UDC 342.721
DOI https://doi.org/10.32849/2663-5313/2023.5.15

Andrii Kolesnikov,
PhD in Economics, Associate Professor at the Department of Security and Law Enforcement, West Ukrainian National University, 11, Lvivska Street, Ternopil, Ukraine, postal code 46009, Kole.ua@gmail.com
ORCID: *orcid.org/0000-0003-3064-4133*

Kolesnikov, Andrii (2023). Cybersecurity as a necessary condition for the functioning of the justice administration system. *Entrepreneurship, Economy and Law, 5*, 101–107, doi https://doi.org/10.32849/2663-5313/2023.5.15

CYBERSECURITY AS A NECESSARY CONDITION FOR THE FUNCTIONING OF THE JUSTICE ADMINISTRATION SYSTEM

Abstract. ***Purpose.*** System analysis of the cybersecurity status in Ukraine, research on its impact on the justice system, and an outline of the ways to eliminate identified threats. ***Research methods.*** The structure of the article is built in accordance with theoretical, analytical, and prognostic tasks; it reflects the use of individual methods of scientific research and scientific materials. The author uses a theoretical method to study the category apparatus. Structural, functional, and systemic methods are applied to study the regulatory framework for cybersecurity. In the study of the problems and threats of cybersecurity violations in the conditions of the military invasion of the Russian Federation, the method of abstraction was used, which made it possible to single out among a large number of criteria the most significant in the author's opinion. The author applies the method of scientific generalization to substantiate the conclusions. ***Results.*** Cybersecurity is defined as the practice of protecting the interests of people, society, and the state in cyberspace for their sustainable development. In the justice administration system, information security is considered an object of legal security to protect the data of all judicial system participants. The author defines the components of administrative and legal support for cybersecurity. The article substantively discusses the need for a systematic approach to countering cyber threats at the international level. The paper defines legal regulation of information security as the legal influence of the state on relevant social relations. Cybersecurity is a component of national security. Ukraine has adopted a number of documents on information society development and ensuring cybersecurity. But it is necessary to improve specialized regulatory acts and harmonize them with international standards, in particular ISO/IEC 27000. It is justified that a complex administrative and legal mechanism for ensuring information security and its subject interaction will allow to identify of problems and ways to solve them. This requires the development of a single document on information security in court proceedings. ***Conclusions.*** Cybersecurity is a critical point to the effective operation of the justice system, ensuring the confidential data protection of the participants in the legal process. Ukraine developed a legal framework in this area, but the war with the Russian Federation revealed a number of problems: insufficient infrastructure protection, weak coordination of cybersecurity entities, etc. To increase the level of protection, it is necessary to improve the legal mechanism for ensuring cybersecurity and adopt a single document on the regulation of all aspects of information security in the judicial system. It is also encouraging to use artificial intelligence, promising that it is properly protected against threats.

Key words: justice, court, information security, cybersecurity, regulatory and legal support of cybersecurity, martial law.

1. Introduction

Rapid progress and widespread use of information and computer technologies have led to the significant dependence of critical national infrastructures on the level of their security in the information aspect. In current conditions, cybersecurity has become an important prerequisite for the viability of society. Its provision is of particular importance for the effective administration of justice, as it provides an opportunity to protect human and civil rights and freedoms. The absence or imperfection of information security tools hinders the ability to achieve this task, which is crucial for the judicial system. In this case, the objects of protection are information systems and software products, as well as registers and databases that contain information about the subjects of the adminis-

tration of justice and all participants in the judicial process. New threats in the field of cyber defense in the context of the military invasion of the Russian Federation add relevance to this scientific research. The purpose of this article is to study the legal foundations of cybersecurity in Ukraine in general, as well as for ensuring human rights and freedoms in particular.

The structure of the article is built in accordance with theoretical, analytical, and prognostic tasks; it reflects the use of individual methods of scientific research and scientific materials. The author uses a theoretical method to study the category apparatus. Structural, functional, and systemic methods are applied to study the regulatory framework for cybersecurity. In the study of the problems and threats of cybersecurity violations in the conditions of the military invasion of the Russian Federation, the method of abstraction was used, which made it possible to single out among a large number of criteria the most significant in the author's opinion. The author applies the method of scientific generalization to substantiate the conclusions.

The purpose of the article is to systematically analyze the cybersecurity condition in Ukraine, to research its impact on the justice administration system, and to outline ways to eliminate the identified threats.

To ensure the systematic presentation of the material, the article is logically divided into the following blocks: introduction, content definition, legal basis for ensuring cybersecurity, cybersecurity problems under martial law, ways to strengthen cybersecurity and conclusions.

2. Content definition

Since information has become the basis of social relations, the need for legal regulation of informational functions of the state and its institutions has arisen. Information is a complex phenomenon. On the one hand, it is a property of objects of living nature to reflect their movement in surrounding world in the form of mental sensations (content side of information, data), and on the other hand, it is an ability of some objects of living nature to convey sensations (images), experienced by them, to other objects of living nature (representative side of information, message).

The dialectic of the law and information interdependence shows that the law remains a key tool in regulating information-related relations under the conditions of information support for all other social relations. Legal norms not only regulate but also get influenced by the information environment. This leads to the emergence of new objects of regulation and changes the methods of their influence on social relations.

The Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity in Ukraine" provides the legal definition of the term cybersecurity. In this law, it is defined as "the protection of human and civil vital interests, society, and the state during the use of cyberspace, which ensures the sustainable development of the information society and digital communication environment and the timely detection, prevention, and counteraction of real and potential threats to the national security of Ukraine in cyberspace" (Law of Ukraine On the Basic Principles of Cybersecurity, 2017).

In the judicial system, information security should be considered as an object of administrative and legal protection, taking into account the fact that it is not only a state of security, but also a system of social relations that contribute to the emergence of a state of security.

From a legal point of view, information is data that is the object of communication. The encroachment on information should be considered on two levels: as an encroachment directly on information and as an encroachment on the possibility of its unimpeded transmission (communication) (Perun, 2019, p. 31). Taking that into account, information in the justice system is a substance that determines the implementation of legal relations in the context of obtaining, possessing, protecting, using, and transferring information to protect human and civil rights and freedoms.

The author agrees with the approach of scientists regarding the definition of the legal content of ensuring information security in relation to its components: administratively sanctioned provision of information security; administrative and jurisdictional provision of information security; administrative casual provision of information security (Ostapenko, Baik, 2021, p. 174).

Taking this into account, the author defines following components of the administrative and legal support of cybersecurity:

– conditions for the emergence and development of information security threats (social, economic, natural, political, technogenic);

– factors affecting the occurrence of threats (natural, technogenic, biological);

– sources of security threats (man-made, natural, biological);

– objects of security infringement (constitutional rights, freedoms and legitimate interests of a person, society, state);

– subjects of information protection (individuals, entities);

– the sphere of administrative and legal regulation of ensuring public safety (objective, subjective, functional, situational) (Ostapenko, Baik, 2021, p. 170).

Today information security has gone beyond the national framework and has become one of the key aspects of the international security system. This system provides the principle of indivisibility of security and state responsibility for their information space (Hetman, Politanskyi, Hetman, 2023, p. 97). This determines the need for a systematic and continuous approach to countering cyber threats at the international level.

3. Legal basis for ensuring

The normative and legal regulation of information security is a form of powerful legal influence of the state on social information relations with the aim of organizing them, consolidating them, and ensuring order.

In the global dimension, cybersecurity is a component of the state's national security. Ensuring information security is defined as one of the important functions of the state in Article 17 of the Constitution of Ukraine (Constitution of Ukraine, 1996).

On May 15, 2013, the Cabinet of Ministers of Ukraine approved the National Strategy of the Information Society in Ukraine. The strategy defines the need for information society development focused on people's interests, open to everyone, in which every person can create and accumulate information and knowledge, have free access to knowledge, use and exchange the knowledge, have the opportunity to fully realize their potential, contribute to social and personal development, and improve the quality of life (Order of the Cabinet of Ministers of Ukraine, 2013) In fact, access to information in order to satisfy people's needs, including the protection of rights and freedoms, is the fundamental basis of information support for the justice administration.

Information security is defined in the Law "On the Basic Principles for the Development of an Information-Oriented Society in Ukraine for 2007–2015" as "a state of protection of the vital interests of a person, society and the state, in which harm is prevented due to: incompleteness, untimeliness and implausibility of the information used; negative information impact; negative consequences of the use of information technologies; unauthorized distribution, use and violation of integrity, confidentiality and availability of information" (Law of Ukraine On the Basic Principles for the Development of an Information-Oriented Society, 2007).

The Information Security Doctrine of Ukraine, approved by the President of Ukraine in 2017, defines the priority directions of state policy in the following areas: ensuring information security; ensuring the protection and development of the information space of Ukraine, as well as the citizens' constitutional right to information; openness and transparency of the state to citizens; formation of a positive international image of Ukraine (Decree of the President of Ukraine On the Information Security Doctrine, 2017).

In 2020, the Decree of the President of Ukraine put into effect the updated National Security Strategy of Ukraine, "Human security – the security of the country". This legal act pays considerable attention to various aspects of countering cyber threats, primarily from the Russian Federation. Paragraph 52 of the Strategy states that the main task of the development of the cybersecurity system is to guarantee the cyber resilience and cybersecurity of the national information infrastructure (Decree of the President of Ukraine On the National Security Strategy, 2020). One of the elements of such an infrastructure is the functioning of the Unified Judicial Information Telecommunication System, the purpose of which is the formation and development of new forms of communication between judicial authorities and other participants in the judicial process.

In 2021, predicting a growing threat from the Russian Federation, a decree of the President of Ukraine put into effect the Decision of the National Security and Defense Council of Ukraine on the Military Security Strategy of Ukraine (Decree of the President of Ukraine On Strategy of Military Security, 2021). In the act, among the tasks, there were defined the countermeasures to the threads to Ukraine in cyberspace. At the same time, the National Security and Defense Council, by Decision 106/2021 as of March 11, 2021, established the Center for Countering Disinformation. The main purpose of the Center is to counter threats to the national security and national interests of Ukraine in the information sphere, fight against propaganda, destructive informational influences, and companies, and prevent manipulation of public opinion (Decree of the President of Ukraine On establishment Center for Countering Disinformation, 2021).

One of the important legal documents in the field of ensuring information space security is the Decree of the President of Ukraine, "Cybersecurity Strategy of Ukraine. Safe cyberspace is the key to the successful development of the country" (Decree of the President of Ukraine On Cybersecurity strategies of Ukraine, 2021). The strategy states that cyberspace is considered to be one of the possible places for conducting military operations, along with other physical spaces. The concept of cyber warfare is growing in popularity, which includes not only the protection

of critical information systems from cyber-attacks but also active actions in cyberspace, such as attacks aimed at paralyzing enemy facilities by destroying their information systems. At the same time, the adoption of these and other doctrinal, regulatory and strategic documents defines only the general principles of ensuring information and cybersecurity. The peculiarities of their implementation in different spheres determine the need to adopt more specialized documents or make appropriate amendments to the existing ones. For example, in Regulation on the Procedure of Functioning the Separate Subsystems of the Unified Judicial Information Telecommunication System (UJITS), approved by the Decision of the Supreme Council of Justice in 2021, it is stated that organizational and financial support for the creation and functioning of individual subsystems (modules) of the Unified Judicial Information Telecommunication System is carried out by the State Judicial Administration of Ukraine, which carries responsibility for their proper functioning and ensuring information protection (Decision of the Supreme Council of Justice on the approval of the Regulation, 2021). However, its functions, tasks, powers of the responsible unit or person, and features of responsibility are not defined.

Another condition for the effectiveness of regulatory and legal protection for cybersecurity is its compliance with international norms. Thus, the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine" defines the need to achieve compatibility with the relevant standards of the European Union and NATO, taking into account the best global practices and international standards on cybersecurity and cyber protection (Perun, 2019). Scientists of the National Institute of Strategic Studies in the analytical note Problems of implementing modern information security standards in the conditions of the national cybersecurity system formation in Ukraine notice that the national information protection standard ND TZI (Regulatory Document of the Technical Information Protection System) 2.5-004-99, oriented on the compliance of the architecture and parameters of the software and hardware of the object, comply with the norms of the ISO/IEC 27000 series of standards, which is focused on information security management (Analytical note, 2018, p. 5). Implementation of ISO/IEC 27000 allows for optimization of the process of information resource protection and risk management for these resources.

Today, in this area, there are the NSTU standards (National Standards of Ukraine) ISO/IEC 27005:2023 for information security, cybersecurity, and privacy protection and the information security risk management guideline (ISO/IEC 27005:2022, IDT).

4. Problems under martial law

In the context of the Russian-Ukrainian war, information products distributed by mass media become a means of psychological and technological influence on the consciousness of society and certain groups of people. Mass media can make wrong conclusions that affect the decision-making process, offering them with certain goals, sometimes even inciting illegal actions (Vyzdryk, Melnyk, 2023, p. 198).

Today, we note that during the military invasion of the Russian Federation, this threat materializes in the form of numerous attacks on the information infrastructure of state bodies.

The factors which made such attacks successful include:

– inconsistency of the state's electronic communications infrastructure, its level of development, and security with modern requirements;

– insufficient level of coordination, interaction, and information exchange between cybersecurity entities;

– unsystematic cyber protection measures for critical information infrastructure;

– poor level of protection of critical information infrastructure, state electronic information resources, and information; protection against cyber threats is required and established by law;

– insufficient development of the organizational and technical infrastructure for ensuring cybersecurity and cyber protection of critical information infrastructure and state electronic information resources;

– deficient effectiveness of the security and defense entities of Ukraine in countering cyber threats of a military, criminal, terrorist, and other nature.

Understanding the influence of the factors above led to the closure of the vast majority of state law registries in the first days of the military invasion of the Russian Federation. This issue, for some time, actually limited the public's access to information about the administration of justice. On February 24, 2022, the State Enterprise "National Information Systems" temporarily suspended the work of the Unified and State Registers. The Registers worked under the authority of the Ministry of Justice of Ukraine. Also, until August 1, 2022, the Open Data Portal was terminated. In this way, state bodies tried to find a balance between ensuring human and civil rights and freedoms and providing tools for countering threats in the field of information security. In fact, this became a manifestation of the application of Article 376-1 of the Criminal Code of Ukraine. The norm of law pro-

hibits and establishes responsibility for illegal interference in the work of automated systems in bodies and institutions of the justice system. An additional threat to cybersecurity is the intensive spread of artificial intelligence, which can potentially become a new tool of cybercrimes.

5. Ways to strengthen

Researcher defines operational and administrative-legal approaches to ensuring information security (Shopina, 2023, p. 30). Actually, the second one considers the creation of a protection mechanism for information in the justice administration system. Scientists have discussed these aspects in recent research (Teremetskyi, Duliba, 2023). The administrative-legal mechanism development for the comprehensive provision of information security and the systemic interaction of its various subjects will fully reveal problematic aspects of information security in the system of justice and outline the vectors of their solution. This would be possible with the adoption of a single system document that would regulate all aspects of ensuring information security in the judicial system.

The threats in cyberspace mentioned above are caused by the spread of artificial intelligence, which, on the other hand, can be considered a new tool for state control and ensuring cybersecurity.

6. Conclusions

Cybersecurity is an essential tool for the effective functioning of all state institutions, including the justice system. It ensures the protection of information systems, registers, and databases containing confidential information about participants in the legal process.

Ukraine has formed a sufficient regulatory and legal framework to ensure cybersecurity. However, the war with Russia revealed a number of problems and threats that require urgent solutions, including in the justice system, in particular, the insufficient level of critical information infrastructure protection, the imperfection of coordination and interaction mechanisms between sub-objects to ensure cybersecurity, etc.

To increase the level of cybersecurity in the justice system, it is necessary to improve the administrative and legal mechanisms for its support and to adopt a single system document that will regulate all aspects of information security in the judicial system.

The implementation of the latest technologies based on artificial intelligence can be a promising direction for strengthening cybersecurity, but this also requires strengthening protection against potential cyber threats associated with the use of these innovations.

References:

Ukaz Prezydenta pro zatverdzhennia Stratehii kiberbezpeky Ukrainy: Bezpechnyi kiberprostir – zaporuka uspishnoho rozvytku krainy: vid 26.08.2021 № 447/2021 [Decree of the President of Ukraine On Cybersecurity strategies of Ukraine: Safe cyberspace is the key to the country's successful development: dated 26.08.2021 No. 447/2021]. Retrieved from https://zakon.rada.gov.ua/laws/show/447/2021#Text [in Ukrainian].

Perun, T.S. (2019). Administratyvno-pravovyi mekhanizm zabezpechennia informatsiinoi bezpeky v Ukraini [Administrative and legal mechanism for ensuring information security in Ukraine]. Candidate's thesis. Lviv: Lviv Polytechnic National University [in Ukrainian].

Zakon Ukrainy Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: vid 05.10.2017 № 2163-VIII [Law of Ukraine On the Basic Principles of Cybersecurity in Ukraine dated October 5, 2017 No. № 2163-VIII]. Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19#Text [in Ukrainian].

Zakon Ukrainy Pro Osnovni zasady rozvytku informatsiinoho suspilstva v Ukraini na 2007–2015 roky: vid 09.01.2007 № 537-V [Law of Ukraine On the Basic Principles for the Development of an Information-Oriented Society in Ukraine for 2007–2015 dated January 9, 2007 No. 537-V]. Retrieved from https://zakon.rada.gov.ua/laws/show/537-16#Text [in Ukrainian].

Konstytutsiia Ukrainy: vid 28.06.1996 № 254к/96-VR [Constitution of Ukraine: dated June 28, 1996 No. 254к/96-BP]. Retrieved from https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text [in Ukrainian].

Ostapenko, O., Baik, O. (2021) Administratyvno-pravova pryroda informatsiinoi bezpeky [Administrative and legal nature of information security]. *Visnyk Natsionalnoho universytetu "Lvivska politekhnika". Seriia: "Yurydychni nauky"*, no. 3 (31), pp. 167–179. Retrieved from http://doi.org/10.23939/law2021.31.167 [in Ukrainian].

Ukaz Prezydenta pro zatverdzhennia Stratehiiu voiennoi bezpeky: vid 25.03.2021 № 121/2021 [Decree of the President of Ukraine On Strategy of Military Security: dated 25.03.2021 No. 121/2021]. Retrieved from https://www.president.gov.ua/documents/1212021-37661 [in Ukrainian].

Ukaz Prezydenta Pro stvorennia Tsentru protydii dezinformatsii: vid 19.03.2021 № 106/2021 [Decree of the President of Ukraine On establishment Center for Countering Disinformation: dated 19.03.2021 No. 106/2021]. Retrieved from https://zakon.rada.gov.ua/laws/show/106/2021#Text [in Ukrainian].

Hetman, A.Ye., Politanskyi, V.S., Hetman, K.O. (2023) Do pytannia praktyky stanovlennia ta rozvytku mizhnarodnoi informatsiinoi bezpeky, yak pravovoho mekhanizmu zdiisnennia elektronnoho uriaduvannia [To the question of the practice of establishing and developing international infor-

mation security as a legal mechanism for implementing electronic governance]. Visnyk Natsionalnoi akademii pravovykh nauk Ukrainy, no. 1 (30), pp. 91–108 [in Ukrainian].

Rozporiadzhennia Kabinetu Ministriv Ukrainy Pro skhvalennia Stratehii rozvytku informatsiinoho suspilstva v Ukraini vid 15.05.2013 № 386-p [Order of the Cabinet of Ministers of Ukraine On the approval of the National Strategy of the Information Society in Ukraine: dated 15.05.2013 No. 386-p]. Retrieved from https://www.kmu.gov.ua/npas/246420577 [in Ukrainian].

Ukaz Prezydenta pro Stratehiiu natsionalnoi bezpeky Ukrainy "Bezpeka liudyny – bezpeka krainy": vid 14.09.2020 № 392/2020 [Decree of the President of Ukraine On the National Security Strategy of Ukraine "Human security—the security of the country": dated 14.09.2020 No. 392/2020]. Retrieved from https://zakon.rada.gov.ua/laws/show/392/2020#n7 [in Ukrainian].

Ukaz Prezydenta pro Doktrynu informatsiinoi bezpeky Ukrainy: vid 25.02.2017 № 47/2017 [Decree of the President of Ukraine On the Information Security Doctrine of Ukraine: dated 25.02.2017 No. 47/2017]. Retrieved from https://www.president.gov.ua/documents/472017-21374 [in Ukrainian].

Rishennia Vyshchoi rady pravosuddia Pro zatverdzhennia Polozhennia pro poriadok funktsionuvannia okremykh pidsystem Yedynoi sudovoi informatsiino-telekomunikatsiinoi systemy: vid 17.08.2021 № 1845/0/15-21 [Decision of the Supreme Council of Justice on the approval of the Regulation on the procedure of functioning the separate subsystems (modules) of Unified Judicial Information Telecommunication System dated 17.08.2021 No. 1845/0/15-21]. Retrieved from https://zakon.rada.gov.ua/rada/show/v1845910-21#Text [in Ukrainian].

Analitychna zapyska Natsionalnoho instytutu stratehichnykh doslidzhen Problemy vprovadzhennia suchasnykh standartiv informatsiinoi bezpeky v umovakh stanovlennia natsionalnoi systemy kiberbezpeky Ukrainy vid 05.2018 [Analytical note of the National Institute of Strategic Studies Problems of implementing modern information security standards in the conditions of the formation of the national cyber security system of Ukraine: dated 05.2018]. Retrieved from https://niss.gov.ua/sites/default/files/2018-06/1_cPPP-standarts_27-04_Gn_var_FIN-732b6.pdf [in Ukrainian].

Vyzdryk, V.S., Melnyk, O.M. (2023) Informatsiina bezpeka v Ukraini: suchasnyi stan [Information security in Ukraine: current state], *Mizhnarodnyi naukovyi zhurnal "Graal nauky"*, no. 24, pp. 196–202. Retrieved from https://doi.org/10.36074/grail-of-science.17.02.2023.034 [in Ukrainian].

Shopina, I.M. (2023) Informatsiina bezpeka tsyfrovoi transformatsii. [Information security of digital transformation], *Naukovyi visnyk Lvivskoho derzhavnoho universytetu vnutrishnikh sprav*, no. 1, pp. 28–35. Retrieved from https://doi.org/10.32782/2311-8040/2023-1-4 [in Ukrainian].

Teremetskyi, V.I., Duliba Ye.V. (2023). Osoblyvosti vprovadzhennia ta funktsionuvannia Yedynoi sudovoi informatsiino-telekomunikatsiinoi systemy yak instrumenta elektronnoho pravosuddia [Peculiarities of implementation and functioning of the Unified judicial information and telecommunication system as an e-justice tool]. *Forum prava*, no. 2 (75), pp.130–143. Retrieved from http://doi.org/10.5281/zenodo.10007341 [in Ukrainian].

Андрій Колесніков,
кандидат економічних наук, доцент, доцент кафедри безпеки та правоохоронної діяльності, Західноукраїнський національний університет, вулиця Львівська, 11, Тернопіль, Україна, індекс 46009, Kole.ua@gmail.com
ORCID: *orcid.org/0000-0003-3064-4133*

КІБЕРБЕЗПЕКА ЯК НЕОБХІДНА УМОВА ФУНКЦІОНУВАННЯ СИСТЕМИ ЗДІЙСНЕННЯ ПРАВОСУДДЯ

Анотація. ***Мета.*** Метою статті є системний аналіз стану кібербезпеки України, дослідження її впливу на функціонування системи здійснення правосуддя, а також окреслення шляхів усунення виявлених загроз. ***Методи дослідження.*** Структура статті побудована відповідно до теоретичних, аналітичних та прогностичних завдань і відображає використання окремих методів наукового дослідження та наукових матеріалів. Для дослідження категорійного апарату використано теоретичний метод, нормативно-правової бази забезпечення кібербезпеки – структурно-функціональний та системний методи. Під час дослідження проблем та загроз порушення кібербезпеки в умовах військового вторгнення Російської Федерації використано метод абстрагування, що дозволив виокремити серед значної кількості критеріїв найбільш значущі, на думку автора. В обґрунтуванні висновків використано метод наукового узагальнення. ***Результати.*** Кібербезпека визначена як захист інтересів людини, суспільства і держави в кіберпросторі для сталого розвитку. У системі здійснення правосуддя інформаційна безпека розглядається як об'єкт правової охорони для захисту даних усіх учасників системи судочинства. Визначено складники адміністративно-правового забезпечення кібербезпеки. Обґрунтовано необхідність системного підходу до протидії кіберзагрозам на міжнародному рівні. Під нормативно-правовим регулюванням інформаційної безпеки розуміємо правовий вплив держави на відповідні суспільні відносини. Кібербезпека є складовою частиною націо-

нальної безпеки. В Україні прийнято низку документів щодо розвитку інформаційного суспільства та забезпечення кібербезпеки, однак потрібно вдосконалювати спеціалізовані нормативні акти, гармонізувати їх з міжнародними стандартами, зокрема ISO/IEC 27000. Обґрунтовано, що комплексний адміністративно-правовий механізм забезпечення інформаційної безпеки та взаємодія його суб'єктів дозволить виявити проблеми та шляхи їх вирішення. Для цього потрібен єдиний документ щодо інформаційної безпеки в судочинстві. ***Висновки.*** Кібербезпека є важливою для ефективного функціонування системи правосуддя, забезпечуючи захист конфіденційних даних учасників процесу. Україна має нормативно-правову базу в цій сфері, проте війна з РФ виявила низку проблем – недостатній захист інфраструктури, слабку координацію суб'єктів кібербезпеки тощо. Для підвищення рівня захисту потрібно вдосконалити правовий механізм забезпечення кібербезпеки, прийняти єдиний документ з регламентації всіх аспектів інформаційної безпеки в судовій системі. Перспективним також є застосування штучного інтелекту за умови належного захисту від загроз.

Ключові слова: правосуддя, суд, інформаційна безпека, кібербезпека, нормативно-правове забезпечення кібербезпеки, воєнний стан.

The article was submitted 16.10.2023
The article was revised 07.01.2023
The article was accepted 27.11.2023