UDC 34:001.102-049.5

Nazariy HUZELA
Higher Education Institution
"Lviv University of Business and Law", postgraduate student,
Master of Laws
nazariyhuzela@gmail.com
ORCID: 0000-0001-6476-6329

THE PROBLEM OF LEGAL SECURITY IN THE INFORMATION SPACE IN THE CONTEXT OF THE EXPANSION OF THE USE OF ARTIFICIAL INTELLIGENCE AT THE MODERN STAGE

http://doi.org/10.23939/law2025.47.074

The article examines the problem of organizing legal security in the information sphere. Based on the provisions of Article 17 of the Constitution of Ukraine and the Information Security Strategy, one of the most important functions of the Ukrainian state at the present stage is to ensure information security. The problem of legal security in Ukraine acquires particular relevance and importance today, during the full-scale invasion of the Russian aggressor, when his insidious aggressive actions are implemented on all fronts, including in the information space. In these conditions, the state policy becomes important, which must be holistic and effective in countering threats.

The author summarizes and supports the understanding of the definition of information security as a state of security of information resources and information systems, which ensures their confidentiality, integrity, availability, as well as reliability and protection from unauthorized access, disclosure, modification, destruction and other forms of unlawful encroachments that pose threats to national security, economic stability and order in society. At the same time, the main components of the information security mechanism, which are the basis of information security for the state as a whole, individual legal entities or individuals, are confidentiality, integrity and availability. The main components of the information security mechanism, in the author's opinion, should be: technical (creation of an appropriate technical infrastructure to ensure the functioning of information security), political (development of state policy aimed at ensuring information security) and legal (adoption of high-quality regulatory legal acts that will determine all information security measures), as well as technologies in the field of artificial intelligence and a number of applied practical elements, which, of course, affect the state and level of information security in the state. These components and elements complement each other and are the basis for creating an effective security system against information threats in the information and cyberspace.

Keywords: legal support, legal regulation, information space, information technologies, artificial intelligence, national security, information security, cybersecurity, threats to information security, information terrorism, cyberterrorism, cybercrimes, offenses in the information sphere, responsibility for committing offenses in the information sphere.

Problem statement. One of the most important functions of the state is ensuring national security, since, in accordance with Part 1 of Article 17 of the Constitution of Ukraine, "the protection of the

sovereignty and territorial integrity of Ukraine, ensuring its economic and information security are the most important functions of the state, the business of the entire Ukrainian people" [1]. Based on the aforementioned constitutional norm, one of the components of the national security system is, first of all, information security. At the same time, in accordance with the Information Security Strategy adopted in Ukraine on December 28, 2021, one of the most important functions of the Ukrainian state at the present stage is ensuring information security [2]. The problem of legal ensuring information security in Ukraine is of particular relevance and importance today, during the full-scale invasion of the Russian aggressor, when its insidious aggressive actions are implemented on all fronts, including in the information space. The enemy is increasingly aggressively and actively conducting information and psychological operations with the aim of destabilizing the situation within our state, creating panic in society, spreading false information about the state of military operations and undermining trust in all state institutions and organizations. Therefore, state policy requires the development of an effective and holistic system, primarily of legal means, to counter threats from the aggressor state. An effective state policy in the field of security in the information space is designed to develop the resilience of citizens and society as a whole to existing information threats and strengthen trust in state institutions in order to maintain stability in their activities in the extremely difficult conditions of martial law.

Analysis of the study of the problem. Based on the above-mentioned Article 17 of the Constitution of Ukraine, as well as the provisions of the current Information Security Strategy, the problem of legal support for information security as a component of the national security of Ukraine is increasingly being paid attention to by both legal scholars and law enforcement practitioners, in particular, this problem is raised in the studies of I. V. Aristova, I. R. Bodnar, B. A. Kormych, V. A. Lipkan, Yu. Ye. Maksymenko, V. Ya. Ruban and many others. At the same time, modern scientific research by such legal scholars as V. S. Vyzdryk, M. T. Gavryltsiv, K. I. Dolzhenko, L. I. Mazurenko, T. S. Perun, O. M. Melnyk, O. Skochilyas-Pavliv, I. M. Shopin, E. O. Solomin and many others are also devoted to various aspects of legal security in the information space and the importance of ensuring information security as a component of the national security of Ukraine.

The purpose of the article is a comprehensive study of the problem of legal security in the information space, in particular, in the context of expanding the possibilities of using artificial intelligence at the present stage.

Presentation of the main material. In the modern dynamic world, information is of decisive importance in all spheres of life of society and the state: in politics, in the economy, in the military sphere, in other spheres. However, the growing information dependence undoubtedly creates opportunities for committing offenses in the information sphere using information technologies and artificial intelligence technologies. Therefore, the problem of ensuring information security for the state is becoming extremely relevant. Almost all states face difficulties in ensuring the security of their information resources due to a number of threats (cyberattacks, cyber espionage, domestic espionage and other forms of cybercrime). Such threats can encroach on national security, economic stability and order in society, which has an extremely negative impact on the state as a whole. In Ukraine, such threats have only intensified in the context of Russian military aggression and the introduction of the legal regime of martial law, and therefore require more effective legal mechanisms for ensuring information security and more radical countermeasures.

As already noted, in accordance with Part 1 of Article 17 of the Constitution of Ukraine, "the protection of the sovereignty and territorial integrity of Ukraine, ensuring its economic and information security are the most important functions of the state, the business of the entire Ukrainian people" [1]. Therefore, information security is a certain element or component of the national security system of Ukraine.

Studying the definition of information security, a number of scientists approach the understanding of information security as a set of technical and software tools to ensure the confidentiality of information data in computer networks. In particular, their scientific works emphasize that information security is a set of

tools and methods developed and used to protect confidential information from change, violation, destruction and verification [4, p. 111]. We believe that such an understanding of information security (security in the information space) is somewhat artificially narrowed.

According to the scientific positions of other legal scholars, information security is the state (or level (N. Guzel) of information security. Thus, O. Stepko, analyzing the problem of information security, in his scientific work considers information security in two dimensions (aspects). On the one hand, the scientist believes that information security is the security of internal information, that is, the quality and reliability of this information, as well as the protection (or level of protection (N. Guzel) of various areas of information from disclosure and the protection (or level of protection (N. Guzel) of information resources. On the other hand, from the scientist's position, information security also includes: control over information flows, restriction of the use of provocative and hostile public information (including control over advertising), as well as protection of the national information space from external information expansion [5, p. 91].

There is also another scientific position, according to which (B. Kormych), information security is the security (or level of protection (N. Guzel) of the rules (legal norms) established by law, in accordance with which information processes take place in the state, which provide the conditions for the existence and development of a person, the entire society and the state guaranteed by the Constitution [6, p. 142].

In addition to the above, it is worth emphasizing that, in accordance with Article 17 of the current Constitution of Ukraine and the approved Information Security Strategy, the information security of Ukraine is an integral part of the national security of Ukraine[1; 2]. Therefore, we consider it correct to state that information security encompasses a certain legal state of protection of state sovereignty, territorial integrity, democratic constitutional order, as well as other vital interests of man, society and the state, in the existence of which the constitutional rights and freedoms of man to collect, store, use and disseminate information, as well as access to reliable and objective information, are properly ensured, there is an effective system of protection and counteraction to harm caused by the spread of negative information influences, including the coordinated spread of unreliable information, destructive propaganda, other information operations, unauthorized distribution, use and violation of the integrity of information (e. g., with limited access) [3, p. 153].

Thus, taking into account the norms of the analyzed legislation, as well as the scientific statements of scientists who have studied the essence of information security, we generally share scientific positions on understanding the essence of information security as a state of security of information resources and information systems, which ensures their confidentiality, integrity, availability and reliability, as well as protection from unauthorized access, disclosure, modification, destruction and other forms of abuse that can lead to a violation of national security, economic stability and public order [3, p. 153]. At the same time, we believe that such a state is formed in the state on the basis of rules established by law (legal norms). The scientific position that the main components of information security, which are the basis for information security for the state as a whole, individual legal entities and individuals, are also correct:

– confidentiality;

– integrity;

– availability [3, p. 153; 8].

If we analyze the above components of information security, then among them, data confidentiality means that data should be accessible only to those who have authorized access. For example, take any government agency. There is information that may belong only to certain employees and is needed only for work. Limiting the number of people who have access to different data sets improves the ability of the government agency to maintain the confidentiality of information. As for data integrity, the information must be intact, complete and accurate. To ensure data integrity, governments can maintain and optimize their IT infrastructure, create backup copies of their data and create a data loss prevention plan that will protect them in the event of a serious data breach. And finally, the component of data availability indicates that the network, system and necessary devices are ready for use as intended by authorized personnel.

It should be noted, in particular, that data availability means the ability of employees to access the necessary data at any time without delay. Yes, there are a number of factors that can prevent access to data even for authorized users, especially in the era of cloud technologies, when so much data is hosted off-site.

The development of digital technologies has led to an unprecedented increase in information threats - from ordinary theft of information or eavesdropping to high-tech cyber espionage at the state level. Yes, with the development of technologies, the tactics of cybercriminals are also changing. This undoubtedly complicates the provision of information security, which is influenced by a number of factors: potential threats, the value and level of sensitivity of information, verification and reliability of information, etc. The main trends in the evolution of information and cyber threats, as part of information security, are related, first of all, to the need to protect computer systems and networks of states, their legal entities or individuals from data leakage, from damage to equipment and software. Such threats today are: ransomware (ransomware attacks are becoming increasingly common, when cybercriminals block systems and demand large ransoms or demand information or access to it), vulnerable devices (weak passwords to work devices, banal theft of laptops or storage media. To avoid this, it is worth holding lectures on cyber hygiene in government institutions, companies, and simply being aware of every individual), attacks using artificial intelligence (AI) (cybercriminals use artificial intelligence and machine learning to create more effective attacks, which makes it extremely important for defenders to implement artificial intelligence to detect threats. It is important that the usual chat GPT or avodocs, which IT lawyers love to use so much for using template contracts, are open source. That is, if a lawyer creates a contract and fills in data in avodocs, then this completed contract can be easily stolen, which poses a threat to clients, the lawyer, and the company), provisions on data privacy (new data privacy regulations such as GDPR and CCPA set strict requirements for organizations. Failure to comply with them not only leads to fines but also creates reputational risks), privacy and data protection (due to growing concerns about data protection, individuals and organizations face constant challenges in protecting personal information, complying with privacy regulations, and protecting user data from unauthorized access) [3, 8].

Yes, one of the largest hacking attacks that threatened the US government is known to date – the hacking attack on SolarWinds in 2020. SolarWinds is a large software company based in Oklahoma that provides system management tools for network and infrastructure monitoring, as well as other technical services to hundreds of thousands of government and non-government organizations around the world. Among the company's products is the Orion IT performance monitoring system. In carrying out the attack, the perpetrators targeted SolarWinds, deploying malicious code in the Orion IT monitoring and management software, which is used by thousands of enterprises and government agencies around the world. The SolarWinds hack was a major event not because it compromised one company, but because it triggered a much larger incident that affected thousands of organizations, as well as the US government. During this hack, the alleged state of origin of the hacking attack was established, which Microsoft identified as the Nobelium group (a Russian hacking group). More than 30,000 public and private organizations, including local, state, and federal agencies, use the Orion network management system to manage their IT resources. It wasn't just SolarWinds customers who were affected. Because the hack exposed the inner workings of Orion users, hackers could potentially gain access to the data and networks of their customers and partners. The malware reportedly affected many U. S. companies and organizations. Even government departments such as the Department of Homeland Security, the Department of State, and the Department of Commerce and the Treasury were affected. Private companies such as FireEye, Microsoft, Intel, Cisco, and Deloitte were also affected by the attack [10].

In Ukraine, the scope of threats and challenges in the field of information security is determined primarily by Russian armed aggression and the established legal regime of martial law. Indeed, several times a month, the aggressor state attacks Ukrainian information systems with the sole purpose of stealing information, including restricted access. Unlike NATO member states, Ukraine, unfortunately, is forced to ensure security in information and cyberspace on its own. Statements by NATO leadership, against the background of "special" concerns about Russia's information war against Ukraine, that attacks in Ukraine's cyberspace may sooner or later spread to other territories, repeatedly emphasize that a cyberattack on a NATO member state may trigger Article 5 (the collective defense clause). Given today's realities, the action of Article 5 is most likely hypothetical [10]. Even in the first days of the full-scale invasion, phishing attacks,

probably from Belarusian hackers and the FSB, were directed against Ukrainian servicemen [12]. There were also a lot of fake messages about "checks" from the SBU, allegedly requiring Ukrainians to click on a link, which later led to the enemy wanting to gain access to Ukrainians' accounts and many other cybercrimes [13].

At the same time, almost all researchers of the analyzed issues agree that Ukraine today has all the opportunities to achieve technological leadership not only in Europe, but also at the level of developed countries of the world, since the state of war has led to rapid information and technological development in the country towards the application of the most modern IT technologies. Achievements in the field of artificial intelligence, as well as high-tech information protection, are already significantly and positively affecting national defense and security, based on revolutionary changes in three main areas - military, information and economic. Thus, in the military sphere today, technologies that use artificial intelligence are available (unmanned aerial vehicles, in particular strike aircraft, unmanned aerial vehicles of various ranges, cruise missiles with automatic target designation, naval drones, etc.). These technologies can provide access to new means of delivering high-precision strikes, in particular at long distances. Another example of this kind is machine learning technology, which can automate the analysis of satellite images and provide cyber protection. In the field of information and cyber security, artificial intelligence will significantly expand the capabilities of data collection and analysis, instant response to cyber incidents, and the creation of aggregated data. When it is necessary to quickly solve intelligence tasks, this will mean systematically taking into account a larger number of sources of objective information, as well as sources of disinformation and information influences [13, p. 149].

Solving the problem of ensuring information security in the state requires solving such large-scale tasks as developing theoretical principles of information security and a regulatory framework that regulates the solution of all aspects of ensuring information security, creating a system of bodies responsible for information security and resolving issues of information security management and its automation, improving the production of information security tools and organizing the training of relevant specialists [5, p. 90].

It is worth noting that the main threats and challenges in the field of information security of states, their legal entities or individuals are growing in parallel with the development of IT technologies and the expansion of the possibilities of illegal attacks on databases, services and archives. Thus, today it is a fact that even the most protected areas, such as political or defense, become objects of illegal actions of attackers with the aim of stealing or distorting information (including limited access).

The ongoing Russian-Ukrainian war for several years has clearly confirmed that any information attacks and information leaks, the use of artificial intelligence capabilities can massively affect both individual individuals and society as a whole. Therefore, today, more than ever, the need to develop an effective legal mechanism that would really and fully guarantee the information security of Ukraine and in Ukraine is relevant. In this regard, the scientific position expressed by Prof. O. Skochylas-Pavliv, that the defining components of this legal mechanism should be: a technical component (creation of an appropriate technical infrastructure to ensure the effective functioning of information security), a political component (development of a state policy aimed at ensuring information security), a legal component (adoption of effective and high-quality regulatory and legal acts that would cover all the previously considered means of ensuring information security. These three components complement each other and are fundamental for creating an effective system of protection against information threats.

It will also not be superfluous to determine a number of practical elements that undoubtedly affect the state and level of ensuring information security in the state. Timely and objective presentation of news and other important information (through state media and online publications, official appeals), constant and, above all, timely during the period of the legal regime of martial law, refutation of fakes, false information inputs and IPSO (through state media and online publications, official appeals), continuous training of citizens in the basics of critical thinking and the ability to recognize disinformation and fakes, as well as compliance with information hygiene (through a public-private partnership to improve citizens' knowledge and skills regarding Internet safety), legal protection and protection of data confidentiality, freedom of

speech and citizens' information rights to access information (transparency and responsibility of media and information platforms) – all this together is designed to form an effective legal mechanism for ensuring information security in Ukraine.

Conclusions. Thus, today, in a period of rapid information development of society, martial law in Ukraine, and the changing geopolitical situation in the world, legal security in information and cyberspace is becoming perhaps the most important state task. Therefore, the state, represented by its bodies (CERT-UA (Computer Emergency Response Team of Ukraine of the State Service for Special Communications), the Cyber Police Department of the National Police of Ukraine, the Department of Counterintelligence Protection of the State's Interests in the Field of Information Security of the Security Service of Ukraine) is called upon to ensure information security in all spheres of public life through the development and implementation of an effective legal mechanism for countering offenses in the information and cyberspace, which would cover a number of components, in particular, technical (creation of an appropriate technical infrastructure to ensure the functioning of information security), political (development of a state policy aimed at ensuring information security) and legal (adoption of high-quality regulatory and legal acts that will determine all information security measures), as well as technologies in the field of artificial intelligence and a number of applied practical elements (education and awareness of citizens, development of the legal framework and international cooperation), which, of course, affect the state and level of ensuring information security in state. The above components and elements complement each other and are the basis for creating an effective security system against information threats in the information and cyberspace. Only through a comprehensive approach and the implementation of appropriate measures (in particular, legal ones) can effective information security be ensured in war conditions, while respecting freedom of speech and information rights of citizens.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Конституція України від 28 червня 1996 року. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96%D0%B2%D1%80#Text (Дата звернення: 28.05.2025).

2. Рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки": Указ Президента України від 15 жовтня 2021 року. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (Дата звернення: 28.05.2025).

3. Скочиляс-Павлів О. (2024). Правові механізми забезпечення інформаційної безпеки в Україні. Вісник Національного університету "Львівська політехніка". Серія: "Юридичні науки" № 2 (42), 2024. С. 151–158.

4. Сопілко І. М. (2021). Інформаційна безпека та кібербезпека: порівняльно-правовий аспект. Юридичний вісник. 2021. № 2 (59). С. 110–115.

5. Степко О. М. (2011). Аналіз головних складових інформаційної безпеки держави. Науковий вісник Національного авіаційного університету. 2011. Том 1. № 3. С. 90–99.

6. Кормич Б. А. (2004). Організаційно-правові основи політики інформаційної безпеки України: дис. ... д-ра юрид. наук: 12.00.07 / Національний ун-т внутрішніх справ. Х., 2004. URL: http://www.disslib.org/orhanizatsiyno-pravovi-osnovy-polityky-informatsiynoyi-bezpeky-ukrayiny.html (Дата звернення: 28.05.2025).

7. DOT Security. What Are the 3 Components of Information Security. 24.10. 2023. URL: https://dotsecurity.com/insights/blog-what-are-the-components-information-security (Дата звернення: 20.05.2025).

8. Rabeya Islam Rima. Cyber security in modern world. 14.01.2024. URL: https://www.educative.io/answers/what-are-some-challenges-in-information-security (Дата звернення: 20.05.2025).

9. Saheed Oladimeji, Sean Michael Kerner. SolarWinds hack explained: Everything you need to know. 03.11.2023. URL: https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-toknow (Дата звернення: 20.05.2025).

10. Пірсон Дж., Лендей Дж. (2022). Кібератака на НАТО може активувати положення про колективну оборону – офіційно. 28.02.2022. URL: https://www.reuters.com/world/europe/cyberattack-nato-could-triggercollective-defence-clause-official-2022-02-28/ (Дата звернення: 28.05.2025).

11. Мазуренко Л. І. (2022). Інформаційна безпека в умовах російсько-української війни: виклики та загрози. Вісник Харківського національного університету імені В. Н. Каразіна. Серія "Питання політології". 2022. Вип. 42. URL: https://periodicals.karazin.ua/politology/article/view/22088/20387 (Дата звернення: 28.05.2025).

12. Мастерс Дж. Російсько-українська війна: кібератака – Хронологія кінетичної війни. 26.01.2024. URL: https://www.msspalert.com/news/ukraine-russia-cyberattack-timeline-updates-amid-russia-invasion (Дата звернення: 28.05.2025).

13. Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA. Офіційна Facebook-Сторінка. URL: https://www.facebook.com/UACERT (Дата звернення: 30.05.2025).

14. Шевченко А. І. (2023). Стратегія розвитку штучного інтелекту в Україні: монографія. Київ, 2023. С. 305. URL: https://jai.in.ua/archive/2023/ai_mono.pdf (Дата звернення: 30.05.2025).

REFERENCES

1. ***Konstytutsiia Ukrainy*** (1996, June 28) [Constitution of Ukraine]. Retrieved from: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text (Accessed: 28.05.2025). [In Ukrainian].

2. ***Rishennia Rady natsionalnoi bezpeky i oborony Ukrainy*** vid 15 zhovtnia 2021 roku "Pro Stratehiiu informatsiinoi bezpeky". (2021, October 15) [On the decision of the National Security and Defense Council of Ukraine dated October 15, 2021 "On Information Security Strategy"]. Retrieved from: https://zakon.rada.gov.ua/laws/show/685/2021#Text (Accessed: 28.05.2025). [In Ukrainian].

3. Skochylyas-Pavliv, O. (2024). ***Legal mechanisms for ensuring information security in Ukraine***. Bulletin of the National University "Lviv Polytechnic". Series: "Legal Sciences" No. 2 (42). P. 151–158. [In Ukrainian].

4. Sopilko, I. M. (2021). ***Informatsiina bezpeka ta kiberbezpeka: porivnialno-pravovyi aspekt*** [Information security and cyber security: a comparative legal aspect]. Yurydychnyi visnyk. No. 2 (59). P. 110–115. [In Ukrainian].

5. Stepko, O. M. (2011). ***Analiz holovnykh skladovykh informatsiinoi bezpeky derzhavy***. [Analysis of the main components of information security of the state]. Naukovyi visnyk Natsionalnoho aviatsiinoho universytetu. T. 1. No. 3. P. 90–99. [In Ukrainian].

6. Kormych, B. A. (2004). ***Orhanizatsiino-pravovi osnovy polityky informatsiinoi bezpeky Ukrainy***. [Organizational and legal foundations of information security policy of Ukraine]. Doctor's thesis. Kharkiv. Retrieved from: http://www.disslib.org/orhanizatsiyno-pravovi-osnovy-polityky-informatsiynoyi-bezpeky-ukrayiny.html (Accessed: 28.05.2025). [In Ukrainian].

7. ***DOT Security. What Are the 3 Components of Information Security*** (24.05.2025). Retrieved from: https://dotsecurity.com/insights/blog-what-are-the-components-information-security (Accessed: 20.05.2025). [In English].

8. ***Rabeya Islam Rima. Cyber security in modern world*** (14.01.2025). Retrieved from: https://www.educative.io/answers/what-are-some-challenges-in-information-security (Accessed: 20.05.2025). [In English].

9. Saheed, Oladimeji, Sean, Michael Kerner. ***SolarWinds hack explained: Everything you need to know*** (03.11.2024). Retrieved from: https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everythingyou-need-to-know (Accessed: 20.05.2025). [In English].

10. Pirson, Dz., Lendei, Dz. ***Kiberataka na NATO mozhe aktyvuvaty polozhennia pro kolektyvnu oboronu – ofitsiino*** (28.02.2025). Retrieved from: https://www.reuters.com/world/europe/cyberattack-nato-could-triggercollective-defence-clause-official-2022-02-28/ (Accessed: 28.05.2025). [In Ukrainian].

11. Mazurenko, L. I. (2022). ***Informatsiina bezpeka v umovakh rosiisko-ukrainskoi viiny: vyklyky ta zahrozy***. [Information security in the conditions of the Russian-Ukrainian war: challenges and threats]. Visnyk Kharkivskoho natsionalnoho universytetu imeni V. N. Karazina. Seriia "Pytannia politolohii". Vyp. 42. Retrieved from: https: // periodicals.karazin.ua /politology/ article/view/ 22088/20387 (Accessed: 28.05.2025). [In Ukrainian].

12. Masters, Dz. ***Rosiisko-ukrainska viina: kiberataka – Khronolohiia kinetychnoi viiny*** (26.01.2024). Retrieved from: https://www.msspalert.com/news/ukraine-russia-cyberattack-timeline-updates-amid-russia-invasion (Accessed: 28.05.2025). [In Ukrainian].

13. ***Uriadova komanda reahuvannia na kompiuterni nadzvychaini podii Ukrainy CERT-U***A. Ofitsiina Facebook-Storinka. Retrieved from: https://www.facebook.com/UACERT (Accessed: 30.05.2025). [In Ukrainian].

14. Shevchenko, A. I. (2023). ***Stratehiia rozvytku shtuchnoho intelektu v Ukraini: monohrafiia*** [Strategy for the development of artificial intelligence in Ukraine]. Kyiv, 305 p. Retrieved from: https://jai.in.ua/archive/2023/ai_mono.pdf (Accessed: 30.05.2025). [In Ukrainian].

Дата надходження статті: 08.06.2025 р.

Назарій ГУЗЕЛА
Заклад вищої освіти
"Львівського університету бізнесу та права", аспірант,
магістр права
nazariyhuzela@gmail.com
ORCID: 0000-0001-6476-6329

ПРОБЛЕМА ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ В ІНФОРМАЦІЙНОМУ ПРОСТОРІ У КОНТЕКСТІ РОЗШИРЕННЯ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ НА СУЧАСНОМУ ЕТАПІ

У статті досліджується проблема організації правового забезпечення безпеки в інформаційній сфері. Виходячи з положень ст. 17 Конституції України та Стратегії інформаційної безпеки, однією з найважливіших функцій Української держави на сучасному етапі є забезпечення інформаційної безпеки. Особливої актуальності та важливості проблема правового забезпечення інформаційної безпеки в Україні набуває сьогодні під час повномасштабного вторгнення російського агресора, коли його підступні агресивні дії реалізуються на усіх фронтах, у т. ч. в інформаційному просторі. У цих умовах важливою стає політика держави, яка має бути цілісною та ефективною для протидії загрозам.

Автор узагальнює і підтримує розуміння дефініції інформаційної безпеки як стану захищеності інформаційних ресурсів та інформаційних систем, який забезпечує їхню конфіденційність, цілісність, доступність, а також надійність та захищеність від несанкціонованого доступу, розголошення, модифікації, знищення та інших форм протиправних посягань, які загрожують національній безпеці, економічній стабільності та порядку в суспільстві. Водночас основними складовими частинами механізму інформаційної безпеки, які є основою інформаційної безпеки для держави загалом, окремих юридичних чи фізичних осіб є конфіденційність, цілісність та доступність. Основними компонентами механізму забезпечення інформаційної безпеки, на думку автора, мають бути: технічна (створення відповідної технічної інфраструктури для забезпечення функціонування інформаційної безпеки), політична (розробка державної політики, спрямованої на забезпечення інформаційної безпеки) та правова (прийняття якісних нормативно-правових актів, які визначатимуть всі заходи інформаційної безпеки), а також технології у сфері штучного інтелекту та низка прикладних практичних елементів, які, безумовно, впливають на стан і рівень забезпечення інформаційної безпеки в державі. Зазначені складові та елементи взаємодоповнюють один одного і є основою для створення ефективної системи безпеки від інформаційних загроз в інформаційному та кіберпросторі.

Ключові слова: правове забезпечення, правове регулювання, інформаційний простір, інформаційні технології, штучний інтелект, національна безпека, інформаційна безпека, кібербезпека, загрози інформаційній безпеці, інформаційний тероризм, кібертероризм, кіберправопорушення, правопорушення в інформаційній сфері, відповідальність за скоєння правопорушення в інформаційній сфері.