Veritas: Legal and Psychological-Pedagogical Research

2025. Vol. 1, No. 1

Legal Sciences

UDC 342.9:004.056.5

Information Security in the Context of National Security: Legal Mechanisms for Protecting State Information Resources

Volodymyr Ortynskyi

Professor, Honoured Lawyer of Ukraine, Lviv Polytechnic National University, Lviv, Ukraine,
volodymyr.l.ortynskyi@lpnu.ua, ORCID: 0000-0001-9041-6330

http://doi.org/

Abstract. The purpose of the article is to analyze the mechanisms of ensuring information security in Ukraine, including legal, technical, organizational, preventive, control, and sanction components. Special attention is paid to identifying the strengths and weaknesses of these mechanisms in the context of modern information challenges.

The article identifies the main elements of information security mechanisms, their functions, and interconnections. The legal mechanism provides a regulatory framework but contains outdated provisions requiring updates. The technical mechanism forms the technological basis of security but suffers from insufficient modernization. The organizational and legal mechanism focuses on coordinating state bodies' actions, but poor communication with the private sector limits its effectiveness. The control mechanism ensures monitoring compliance with security standards, yet technical and staffing deficiencies remain a challenge. Preventive measures, including personnel training and public awareness, are underdeveloped. The sanction mechanism establishes legal accountability, but its practical implementation faces significant challenges.

A comprehensive approach is to evaluate the effectiveness of information security mechanisms has been developed, to consider their structural interaction and functional interconnections. Special attention is given to integrating various components of the system, including legal, technical, and organizational mechanisms, to ensure their coordinated functioning. Recommendations have been proposed for modernizing the existing mechanisms by implementing advanced technologies, updating the regulatory framework, and aligning with international standards. Additionally, the need to enhance coordination between state authorities and the private sector in the field of cybersecurity has been substantiated.

The study's findings can be used to improve the national information security system, develop new strategic documents, and implement innovative technologies in the field of information protection.

Keywords: information security, mechanisms, legal protection, cybersecurity, control measures, sanction mechanism, preventive measures.

Introduction

In our opinion, in the context of global digitalization, which has become an inevitable part of the modern world, information security issues are gaining special importance. In particular, the state's information resources (as a strategically important

Suggested Citation:
Ortynskyi, V. (2025). Information Security in the Context of National Security: Legal Mechanisms for Protecting State Information Resources. *Veritas: Legal and Psychological-Pedagogical Research*, 1(1), 1–9. DOI: doi.org/

Journal homepage: https://science.lpnu.ua/veritas
Article history: Received: 06.03.2025. Revised: 20.03.2025. Accepted: 30.05.2025.

element of the national infrastructure) are becoming the object of continuous threats, which obviously affects the stability of the national security system. We believe that in the context of the intensive development of information technologies, ensuring effective protection of state information resources requires not only technological innovations, but also clearly defined and effective legal mechanisms that regulate this issue.

In our opinion, legal instruments should serve as the foundation on which the system of countering threats to information security is built. It is worth noting (and this is quite obvious) that any state that seeks to preserve sovereignty and national stability is forced to adapt legislative norms to the dynamically changing conditions of the information environment. At the same time, the analysis of current legal mechanisms demonstrates the presence of not only achievements, but also certain problems associated with the regulation of this complex issue.

Literature Review

In our opinion, the study of information security issues has become one of the priorities of scientific thought in Ukraine in recent years, which is due to both global information challenges and the influence of Russian aggression. Analysis of research in this area allows us to outline the main trends and approaches that shape the modern discourse.

A significant contribution to the study of the current state of information security was made by V. Vyzdryk and O. Melnyk, who focus on its general characteristics, as well as the problems of implementing legal mechanisms for information protection in Ukraine [1, pp. 196–202]. In their opinion, the formation of an effective information security system is possible only under the conditions of a combination of technological and legal instruments.

The results of the research of D. V. Smotrych and L. Brailko, who in their work consider the impact of martial law on information security and emphasize the importance of its provision for maintaining state sovereignty [2, pp. 121–127], are also quite valuable.

M. V. Goncharov in his study analyzes the concept of "information security", outlining its legal and technological aspects, which allows us to better understand the essence of this phenomenon [3, pp. 34–37]. His work complements the conclusions of G. A. Goncharenko, who focuses on the distinction between the concepts of "information security" and "cybersecurity", emphasizing their differences in legal regulation [4, pp. 466–471].

The issue of information security at the organizational level was studied by L. V. Maznyk and O. I. Dragan, who emphasize its role in forming a positive image of the employer, which is especially relevant for modern business [5, pp. 39–44].

Of considerable scientific interest is the work of O. Myslyva, who analyzes aspects of information security in temporarily occupied territories. In her opinion, special attention should be paid to maintaining the information stability of the population [6, pp. 137–138].

Concluding the review, it is worth noting the study of E. O. Solomin, who examines the issue of information security in wartime, in particular the impact of interventions in the media environment on the formation of public opinion. He emphasizes the importance of information hygiene and strategies for countering disinformation [7, pp. 40–47].

Taking into account the above, it can be argued that modern research on the issues of information security is multi-vector and covers various aspects – from conceptual definitions to applied issues of information protection in wartime. Such a comprehensive approach contributes to the formation of effective mechanisms for countering threats to the information space of Ukraine.

Purpose

Taking into account the above, the main purpose of this article is to study the legal mechanisms for protecting state information resources in the context of ensuring national security. It seems that this issue is extremely relevant, since the imperfection of legal regulation or the absence of clear procedures can lead to critical consequences for the state.

The article will analyze key legislative acts regulating the sphere of information security, identify existing gaps and propose possible directions for improving the legal mechanisms for protecting state information resources. In our opinion, such an approach allows for a comprehensive assessment of the issues and the formulation of practical recom-

mendations aimed at strengthening the information security of Ukraine.

Thus, solving the above problem is not only a legal, but also a strategic task for any state that seeks to maintain stability in the changing conditions of the globalized world.

Methodology

This study uses a thorough method that incorporates both theoretical and practical investigation. Within the theoretical section, the author examines the main legislative acts regulating the sphere of information security, such as the Law of Ukraine "On National Security of Ukraine", the Law of Ukraine "On Information", the Law of Ukraine "On the Fundamentals of Ensuring Cybersecurity in Ukraine".

The empirical part of the study identifies existing gaps and suggests possible directions for improving legal mechanisms for protecting state information resources.

In addition, the work used the monitoring and evaluation method to analyze the effectiveness of the control mechanism, including state oversight, audit of information systems, and measures aimed at increasing the cyber protection of critical infrastructure.

The conclusions formulate recommendations for strengthening information security in Ukraine.

Results and Discussion

The analysis proposed below is devoted to the regulatory, organizational and legal, protective and control mechanisms for ensuring information security as the basis of national security.

The structure of the regulatory mechanism for ensuring information security in Ukraine is based on the interaction of several key elements, which include the regulatory framework, institutional apparatus, preventive and sanctioning measures, as well as strategic planning.

The first element of this mechanism is the regulatory framework, which lays the foundations for the functioning of the information security system. For example, the Law of Ukraine "On National Security of Ukraine" stipulates that information security is a component of national security, and its provision involves coordination between executive bodies and the implementation of international security standards (Article 17) [8]. At the same time, the Law of Ukraine "On Information" contains the main concepts related to information and regulates the procedure for its protection, in particular for information with limited access (Articles 7, 10) [9].

The second component is the institutional structure, which includes state authorities responsible for implementing information security policy. For example, the Law of Ukraine "On the basic principles of ensuring cybersecurity of Ukraine" specifies the role of the Security Service of Ukraine, which coordinates between executive authorities in the field of cybersecurity (Article 8), as well as the functions of the State Service for Special Communications and Information Protection of Ukraine, which is responsible for the technical protection of information systems (Article 10) [10].

Preventive measures, as an important component of this mechanism, include the implementation of a monitoring and audit system. For example, Article 5 of the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine" stipulates the obligation of cybersecurity entities to regularly monitor the state of critical information infrastructure, as well as to develop and implement protective technologies [10].

The next element is the sanction mechanism, which provides for legal liability for violations in the field of information security. The Criminal Code of Ukraine defines the crimes related to unauthorized access to information systems (Article 361), violation of the procedure for processing information (Article 361-1), and disclosure of state secrets (Article 328) [14]. The sanctions provided for by these norms are aimed at ensuring a preventive effect and establishing liability for violations.

Strategic planning, as a subsystem of the regulatory mechanism, is aimed at long-term formation of information security policy. In particular, the Cybersecurity Strategy of Ukraine, approved by Decree of the President of Ukraine No. 447/2021, provides for the development of the national cybersecurity system by expanding international cooperation, introducing modern technologies, and strengthening human resources [15]. Similarly, the Information Security Strategy of Ukraine, approved by Decree No. 685/2021, defines measures to counter information aggression, in particular through streng-

thening state governance mechanisms and coordination between various information policy actors [16].

Thus, the structure of the regulatory mechanism for ensuring information security in Ukraine is multi-level and complex. Its effectiveness depends on clear coordination between the legislative framework, the activities of state institutions, the implementation of preventive and sanctioning measures, as well as the implementation of strategic initiatives that meet modern challenges in the field of information security.

In our opinion, organizational and legal mechanisms are a key element of the information security system, as they ensure the coordination of the activities of state bodies, their interaction with the private sector and the public, as well as the implementation of legal norms and strategic initiatives. An analysis of the current legislation of Ukraine allows us to identify the main aspects of these mechanisms.

According to the Law of Ukraine "On National Security of Ukraine", the main body ensuring the implementation of state policy in the field of information security is the National Security and Defense Council of Ukraine (NSDC). Its functions include preparing decisions on ensuring information security, which are approved by the President of Ukraine (Article 11) [8]. In addition, Article 17 of this law emphasizes the importance of coordination between executive authorities in implementing cybersecurity and information protection measures [8]. However, in our opinion, the mechanisms of such coordination remain insufficiently detailed, which leads to duplication of functions and inconsistency between different structures, such as the Security Service of Ukraine (SBU), the State Service for Special Communications and the Ministry of Digital Transformation. This, in our opinion, complicates the prompt response to threats, in particular in cyberspace.

The Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity in Ukraine" details the structure of bodies that manage cyber security. For example, the Security Service of Ukraine acts as a coordinator between the subjects of the national cybersecurity system, including state authorities, private enterprises and public organizations (Article 8). This law also defines the tasks of the State Service for Special Communications and Information Protection of Ukraine (Dershpetszvyazok), which is responsible for the development technical standards and the implementation of a technical system information protection (Article 10) [10].

A separate role in ensuring organizational and legal mechanisms is played by the Ministry of Digital Transformation of Ukraine, whose functions are related to the implementation of innovative technologies in the field of information security and the development of digital infrastructure. Although the specific provisions regarding the activities of this ministry are not directly regulated in the aforementioned laws, it operates within the framework of the general concept of digital transformation and cybersecurity defined in strategic documents [15; 16].

According to the Law of Ukraine "On State Secrets", the Ministry of Defense of Ukraine and other security sector bodies are obliged to ensure the preservation of information that constitutes a state secret, as well as to control access to it. Article 6 of this law states that law enforcement agencies are also involved in ensuring the protection of state secrets, which are responsible for detecting violations in this area [11].

The Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine" provides for the distribution of powers between the main entities of the national cybersecurity system (Articles 8, 10) [10]. At the same time, the lack of clear criteria for assessing the effectiveness of their activities makes it impossible to objectively analyze the implementation of the tasks set. For example, the SBU, which, according to the law, performs a coordinating role, often faces shortcomings in the exchange of information between state bodies and the private sector.

In the field of managing access to public information, the implementation of e-governance mechanisms regulated by the Law of Ukraine "On Access to Public Information" plays a special role. Article 13 of this law stipulates the obligations of state authorities to create conditions for transparent access to information, without violating security requirements [12].

Strategic planning in this area is ensured through the implementation of tasks defined in the Cybersecurity Strategy of Ukraine, which provides for the creation of a Cybersecurity Response Center (CERT-UA) and the integration of Ukraine into the international cybersecurity system [15]. In addition,

the Information Security Strategy of Ukraine pays special attention to issues of state management information processes and the implementation coordination mechanisms between state and non-state actors [16].

Thus, the organizational and legal mechanisms for ensuring information security in Ukraine have a multi-component structure that combines the functions of state bodies, preventive measures, educational activities and strategic planning. Their effective implementation allows creating a holistic system for protecting the information space that meets modern challenges.

The information security protection mechanism is an integral part of the national security system, aimed at preserving the integrity, confidentiality and availability of information resources. Its structure is based on a multi-level approach, which includes regulatory, technical, organizational and preventive components, each of which performs its specific function within the framework of the overall system.

The legal basis of the protection mechanism is laws and regulatory acts that establish the rules for processing, storing and transmitting information, as well as regulating the procedure for its protection. For example, the Law of Ukraine "On State Secrets" establishes procedures for classifying, declassifying and protecting state information. Article 6 of this law states that access to state secrets must be regulated by clear rules that take into account the level of secrecy of information and the status of the subject providing access [11].

The key role in the functioning of the protective mechanism is played by the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine", which provides for the introduction of monitoring and response systems for cyber threats, ensuring the protection of critical information infrastructure, and the introduction of modern security technologies. Article 5 of this law stipulates the obligation of cybersecurity entities to conduct regular audits of information systems and implement protection protocols to prevent unauthorized access or destruction of data [10]. The technical component of the protective mechanism is one of its most important elements, as it includes the implementation of encryption technologies, traffic filtering, data backup, and other means of cyber protection.

According to the Law of Ukraine "On Electronic Communications", telecommunications operators and providers are obliged to implement technical measures to protect their networks and ensure resilience to external threats, in particular through the installation of automatic detection and prevention systems for attacks (Article 22) [13].

The organizational component of the mechanism is based on the activities of authorized bodies, such as the Security Service of Ukraine, which coordinates work in the field of cyber defense, and the State Service for Special Communications and Information Protection, which develops technical security standards and ensures their implementation in critical information infrastructure. Article 8 of the Law of Ukraine "On the Basic Principles of Ensuring Cyber Security in Ukraine" stipulates that the State Service for Special Communications and Information Protection is responsible for monitoring the technical condition of information systems and ensuring their compliance with security standards [10].

Preventive measures of the protective mechanism include regular monitoring of information systems, training personnel in information hygiene rules, and the implementation of educational initiatives for the public. These measures are designed to minimize the human factor as one of the main causes of information threats. Article 5 the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine" emphasizes the need to improve the skills of specialists in the field in cybersecurity and implement educational programs aimed at raising public awareness at information risks [10].

Legal liability for violations of information security standards is an important component of the protective mechanism. The Criminal Code of Ukraine contains articles that provide for punishment for crimes in the field of information security, including unauthorized access to information systems (Article 361) and disclosure state secrets (Article 328). These norms create a legal basis for preventing offenses and strengthening discipline in the field of information protection [14].

Thus, the structure of the protective mechanism for ensuring information security in Ukraine is

multi-level and includes regulatory and legal frameworks, technical means, organizational measures and preventive actions. However, its effective functioning depends on the modernization of the technical infrastructure, the improvement of legal norms and the increase in the level coordination between state bodies and the private sector. This requires continuous updating of both technologies and approaches to information security management.

Finally, the control mechanism is an important component of the information security system, since it is aimed at monitoring, assessing and ensuring compliance with regulatory requirements in this area. This mechanism covers both state control over the implementation of legislation and internal audit of information systems and processes.

The legal basis for the functioning of the control mechanism is the norms enshrined in the fundamental regulatory legal acts. For example, the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine" provides for the obligation of subjects the national cybersecurity system to monitor the state critical information infrastructure and report on identified risks (Article 5) [10]. In addition, Article 8 the same law establishes the authority of the Security Service in Ukraine to conduct inspections critical infrastructure facilities in order to assess their security against cyber threats [10].

State control is also carried out within the framework of the functions the State Service for Special Communications, which, in accordance with Article 10 the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity in Ukraine", ensures the verification compliance of technical means, information protection with established standards [10]. The control body is obliged to conduct regular audits, including an assessment the security information systems against potential threats, and issue recommendations for eliminating identified shortcomings.

Control over compliance with the secrecy regime is carried out on the basis the Law of Ukraine "On State Secrets". Article 6 this law states that entities responsible for storing classified information must regularly report on compliance with the requirements the legislation on state secrets [11]. The Ministry of Defense in Ukraine, the Security Service in Ukraine and other law enforcement agencies are authorized to conduct inspections facilities working with classified information to ensure its proper protection.

The control mechanism also provides for an internal audit carried out by the subjects of information relations. In particular, Article 13 the Law of Ukraine "On Access to Public Information" obliges state authorities to implement mechanisms for internal monitoring compliance with the rules access to information in order to prevent violations in the field of public access [12]. Technological monitoring tools occupy a special place in the structure of the control mechanism. For example, the Cyber Threat Response Center (CERT-UA), established within the framework implementation of the Cybersecurity Strategy in Ukraine, provides round-the-clock monitoring of cyber incidents and collection data on potential threats [15].

The Center also provides technical advice on preventing cyber threats and eliminating their consequences, which significantly enhances the effectiveness of the cyber defense system.

The sanction aspect of the control mechanism involves holding entities that have violated information security standards accountable. For example, Articles 361 and 362 the Criminal Code in Ukraine provide for punishment, for unauthorized interference with the operation of information systems or their damage [14]. In addition, entities that improperly comply with information protection requirements may be subject to disciplinary or administrative sanctions in accordance with the law.

The control mechanism for ensuring information security in Ukraine has a multi-level structure that includes state control, internal audit, and technological monitoring. Although this mechanism is an important component of the national security system, its effectiveness depends on adequate funding, technical support, and coordination between authorized bodies. Improving the control mechanism, in particular through the modernization technical means and automation monitoring processes, is the key to ensuring the stability of the information space in Ukraine.

In general, the structure of information security mechanisms can be presented as follows (Table):

Table

Structure of information security mechanisms

Mechanism element	Key features	Legal basis
Legal framework	Regulates the rights, obligations of subjects, the procedure for protecting information	Law "On State Secrets" (Article 6), Law "On Basic Principles of Ensuring Cybersecurity in Ukraine" [10]
Technical measures	Includes encryption, backup, automatic monitoring	Law "On Electronic Communications" (Article 22) [13]
Organizational measures	Implemented by state bodies: SBU, State Special Communications Service, CERT-UA	Law "On Basic Principles of Ensuring Cybersecurity in Ukraine" (Articles 8, 10) [10]
Preventive measures	Monitoring, training, raising awareness subjects information relations	Law "On Basic Principles of Ensuring Cybersecurity in Ukraine" (Article 5) [10]
Control measures	Implemented through state control, internal audit and technological monitoring	Law "On Basic Principles of Ensuring Cybersecurity in Ukraine" (Articles 8, 10) [10]

Conclusions

The mechanisms for ensuring information security in Ukraine are a complex multi-component system that combines regulatory, technical, organizational, legal, preventive and control measures. Their main goal is to create effective conditions for protecting state information resources, ensuring information stability and neutralizing threats in the modern global information space. At the same time, the effectiveness of this system significantly depends on the level of its coherence, technical modernization and adaptation to new challenges.

The regulatory and legal mechanism forms the basis for the functioning of the entire system, determining the rights, obligations of subjects information relations and the procedure for ensuring information protection. Its elements, such as the laws "On State Secrets," "On the Basic Principles of Ensuring Cybersecurity in Ukraine" and the Criminal Code of Ukraine, regulate the procedures for accessing information, classifying, declassifying and liability for violations.

The technical mechanism provides the technological foundation for protection through the use of such means as encryption, backup, automatic monitoring and response to attacks. The organizational and legal mechanism ensures coordination actions between the subjects of the national cybersecurity system, such as the SBU, the State Service for Special Communications and CERT-UA. An important role in this mechanism is played by technical protection standards and strategic documents, for example, the Cybersecurity Strategy in Ukraine. The preventive mechanism is aimed at monitoring risks, training personnel, raising public awareness and regular auditing of information systems.

The control mechanism is implemented through state control, internal audit and monitoring the state critical infrastructure. Important tools in this mechanism are inspections carried out by authorized bodies, for example, the State Service for Special Communications. However, shortcomings in technical support and the difficulty of proving violations limit its effectiveness.

In general, the modern system of mechanisms for ensuring information security in Ukraine faces a number of challenges. The main problems are outdated approaches to information risk management, insufficient funding, limited coordination between public and private structures, as well as insufficient attention to raising public awareness.

Further research should focus on adapting international standards to national legislation, implementing modern technologies (artificial intelligence, blockchain), developing models of effective interaction between all information security actors, and improving methods for assessing the effectiveness of existing mechanisms. Modernizing these compo-

nents will contribute to the creation of a more reliable and sustainable information security system that meets modern challenges and threats.

Acknowledgements. None.

Funding. The author declares no financial support for the research, authorship, or publication of this article.

Author contributions. The author confirms sole responsibility for this work. The author approves this work and takes responsibility for its integrity.

Conflict of interest. The author declares no conflict of interest.

Institutional review board statement. Not applicable.

REFERENCES

1. Vyzdryk, V., Melnyk, O. (2023). Information Security in Ukraine: Current State. Grail of Science, (24), 196–202. DOI: 10.31470/2786-6246-2023-3-59-65

2. Smotrych, D. V., Brailko, L. (2023). Information Security under Martial Law. Scientific Bulletin of Uzhhorod National University. Series: Law, 77(2), 121–127. DOI: 10.24144/2307-3322.2023.77.2.20

3. Honcharov, M. V. (2024). Research on the Concept of "Information Security". Scientific Bulletin of Uzhhorod National University. Series: Law, 82, 34–37. DOI: 10.24144/2307-3322.2024.82.1.4

4. Honcharenko, H. A. (2024). On the Problem of Defining and Differentiating the Terms "Information Security" and "Cybersecurity". Analytical and Comparative Jurisprudence, (5), 466–471.

5. Maznyk, L. V., Dragan, O. I. (2023). Information Security of an Organization as a Factor in Strengthening the Employer's Brand. Kyiv Economic Scientific Journal, (1), 39–44.

6. Myslyva, O. (2023). Certain Aspects of Information Security of the Ukrainian Population in Temporarily Occupied Territories. Conference Proceedings of MCND (June 23, 2023; Poltava, Ukraine), 137–138.

7. Solomin, Ye. O. (2023). Information Security in Wartime and Interventions in the Media Environment. State and Regions. Series: Social Communications, 2(54), 40–47. DOI: 10.32840/cpu2219-8741/2023.2(54).5

8. Law of Ukraine No. 2469-VIII. (2018, June). *On National Security of Ukraine*. Bulletin of the Verkhovna Rada of Ukraine, 2018, No. 31, art. 241. DOI: zakon.rada.gov.ua/laws/show/2469-19#Text

9. Law of Ukraine No. 2657-XII. (1992, October). *On Information.* Bulletin of the Verkhovna Rada of Ukraine, 1992, No. 48, Art. 650.

10. Law of Ukraine No. 2163-VIII. (2017, October). *On the Basic Principles of Ensuring Cybersecurity of Ukraine*. Bulletin of the Verkhovna Rada of Ukraine, 2017, No. 45, art. 403.

11. Law of Ukraine No. 3855-XII. (1994, January). *On State Secrets*. Bulletin of the Verkhovna Rada of Ukraine, 1994, No. 16, art. 93.

12. Law of Ukraine No. 2939-VI (2011, January). *On Access to Public Information*. Bulletin of the Verkhovna Rada of Ukraine, 2011, No. 32, art. 314.

13. Law of Ukraine No. 1089-IX (2020, December). On Electronic Communications. Bulletin of the Verkhovna Rada of Ukraine, 2023, No. 10–11, art. 26.

14. Criminal Code of Ukraine: Code of Ukraine No. 2341-III of April 5, 2001. Official Bulletin of the Verkhovna Rada of Ukraine, 2001, No. 25–26, art. 131.

15. On the Decision of the National Security and Defense Council of Ukraine of May 14, 2021, "On the Cybersecurity Strategy of Ukraine": Presidential Decree No. 447/2021 of August 26, 2021. Retrieved from: https://zakon.rada.gov.ua/laws/show/447/2021#Text

16. On the Information Security Strategy of Ukraine: Presidential Decree No. 685/2021 of December 28, 2021.

Інформаційна безпека в контексті національної безпеки: правові механізми захисту державних інформаційних ресурсів

Володимир Ортинський

Доктор юридичних наук, професор, Заслужений юрист України, Національний університет "Львівська політехніка", Львів, Україна, volodymyr.l.ortynskyi@lpnu.ua, ORCID: 0000-0001-9041-6330

Анотація. Метою статті є аналіз механізмів забезпечення інформаційної безпеки України, зокрема нормативно-правові, технічні, організаційні, превентивні, контрольні та санкційні аспекти. Особлива увага надається виявленню сильних і слабких сторін функціонування цих механізмів у контексті сучасних інформаційних викликів.

У статті визначено основні елементи механізмів забезпечення інформаційної безпеки, їхні функції та взаємозв'язки. Нормативно-правовий механізм забезпечує правову базу функціонування системи, проте його окремі положення є застарілими та потребують оновлення. Технічний механізм формує технологічний фундамент безпеки, однак страждає від недостатньої модернізації. Організаційно-правовий механізм спрямований на координацію дій державних органів, проте низький рівень комунікації з приватним сектором обмежує його ефективність. Контрольний механізм забезпечує моніторинг виконання норм безпеки, однак технічна та кадрова оснащеність мають недоліки. Превентивні заходи, зокрема навчання персоналу та інформування населення, є недостатньо розвиненими. Санкційний механізм забезпечує юридичну відповідальність, але практична реалізація санкцій стикається зі складнощами.

Розроблено комплексний підхід до оцінки ефективності механізмів інформаційної безпеки, що враховує їхню структурну взаємодію та функціональні взаємозв'язки. Особливий акцент зроблено на інтеграції різних компонентів системи, включаючи правові, технічні та організаційні механізми, з метою забезпечення їх скоординованого функціонування. Запропоновано рекомендації щодо модернізації наявних механізмів через впровадження сучасних технологій, оновлення нормативно-правової бази та адаптації до міжнародних стандартів. Окремо обґрунтовано потребу вдосконалення координації між державними органами та приватним сектором у сфері кібербезпеки.

Результати дослідження можуть бути використані для вдосконалення національної системи інформаційної безпеки, створення нових стратегічних документів і впровадження інноваційних технологій у сфері захисту інформації.

Ключові слова: інформаційна безпека, механізми, нормативно-правовий захист, кібербезпека, контрольні заходи, санкційний механізм, превентивні заходи.