UDC.342.9.
DOI https://doi.org/10.24144/2307-3322.2026.93.3.51

ENSURING CYBERSECURITY AS A COMPONENT OF NATIONAL SECURITY: CURRENT CHALLENGES AND MECHANISMS FOR COUNTERING THREATS

Tsomenko A.V.,
PhD, Assistant Professor, Department of Administrative Law and Process
Educational and Scientific Institute of Law of
Taras Shevchenko National University of Kyiv
ORCID: 0000-0002-5615-7838

Tsomenko A.V. Ensuring cybersecurity as a component of national security: modern challenges and mechanisms for countering threats.

Cybersecurity is an integral part of national security, especially in the context of rapid digitalization and the growth of cyber threats. Currently, Ukraine faces numerous challenges, in particular, cyber attacks on information systems and personal data of citizens. Such attacks have negative consequences, leading to political destabilization, economic losses, as well as violations of the rights of individuals. In the context of globalization and the integration of digital technologies into all aspects of public life, the issue of cybersecurity is becoming even more relevant, as the state is increasingly faced with cyber threats, which has consequences for national security.

The relevance of studying this problem is due to the need to develop effective mechanisms for countering cyber threats, improve the legal framework, strengthen international cooperation, introduce modern cyber protection technologies, and increase the level of digital awareness of the population. In this context, the analysis of theoretical approaches to defining cybersecurity, as well as the study of the legal definition of this category in national legal systems, is particularly important.

The article examines the main theoretical approaches to defining cybersecurity, which reflect the diversity of views of domestic scientists on this problem. In particular, it emphasizes the importance of defining clear mechanisms for legal regulation of cybersecurity, which allow for a prompt response to new cyber threats and ensure the stability of state registries.

One of the important results of the study is the author's definition of the category «right to cybersecurity «. The article also examines the challenges that Ukraine faced in the context of Russian aggression, in particular in the context of attacks on state registries. Cyberattacks that were directed at critical information systems of the state were aimed at destabilizing government bodies and disrupting access to important registries and databases, which creates risks for national security.

The article pays special attention to the need to protect the information of particularly vulnerable categories of persons, in particular, military personnel, veterans, prisoners of war, and internally displaced persons.

Key words: cybersecurity, national security, armed aggression, information and telecommunications technologies, personal data, ensuring the protection of vulnerable categories of persons.

Цьоменко А.В. Забезпечення кібербезпеки як складової національної безпеки: сучасні виклики та механізми протидії загрозам.

Кібербезпека є невід'ємною складовою національної безпеки, особливо в умовах стрімкої цифровізації та зростання кіберзагроз. Нині, Україна стикається з численними викликами, зокрема, з кібератаками на інформаційні системи та персональні дані громадян. Такі атаки несуть негативні наслідки, призводячи до політичної дестабілізації, економічних втрат, а також порушення прав приватних осіб. В умовах глобалізації та інтеграції цифрових технологій до всіх суспільного життя, питання кібербезпеки набуває ще більшої актуальності, оскільки держава все частіше стикаються з кіберзагрозами, що має наслідки для національної безпеки.

Актуальність дослідження цієї проблеми зумовлена необхідністю розробки ефективних механізмів протидії кіберзагрозам, удосконалення правової бази, посилення міжнародної

співпраці, впровадження сучасних технологій кіберзахисту та підвищення рівня цифрової обізнаності населення. У цьому контексті особливо важливим є аналіз теоретичних підходів до визначення кібербезпеки, а також дослідження легального визначення цієї категорії в національних правових системах.

У статті досліджуються основні теоретичні підходи до визначення кібербезпеки, які відображають різноманітність поглядів вітчизняних науковців на цю проблему. Зокрема, підкреслюється важливість визначення чітких механізмів правового регулювання кібербезпеки, які дозволяють оперативно реагувати на нові кіберзагрози і забезпечити стабільність діяльності державних реєстрів.

Одним з важливих результатів дослідження є авторське визначення категорії «право на кібербезпеку». Також у статті розглядаються виклики, з якими стикалася Україна в умовах російської агресії, зокрема у контексті атак на державні реєстри. Кібератаки, що були спрямовані на критичні інформаційні системи держави, мали на меті дестабілізацію органів влади та порушення доступу до важливих реєстрів і баз даних, що створює ризики для національної безпеки.

Окрему увагу в статті приділено необхідності захисту інформації особливо вразливих категорій осіб, зокрема, військовослужбовців, ветеранів, полонених, внутрішньо-переміщених осіб .

Ключові слова: кібербезпека, національна безпека, збройна агресія, інформаційно-телекомунікаційні технології, персональні дані, забезпечення захисту вразливих категорій осіб.

Statement of the problem. The issue of cybersecurity is multifaceted and complex, since, in addition to technical and technological aspects, it covers a wide range of legal, political, economic, social, psychological and cultural dimensions. Each of these aspects has a significant impact on the formation, development and evolution of both general and specific problems in the field of cybersecurity . In particular, legal issues include ensuring the legal protection of information resources, regulating access to personal data and mechanisms for their protection, as well as adapting national legislation to the requirements of modern cyber threats.

The purpose of the scientific article is research into the doctrinal and practical aspects of the category of cybersecurity as a component of national security in the face of modern challenges and analysis of mechanisms for countering such threats.

The state of development of the problem. The mentioned problem has been given sufficient attention in the scientific works of domestic scientists, among whom it is worth highlighting O. Baranov, A. Bilyuga, G. Bondar, S. Globenko, V. Yemelyanov, O. Kret, O. Kundeus, S. Polyakova, O. Stepko, P. Sumin, V. Furashev, V. Yashchuk and others.

Presentation of the main material. In the conditions of the rapid development of information and telecommunication technologies, which have covered all spheres of public life and significantly contribute to its simplification on the one hand. However, such changes also create new challenges and risks for individuals, in particular in the field of public administration. Thus, the strengthening of digitalization processes in the state, in particular the creation and functioning of state electronic registers, on the one hand, ensures a more effective, fast and convenient implementation of the rights and legitimate interests of individuals, but on the other hand, also generates a number of significant risks. Among them, a special place is occupied by threats in the field of cybersecurity and protection of data stored in registers, including personal data, which is becoming exceptionally relevant in the conditions of Russian armed aggression and the growth of cyber threats.

In particular, O.A. Baranov considers it as a component of information security in the context of the use of computer systems and telecommunication networks. Alternatively, it is the protection of critically important interests of an individual, society and the state in the conditions of the use of these technologies, aimed at minimizing damage from incomplete, untimely and unreliable use of information, negative information impact, as well as unauthorized data distribution. In turn, V.M. Furashev characterizes cybersecurity primarily as the ability of individuals, communities and governments to prevent and mitigate negative consequences or manipulation of information, whether intentional or unintentional [3, p. 94].

At the legal level, the legislator also defined the category of cybersecurity as the protection of the vital interests of a person and citizen, society and the state when using cyberspace, which ensures the sustainable development of the information society and the digital communication environment, as well as the timely detection, prevention and neutralization of real and potential threats to the national security of Ukraine in cyberspace [4].

At the same time, in our opinion, the above definition is quite broad and requires clarification for a clearer understanding of the essence of this category. This definition focuses on general categories, such as «protection of vital interests» of a person, society and the state, but does not focus on what rights and interests can be violated, as well as how these violations can occur, in particular, it is not stated that we are talking about the protection of information , personal data , information resources and information and telecommunications systems . Without specifying these aspects, cybersecurity appears more as an abstract concept of «security» than as a clearly defined legal category.

In a situation of ongoing armed aggression against Ukraine, the emphasis is on national security in the context of cyber threats is quite justified and relevant. However, this approach does not fully correspond to modern European and international trends, where cybersecurity is increasingly viewed through the prism of human rights, in particular the right to privacy, protection of personal data and informational self-determination.

Taking into account the above, it seems appropriate to supplement this law with the category of "right to cybersecurity " as the right of an individual, guaranteed by the state, to protect information about him or her stored on electronic media and information and communication networks, the illegal access, leakage, loss or transfer of which may lead to a violation of human rights and freedoms, primarily the right to privacy, as well as a set of legal, organizational and technical measures aimed at preventing such violations in peacetime and armed aggression.

From a practical point of view, the need to strengthen cybersecurity in Ukraine was emphasized even before the full-scale invasion. Scientists emphasized the need to continue developing a national model of cyber defense, using the best practices of NATO and EU countries. Given the impossibility of completely eliminating cyber risks, it is important to focus on comprehensive measures: improving legislation in accordance with modern challenges, international coordination of efforts, technology exchange and financial support from partners. Since Ukraine has become one of the main targets for cyber attacks, especially from Russia, it is critically necessary to invest in advanced cyber defense technologies, strengthen the cyber resilience of critical infrastructure and develop new mechanisms to counter modern threats [2, p. 515].

Strengthening cybersecurity in Ukraine has become extremely urgent in connection with Russian armed aggression, as cyberspace has become another battlefield alongside traditional military operations. The aggressor systematically carries out cyberattacks on Ukrainian critical infrastructure, state institutions, the financial sector, and the media space with the aim of destabilizing, destroying data, spreading disinformation, and influencing public opinion. The occupiers are actively using cyberattacks as an element of hybrid warfare.

In this regard, it is worth mentioning the large-scale cyberattack in December 2024 on the state registers of Ukraine, carried out by Russian hackers, which is another confirmation of the aggression of the occupying state in cyberspace. As a result of the attack, the work of critically important state infrastructure was temporarily suspended. Its main goal was to destabilize the country, create chaos and undermine trust in state institutions. [5].

The above-mentioned cyberattack led to the shutdown of the state registers of the Ministry of Justice, which are the basis for legal and notarial transactions. The work of such critically important registers as the State Register of Civil Status Acts of Citizens, the Unified State Register of Legal Entities, Individual Entrepreneurs and Public Organizations, the State Register of Real Rights to Real Estate and many others was disrupted. Problems also affected the «Diya» service, although there was no direct data leak from it.

Despite official assurances that there was no data leak, Russian hackers claimed to have stolen and deleted over 1 billion rows of data, including data stored in Poland. Even if these claims are exaggerated, the fact of the intrusion into the system itself calls into question the security of the data stored in the registries.

It is worth noting that this is not the first large-scale cyberattack: a similar one occurred a week before the full-scale invasion in 2022, when hackers attacked government websites and the «Diya» system, which indicates a systemic cyberwar that the aggressor state is waging against Ukraine.

In this context, given the large-scale cyberattacks on state registers of Ukraine, the justification of the critical importance of ensuring stability and a high level of data security in state information systems, one of the main aspects of which is the development of special approaches to protecting, in particular, the personal data of individuals, including vulnerable categories, such as military personnel, prisoners of war, internally displaced persons, etc.

Particular attention should be paid to registries containing data on vulnerable categories of the population, such as military personnel and veterans. For example, the “Reserve+” and “E-Veteran” systems store confidential information on individuals who have participated in combat operations or are in the reserve. Therefore, the leakage of this information from the above systems can have serious consequences for both individuals and national security.

The next cyberattack in 2025 caused a number of serious problems in the functioning of the judicial system. As a result of the attack, the registration of procedural documents received by the courts of cassation was suspended, which made it difficult to submit documents electronically. In addition, the automated distribution of cassation appeals to judges became impossible, which significantly slowed down the process of considering cases and created additional difficulties for the participants in the trial. Another serious problem was the malfunction of the court’s document management program, which made it impossible to properly maintain court documents and process them. In addition, the ESITS «electronic court» subsystem, in particular, the videoconferencing system , which is usually used for conducting remote court sessions, especially in criminal and administrative cases, stopped working. The final consequence of the cyberattack was the inability to enter court decisions into the Unified Register of Court Decisions, which made it difficult to access information on decisions made [6].

The consequences of these attacks emphasized the urgent need to strengthen the cyber defense of public institutions, and the corresponding legislative response was the adoption of the National Plan for Response to Cyber Incidents, Cyber Attacks, and Cyber Threats, which defined general procedures and mechanisms for responding to cyber threats at the state level.

The main objective of this Plan is to ensure effective coordination and interaction between all entities of the national system of response to cyber incidents , cyber attacks and cyber threats, as well as between entities providing cybersecurity. These entities include state authorities, local governments, critical infrastructure operators, owners and managers of critical information infrastructure facilities and other organizations involved in ensuring cybersecurity in accordance with the legislation.

Within the framework of this plan, special attention is paid to defining clear roles of each entity within the framework of the functioning of the national response system. This includes both legal and organizational and technical measures aimed at ensuring the rapid detection, identification and analysis of cyber incidents and cyber attacks. Prompt information about such threats is one of the key elements that allows reducing their impact and maintaining the stability of the national cyber infrastructure.

The national response system is defined as a set of legal, organizational and technical measures, including the identification of cyber threats, analysis of detected incidents and their consequences, as well as taking necessary measures to minimize these consequences, including eliminating vulnerabilities in information systems and restoring their stable and reliable functioning after cyber attacks or cyber incidents. Such a system allows the state and other cybersecurity entities respond promptly to emerging threats, while ensuring the integrity and security of critical information resources and infrastructures.

In addition, an important aspect is the functioning of a national system for exchanging information on cyber incidents, cyber attacks and cyber threats, which allows for interaction between various cybersecurity actors at the national level and timely exchange of important information to increase the effectiveness of response and prevention of new cyber threats. Such integration of information flows between different bodies and institutions helps to create a single, coherent system capable of quickly and effectively responding to complex cyber incidents in a rapidly changing cyberspace [7].

Conclusions. Therefore, cybersecurity not only ensures the stability of the functioning of information systems, but also acts as an important element of national security, since cyber threats can have strategic consequences for the economic, political, and social stability of the state.

In the event of armed aggression, when cyberattacks are part of a complex aggression, it is important to have clear and effective mechanisms to counter such digital threats. Such mechanisms should include several key components:

Firstly, the regulatory component, which provides for a timely legislative response to the public need to ensure cyber protection. This includes the adoption and adaptation of relevant regulatory legal acts that regulate cybersecurity issues at all levels, ranging from general provisions to specialized laws and by-laws that meet the requirements of the rapidly changing technological situation. Legislative initiatives must be timely in order to promptly respond to new threats and technological challenges in cyberspace, thereby ensuring legal protection for both the state and citizens.

Secondly, the technical component, which includes the availability of appropriate technical capabilities to prevent, detect and protect against cyber threats. This includes the development, implementation and continuous improvement of cyber protection systems, in particular, encryption technologies, monitoring and response systems for cyber incidents, as well as the creation and maintenance of technical infrastructures to ensure the protection of critical information resources.

Third, human resource capacity, especially within public authorities, is critical for the successful implementation of a cyber defense strategy. Training qualified personnel capable of effectively responding to cyber threats.

REFERENCES:

1. Biliuha A.D. Kiberzbroia: suchasni zahrozy natsionalnii bezpetsi ta shliakhy protydii [Cyberweapons: modern threats to national security and ways to counter them. Science and Defense]. *Nauka i oborona*. 2021. № 2. S. 42-49 . URL: https://nio.nuou.org.ua/article/view/239047/281781.
2. Iemelianov V.M., Bondar H.L. Kiberbezpeka yak skladova natsionalnoi bezpeky ta kiberzakhyst krytychnoi infrastruktury Ukrainy [Cybersecurity as a component of national security and cyber protection of critical infrastructure of Ukraine. Public administration and regional development]. *Publichne upravlinnia ta rehionalnyi rozvytok*. 2019. № 5. S. 493-523 . URL: irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILEDOWNLOAD=1&Image_file_name=PDF/purr_2019_5_4.pdf
3. Kret O., Kret R., Kundeus O. Systema kiberbezpeky yak skladova natsionalnoi bezpeky [Cybersecurity system as a component of national security]. *Hrani. Politolohiia*. 2024. № 5(27). S. 92-99 . URL: https://grani.org.ua/index.php/journal/article/view/2092.
4. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy vid 05.10.2017 № 2163-VIII. *Vidomosti Verkhovnoi Rady Ukrainy* [On the basic principles of ensuring cybersecurity in Ukraine: Law of Ukraine dated 05.10.2017 No. 2163-VIII]. 2017. № 45. St. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text .
5. Rosiiski khakery zlamaly derzhavni reiestry Ukrainy. Shcho vidomo [Russian hackers hacked state registers of Ukraine. What is known] (2024). URL: https://www.bbc.com/ukrainian/articles/c7ve1298ndgo .
6. Verkhovnyi Sud zaznav masshtabnoi kiberataky [The Supreme Court suffered a large-scale cyberattack]. *Sudovo-yurydychna hazeta*. URL: https://sud.ua/uk/news/publication/333430-verkhovniy-sud-zaznav-masshtabnoyi-kiberataki-scho-vidomo .
7. Deiaki pytannia reahuvannia na kiberintsydenty, kiberataky ta kiberzahrozy: Postanova Kabinetu Ministriv vid 26 lystopada 2025 r. № 1533 [Some issues of responding to cyber incidents, cyber attacks and cyber threats: Resolution of the Cabinet of Ministers of November 26, 2025 No. 1533]. URL:https://zakon.rada.gov.ua/laws/show/1533-2025-%D0%BF.

Дата першого надходження рукопису до видання: 3.02.2026
Дата прийняття до друку рукопису після рецензування: 20.02.2026
Дата публікації: 5.03.2026