

LAW, POLICY AND SECURITY

Journal homepage: <https://lpas.com.ua/>

Law, Policy and Security, 1(1), 18-25

Received: 01.03.2023 Revised: 11.05.2023 Accepted: 08.06.2023

UDC 343.9

Ihor Metelskyi*

PhD in Law, Associate Professor
West Ukrainian National University
46000, 46-a Mykulynetska Str., Ternopil, Ukraine
<https://orcid.org/0000-0001-8518-9321>

Mariana Kravchuk

Doctor of Law, Associate Professor
West Ukrainian National University
46000, 46-a Mykulynetska Str., Ternopil, Ukraine
<https://orcid.org/0000-0001-9987-0484>

Features of cybercrime and its prevalence in Ukraine

Abstract. The relevance of the study is due to the fact that the twenty-first century has become a challenge for all mankind. All spheres of public life have been developing and undergoing changes, including negative ones, which, of course, required the search for and application of effective methods to counteract such negative phenomena. One such phenomenon was the widespread spread of cybercrime and its impact on the quality of life. The COVID-19 pandemic, which has forced humanity to switch to remote work and study, has also contributed to the catalysts of this process. In this regard, this article aims to study the concept of cybercrime and cybercrime, identify the causes and conditions that facilitate its commission, and provide recommendations for improving Ukrainian legislation to prevent cybercrime. The following methods were used in the course of the study: dialectical, logical and dogmatic, comparative legal, sociological methods, general and statistical methods of scientific knowledge. The article substantiates the need to study the concepts of cybercrime and cybercrime; establishes the trend towards an increase in the number of criminal offences committed in the cyberspace; proves the insufficient attention of the authorized public authorities to the problem of cybercrime; and argues for the search for and application of new methods, ways and means of combating cybercrime. The materials of the article are of theoretical and practical value in the research area for further study and research of cybercrime issues; in lawmaking – for improvement of legislation based on the proposed recommendations; in law enforcement – for effective and uniform application of cyberlaw and impact on the level of cybercrime; in the educational process – for development of teaching and methodological materials relating to the study of cybercrime; in the legal and educational area – as practical and theoretical references

Keywords: security; information protection; cyberspace offences; computer virtual reality; computer crimes

INTRODUCTION

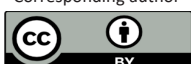
Given the development trends of the modern world, access to the Internet is an integral part of the normal existence of society. The real challenge of our time has been the spread of the Covid-19 coronavirus infection, which has acted as a catalyst for the transition of

humanity to remote work using gadgets and, of course, the Internet. This situation has provoked an increase in cases of malpractice on the part of criminals. In addition, criminal acts in cyberspace, such as identity theft, phishing, attacks on websites, and others, can cause

Suggested Citation:

Metelskyi, I., & Kravchuk, M. (2023). Features of cybercrime and its prevalence in Ukraine. *Law, Policy & Security*, 1(1), 18-25.

*Corresponding author



Copyright © The Author(s). This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (<https://creativecommons.org/licenses/by/4.0/>)

significant damage to individual users, companies, and government organisations. In Ukraine, such incidents are on the rise, indicating that cybercrime is becoming more widespread. Indeed, in 2021, 41 million suspicious information security events were recorded in Ukraine, 160,000 critical events were processed, and 147 cyber incidents were registered. The most common cyber incidents were related to: malicious software code (28%); information collection by intruders (18%); fraud (6%). (The number of cyber..., 2022). In 2022, the State Service of Special Communications registered more than 2,000 cyber incidents and an even greater number of cyberattacks in Ukraine.

In addition, Ukraine is an active participant in cyberspace, which can be used both to its advantage and disadvantage. Our Internet resources can be targeted by cyberattacks from other countries, or vice versa, we can use our knowledge to launch cyberattacks on other states. Thus, the study of cybercrime is important not only to protect our own interests, but also to prevent such actions on our part (Letter of the National Bank...2022).

In addition, cybercrime is complex and often overlaps with other types of crime, such as organised crime, human trafficking, terrorism and others. Cybercrime research can help identify such links and prevent serious criminal acts. In this regard, it seems extremely relevant to study the concept of cybercrime and the specifics of its counteraction. Cybersecurity company Trend Micro has published its own vision of the main cybersecurity threats that companies may face in 2023. These include: greater attention of cybercriminals to mistakes made by cloud users; more threats to the industrial Internet of Things (IIoT); even greater efforts by criminals to use social engineering; increased attention of cybercriminals to non-dissemination of information rather than ransom for encryption. In this regard, the study and research of this topic seems particularly relevant and necessary.

A significant number of scholars have studied this issue, including: V.G. Kundeus (2020), who studied the concept and types of cybercrime, in particular, the scientist understands cybercrime as socially dangerous criminal acts committed in cyberspace and/or with its use under the Criminal Code of Ukraine. Among the types of cybercrime, the latter distinguishes those committed in cyberspace and/or with its use, liability for which is provided for in various sections of the Criminal Code of Ukraine and crimes in the field of use of electronic computers, systems and computer networks provided for in Section XVI of the Criminal Code of Ukraine; K.V. Yurtayeva (2009), who studied the theoretical and practical issues of determining the place of commission of crimes using computer technology and establishing the criminal jurisdiction of the country.

Thus, among other things, the author's achievements include the statement that today countries apply traditional principles of criminal jurisdiction to cybercrime based on the ideology of geographical territoriality, i.e. the place of commission of international crimes using computer technologies should be considered not the territory of the country or other geographical area, but cyberspace itself; A. Rusetskyi & D. Kutsolabskyi (2017), who analysed the concepts of "cybercrime" and "cybercrime" used in the scientific legal literature and characterised the main types of cybercrime. In their scientific contributions, the authors report that cybercrime is much broader than computer crime, as it reflects not only those crimes whose object and means of attack are computers, but also crimes whose object of attack is information in general, and also provide various classifications of cybercrime, among which the most common types of cybercrime are carding, phishing, vishing, online fraud, piracy, card-sharing, social engineering, malware, illegal content, refiling; B. Belenkyi (2016), who carried out a comparative legal analysis of liability for cybercrime under the criminal law of the United States, the United Kingdom and Ukraine, and in his scientific works explores the concepts of cybercrime, cybercrime and computer crime and types of cybercrime. Quite interesting are the achievements of S.A. Buyadzhu (2018), who scientifically substantiated the concept of "mechanism of legal regulation and revealed in detail the content of the features of legal regulation of the fight against cybercrime in the European Union". Other researchers have also worked on the concept and features of cybercrime and its types, while some issues remain open and require study and improvement.

The purpose of the study is to examine and analyse the concept of cybercrime, to identify the causes and conditions that facilitate their commission, to analyse the factors that contribute to the spread of cybercrime and to provide recommendations for improving legislation in this area.

MATERIALS AND METHODS

This study was based on a system of general and special methods of cognition. The use of the empirical method made it possible to observe the peculiarities of committing cybercrime and the state of bringing the perpetrators to justice. The dialectical method was used to define the concepts and categories under study (such as cybercrime, online crime, etc.). The logical and dogmatic method was used to analyse and interpret certain legal concepts and terms. The use of the systematic method in the course of the study allowed us to assess the problem of cybercrime in a comprehensive manner and to propose ways to solve these problems. The comparative

legal method was used to determine the content of the new EU Cybersecurity Strategy¹. The study also reflects specific sociological methods (study of documents, descriptions, content analysis, etc.). General methods (analysis, synthesis, induction, deduction, abstraction, generalisation) were used to analyse legal acts, scientific sources, and to formulate interim and final conclusions. Statistical methods (grouping, classification, tabular method, etc.) were used to process and evaluate court decisions on cybercrime.

The regulatory framework of the study is the Constitution of Ukraine², provisions of the national criminal legislation^{3,4,5}, provisions of the EU Cybersecurity Strategy⁶.

The theoretical basis of the work is the scientific works of Ukrainian and foreign scholars in the field of theory of state and law, administrative, criminal,

criminal procedure law related to the subject of research. (Bregant, J., & Bregant, R., 2014; Junger *et al.*, 2017; Rusetskiy & Kutsolabskiy, 2017; Havlovskiy, 2019).

The empirical basis of the study is based on sociological surveys (Remote work in Ukraine, 2020), cybersecurity statistics (Cyber security statistics..., 2020), report of the National Police (n.d.), reports of the State Judicial Administration (Havlovsky, 2019), court verdicts^{7,8}, official statistics of the Office of the Prosecutor General (Fighting cybercrime..., 2022).

RESULTS AND DISCUSSION

The importance of working in a global network is growing every year. This is evidenced by the data of a sociological survey conducted in 2020 by EY/American Chamber (Table 1).

Table 1. Availability of an internal policy in the company to regulate remote work

The policy existed even before the quarantine began	33%
The policy has been linked to the quarantine	24%
Policy under development / planned Policy development	32%
There is no policy and no plans	11%

Source: (Remote work in Ukraine..., 2020)

As can be seen from this table, only 11% of companies do not plan to introduce remote work via the Internet, while 89% have already introduced or plan to introduce such a work option in the near future. At the same time, it is important to remember that the active development of a particular sphere of society's life also provokes any illegal actions by lawbreakers aimed at quick enrichment at minimal cost (Fighting cybercrime..., 2022).

Thus, according to Internet resources, 1120 leaks and cyberattacks were recorded in 2020 (Fighting cybercrime..., 2022). Most of these incidents were reported by the world's leading media. In total, 20,120,074,547 records were hacked. The number of detected incidents that occurred in the second half of the year shows how much impact COVID-19 has had on organisations. In addition, the number of hacked records increased by 50%

compared to 2019. According to the 2020 report of the National Police (n.d.), "...more than 5,000 cybercrimes were registered in total, in which 106 persons involved in criminal proceedings were promptly detained, including 13 paedophiles".

For comparison, in 2018, the number of criminal offences under Chapter XVI of the Criminal Code of Ukraine was 2374 (Havlovsky, 2019). According to the official statistics of the Office of the Prosecutor General of Ukraine, in the last 8 years alone, the number of detected cybercrimes has increased by almost 7.5 times (and this is without taking into account classic offences involving computer equipment and the level of latency of such crime) (Fighting cybercrime..., 2022).

Therefore, there is an obvious need to study the issues related to the commission of offences in the field of

¹New EU Cybersecurity Strategy. (2020, December). Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391.

²Constitution of Ukraine. (1996, June). Retrieved from <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text>.

³Law of Ukraine No. 2149-IX "On Making Changes To the Criminal Code of Ukraine to Improve the Effectiveness of Combating Cybercrime under Martial Law". (2022, March). Retrieved from <https://zakon.rada.gov.ua/laws/show/2149-20#Text>.

⁴Law of Ukraine No. 2149-IX "On Amendments to the Criminal Code of Ukraine to Increase the Effectiveness of the Fight Against Cybercrime in the Conditions of Martial Law". (2022, February). Retrieved from <https://zakon.rada.gov.ua/laws/show/2149-20#Text>.

⁵Criminal Code of Ukraine. (2001, May). Retrieved from <http://zakon2.rada.gov.ua/laws/show/2341-14>.

⁶New EU Cybersecurity Strategy. (2020, December). Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391.

⁷Verdict of the Khmelnytskyi City and District Court of the Khmelnytskyi Region in case No. 686/18382/17. (2021, November). Retrieved from <https://reyestr.court.gov.ua/Review/101320044>.

⁸Verdict of the Ternopil City and District Court of the Ternopil Region in case No. 607/26266/18. (2022, August). Retrieved from <https://reyestr.court.gov.ua/Review/105580335>.

cyberspace, as well as the problems of law enforcement practice of courts in this area, which, according to the authors, is to some extent dependent on the number of committed or registered offences.

It is advisable to start this study with an analysis of the concepts of cybercrime and cybercrime, since the correctness of conclusions depends on their correct understanding. There is no consensus among the scientific community on the understanding of these concepts.

Thus, in particular, according to A. Rusetskyi and D. Kutsolabskyi (2017) is an unlawful culpable act (action or inaction) that involves interference with the data of personal computers, computer programs and computer networks, or an act committed with the help of computers and other modern technologies, for which criminal liability is provided and which may create personal danger to citizens, a threat to the national security of the state and world security. At the same time, scholars understand cybercrime as a set of crimes the object and means of which is information. B. Belenkyi (2016) understands cybercrime as a culpable, socially dangerous, criminal interference with the security of computer information circulation, operation of computers, computer programs, computer networks, unauthorised modification of computer data, as well as other unlawful socially dangerous acts committed with the help of computers, computer networks and programmes, as well as other devices with built-in processors and controllers that can access the information space. Other scientists (Bachmann, 2010; Pyvovarov & Lysenko, 2016) believe that cybercrime should be called a set of crimes committed in cyberspace with the help or indirect use of computer systems or computer networks, 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. International law addresses this issue (Volevodz, 2002) by dividing cybercrime into two types: broad and narrow. At the same time, cybercrime in the narrow sense is computer crime, i.e. any unlawful acts committed through electronic operations aimed at overcoming the protection of computer systems and the data they process, and cybercrime in the broad sense is crime are

any unlawful acts committed through or in connection with a computer system or network, including crimes such as the unlawful storage, offer or dissemination of information through computer systems or networks. In 2017, when the Verkhovna Rada of Ukraine adopted the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine" on 5 October. According to clause 9 of Article 1 of the said Law, cybercrime is defined as a set of cybercrimes. At the same time, according to the same law, a cybercrime is a socially dangerous criminal act in cyberspace and/or with its use, liability for which is provided for by the law of Ukraine on criminal liability and/or which is recognised as a crime by international treaties of Ukraine¹.

Next, we propose to consider the statistics of cybercrime (and computer crime) in Ukraine. As it turned out, Ukrainian legislation^{2,3}, does not have a clear list of cybercrime or its classification, and offences in this area are included in different sections of the Criminal Code of Ukraine, and the offences provided for in Section XVI of the Criminal Code of Ukraine are only part of the totality of such crimes, which in turn has a negative impact on the statistics of such crimes and on the ways to prevent and counteract them.

It seems expedient to focus on the study of criminal offences under Section XVI of the Criminal Code of Ukraine, since this section groups some offences in the field of cyberspace. At the same time, the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine" defines cyberspace as an environment (virtual space) that provides opportunities for communication and/or implementation of social relations, formed as a result of the functioning of compatible (connected) communication systems and electronic communications using the Internet and/or other global data transmission networks.

Having analysed the statistics for 2017-2020, the number of criminal offences under Chapter XVI of the Criminal Code of Ukraine and, despite its latency, has been decreasing and increasing. At the same time, in 2020, compared to 2019, the number of such criminal offences significantly increased, as shown in the following graph (Fig. 1). (Taran & Havlovskyi, 2021).

¹Law of Ukraine No. 2163-VIII "On the Basic Principles of Ensuring Cyber Security of Ukraine". (2017, October). Retrieved from <https://zakon.rada.gov.ua/laws/show/2163-19#Text>.

²Ibidem, 2017.

³Criminal Code of Ukraine. (2001, May). Retrieved from <http://zakon2.rada.gov.ua/laws/show/2341-14>.

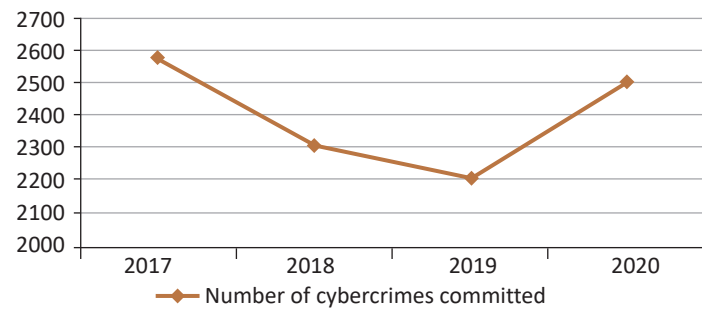


Figure 1. Statistics of the number of criminal offences (2017-2020)

Source: (Taran & Havlovskiy, 2021)

In such a situation, the question arises as to the effectiveness of the means of preventing and counteracting such offences. One of the most effective methods of combating such unlawful phenomena is the establishment of liability, in particular criminal liability as the most severe type of liability. It is through the means of combating criminal law that the state can prevent the commission of new criminal offences in the field of cybersecurity, as well as respond to such cases through special state bodies.

The main section of the Criminal Code of Ukraine that focuses on combating criminal offences in the cyberspace is Section XVI. It provides for criminal offences that encroach on the cybersecurity of the state (Articles 361-363-1 of the Criminal Code of Ukraine)¹. After analysing the sanctions of these articles of the Criminal Code of Ukraine, it can be determined that the penalties for such offences include: fines, correctional labour, restriction of liberty, imprisonment, deprivation of the right to hold certain positions or engage in certain activities. Among them, there are three types of punishment that are the main types of punishment (correctional labour, restriction of liberty, imprisonment), i.e. can be applied only as an independent punishment, and two punishments that can be imposed both as the main and additional punishments (fine and deprivation of the right to hold certain positions or engage in certain activities), i.e. can be imposed both as the main punishment and as an additional punishment. At the same time, when analysing the effectiveness of these punishments, it is necessary to establish which punishments are most often imposed by courts.

According to Havlovsky (2019), referring to the State Judicial Administration, 3 people were sentenced to imprisonment for a certain period of time for committing cybercrime (in 2017 – 7), 23 people were fined, 20 people

were released from punishment with a probationary period and 3 people were released as a result of amnesty.

According to the statistics of the State Judicial Administration (Data overview...2020), in 2020, 2 persons were sentenced to imprisonment for a certain period of time for cyber offences (over 2 years up to 3 years inclusive and over 3 years up to 5 years inclusive, respectively), 14 persons were fined in the appropriate amounts and 1 person was sentenced to another penalty. At the same time, 23 people were released from punishment, 9 people were sentenced to an additional type of punishment in the form of deprivation of the right to hold certain positions or engage in certain activities, and 23 people were sentenced for a combination of criminal offences.

This suggests that in 2020, courts began to impose less imprisonment for a fixed term as a punishment for criminal offences in the field of cybersecurity compared to 2017 and 2018, and the number of fines decreased, while the number of people released from punishment increased. Having compared the statistics, we can confidently state that one of the factors behind the increase in the number of cases of criminal offences under Section XVI of the Criminal Code of Ukraine is the increase in the number of persons released from punishment and the decrease in the number of persons who are sentenced to actual punishment, as we can see the dependence of these factors on each other.

The emphasis on combating cybercrime through sanctions is also reflected in the updated EU Cybersecurity Strategy². Thus, in view of the increasing number of cyberattacks in the European space, the application of sanctions in the event of restrictive and negative consequences for those found guilty of cybercrime seems to be a very effective mechanism for combating such phenomena. In addition, the updated Strategy envisages the activities of the Joint Cyber Division, one of the areas of

¹Law of Ukraine No. 2163-VIII "On the Basic Principles of Ensuring Cyber Security of Ukraine". (2017, October). Retrieved from <https://zakon.rada.gov.ua/laws/show/2163-19#Text>.

²New EU Cybersecurity Strategy. (2020, December). Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391.

which will be the prevention and counteraction of cybercrime and cooperation with the national authorities of partner countries.

Given the points of view on the concepts of cybercrime and cybercrime that we have studied, there are no problems with the latter, since it is logical that cybercrime should be understood as a set of cybercrimes. As for cybercrime, critically analysing the approaches to its definition available in the legislation, it should be noted that the Ukrainian legislator does not clearly distinguish between acts committed with the use of electronic computers and acts committed through electronic operations aimed at overcoming the protection of such machines' systems, as it equates them¹. We believe that it would be advisable to distinguish between these two concepts (cybercrime and computer crime) and introduce them into scientific and legislative circulation. As for the scientific approaches, based on the scientific authors we have studied, we will offer our own definition of the concept of cybercrime, i.e. a socially dangerous, culpable, unlawful act (action or inaction) committed through electronic operations, the purpose of which is to overcome the protection of computer systems and the data they process, and cybercrime in a broad sense, i.e. crimes related to the use of computers and/or committed through or in connection with a computer system or network, including such crimes as illegal storage, offering or dissemination of information through computer systems or networks.

It is obvious that with the growth of practical activities of people on the Internet, and the development of the network itself, the number of cybercrimes committed is increasing. Moreover, the offences committed in cyberspace are latent, which negatively affects their statistics and prevention. The scattering of cyber offences in different sections of the Criminal Code of Ukraine also has a negative impact on the prevention and counteraction to such violations of the law. Failure of the state and its bodies to pay due attention to the statistics of cybercrime and the sentencing of persons found guilty of committing them gives rise to the rule that "cybercriminals are forgiven for their actions". From the above, it is obvious that the combination of all these factors and the courts' loyalty to cyber offenders and their exemption from liability negatively affects the state of cybercrime in the country.

CONCLUSIONS

When planning the research, the task was to study and analyse the concept of cybercrime, cybercrime, which was done in the scientific work, while based on the

available scientific achievements, the author proposed his own definition of the concept of cybercrime. In addition, it was necessary to identify the causes and conditions that facilitate the commission of offences in the cybersphere, and to analyse the factors that contribute to their spread. Achieving this goal was made possible by studying various statistical data and sociological surveys, which led to the conclusion that the prevalence of cybercrime is influenced by a large number of factors, including the COVID-19 pandemic, increased demand for remote work and education, digitalisation of society, and the insufficiency and ineffectiveness of sanctions for criminal cybercrime. In addition, the study has resulted in a number of recommendations for combating criminal offences in the cybersphere and their implementation in various areas of legal activity. In particular, in the legislative sphere, the legislator needs to resume work in this area that will meet the requirements of the times and provide for all cybercrimes, including computer crimes, which are scattered in different sections of the Criminal Code of Ukraine in one section entitled "Criminal offences in the field of cyberspace and computer crimes", or classify them in a certain way, defining their totality. In the public administration sphere, in order to ensure effective counteraction to criminal offences in the field of cyberspace, we consider it expedient to create a new state body such as the Joint Cyber Department, which will become an effective part of the mechanism for combating cybercrime, as it will ensure coordination and uniformity of cyberlaw enforcement agencies' response to cybercrime. In the area of law enforcement, we also believe that it is advisable to increase attention to cybercrime on the part of the criminal justice authorities, ensuring that realistic sentences are imposed for their commission.

In the research area, it is necessary to continue to work on the study of the analysed topics and to offer the knowledge and experience gained for implementation in practice. In addition, it should be emphasised that in the educational sphere, it is necessary to improve the system of combating cybercrime, including, among other things, training on information security and information hygiene among students and adults, as well as among adults, which will effectively contribute to the prevention and deterrence of cybercrime.

ACKNOWLEDGEMENTS

None.

CONFLICT OF INTEREST

None.

¹Law of Ukraine No. 2163-VIII "On the Basic Principles of Ensuring Cyber Security of Ukraine". (2017, October). Retrieved from <https://zakon.rada.gov.ua/laws/show/2163-19#Text>.

REFERENCES

- [1] Bachmann, M. (2010). The risk propensity and rationality of computer hackers. *The International Journal of Cyber Criminology*, 4, 643-656.
- [2] Belenkyi, V. (2016). Liability for cybercrimes under the criminal law of the United States, Great Britain and Ukraine. (Dissertation, Academy of Advocacy of Ukraine, Kyiv, Ukraine).
- [3] Bregant, J., & Bregant, R. (2014). Cybercrime and computer crime. In *The encyclopedia of criminology and criminal justice*. Hoboken: Blackwell Publishing Ltd. doi: 10.1002/9781118517383.wbeccj244.
- [4] Buyadzhy, S.A. (2018). *Legal regulation of combating cybercrime: Theoretical and legal aspect*. (PhD dissertation, Classical Private University Of King Danylo, Kyiv, Ukraine).
- [5] Conteh, N.Y., & Royer, M.D. (2016). [The rise in cybercrime and the dynamics of exploiting the human vulnerability factor](#). *International Journal of Computers (IJC)*, 20(1), 1-12.
- [6] Cyber security statistics for 2020. (2020). Retrieved from <https://10guards.com/ua/articles/2020-cybersecurity-statistics>.
- [7] Data overview about the state of administration of justice in 2020. (2020). Retrieved from https://court.gov.ua/inshe/sudova_statystyka/ogl_2020.
- [8] Fighting cybercrime under martial law: Law 2149-IX. (2022). Retrieved from https://jurliga.ligazakon.net/analitics/210562_borotba-z-kberzlochinstyu-v-umovakh-d-vonnogo-stanu-zakon-2149-ix.
- [9] Havlovskiy, V.D. (2019). [Analysis of the state of cybercrime in Ukraine](#). *Information and Law*, 1(28), article number 112.
- [10] Junger, M., Montoya, L., Hartel, P., & Heydari, M. (2017). Towards the normalization of crime victimization. A routine activities analysis of cybercrime in Europe. In *The International Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA 2017)*. London: IEEE. doi: 10.1109/CyberSA.2017.8073391.
- [11] Kundeus, V.G. (2020). Concepts and types of cybercrimes. In *State and crime. New challenges in the Postmodern era* (pp. 44-45). Kharkiv: KhNUVS
- [12] Letter of the National Bank of Ukraine No. 56-0009/13399 "Recommendations for reducing the risk of fraudulent transactions". (2022, February). Retrieved from <https://document.vobu.ua/doc/9995>.
- [13] Pyvovarov, V.V., & Lysenko, S.Yu. (2016). [Cybercrime: Criminal Logical View on the Genesis of the Phenomenon and Ways of Prevention](#). *Law and Society*, 3, 177-181.
- [14] Remote work in Ukraine. (2020). Retrieved from http://publications.chamber.ua/2020/Human%20Capital/EY_AmCham_Remote%20work_Presentation_August_2020.pdf?fbclid=IwAR0drD89glOHm1Q9WbUjpnKe4paDFDXvt--7fAEGTlbZeEKY69Z-GzqDrY.
- [15] Report of the National Police of Ukraine on the results of work for 2020. (n.d.). Retrieved from <https://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit2020/npu-zvit-2020.pdf>.
- [16] Rusetskyi, A., & Kutsolabskyi, D. (2017). Theoretical and legal analysis of the concepts of cybercrime and cybercrime. *Law and Security*, 1(64), 74-78.
- [17] Taran, O.V., & Havlovskiy, V.D. (2021). Organized cybercrime in Ukraine: Problems of forming official statistics and their analysis. *Information and Law*, 4(39), article number 197. doi: 10.37750/2616-6798.2021.4(39).249306.
- [18] The number of cyber crimes recorded in 2021 was named by the state special communication. (2022). Retrieved from <https://zn.ua/ukr/TECHNOLOGIES/derzhspetszvjazku-nazvalo-kilkist-zafiksovanikh-u-2021-rotsi-kiberzlochiv.html>.
- [19] Volevodz, A.G. (2002). *Combating computer crimes: Legal foundations of international cooperation*. moscow: LLC Yurlitinform.
- [20] Yurtayeva, K.V. (2009). [Definition of a place where crimes with use of computer technologies are committed](#). *Law Forum*, 2, 434-441.

Ігор Дмитрович Метельський

Кандидат юридичних наук, доцент
Західноукраїнський національний університет
46000, вул. Микулинецька, 46-а, м. Тернопіль, Україна
<https://orcid.org/0000-0001-8518-9321>

Мар'яна Юрїївна Кравчук

Доктор юридичних наук, доцент
Західноукраїнський національний університет
46000, вул. Микулинецька, 46-а, м. Тернопіль, Україна
<https://orcid.org/0000-0001-9987-0484>

Особливості кіберзлочинів та їх поширеність в Україні

Анотація. Актуальність дослідження зумовлена тим, що XXI століття стало викликом для усього людства. Усі сфери суспільного життя розвивалися та зазнавали змін, в тому числі і негативних, що, звичайно вимагало пошуку та застосування ефективних методів протидії таким негативним явищам. Одним із таких явищ стало значне поширення кіберзлочинності та її вплив на якість життя. До каталізаторів цього процесу долучилася пандемія COVID-19, яка змусила людство перейти на дистанційний режим роботи та навчання. У зв'язку з цим дана стаття спрямована на дослідження поняття кіберзлочину та кіберзлочинності, виявлення причин та умов, що сприяють його вчиненню, а також надання рекомендацій щодо вдосконалення законодавства України з метою запобігання вчиненню злочинів у кіберсфері. Під час здійснення дослідження використовувались такі методи: діалектичний, логіко-догматичний, порівняльно-правовий, соціологічні методи, загальні та статистичні методи наукового пізнання. У роботі обґрунтовано необхідність дослідження понять кіберзлочин та кіберзлочинність; встановлено тенденцію до зростання кількості вчинених кримінальних правопорушень у кіберсфері; доведено недостатність уваги уповноважених органів державної влади до проблеми кіберзлочинності; аргументовано пошук та застосування нових методів, способів та засобів боротьби із кіберзлочинами. Матеріали статті становлять практичну цінність у науково-дослідній сфері для наступного вивчення та дослідження проблем кіберзлочинності; у правотворчості – для удосконалення законодавства на основі запропонованих рекомендацій; у правозастосовній сфері – для ефективного та одноманітного застосування кіберзаконодавства та впливу на рівень кіберзлочинності; у навчальному процесі – для розробки навчально-методичних матеріалів, що стосуються вивчення кіберзлочинності; у правовиховній сфері – в якості практичних та теоретичних рекомендацій для досягнення вищого рівня правової культури та формування правосвідомості у кіберсфері

Ключові слова: захист інформації; правопорушення у кіберпросторі; комп'ютерна віртуальна реальність; комп'ютерні злочини