Ivan Toronchuk, PhD in Law, Senior Vice-Dean, Associate Professor, the Department of European Law and Comparative Law Studies, Faculty of Law, Yuriy Fedkovych Chernivtsi National University, Chernivtsi, Ukraine, [i.toronchuk@chnu.edu.ua](mailto:i.toronchuk@chnu.edu.ua)

Pavlo Krainii, Vice-Dean, Assistant Professor, the Department of Public Law, Faculty of Law, Yuriy Fedkovych Chernivtsi National University, Chernivtsi, Ukraine; [p.krayniy@chnu.edu.ua](mailto:p.krayniy@chnu.edu.ua)

**Criminal Legislation of Ukraine on Crimes in the Field of Information Technologies.**

The article under studies reveals the general aspects of legal regulation of crime prevention in the field of information technology, analyzes the statistics of crimes in this area, as well as identifies the basic issues of the criminal-legal qualification of offenses in the field of applying computers, computer systems, computer and telecommunication networks.

**Issue.** The beginning of the XXI century was marked with the active use by the humanity of computer systems in commercial, banking, manufacturing and other areas. The active application of such high-tech tools has led to the problems regarding the quality protection of systems from unauthorized interference by outsiders. As a result, it was essential to develop an adequate system to protect them from unauthorized intrusion**.**

The solution of the above problem became even more complicated along with the increase in the amount of information that was accumulated and processed by computers, the Internet, etc. The crimes committed in this area did not require thorough preparation. The problematic aspects of establishing guilt, the difficulty of proving a crime, the remoteness of the object of encroachment and the possibility of obtaining a high income have made this type of crime one of the most profitable for criminals around the world.

The following scientists studied the issue of computer crimes in Ukraine: D. Azarov, P. Andrushko, Yu. Baulin, P. Bilenchuk, A. Bilousov, V. Holina, B. Holovkin, V. Holubiev, M. Hutsalyuk, Y. Zaika, M. Karchevskyi, M. Kovalenko, N. Kozak, O. Korystin, V. Kuznetsov, B. Kuzmenko, S. Kuzmin, O. Litvinov, A. Muzyka, D. Nikiforchuk, Yu. Orlov, S. Ostapets, M. Plugatyr, N. Rosenfeld, D. Rychka, A. Savchenko, H. Usatiy, V. Khakhanovskyi, V. Tsymbalyuk, V. Shelomentsev, J. Yakubovskyi and others. In view of the above, the authors of the article attempted to analyze the features of the legal regulation of the counteraction to the crimes in the field of information technology, the international standards regulating this area and the peculiarities of formation and functioning of the national system of counteracting to crimes in the field of information technology.

**The Main Body.** In order to ensure the protection of individual rights in the field of information technology in Ukraine, in 1994 there were introduced certain amendments into the Criminal Code of 1960, whereby Art. 198-1 ”Violation of the Automated Systems” provides criminal liability for intentional interference with the operation of automated systems that have led to the distortion or destruction of information or bearers of information, or the distribution of software and hardware tools, designed to illegally enter the automated systems and capable of causing distortion or destruction of information or bearers of this information.

Taking the above-mentioned measures concerning the legal regulation of liability for crimes in the field of the automated systems was not sufficient. In 2001, with the adoption of the Criminal Code of Ukraine, this activity passed onto a qualitatively new level. However, a systematic approach to counteracting cybercrimes (with a due regard of contemporary challenges and threats that information security is currently facing) has not been developed so far.

The registered criminal encroachments in the area under discussion show a significant increase in the level of these crimes over the recent years in Ukraine. The indicators are as follows: in 2013, 595 crimes were recorded, in 2014 - 443, in 2015 - 598, in 2016 - 865, in 2017 - 2573, in 2018 - 2301 crimes [1].

The main international act, which legislator in the field of counteracting cybercrimes relies on, is the Convention on Cybercrime of November 23, 2001 (hereinafter - the Convention) [2]. In July 2006, our state ratified an additional protocol to the Convention on the Criminalization of Racist and Xenophobic Acts Committed through Computer Systems (Additional Protocol) [3]. Unfortunately, the terms used in the Convention and its Additional Protocol have not yet been fully reflected in Ukrainian legislation.

Taking into account its international obligations and the effect of generally recognized methods of counteracting cybercrimes in the world, Ukraine is trying to develop its own ways of resisting this category of crimes. The issue of cybersecurity has become especially acute during the period of military aggression against Ukraine. The latter, among other things, is manifested through cyber attacks in the digital area of activities of government, enterprises, institutions and organizations. This may be proved by a number of recently adopted normative-regulatory acts. Among them are: the Law of Ukraine ”On Basic Principles of Cyber ​​Security of Ukraine”, “The Cyber ​​Security Strategy”, of March 15, 2016, “The Concept of Security and Defense Sector Development of Ukraine” of March 14, 2016, “The Strategic Defense Bulletin” of June 6, 2016, “The Regulations on the National Coordination Center for Cyber Security of Ukraine” of June 7, 2016, “The Procedure for Making a List of Information and Telecommunication Systems of the State’s Critical Infrastructure Objects” of August 23, 2016.

Despite the existing normative-regulatory acts, Ukraine’s legislation meets the needs of legal regulation to a very small extent, since it does not contain definitions of concepts that are most essential in the field of information security. According to A. Amelin, solving the problem requires the improvement of regulations, the latter being the basis of a unified state policy in ensuring information (cyber) security and its implementation [4, p. 7]. It is interesting to make a brief survey of the views of some scientists on this issue.

Scholars D. Azarov [5, p. 53-54] and N. Kozak [6, p. 156] are more prone to use the notions ”crimes in the field of information and telecommunications systems” and ”cybercrime”, rather than the concepts ”crimes in the field of computers, automated systems, computer or telecommunications networks”, regarding the former as more universal and relevant.

On the other hand, M. Pohoretskyi and V. Shelomentsev disagree with the opinion of the scientists who consider crimes in the area of using computers, automated systems, and computer and telecommunication networks as crimes committed in the information environment. According to the latter, the terms ”information environment”, ”information resources”, ”information tools” are too general for the field of using computer systems and do not reveal the essence of automated information processing [7, p. 90-92].

Thus, most scholars define cybercrimes as a combination of criminally punishable, socially dangerous acts (actions or inaction) that infringe on the right to protection against unauthorized dissemination and use of information, as well as the negative consequences of information or the functioning of information technology. Cybercrimes also include other socially dangerous acts related to the violation of the right to ownership of information and information technology, the right of owners or users of information technology to receive or disseminate reliable and complete information in due time.

It is expedient to agree with the opinion of D. Rychka that “cybercrimes should be considered as crimes committed with the help of or through computer systems or related to computer systems, i.e. a set of devices, one or more of which, according to a particular program, perform the automatic data processing” [8, p. 43-44].

To better understand the increase in the number of cybercrimes, it is worth considering the reasons for their committing. First of all, these are legal reasons. They include: insufficient legal regulation of relations (both already acting and those only being implemented) in the field of information technology and its usage. Secondly, insufficient legislative regulation within the framework of International Law, which is one of the grounds for the high level of cybercrime - the national legislation of a particular country can not solve all the problems of computer technology protection. There arises the necessity to apply common approaches and similar modes of behavior, which is possible only in case of kinship or identity of states’ national criminal legislation or additional agreements on the prosecution of offenders [9, p. 93].

According to D. Rychka, the increasing amount of the crimes committed in the field of using computers, computer systems and networks both in the world and in Ukraine may not only slow down the positive tendencies of development, but also do irreparable harm to the society, the state and the participants of information relations in all areas of economy. It is difficult to oppose them from the point of view of both criminal prosecution, and application of organizational-administrative and criminological measures that aim at their prevention [10, p. 267].

We share the idea of the above scientist. Perhaps, the rapid development of information technology and the transfer of all spheres of our lives into the digital space will only increase the number of attempts to encroach on the data that are placed in such a space. The point here is not so much in the effectiveness of legal regulation as in the rapid development of technological tools, by which the offender can use his own, unique way of committing a crime. In this case, the authorized law enforcement agencies will most likely fall behind the criminals. .

Presently, Ukraine has introduced criminal liability for crimes in this area, which are envisaged in Chapter XVI ”Crimes in the field of using computers, systems, computer and telecommunications networks” (Art. 361–363-1) of the Criminal Code of Ukraine [11]:

* unauthorized interference in the work of computers, automated systems, computer or telecommunication networks (Article 361 of the Criminal Code of Ukraine);
* creation (with the purpose of use, distribution or sale) of malicious software or hardware technologies, as well as their distribution or sale (Article 361-1 of the Criminal Code of Ukraine);
* unauthorized sale or dissemination of information with limited access, which is stored in computers, automated systems, computer networks or on the bearers of such information (Article 361-2 of the Criminal Code of Ukraine);
* unauthorized actions with information processed in computers, automated systems, computer networks or stored on bearers of such information, committed by a person who has the right to access it (Article 362 of the Criminal Code of Ukraine);
* violation of the rules of operation of computers, automated systems, computer or telecommunication networks or the violation of the procedure or rules of protection of the information processed in them (Article 363 of the Criminal Code of Ukraine);
* interference with the work of computers, automated systems, computer or telecommunication networks by mass distribution of telecommunication messages (Article 363-1 of the Criminal Code of Ukraine) [11].

It is important to point out that the Criminal Code of Ukraine provides a number of penalties for committing the crimes in the above Chapter: a fine (Articles 361; 361-1; 361-2; 362; 363; 363-1 of the Criminal Code of Ukraine); deprivation of the right to hold certain positions or engage in certain activities (Part 2, Article 3, 362, Article 363, Part 2, Article 363-1 of the Criminal Code of Ukraine); corrective work (Part 1 of Article 361-1, Part 1 of Article 362 of the Criminal Code of Ukraine); restrictions on freedom (Part 1 of Article 361 of the Criminal Code of Ukraine); imprisonment (part 1.2 of Article 361, part 1.2 Article 361-1, part 1.2 Article 361-2, part 1,2,3 Article 362, Part 2 of Article 363-1 of the Criminal Code of Ukraine) [11].

Today, the counteraction to computer crimes is carried out by specially authorized bodies operating within the system of the Ministry of Internal Affairs and the Security Service of Ukraine.

However, despite the already existing system of bodies, the introduction of a separate chapter in the Criminal Code of Ukraine and the adoption of regulations regarding the counteraction to the crimes in the field of information technology, there are still problems of organizational and legal nature. They may classified in the following way.

The first group of problems is associated with the need to improve the system of accounting, monitoring of computer crimes and the development of an up-to-date algorithm of analytical activities of the bodies authorized to deal with this category of crimes. The information obtained as a result of such activities can be effectively used to prevent computer crimes, their comprehensive analysis and assessment.

The second group aims at directing the legislation in the field of computer information to the development of interstate and domestic lawmaking, which lies in the information exchange. Mutual development and further implementation of new international agreements with foreign states will guarantee a safe transition of our country to a secure global information space.

Тhe third group of problems is closely related to the peculiarities of criminological aspects of this category of crimes, as in the course of defining the perpetrators, the authorized law enforcement agencies faced the suspects and accused who possess specific knowledge in the field of information systems. Therefore, it is extremely important to select police officers, prosecutors with specific knowledge and skills.

**References:**

1. Unified report on criminal offenses in the country: the official website of the Prosecutor General's Office of Ukraine. Available at: <https://www.gp.gov.ua/ua/stst2011.html?dir_id=104402>.
2. On Ratification of the Convention on Cybercrime: the Law of Ukraine of September 7, 2005 № 2824-IV. Available at: zakon.rada.gov.ua/laws/show/2824-15.
3. Additional Protocol to the Convention on Cybercrime, which regards the criminalization of actions of a racist and xenophobic nature committed through computer systems: the Law of Ukraine of 21.07.2006 № 23-V (ratified on 21.07, 2006). Available at: <https://zakon.rada.gov.ua/laws/show/994_687>.
4. Amelin O. Definition of Cybercrime in National Legislation. Kyiv: National Academy of the Prosecutor's Office of Ukraine, 2016. P.1–10.
5. Azarov D. Crimes in the Field of Computer Information (criminal-legal investigation). Kyiv: Atica, 2007. 304 p.
6. Kozak N. Criminal-Legal Characteristics of Crimes in the Field of Using Computers, Systems, Computer and Telecommunication Networks. Irpin:Financial-Juridical Academy, 2013. 159 p.
7. Pohoretskyi M., Shelomentsev V. Cybercrimes: to the Definition of Notions. Kyiv: National Academy of the Prosecutor's Office of Ukraine, 2012. P. 89–96.
8. Rychka D. The Peculiarities of Criminal-Legal Qualification of the Crimes in the Field of Using Computers, Systems, Computer and Telecommunication Networks. PhD Thesis. Irpin: University of State Fiscal Service, 2019.
9. Hrynchak I. Cybercrime as a Crime of International Nature. Ivano-Frankivsk: King Danylo Halytskyi Law University, 2015. P. 93-98. Available at: http://nbuv.gov.ua/UJRN/Nivif\_2015\_12\_15.
10. Rychka D. Prerequisites for the Emergence of Crimes in the Field of Using Computers. Dnipro, 2017. P. 267-268.
11. The Criminal Code of Ukraine [Electronic Resource]. Available at: https://zakon.rada.gov.ua/laws/show/2341-14#Text.