УДК 341.1.; 343.1 + 004

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

THE ESSENCE OF CYBER-OFFENCES COMMITTED IN THE CONDITIONS OF DIGITALIZATION OF SOCIETY: CRIMINAL-LEGAL AND ADMINISTRATIVE-LEGAL ASPECTS

http://doi.org/10.23939/law2025.46.096

The article is devoted to the study of the essence and classification of cyber-offences committed in the conditions of total digitalization of society, as well as administrative-legal means of counteracting the indicated types of cyber-offences. The author analyzes different approaches to defining the terms "computer crimes", "cybercrime", "internet crime" and others, emphasizing the significant differences in the essence of these concepts, since the essence of cybercrime is not a static category, but continues to develop in view of the rapid development of technologies and the digitalization of society, which undoubtedly gives rise to discussions on methods, including administrative and legal, of counteracting these offenses. Therefore, today cybercrime can be defined as a complex of offenses that include the misuse of computer equipment, programs or cyberspace to commit illegal actions that cause harm to individuals, organizations or the state.

The author states that two approaches to understanding cybercrime have now been formed, narrow and broad. The narrow approach focuses on the protection of information security, while the broad approach covers all types of offenses committed using information and telecommunications technologies. The lack of a unified approach to defining cyber offenses negatively affects the organization of counteraction to these criminally unlawful acts in practice. The author emphasizes the importance of unifying the conceptual apparatus and adapting both criminal and administrative legislation to the growing challenges in the field of cybersecurity.

The author analyzes the norms of individual international legal acts, in particular the Convention on Cybercrime, which defines certain groups of cyber offenses, in particular: – against the confidentiality of computer data, – against the integrity of computer data, against the availability of computer data, – related to content, – related to copyright infringement. The norms of the Criminal Code of Ukraine and the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity in Ukraine" are also analyzed. An analysis of various current positions on the classification features of cybercrimes is presented, in particular in the field of violation of constitutional rights, in the field of violation of property rights, in the field of public morality, and state security.

Keywords: cyberspace, cybercrimes, computer crimes, cybercrime, administrative and legal counteraction to cybercrimes.

Problem statement. Over the past decades, the number of cybercrimes in the world has increased significantly, which is confirmed by the huge reputational and financial losses of both state structures and individuals and legal entities. Therefore, there is a need for effective countermeasures to solve this large-scale problem. For this purpose, the creation of cyber police was announced in October 2025. The creation of this body is an integral element of the development of the domestic cybersecurity system [1], which is designed to organize counteraction to illegal encroachments in the information space. High-quality structural development of cyber police is impossible without the application of a complex of administrative and managerial actions both in relation to its employees themselves and other subjects of legal relations in the cyber sphere. The implementation of these actions should become the basis for the creation of an effective law enforcement body of the European model. However, despite this, it should be noted that the level of cybercrime and the complexity of offenses in this area are increasing, while the resolution of proceedings and the effectiveness of countering criminal illegal activities in cyberspace are decreasing. Moreover, the law enforcement system today faces challenges related to the international nature of cybercrimes, when actions committed in one country lead to consequences in another, which requires interstate cooperation and unification of legal norms. The cross-border nature of such criminal acts complicates the process of identifying perpetrators and bringing them to justice. In addition, there is the importance of adapting criminal legislation to rapidly changing technologies, which requires constant updating of legislative acts and methods of their application. This includes not only the creation of new legislative norms, but also the modification of existing ones so that they can adequately reflect the realities of modern digital society. That is why acts related to cybercrimes require comprehensive analysis and the development of a comprehensive approach to their essence and classification.

Analysis of the research problem. Research into the sphere of offenses in the information sphere (cyber offenses) and methods of countering cyber offenses are extremely relevant today and are reflected in the works of such well-known Ukrainian scientists as O. Amelin, Y. A. Belsky, B. M. Golovkin, A. Holub, M. Gutsalyuk, O. P. Dzyuban, V. B. Dzyundzyuk, M. M. Dmytruk, D. V. Dubov, S. B. Zhdanenko, Y. B. Irkha, N. V. Karchevsky, E. V. Kovalenko, O. Kopatin, M. S. Kornienko, E. M. Manuilov, G. Nagornyak, Y. Nedilko, M. A. Pogoretsky, A. V. Savchenko, M. Sambor, V. I. Tymoshenko, S. Fedonyuk, O. I. Yaremenko. Also relevant are the studies of foreign scientists: L. Lessig, L. Nottage, T. Tropina, Ivana dos Santos Teixeira, M. William, D. Sheldon, M. E. Katsh, D. G. Post, K. Ferzan, Neil Boister, Vermeulen Gert, Wendy De Bondt, Charlotte Ryckman, B. Dupont, N. Kshetri.

The purpose of the article is to analyze the essence and classification of cybercrimes committed in the conditions of total digitalization of society in the context of improving the current criminal legislation in order to determine their legal features and specifics, as well as to study administrative and legal means of combating the above cybercrimes in order to eliminate gaps in the organization of such counteraction.

Presentation of the main material. The essence of cybercrime has become widespread today due to the information and telecommunications breakthrough that occurred at the turn of the 20th and 21st centuries. Cybercrime is a set of offenses committed in “cyberspace” using computer systems or computer networks, with the use of information technologies, as well as other means of access to cyberspace within computer systems or networks, as well as against computer systems, computer networks and computer data. It should be noted that various terms are used to define criminally unlawful acts committed using information and telecommunications technologies: “computer offenses”, “cyber offenses”, “Internet offenses”, “offenses committed using Internet technologies”, “offenses committed in a virtual environment”, “offenses committed on the Internet”, “offenses committed using information and telecommunications technologies”, “computer crime”, “cybercrime”, “Internet crime”, “cyberattacks”, “cyberwars”, “cyberconflicts”, etc. [2, p. 11; 24]. However, a study of scientific sources, regulatory legal acts

relating to the issues of countering actions carried out using information and telecommunications technologies states that the understanding of the law enforcement object is covered by the concept of information security (narrow approach). In a broad approach, these terms are used to designate a wide variety of offenses committed in virtual space using computer technology and information and telecommunications networks, as well as other means of access. There is also a position that the terms "computer offenses" and "cyber offenses" should be used for effective implementation of applied (criminological, forensic) and criminal procedural research. However, in the general context, the term "offenses in the field of information technology use" is still used [3, p. 54].

One of the studies examines the concepts of "information technology offenses" and "information security" and concludes that information technology offenses belong to the category of criminal offenses related to information security, defined by the Criminal Code of Ukraine as socially dangerous acts committed by the subject of the offense, which harm relations in the field of satisfying information needs using computer technology. The current norms of the Criminal Code of Ukraine allow us to establish that such crimes include acts that correspond to Articles 361, 361-1, 361-2, 362, 363, 363-1, 376-1 of the Criminal Code [4]. Therefore, we believe that the stated statement about the classification of certain actions as "criminal offenses in the field of information technology" is unfounded, since a contradiction arises: for example, copyright infringement through interference with the operation of a computer, according to this logic, is not considered harm to "relations in the field of satisfying information needs" and is not carried out using "computer technology means". And this is actually not the case.

According to another position, computer criminal offenses and cybercrimes constitute separate categories of criminal unlawful acts in the field of modern information technologies and are classified depending on the features: computer offenses are determined by the use of computer equipment as a tool for committing the offense. At the same time, cybercrimes are characterized by the peculiarity of the environment where they are committed– cyberspace, which includes computer systems and networks. The author also emphasizes that the object of attack in such criminal actions is social relations that regulate automated information processing and, based on the provisions of the Convention and its Additional Protocol, argues that only the actions listed in these documents can be classified as cybercrimes [5, pp. 5–6]. At the same time, O. Kopatin and E. Skulyshyn define cybercrime as a criminal offense that is associated with the use of cybernetic computer systems or is committed in cyberspace. From their position, its difference from computer crime is that the latter concept concerns the use of any computer technologies, while cybercrime has a narrower nature and concerns only the functioning of cybernetic computer systems [6, pp. 85–86]. From the position of M. Dumchykov, cybercrime is understood as offenses in the field of high information technologies committed by perpetrators who use these technologies for illegal purposes. Other authors define cybercrime through the concept of "cyberspace" (cybercrime is crime in cyberspace [7, p. 66; 23]. Thus, among scientists there is one established position in the definition of cybercrime, which is due to different interpretations of the methods of using computer systems in committing relevant illegal actions.

We share the position that a broad interpretation of the term "cybercrime" is legitimate, since the results of criminological research indicate a steady trend towards the emergence in virtual space of new types of encroachments on various legally protected social relations (life, health, sexual development of minors, property, including intellectual, public safety, public health, public morality, the foundations of the constitutional order, peace and security of humanity, etc.). Cybercrime is characterized by the fact that information, information and telecommunication technologies can act as the subject, a tool or means of committing a socially dangerous act [23; 24].

A broad interpretation of the analyzed concepts was also manifested in the discussion of current problems of combating cybercrime within the framework of the 10th UN Congress in 2000, which adopted the Convention on Combating Cybercrime. Speakers at this UN Congress used the concept of cybercrime to refer to "computer" offenses, where the object is information security and the subject is a computer, as well as encroachments on any social relations carried out using computers as a tool or means [23]. It is worth noting that the first international legal act in which measures were taken to unify the list and

characteristics of cybercrime was the Convention on Cybercrime, adopted by the Committee of Ministers of the Council of Europe on November 8, 2001 in Budapest [8]. In summary, we note that the CoE Convention and Protocol No. 1 (adopted in 2002) to the Convention on Cybercrime provide for five groups of offenses: 1. Offenses against the confidentiality, integrity and availability of computer data and systems. 2. Offenses related to the use of computer facilities. 3. Offenses related to the content of data. 4. Offenses related to the violation of copyright and related rights. 5. Offenses in the form of acts of racism and xenophobia committed using computer networks.

To date, the above-mentioned UN Convention has been ratified by more than a third of the world's states. The participating states are invited to criminalize attacks on such objects as information (computer) security, property, intellectual property, as well as to criminalize actions related to the dissemination of illegal content on information networks (child pornography; extremist information). A similar interpretation of cybercrime is also observed in other directives of the countries participating in the Convention, devoted to the problems of countering attacks on information networks, as well as maintaining the security of networks and information systems [9, p. 20]. It should be noted that in the above-mentioned UN and European Union documents, cybercrime includes not only "computer" offenses that encroach on information security, but also other criminal actions that use a computer as a weapon (computer-facilitated) or a means of offense (computer-related). This position seems to be generally correct, since the use of information and telecommunication technologies as a tool or means of criminal encroachment on any objects increases the effectiveness of criminal activity, giving it a qualitatively new form, making it cross-border, large-scale and difficult to investigate.

However, it should also be noted that, unfortunately, the above-mentioned UN and EU documents ignore the problem of countering the use of information and telecommunication technologies as weapons in military-political conflicts, for interference in the internal affairs of states, for subversive, terrorist, espionage and sabotage activities. In addition, the analyzed official acts of the UN and the EU do not take into account the possibilities of "mobile" access to the Internet for committing cybercrimes. This does not allow us to attribute to cybercrimes encroachments during which non-computer devices, other devices that provide access to the network are used, in particular, "portable" mobile phones. Therefore, it would be more correct to consider cybercrime as a set of offenses committed using information and telecommunications technologies that violate information security and (or) use a computer, as well as other devices that provide access to the network, as tools or means of committing an offense [10, p. 313].

In the context of national legislation, the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity in Ukraine" defines "cybercrime" (computer crime) as an act that is socially dangerous and culpable, committed in or through cyberspace, liability for which is provided for by the criminal legislation of Ukraine or which is recognized as a crime in accordance with international treaties that Ukraine has ratified [11]. At the same time, we believe that the term "computer crime" refers only to offenses committed against a computer or computer data.

Thus, the above definitions emphasize the key features of cybercrime, most revealing its nature, since: – firstly, they reflect the attitude of cyberspace to information space as private to public; – secondly, they specifically draw attention to the fact that information and telecommunication networks (including the Internet) are material components of cyberspace. Taking into account the concept of "cyberspace", cybercrime can be characterized as a set of acts committed in cyberspace using computer systems or networks, as well as other tools for accessing this space, carried out within computer systems or networks or directed against these systems, networks and their data [12, p. 92].

There is a new position on the use of the term "cyberspace" to reveal the essence of the concept of "cybercrime". Cybercrime is understood as an offense that causes harm to diverse social relations, committed remotely, through the use of computer technology and information and telecommunication networks and cyberspace [13, p. 17]. In the above definition, cyberspace acts as a direct means of committing an offense. We believe that defining the essence of the concepts of "cybercrime" and, accordingly, "cyberoffense" through the concept of "cyberspace" is appropriate, since its use allows not only to

most fully reveal the features of phenomena occurring in various information networks, but also to cover a much wider range of social relations: for example, a specific offense will not be limited to a separate object of encroachment and an information and telecommunications network, which mediates the possibility of classifying it as cybercrime as illegal access to computer information, and, for example, fraud on the Internet. However, most scholars hold the opinion that the use of the concept of "cyberspace" in domestic legal science is limited [24]. Moreover, in order to prevent excessive use of Anglicisms, it is advisable to turn to domestic types of terminology [14, p. 122; 24].

It should be summarized that now, along with the term "cybercrime", in international and domestic legal science, such concepts as "criminal acts in the field of computer information" and "crimes committed with the use of information technologies" are most often used. In the scientific literature, one can find different approaches to their understanding and use. The position of some scientists is that these are different concepts, while others consider them equivalent [15, p. 415]. We believe that the term "cybercrime" should be interpreted more broadly, since in terms of content it includes both of the above definitions. Moreover, if we turn to the primary source – foreign terminology – we can see that abroad the concepts of "computercrime" and "cybercrime" have substantive differences. In particular, the first term covers only criminal acts that encroach on computer data, while the second term also includes acts using both global networks, information technologies, and computers [16, pp. 13–14], which indicates the benefit of a broader understanding of the concept of "cybercrime".

In the scientific research of foreign researchers, including P. Morrison, B. Colin, Donn V. Parker, S. W. Brenner, Shelley, I. Louise, P. Williams, U. Sieber, and others, which are devoted to the analysis of cybercrime, there are also statements about the analyzed phenomena that provide an understanding of the further study of cybercrime in a broad (global) direction [17].

It is worth emphasizing that today there is no consensus on the list of cybercrimes. However, they can still be conditionally divided into Yes, according to the United Nations Office on Drugs and Crime, a wide range of cybercrimes can be conditionally divided into offenses that: – are committed for selfish gain; – are related to the use of information stored in computers; – are directed against the integrity, confidentiality and availability of computer systems; – are related to the violation of copyright and related rights [18]. Thus, based on the analysis, cybercrimes (computer offenses) should be classified as socially dangerous criminal acts committed in cyberspace and/or using its resources, for which criminal liability is provided. Such cybercrimes can be divided into the following two groups: 1. Offenses committed in cyberspace or using it, for which liability is provided under various sections of the Criminal Code of Ukraine. These offenses affect various areas of criminal law protection: national security, public security, protection of intellectual property rights, property, economic relations, as well as individual rights and freedoms. The use of the latest information technologies and computer equipment in their commission is characteristic. For example, theft of payment card details (phishing, vishing, shimming, skimming); illegal financial transactions using payment cards without the owner's consent (carding); appropriation of funds through non-existent online stores, online auctions or other online platforms (Internet fraud); violation of copyright and related rights through illegal distribution of software through networks (piracy). 2. Offenses in the field of use of computers, their systems and networks, which are regulated by Chapter XVI of the Criminal Code of Ukraine. These actions affect the relationships that arise in the process of using electronic computers, their systems and networks, as well as telecommunications networks [19, pp. 60–61].

We also consider it necessary to emphasize that the list of offenses in the field of computer information, reflected in a special part of the Criminal Code of Ukraine, does not cover all possible criminally unlawful acts committed in cyberspace, and therefore we consider the most appropriate classification proposed by A. Golub, who proposes to classify cyber offenses into the following categories: – criminal offenses in the field of computer information, directed against information computer relations; – criminal offenses in the information computer space, which affect relations on the exercise of rights to information resources; – other criminal offenses, characteristic of the conditions of use of computer information or its components [19].

Professor A. V. Savchenko believes that cybercrimes may also include other criminal acts specified in the Criminal Code of Ukraine, if information network technologies are chosen as the instrument of commission, and the consequences of such acts are manifested in cyberspace [20, p. 154]. The author includes in the category of criminal acts committed in cyberspace such criminal acts as treason, espionage, sabotage, violation of voting secrecy, illegal disclosure of medical secrets, as well as disclosure of secrets in the commercial and banking spheres, pimping, and others. It can be argued that practically in every section of the special part of the Criminal Code of Ukraine there are criminal acts that can be committed in cyberspace using computers and software.

The classification of cybercrimes proposed by V. Dzyundzyuk is also correct, indicating: 1. Crimes against constitutional rights and freedoms of man and citizen, which include violations of privacy, secrecy of correspondence and other messages, as well as violations of copyright; 2. Crimes against life and health, which include recipes for making narcotic substances at home and their distribution; 3. Crimes against honor and dignity, including the distribution of compromising information and slander; 4. Crimes against property, in particular criminal actions in the field of payment and banking systems; 5. Crimes in the field of computer information, which include illegal access to information, creation and distribution of viruses; 6. Crimes against public morality; 7. Crimes against state security, such as illegal access to state secrets, which becomes possible through the use of the Internet in state structures [21]. The proposed rather extensive system of types of cybercrimes indicates that the scale of cybercrime is increasing. Thus, the need for interaction between the state and society and the international community in order to overcome this negative phenomenon is increasing. As for the legal forms of administrative and legal counteraction to cybercrime, the following should be included: – adoption of regulatory legal acts in the field of counteraction to cybercrime, – adoption of individual acts in the field of counteraction to cybercrime, – conclusion of administrative agreements. One of the forms of administrative–legal counteraction to cybercrime is an administrative contract – a voluntary agreement between two or more subjects of administrative law, one of which is endowed with its own or delegated powers in the field of public administration regarding the resolution of executive and administrative issues, concluded in the form of a legal act that establishes (terminates, changes) their mutual rights, obligations and responsibilities [1, p. 10]. Among the legal forms, it is also worth highlighting legal implementation, which is manifested in the implementation of administrative-legal norms in the field of counteraction to cybercrime in the activities of legal subjects, which is ensured by observing prohibitions, using subjective rights and fulfilling legal obligations when countering cybercrime. Organizational administrative and legal forms of combating cybercrime include: holding meetings, round tables, seminars, trainings, etc., carrying out administrative supervision in the form of observation, inspection, inspection of facilities, preventive accounting, etc. Specific administrative and legal forms of combating cybercrime are the inspection of facilities in the information and telecommunications sector and monitoring the work of facilities that provide information services (providers and telecommunications operators) [22].

Conclusions. Thus, it can be stated that the concept of “cybercrime” reflects a wide range of criminally unlawful acts committed in cyberspace using and with the help of computer systems and networks, as well as through the application of the latest artificial intelligence technologies. Therefore, the specified offenses, depending on the object of the offense, are of a diverse nature and include offenses ranging from the field of information security to fraud and cyberattacks. Therefore, various terms are used to characterize these offenses (“computer offenses”, “cybercrime”, etc.), which are characterized by their specificity. Such differences in the interpretation of offenses have a rather negative impact on the legislative and practical aspects of countering cybercrime. It is important to note that the essence of cybercrime is not a static category, but continues to develop in view of the rapid development of technologies and the digitalization of society, which undoubtedly gives rise to discussions about methods, including administrative and legal, counteraction to the specified offenses. Therefore, we consider it necessary to support the position that currently cybercrimes can be defined as a set of offenses that include

the misuse of computer equipment, programs or cyberspace to commit illegal actions that cause harm to individuals, organizations or the state [24]. As for the administrative and legal forms of counteraction to offenses, such forms are determined, first of all, by the specifics of a particular subject of counteraction to cybercrime, in particular: the range of tasks it solves, the system of relevant functions and powers assigned to this subject. The specified forms of administrative and legal counteraction to cybercrimes are determined by the current legislation, as well as the objective real circumstances of their commission. Therefore, there is a need for their further research, systematization, and legislative consolidation, taking into account the rapid development of information technologies, which will undoubtedly ensure the organization and effectiveness of responding to criminally unlawful incidents in the cyberspace.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Афанасьєв К. К. (2002) Адміністративний договір як форма державного управління (теоретико-правовий аспект) : автореф. дис... канд. юрид. наук: 12.00.07 / Нац. ун-т внутр. справ. Х., 2002. 19 с.

2. Кіберзлочинність та електронні докази = Cybercrime and digital evidence (2022): навч. посіб. / Б. М. Головкін, О. І. Денькович, В. В. Луцик, Д. М. Цехан]; за ред. канд. юрид. наук, доц. Ольги Денькович, д-р права, проф. Габріеле Шмельцер. Електрон. вид. Львів: ЛНУ ім. Івана Франка, 298 с.

3. Неділько Я. (2018). Поняття кіберзлочинів та їх види. Науковий часопис Національної академії прокуратури України. № 4. С. 49–60.

4. Кримінальний кодекс України. Закон України від 05.04.2001 № 2341-III. Відомості Верховної Ради України (ВВР). 2001. № 25–26, ст. 131.

5. Амелін О. (2016). Визначення кіберзлочинів у національному законодавстві. Науковий часопис Національної академії прокуратури України. № 3. С.1–6.

6. Копатін О. (2012). Словник термінів з кібербезпеки / О. Копатін, Є. Скулишин. Київ: ВБ “Аванпост-Прим”, 214 с.

7. Думчиков М. О. (2022). Кримінально-правова характеристика поняття та видів кіберзлочинів. Науковий вісник Міжнародного гуманітарного університету. Сер.: Юриспруденція. № 55. С. 65–68.

8. Конвенція про злочинність у сфері комп’ютерної інформації ETS No 185 (Будапешт, 23 листопада 2001 р.). URL: https://rm.coe.int/1680081580 (Дата звернення: 11.10.2024).

9. Гуцалюк М. (2002). Європейська конвенція з кіберзлочинів /Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні: науково-технічний збірник. Вип. 4. С. 19–23.

10. Грицун О. О. (2014). Питання міжнародно-правового регулювання інформаційного тероризму. Часопис Київського університету права. № 4. С. 312–317.

11. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. Відомості Верховної Ради (ВВР), 2017, № 45, ст. 403.

12. Погорецький М. А. (2012). Кіберзлочини: до визначення поняття. Вісник прокуратури. № 8. С. 89–96.

13. Дмитрук М. М. (2017) Питання термінології у визначенні системи злочинів в сфері ІТ (досвід інших держав) Кібербезпека в Україні: правові та організаційні питання: матеріали Всеукраїнської науково-практичної конференції (м. Одеса, 17 листопада 2017 р.). Одеса: Одеський державний університет внутрішніх справ, С. 16–18.

14. Шемчук В. В. (2018). Кіберзлочинність як перешкода розвитку інформаційного суспільства в Україні. Вчені записки ТНУ імені В. І. Вернадського. Серія: юридичні науки. Том 29 (68). № 6. С. 119–124.

15. Бельський Ю. А. (2014). Щодо визначення поняття кіберзлочину. Юридичний вісник. Вип. 6. С. 414–418.

16. Privacy and legal issues in cloud computing. Elgar law, technology and society (2015) / ed. by R. H. Weber, A. Cheng. London: Edward Elgar Pub, XIV, 290, 14 p.

17. Schriver R. (2002). You cheated, you lied: the safe harbor agreement and its enforcement by the Federal Trade Commission. Fordham Law Review. Vol. 70, iss. 6. P. 2777–2818.

18. Коваленко Є. В. (2019). Передумови загроз у сфері інформаційної безпеки та перспективи їх подолання. Актуальні проблеми управління інформаційною безпекою України: зб. тез наук. доповідей X Всеукраїнська наук.-практ. конф., Київ, 4 квітня 2019 року / Нац. акад. СБУ. Київ. С. 57–61.

19. Голуб А. Кіберзлочинність у всіх її проявах: види, наслідки та способи боротьби. URL:http://www.gurt.org.ua/articles/34602 (Дата звернення: 13.10.2024).

20. Савченко А. В. (2012). Кваліфікація кіберзлочинів. Протидія кіберзлочинності в Україні: правові та організаційні засади: навч. посіб. Київ: Видавничий дім "Скіф". С. 140–210.

21. Дзюндзюк В. Б. Поява і розвиток кіберзлочинності. Державне будівництво. 2013. № 1. URL: http://nbuv.gov.ua/UJRN/DeBu_2013_1_3 (Дата звернення: 13.10.2024).

22. Марков В. В. (2015) Поняття та види форм адміністративноправової протидії кіберзлочинності в Україні / Європейські перспективи. № 7. 2015. С. 43–47.

23. Шак Р. І. (2024). Поняття та види кіберправопорушень в кримінальному праві / Вісник Національного університету "Львівська політехніка". Серія: "Юридичні науки". Вип. 11. №4 (44). 2024. С. 325–335.

24. Шак Р. І., Гузела Н. М. (2024). Застосування штучного інтелекту у кіберправопорушеннях / Право UA. № 4. 2024. С. 163–172. DOI: https://doi.org/10.32782/LAW.UA.2024.4.24

REFERENCES

1. Afanasiev, K. K. (2002) Administrative contract as a form of public administration (theoretical and legal aspect): author's abstract of the dissertation... candidate of legal sciences: 12.00.07; National University of Internal Affairs. Kh., 2002. 19 p. [In Ukrainian].

2. ***Kiberzlochynnist ta elektronni dokazy*** [Cybercrime and electronic evidence] = Cybercrime and digital evidence (2022): navch. posibnyk / B. M. Holovkin, O. I. Denkovych, V. V. Lutsyk, D. M. Tsekhan]; za red. kand. yuryd. nauk, dots. Olhy Denkovych, d-r prava, prof. Habriele Shmeltser. Elektron. vyd. Lviv: LNU im. Ivana Franka, 298 p. [In Ukrainian].

3. Nedilko, Ya. (2018). ***Poniattia kiberzlochyniv ta yikh vydy*** [The concept of cybercrimes and their types]. Naukovyi chasopys Natsionalnoi akademii prokuratury Ukrainy No. 4. P. 49–60. [In Ukrainian].

4. ***Kryminalnyi kodeks Ukrainy*** [Criminal Code of Ukraine]. Zakon Ukrainy vid 05.04.2001 No. 2341-III. Vidomosti Verkhovnoi Rady Ukrainy (VVR). 2001. No. 25–26. 131 p. [In Ukrainian].

5. Amelin, O. (2016). ***Vyznachennia kiberzlochyniv u natsionalnomu zakonodavstvi*** [Definition of cybercrime in national legislation]. Naukovyi chasopys Natsionalnoi akademii prokuratury Ukrainy. No. 3. P. 1–6. [In Ukrainian].

6. Kopatin, O. (2012). ***Slovnyk terminiv z kiberbezpeky*** [Glossary of cyber security terms] / O. Kopatin, Ye. Skulyshyn. Kyiv: VB "Avanpost-Prym", 214 p. [In Ukrainian].

7. Dumchykov, M. O. (2022). ***Kryminalno-pravova kharakterystyka poniattia ta vydiv kiberzlochyniv*** [Criminal law characteristics of the concept and types of cybercrimes]. Naukovyi visnyk Mizhnarodnoho humanitarnoho universytetu. Ser.: Yurysprudentsiia. No. 55. P. 65–68. [In Ukrainian].

8. ***Konventsiia pro zlochynnist u sferi kompiuternoi informatsii ETS No. 185*** [Computer Information Crime Convention ETS No. 185] (Budapesht, 23 lystopada 2001 r.). Retrieved from: https://rm.coe.int/1680081580 (Accessed: 11.10.2024). [In Ukrainian].

9. Hutsaliuk, M. (2002). ***Yevropeiska konventsiia z kiberzlochyniv /Pravove, normatyvne ta metrolohichne zabezpechennia systemy zakhystu informatsii v Ukraini: naukovo-tekhnichnyi zbirnyk*** [European Convention on Cybercrimes / Legal, regulatory and metrological support of the information protection system in Ukraine: scientific and technical collection]. Vyp. 4. P. 19–23. [In Ukrainian].

10. Hrytsun, O. O. (2014). ***Pytannia mizhnarodno-pravovoho rehuliuvannia informatsiinoho teroryzmu. Chasopys Kyivskoho universytetu prava*** [The issue of international legal regulation of information terrorism]. No. 4. P. 312–317. [In Ukrainian].

11. ***Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy*** [About the main principles of ensuring cyber security of Ukraine]: Zakon Ukrainy vid 05.10.2017 No. 2163-VIII. Vidomosti Verkhovnoi Rady (VVR), 2017, No. 45, 403 p. [In Ukrainian].

12. Pohoretskyi, M. A. (2012). ***Kiberzlochyny: do vyznachennia poniattia*** [Cybercrime: to the definition of the concept]. Visnyk prokuratury. No. 8. P. 89–96. [In Ukrainian].

13. Dmytruk, M. M. (2017). ***Pytannia terminolohii u vyznachenni systemy zlochyniv v sferi IT (dosvid inshykh derzhav) Kiberbezpeka v Ukraini*** [Issues of terminology in defining the system of IT crimes (experience of other countries) Cybersecurity in Ukraine]: pravovi ta orhanizatsiini pytannia: materialy Vseukrainskoi naukovo-praktychnoi konferentsii (m. Odesa, 17 lystopada 2017 r.). Odesa: Odeskyi derzhavnyi universytet vnutrishnikh sprav. P. 16–18. [In Ukrainian].

14. Shemchuk, V. V. (2018). *Kiberzlochynnist yak pereshkoda rozvytku informatsiinoho suspilstva v Ukraini* [Cybercrime as an obstacle to the development of the information society in Ukraine]. Vcheni zapysky TNU imeni V.I. Vernadskoho. Seriia: yurydychni nauky. T. 29 (68). No. 6. P. 119–124. [In Ukrainian].

15. Belskyi, Yu. A. (2014). ***Shchodo vyznachennia poniattia kiberzlochynu*** [Regarding the definition of cybercrime]. Yurydychnyi visnyk. Vyp. 6. P. 414–418. [In Ukrainian].

16. ***Privacy and legal issues in cloud computing***. Elgar law, technology and society (2015) / ed. by R. H. Weber, A. Cheng. London: Edward Elgar Pub, XIV, 290, 14 p. [In English].

17. Schriver, R. (2002). ***You cheated, you lied: the safe harbor agreement and its enforcement by the Federal Trade Commission***. *Fordham Law Review*. Vol. 70, iss. 6. P. 2777–2818. [In English].

18. Kovalenko, Ye. V. (2019). ***Peredumovy zahroz u sferi informatsiinoi bezpeky ta perspektyvy yikh podolannia*** [Prerequisites of threats in the field of information security and prospects for overcoming them]. Aktualni problemy upravlinnia informatsiinoiu bezpekoiu Ukrainy: zb. tez nauk. dopovidei Kh Vseukrainska nauk.-prakt. konf., Kyiv, 4 kvitnia 2019 roku / Nats. akad. SBU. Kyiv. P. 57–61. [In Ukrainian].

19. Holub, A. ***Kiberzlochynnist u vsikh yii proiavakh: vydy, naslidky ta sposoby borotby*** [Cybercrime in all its manifestations: types, consequences and methods of combat] Retrieved from: http://www.gurt.org.ua/articles/34602. (Accessed: 13.10.2024). [In Ukrainian].

20. Savchenko, A. V. (2012). ***Kvalifikatsiia kiberzlochyniv*** [Qualification of cybercrimes]. Protydiia kiberzlochynnosti v Ukraini: pravovi ta orhanizatsiini zasady: navch. posib. Kyiv: Vydavnychyi dim “Skif”. P. 140–210. [In Ukrainian].

21. Dziundziuk, V. B. ***Poiava i rozvytok kiberzlochynnosti*** [Emergence and development of cybercrime]. Derzhavne budivnytstvo. 2013. No. 1. Retrieved from: http://nbuv.gov.ua/UJRN/DeBu_2013_1_3 (Accessed: 13.10.2024). [In Ukrainian].

22. Markov, V.V. (2015). Concepts and types of forms of administrative legal counteraction to cybercrime in Ukraine / European Perspectives No. 7, 2015. P. 43–47. [In Ukrainian].

23. Shak, R. I. (2024). Concepts and types of cybercrimes in criminal law / Bulletin of the National University “Lviv Polytechnic”. Series: “Legal Sciences”, Issue 11, No. 4 (44), 2024. P.325–335. [In Ukrainian].

24. Shak, R. I., Huzela, N. M. (2024). Application of artificial intelligence in cybercrimes / Pravo UA, No. 4, 2024. P. 163–172. DOI: https://doi.org/10.32782/LAW.UA.2024.4.24

Дата надходження статті: 25.04.2025 р.

Назарій ГУЗЕЛА
Заклад вищої освіти
“Львівський університет бізнесу та права”,
аспірант
nazariyhuzela@gmail.com
ORCID: 0000-0001-6476-6329

СУТНІСТЬ КІБЕРПРАВОПОРУШЕНЬ, ЯКІ СКОЮЮТЬСЯ В УМОВАХ ЦИФРОВІЗАЦІЇ СУСПІЛЬСТВА: КРИМІНАЛЬНО-ПРАВОВІ ТА АДМІНІСТРАТИВНО-ПРАВОВІ АСПЕКТИ

Стаття присвячена дослідженню сутності та класифікації кіберправопорушень, які скоюються в умовах тотальної цифровізації суспільства, а також адміністративно-правовим засобам протидії зазначеним такого роду кіберправопорушенням. Автор аналізує різні підходи до визначення термінів “комп’ютерні правопорушення”, “кіберправопорушення”, “інтернет-зло-

чинність" та інших, підкреслюючи істотні відмінності у сутності зазначених понять, оскільки сутність кіберправопорушення не є категорією статичною, а продовжує розвиватися з огляду на швидкий розвиток технологій та цифровізацію суспільства, що, безсумнівно, породжує дискусії щодо методів, в т. ч. адміністративно-правових, протидії зазначеним правопорушенням. Тому нині кіберправопорушення можна визначити як комплекс правопорушень, що містять зловживання комп'ютерною технікою, програмами або кіберпростором для здійснення протиправних дій, які заподіюють шкоду фізичним особам, організаціям чи державі.

Автор констатує, що нині сформувалися два підходи до розуміння кіберправопорушень: вузький та широкий. Вузький підхід зосереджується на захисті інформаційної безпеки, тоді як широкий охоплює всі види правопорушень, що здійснюються з використанням інформаційно-телекомунікаційних технологій. Брак єдиного підходу до визначення кіберправопорушень негативно впливає на організацію протидії цим кримінально протипраним діянням на практиці. Автор статті підкреслює важливість уніфікації понятійного апарату та адаптації як кримінального, так і адміністративного законодавства до все більших викликів у сфері кібербезпеки.

Автор аналізує норми окремих міжнародно-правових актів, зокрема Конвенції про кіберзлочинність, яка визначає групи кіберправопорушень, зокрема: проти конфіденційності, цілісності та доступності комп'ютерних даних та систем; пов'язані з використанням комп'ютерних засобів; пов'язані із змістом даних (контентом); пов'язані з порушенням авторських та суміжних прав; акти расизму та ксенофобії, вчинені за допомогою комп'ютерних мереж.

Ключові слова: кіберпростір, кіберправопорушення, комп'ютерні правопорушення, кіберзлочинність, адміністративно-правова протидія кіберправопорушенням.