Cybercrime In Ukraine: Methods Of Investigation And Ways To Improve Them

Andrii Cherniak[†], **Mykola Karpenko**[††], **Ruslan Chornyi**[†], **Andrii Prozorov**[†], **Leonid Shcherbyna**[†]

[†] National Academy of Security Service of Ukraine, Ukraine
[††]Ivan Cherniakhovskyi National Defence University of Ukraine, Ukraine

Summary

A number of problems that really threaten the investigation of cybercrime in modern conditions are analyzed. The most common types of opposition to the investigation of such crimes by law enforcement agencies, which are manifested in various types and forms, are described. The need to overcome opposition to the investigation of cybercrimes is argued. The main directions of the fight against overcoming the investigation of cybercrime and illegal activities of stakeholders, which is aimed at concealing the detection of crimes and their investigation, are considered. The issue of the quality of cybercrime investigation in Ukraine by analyzing the legal framework for the quality of regulation of legal relations in this area is considered, the list of methods and means used to form the evidence base is outlined.

Key words: *cybercrime, investigative actions, place and time of cybercrime, examination, information technologies*

1. Introduction

Modern society is an information technology society based on the daily use of computers, communication networks, mobile communications and other technical means. The day-to-day operation of government, banking, energy, transportation and other systems is impossible without the reliable operation of computers and communications. Information technology has become a constant companion of modern man not only in the workplace, they have entered almost all spheres of human life. The spread of new information technologies, which is based on the widespread use of computer technology and communications, optimization and automation of processes in all spheres of life, has led to the leveling of borders and the intertwining of national economies and national infrastructures.

Analysis of recent research and publications. The results of the study of the special literature show that at the moment there is a large number of works that address some aspects of the fight against cybercrime. In particular, the works of Yu. M. Baturin, V. M. Butuzov, V. O. Golubev, O. Yu. Ivanchenko, M. V. Karchevsky, N. V. Kovalenko, A. A. Muzyky, D. V. Pashnev, V.S. Tsymbalyuk, VP Shelomentsev and others. At the same time, the rapid development of computer technology and areas of application of computer technology and the dynamics of the spread of cybercrime confirm that one of their first "consumers" are criminals. The latest arsenal of technical means and information, unfortunately, very quickly reach the representatives of the criminal world, because they are not limited in spending and material support, as law enforcement agencies. According to the Cyber Security Strategy of Ukraine [1], the main body responsible for information security is a unit of the National Police - cyberpolice. In addition, responsibilities for combating cybercrime are assigned to the Ministry of Defense of Ukraine, the State Service for Special Communications and Information Protection of Ukraine, the Security Service of Ukraine, the National Bank of Ukraine, intelligence agencies [1].

The Strategy for the Development of Cyber Security of Ukraine envisages that the main areas of security in the cyberspace of Ukraine are:

- development of safe, stable and reliable cyberspace, ie the creation of a single regulatory framework and bringing it to the masses in order to raise public awareness.
- cyber protection of state electronic information resources and information infrastructure designed for information processing, the requirement for protection of which is established by law, ie the development of effective methods of counteraction at the level of state and local authorities;
- cyber protection of critical infrastructure – provides development of a single public-private mechanism partnerships in cyber threat prevention;

Manuscript received October 5, 2021
Manuscript revised October 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.10.14

- development of the potential of the security and defense sector in all previous categories and connects them into a single complex.

The hardware and programs that control them are consistently determined. The information data operated by users are investigated. It shows how individual stations connect and function in a network environment.

In Ukraine and around the world, tens of thousands of crimes are committed every year using information and communication technologies, software, software and hardware, other technical and technological means and equipment. Every day, people and companies are robbed of personal data, funds from accounts, collect a lot of confidential and commercial information, block activities and more. Detection of cybercrimes is a rather difficult and difficult task of the pre-trial investigation body. This is due to the fact that criminals have special knowledge and technical means that they use to commit cybercrime, as well as the problem of detecting, recording and using electronic traces.

2. Theoretical Consideration

In Ukraine, at the legislative level, relevant laws and regulations governing relations in this area are adopted. The legal basis of cyber security of Ukraine includes the following regulations: the Constitution of Ukraine, the Criminal Code of Ukraine, the laws of Ukraine "On the basic principles of cyber security of Ukraine", "On information", "On protection of information in information and telecommunications systems", "On the basics National Security ”and other laws, the Doctrine of Information Security of Ukraine, the Council of Europe Convention on Cybercrime and other international treaties, the binding nature of which has been approved by the Verkhovna Rada of Ukraine.

According to Ukrainian legislation, cybersecurity is the protection of vital interests of man and citizen, society and the state in the use of cyberspace, which ensures sustainable development of the information society and digital communication environment, timely detection, prevention and neutralization of real and potential threats to Ukraine's national security in cyberspace. (Article 5, Part 1, Article 1 of the Law of Ukraine "On Basic Principles of Cyber Security of Ukraine"). In a global sense, cybersecurity is the implementation of measures to protect networks, software products and systems from digital attacks.

According to the Convention on Cybercrime, which has been part of Ukrainian legislation since 11.10.2005, cybercrimes are conditionally divided into four types.

The first type includes offenses against the confidentiality, integrity and availability of computer data and systems. This type of cybercrime includes all crimes against computer systems and data (for example, intentional access to a computer system or part thereof; intentional damage, destruction, deterioration, alteration or concealment of computer information; intentional commission, not having the right to manufacture, sell, otherwise purchase, distribute or otherwise make available devices, including computer programs).

The second type of cybercrime includes computer-related offenses. Such crimes are characterized by an intentional act that results in the loss of another person's property by any introduction, alteration, destruction or concealment of computer data or any interference with the operation of a computer system, with fraudulent or dishonest acquisition, without having to it is a right, an economic advantage for oneself or another person.

The third type of cybercrime covers offenses related to content (content), which is the commission of intentional illegal acts to produce, offer or provide access, distribution of child pornography, as well as possession of such files in their system.

The fourth type is intentional actions related to infringement of copyright and related rights, in accordance with the requirements of the Berne Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Agreement, as well as national legislation of Ukraine.

There are also other classifications of cybercrime, but the proposed convention is the most popular [2].

The investigation of a crime by a pre-trial investigation body, in most cases, begins with the perception and investigation of the situation in which it was committed. Finding out the circumstances of the crime helps the investigator to formulate an idea of the mechanism of the crime, the probable places of search for traces of the crime, the subject (subjects) of the crime, motive and purpose, as well as some aspects of the method.

When investigating cybercrimes, information about the probable place and time of its commission is of great importance. It is important for the investigator to establish the place of commission of this crime. First of all, establishing the place of the crime helps to establish the location of possible evidence and the range of persons involved in the crime [3]. The time of committing a cybercrime allows us to establish in what sequence the criminal acts were committed and their duration.

Instead, there is no unanimity among scientists in defining the concept of place and time of cybercrime. When investigating the crime scene, it should be noted that it is not chosen by the subjects of the crime by chance [4]. Having previously assessed the probable location from different angles, the subject actually uses it as a means of realizing his criminal intent [5]. The place of the crime is considered as a specific geographical point (territory, premises, etc.), which is closely related to other elements of the crime situation [6]. Analyzing the time of the crime, it is appropriate to note that time is not limited to astronomical properties (year, month, date, hours, minutes, seconds). This can be the time associated with seasonality, the onset of darkness or daylight hours, the time of rest and the time of absence of victims at the place of residence, the hour of "peak", the time associated with a certain frequency, etc. [6]. Given the specifics of cybercrime, we can distinguish the places of their commission: the physical environment (areas) and electronic environment (network nodes), where are: - software and hardware (media) that have been criminally affected, and their points of access to certain networks; - software and hardware that the offender used indirectly, and their points of access to certain networks; - network nodes of communication channels, with the use of which there was an exchange of information between the software and hardware of the offender and the victim [6]. As for the choice of physical environment by the offender, we must agree with the opinion of O.I. Motlyakh that criminals mainly choose the following places: - administrative and office premises of various types of business entities (enterprises, organizations, companies, firms, etc.), which use electronic devices in their production activities; - own and rented living quarters (offices, apartments, rooms, etc.), in which electronic devices are installed, provided with access to the world wide web system; - premises of communal property or related to them (basement, semi-basement or those adjacent to residential buildings), which on the rights of ownership or lease can be used for computer clubs, Internet cafes, etc. [7].

Many issues also remain problematic for Ukraine, in particular regarding the technical equipment of the investigation team. We believe that in parallel with the traditional forensic suitcases to introduce specialized scientific and technical equipment to detect, record and select information traces at the crime scene. For example, it is necessary to create specialized software that could analyze cybercrime, help identify and investigate evidence of these crimes.

The next issue is the conduct of examinations of covert investigative actions, as the law does not specify how and who should conduct them. Forensic examination is considered the main type of use of special knowledge in the investigation of computer crimes, is appointed and conducted after the initiation of a criminal case in compliance with the requirements of Art. 75–77 and 196 of the Criminal Procedure Code of Ukraine. The list of examinations that can be conducted in cases of computer crimes is quite wide. These are traditional examinations - trasological, dactyloscopic, technical-criminological, examination of documents, forensic-economic, and specialized - computer-technical and software-technical, which play a leading role in the investigation of crimes of this category. Obviously, this should be done by a specialist, but to the tasks of technical assistance of a specialist, listed in Part 2 of Art. 71 of the Criminal Procedure Code of Ukraine, these actions are not included, but the possibility of involving such specialists is probably determined by law in paragraph 6 of Art. 246 of the Criminal Procedure Code of Ukraine, which provides for participation in such actions, in addition to the procedural persons listed in it, also "other" [8].

Conclusions

The main way to fight cybercrime is to prevent cybercrime. Installing and improving security systems is the method that will be most effective in combating cybercrime.

Given the cross-border nature of cybercrime, law enforcement cooperation in investigating cybercrime at the operational level needs to be established; creating and ensuring the functioning of the mechanism for resolving jurisdictional issues in cyberspace. In the modern information society, where cyber threats are widespread and will continue to spread, it is important to constantly and systematically, in a timely manner to take effective measures to combat cybercrime, as well as to improve its methods and forms of prevention. This applies to almost all spheres of public and state life, business and socio-humanitarian environment.

Also, we can say that cybercrime has gained popularity among criminals and it poses a danger not only to the state but also to society. Law enforcement agencies are not able to effectively combat cybercrime because they need more specialists, special knowledge and skills. From the point of view of criminology, special attention needs to be paid to the development of the latest technical means and methods of detecting, extracting, recording and investigating traces of computer crimes using special knowledge. Also, we should not forget about the fruitful work of scientists and legislators.

References

[1] Cybersecurity strategy of Ukraine. URL: http://zakon.rada.gov.ua/laws/ show / 96/2016 # n11.

[2] Kuryliuk Y., Khalymon S. (2020). Criminal profile of migrants' smuggler across the State Border of Ukraine. Amazonia Investiga. Vol. 9, No. 27. pp. 195–208.

[3] Iasechko S., Kuryliuk Y., Nikiforenko V. et al. (2021). Features of Administrative Liability for Offenses in the Informational Sphere. International Journal of Computer Science and Network Security. Vol. 21. No.8. pp. 51–54.

[4] Zadorozhnia H., Mykhtunenko A., Kuryliuk Y. et al. (2021). Protection of Information Sovereignty as an Important Component of the

Political Function of the State. International Journal of Computer Science and Network Security. Vol. 21. No.9. pp. 151–154.

[5] Nikiforenko V. (2021). Modern Threads to the National Security of Ukraine Related to Incomplete Legal Formalization Process of Ukrainian State Border. Cuestiones Politicas. Vol. 39. No. 68. pp. 866–881.

[6] Butuzov V.M. Documenting crimes in the field of the use of computers, systems and computer networks and telecommunication networks during the research: a scientific and practical guide. K., 2010. 245 p.

[7] Motlyakh O.Iє Questions of methods of investigation of crimes in the field of information computer technologies: dis. … cand. jurid. Science: 12.00.09. Kyiv, 2005. 221 p.

[8] Criminal Procedure Code of Ukraine. URL: http://zakon.rada.gov.ua/laws/show/4651-17