. Therefore, the relevance of research into the problems of ensuring information security determines the need to improve existing protection mechanisms, integrate national efforts in this area, and implement the best international practices. The success of the state in countering hybrid threats directly depends on how holistic and effective the information security system will be built at all levels – from strategic to local.

Information security as a component of national security is today a key priority of state policy. The rapid spread of digital technologies and the transition of many social processes to cyberspace have presented the state with new challenges and threats that require an adequate legal, organizational and technical response. In Ukraine, which is under constant pressure from hybrid aggression, the issue of ensuring the security of the information space has become extremely urgent, because the stability of the domestic political situation, the preservation of state sovereignty and democratic institutions depend on the effectiveness of countering information-psychological and cyber threats.

Information security is defined as the protection of the information environment of the state, society and the individual from external and internal threats that may harm the interests of Ukraine. According to scientists, modern challenges are complex in nature – they combine cyber attacks, disinformation campaigns, manipulation of public opinion and attempts to undermine critical infrastructure facilities. The development of digital technologies has led to the emergence of fundamentally new threats: cybercrime has acquired a transnational nature and is capable of causing significant harm to the interests of the individual, society and the state as a whole [4].

These threats cannot be neutralized solely by technical measures. They require a systemic approach, namely: creating a regulatory framework, training personnel, introducing innovative technologies, raising the level of culture, and ensuring safe behavior of citizens in the digital environment. Researchers note that information security is a component of defense policy and an important factor in democratic development, as it ensures the publicity and transparency of government, protects citizens from manipulation and propaganda, and maintains a high level of trust in state institutions [4].

In modern conditions, information security has become not only a technical challenge, but also a strategic component of defense capability. The Ukrainian state is experiencing new cyber, informational and psychological attacks, which the aggressor directs to undermine trust in national institutions and increase social tension. Counteracting these threats requires the creation of an effective cyber defense system integrated into the state's defense architecture.

According to P. M. Snitsarenko, cyber defense should not be considered as a separate area, but as an integral part of the state defense sector with a clearly defined structure, components, and implementation stages [1]. The scientist substantiated the essence of cyber defense, outlined the elements of the nationwide defense system and the relationship between them, which constitutes an important basis for our research.

Cyber defense should also be considered as an interdisciplinary field that brings together specialists from different fields: information technology, law, sociology, psychology, and military affairs. Only their coordinated work will allow creating an effective and adaptive model of response to constantly changing threats. The success of such teams depends on flexibility, interagency cooperation, and a shared strategic vision.

One of the promising areas of cyber defense development is the creation of integrated incident response centers operating at the interface of the defense and civilian sectors. Such centers are able to provide round-the-clock monitoring of the information space, quickly detect and localize cyberattacks, conduct incident investigations, and coordinate actions between agencies and private structures. The experience of European countries and the United States demonstrates that it is the integration of state and non-state resources under a single command that provides maximum protection against hybrid threats [9, 10].

The modern model of cyber defense, according to P. M. Snitsarenko, should cover the protection of information resources and the prevention of unauthorized access to them, provide for active actions in response to cyber threats, which is part of the military-political strategy of the state. The author emphasizes the need for a clear normative definition of the term "cyber defense", which will allow the systematization of the functional responsibilities of national security and defense entities in the digital space, the formation of an interdepartmental division of powers and ensure coordination of actions within a single state mechanism [5, 1]. This position fully correlates with the needs of Ukraine in conditions of constant hybrid aggression, when the information and communication space has become one of the key arenas of confrontation.

S. A. Zaporozhets also draws attention to the relevance of forming an effective interagency mechanism for cyber defense. In his study, he emphasizes that information influences and cyber attacks in the conditions of hybrid warfare are a means of demoralizing the population and an effective tool for destabilizing the defense sector. Therefore, the formation of a cybersecurity system requires a comprehensive approach - combining the resources of state structures, armed forces, special services and civil society. Such a model will allow for effective coordination of actions in the event of a large-scale cyber attack, quickly localize the consequences and restore the operability of critical infrastructure [3].

The concept of cyber resilience is becoming particularly relevant - the ability of the state, its institutions and civil society to withstand, adapt and respond to cyberattacks with minimal losses. The article by P. M. Snitsarenko, Y. M. Sarychev, V. A. Gordiychuk and V. I. Hrytsyuk substantiates that the development of cyber resilience is a key element of the strategy for countering hybrid threats. In their opinion, resilience is determined by the availability of technical means of protection, personnel training, the availability of clear response algorithms, international support and the level of trust of citizens in state institutions. The authors recognize the important role of cyber volunteer associations, which at the beginning of the full-scale aggression of the Russian Federation to a large extent compensated for the weakness of the state cyber defense system, and emphasize the need to institutionalize such cooperation [6].

Within the framework of building sectoral cyber resilience, it is also important to focus on the educational component. In the context of rapid technological development and changes in the nature of threats, professional training of cyber defense specialists should take into account the latest trends, be adaptive, interdisciplinary and based on both theoretical knowledge and practical skills. Education in the field of information security should not be limited to narrow technical specializations, but should include knowledge of information policy, psychology, law and management. Such an approach will enable the training of specialists capable of working at the intersection of technology and national security, which is critically important for the defense sector.

Conclusions

Summarizing the above, it can be argued that an effective model of information security as a component of the defense sector of Ukraine should be based on the following key principles:

1) regulatory certainty and coordination of actions of all involved entities;
2) development of technical infrastructure and operational response;
3) systematic education and training of specialists;
4) development of cyber resilience, covering both technological and social factors.

The success of the state in countering modern threats in the information space depends on the ability to integrate these elements into a single state cyber defense system. Given the experience of recent years, in particular 2022–2024, when cyberattacks became an integral part of military operations, it is obvious that building a strong information security system is not only a strategic goal, but a matter of the state's survival in the conditions of hybrid warfare.

Scientific research will be directed towards further investigation of the threats posed by telecommunications technologies.

References

1. Snitsarenko P. M. (2024). *Kiberoborona Ukrainy yak skladova oborony derzhavy* [Cyber defense of Ukraine as a component of state defense]. *Nauka i oborona*, no. 4, pp. 40–48 [in Ukrainian].

2. *Zakon Ukrainy "Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy" № 2163-VIII* [Law of Ukraine about the Basic Principles of Ensuring Cybersecurity of Ukraine activity no. 2163-VIII]. (2017, 5 October). Retrieved from: https://zakon.rada.gov.ua/laws/show/2163-19 (accessed 2 August 2025) [in Ukrainian].

3. Zaporozhets S. A. (2019). *Stan zabezpechennia informatsiinoi bezpeky Ukrainy u viiskovii sferi v umovakh hibrydnoi viiny* [The state of ensuring information security of Ukraine in the military sphere under conditions of hybrid warfare]. *Politolohichnyi visnyk*, no. 83, pp. 16–25 [in Ukrainian].

4. Koval H. V., Kobko Ye. V., Kobko V. A. (2022). *Informatsiina bezpeka v systemi natsionalnoi bezpeky: administratyvno-pravovyi aspekt* [Information security in the national security system: administrative and legal aspect]. *Visnyk KhNTU. Publichne upravlinnia ta administruvannia,* vol. 1 (80), pp. 103–108 [in Ukrainian].

5. Snitsarenko P. M. (2024). *Pro sutnist kiberoborony yak vydy viiskovykh dii* [On the essence of cyber defense as a type of military action]. *Nauka i oborona,* no. 3, pp. 45–54 [in Ukrainian].

6. Snitsarenko P. M., Sarychev Yu. O., Hordiichuk V. V., Hrytsiuk V. V. (2023). *Kiberstiikist v umovakh viiskovoi ahresii RF: dosiahnennia Ukrainy ta problemni pytannia* [Cyber resilience under conditions of russian military aggression: Ukraine's achievements and problematic issues]. *Zbirnyk naukovykh prats Tsentru viiskovo-stratehichnykh doslidzhen Natsionalnoho universytetu oborony Ukrainy,* no. 3, pp. 31–38 [in Ukrainian].

7. *Ukaz Prezydenta Ukrainy Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 veresnia 2020 roku "Pro Stratehiiu natsionalnoi bezpeky Ukrainy" № 392/2020* [Decree of the President on the Decision of the National Security and Defense Council of Ukraine of September 14, 2020 "On the National Security Strategy of Ukraine" activity no. 392/2020]. (2020, 14 September). Retrieved from: https://surl.lt/tvhhyj (accessed 2 August 2025) [in Ukrainian].

8. *Ukaz Prezydenta Ukrainy Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 19 liutoho 2021 roku "Pro stan vykonannia rishen Rady natsionalnoi bezpeky i oborony Ukrainy" № 77/2021* [Decree of the President of Ukraine on the implementation of the decisions of the National Security and Defense Council of Ukraine dated July 19, 2021 "On the state of implementation of the decisions of the National Security and Defense Council of Ukraine activity no. 77/2021]. (2021, 26 February). URL: https://zakon.rada.gov.ua/laws/show/77/2021#Text (accessed 2 August 2025) [in Ukrainian].

9. NATO (2024). Allies agree new NATO Integrated Cyber Defence Centre. Retrieved from: https://surl.li/dhyhvk (accessed 2 August 2025) [in English].

10. Cybersecurity and Infrastructure Security Agency (CISA) (2025). The National Cyber Incident Response Plan (NCIRP). Retrieved from: https://surl.lt/noouvk (accessed 2 August 2025) [in English].

The article was submitted to the editorial office on 16 August *2025*

УДК: 355.45:004.056(477)

В. В. Мальцев, В. І. Тробюк, І. О. Герасименко

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК СКЛАДОВА СЕКТОРУ ОБОРОНИ УКРАЇНИ

Сучасні війни дедалі більше переносяться в інформаційно-психологічну площину. Україна, перебуваючи в умовах тривалої гібридної агресії Росії, зазнає масштабних кібератак, стикається з дезінформаційними кампаніями та спробами підриву довіри до державних інституцій і суспільної єдності. Відповідно до таких викликів змінюється й розуміння ролі інформаційної безпеки, яка стала ключовим елементом оборонної політики держави та важливою умовою її виживання й розвитку.

У статті увага зосереджена на визначенні місця інформаційної безпеки у секторі оборони України та її значенні для захисту суверенітету й демократичних інститутів. Окреслюються особливості сучасних загроз: кібердиверсії проти критичної інфраструктури, маніпуляції громадською думкою, дискредитаційні кампанії проти Збройних Сил та органів влади. У такій ситуації класичне озброєння та оборонні структури без потужного захисту інформаційного простору залишаються вразливими, оскільки протистояння ворогу потребує як сучасних технічних рішень, так і злагоджених дій усіх державних інституцій, взаємодії з громадянським суспільством та міжнародними партнерами.

Розглянуто поняття кіберстійкості як спроможності держави, інституцій та громадян протидіяти загрозам і відновлювати функціонування після атак. Проаналізовано досвід створення інтегрованих центрів реагування на інциденти, що поєднують ресурси державного і приватного секторів, забезпечуючи оперативний моніторинг та координацію дій.

Акцентовано на ролі підготовки фахівців із кіберзахисту на міждисциплінарній основі та підвищенні рівня медіаграмотності населення, що позитивно впливає на стійкість суспільства до інформаційних впливів.

Інформаційна безпека в умовах гібридної війни є не лише технічним чи організаційним завданням, а й стратегічною складовою оборони держави, що поєднує політичні, соціальні та технологічні чинники. Формування ефективної системи інформаційної безпеки та кібероборони визначає успішність України у протидії сучасним загрозам і збереженні державності.

Ключові слова*: інформаційна безпека, гібридна війна, кібероборона, критична інфраструктура, кіберстійкість, медіаграмотність.*

Maltsev Vitalii – Candidate of Law, Senior Researcher, Associate Professor of the Department of State Security, Kyiv Institute of the National Guard of Ukraine
https://orcid.org/0009-0003-3520-1152

Trobiuk Volodymyr – Candidate of Military Sciences, Professor, Head of the Educational and Scientific Center for the Organization of the Educational Process, National Academy of the National Guard of Ukraine
https://orcid.org/0000-0002-3248-2935

Herasymenko Ihor – Graduate, Kiev Institute of the National Guard of Ukraine
https://orcid.org/0009-0005-1362-3236