JOURNAL OF MULTIDISCIPLINARY SCIENCES AND INNOVATIONS
VOLUME 04, ISSUE 09
MOPNTHLY JOURNALS
ISSN NUMBER: 2751-4390
IMPACT FACTOR: 9,08

THE CONCEPT OF CYBERCRIMES IN THE SPHERE OF ECONOMY AND THE SOCIAL NEED TO COMBAT THEM

Nurmanov Kholbek Rahmatilla ugli
Independent researcher Tashkent State University of Law,
E-mail: xolbek.nurmanov123@gmail.com.

Annotation: In this research article, the author examines the concept of cybercrime in the economic sphere, which poses a very serious threat today, and the social need to combat it. This article also examines in detail the ideas, concepts, and scholarly debates existing in legal science on this issue. Based on these scholarly ideas, views, and debates, the author concludes that there is no consensus in scientific theory regarding the concept of cybercrime. He also notes that while national legislation currently establishes measures of legal liability for certain types of economic cybercrime, they do not cover new types of modern cybercrime. At the same time, in the science and practice of developed countries, liability standards for most modern cybercrime in the economic sphere are currently formulated in special laws. Therefore, the author concludes that it is necessary to consider a number of requirements already established in global practice when determining liability for these specific criminal acts. The author also provides his proposals regarding the concept of cybercrime in the economic sphere.

Keywords: cybercrime, economics, greed, profit, theft, computer information, confidentiality, economic secrecy.

Introduction

The world community has entered a new era - the era of the information society, when computers and telecommunication systems have covered all spheres of human and state life. However, humanity, having put itself at the service of telecommunications and global computer networks, did not foresee what opportunities these technologies would create for abuse. Today, the victims of criminals operating in the virtual space can become not only people, but also entire countries. At the same time, crimes against information security can be committed by several criminal associations or groups. The number of crimes committed in the cyber environment is growing in proportion to the number of users of computer networks, and according to the calculations of the International Criminal Police Organization - Interpol, the growth rate of this crime in the global Internet network is the fastest on our planet [1].

Of course, the development of global communication and information systems is inevitable and has many benefits. However, as globalization has happened in other areas, new modern means of information exchange and technological advances are increasingly being used for criminal purposes, and crimes in the field of information technology are being committed under the influence of globalization in new forms and using previously non-existent techniques. As of January 1, 2024, the number of subscribers connected to the Internet in Uzbekistan amounted to 30.1 million people (this corresponds to 80% of the total population) [2], as of April 1, 2022, the number of mobile phone subscribers in Uzbekistan amounted to 29.9 million [3], and the total bandwidth of connections to the international Internet network in Uzbekistan increased by 2.6 times to 3,200 Gbit/s [4].

As of 2021, 100,015 domains were registered in the national segment of the Internet of the Republic of Uzbekistan ".uz", of which about 38,000 are active [5]. In 2017, there were about 53 thousand active domains in Uzbekistan, and in 2018 their number reached 65 thousand. The fact that each user has Internet services means that they can become a victim of cyberterrorism.

According to the UZCERT Information Security Incident Response Service, in 2021 the Center identified 17,097,478 cases of malicious and suspicious network activity originating from the address space of the national segment of the Internet [6]. In short, in the age of global informatization and computerization, along with amazing inventions, huge problems such as computer crime, which threatens information security, are entering human life . The International Cyber Security Forum (Cyber Security Forum - 2017) held in Moscow on February 7, 2017, identified three of the most common attacks in the world of cybercrime today.

Material and methods

The research used methods such as logical, historical, comparative-legal, specific sociological, complex research of scientific sources, analysis of statistical data, interpretation of legal documents, and study of the practice of applying the law.

Research result

Crimes committed through information technology are already called "cybercrimes" in developed foreign countries, and measures to combat, prevent, and hinder these socially dangerous acts are established in legislation. In general, the specific characteristics of cybercrimes are as follows:

¬crimes of this category do not choose a place, it can be expected at any time from different parts of the world;

¬the constant creation of new and more dangerous viruses and other malicious programs every day;

¬ the lack of qualified experts with excellent knowledge in this field in the bodies fighting against cybercrimes, and as a result, the crime is detected late;

¬Cybercrime results in the loss of ownership rights to information, not specific property;

¬Errors made during information processing are not detected and corrected in a timely manner, resulting in future errors not being prevented [7, P. 6];

¬committed computer crimes are not announced in time (to hide from others the presence of flaws in computer networks, to maintain the reputation of the institution's work and for other purposes);

¬The inherent difficulty of investigating and solving cybercrime, the enormous damage it causes, and the lack of a single legal basis for combating criminals and preventing it .

It is clear that cybercrime should be distinguished both as a legal category and as a social phenomenon. As is known, cybercrime does not know state borders. Perhaps the experience of international organizations should be used to develop the most appropriate standard definition . One of the main steps taken to resolve this problem was the adoption of the Convention on Cybercrime by the Council of Europe on November 23, 2001.

Given the complexity of the problem, the Council of Europe prepared and published a draft Convention on combating crime committed in the cyber environment in early 2000. This document was the first international agreement on the legal and procedural aspects of investigating and prosecuting cybercriminals. The Convention on combating cybercrime provides for coordinated action at national and international levels to prevent unauthorized access to computer systems, unlawful interception of data and interference with computer systems. According to this European Convention on Cybercrime, cybercrime is a crime against the confidentiality, integrity and availability of computer systems, networks and data, and the unlawful use of such systems, networks and data [8].

The Council of Europe Convention on Cybercrime classifies four types of computer crimes as "specific cybercrimes" and defines them as crimes against the confidentiality, integrity and availability of computer data and systems:

1. Unlawful access to a computer system – Article 2 (unlawful intentional access to a computer system or part thereof);
2. Illegal acquisition of computer information - Article 3 (intentional illegal acquisition of computer data transmissions not intended for the public);
3. Modification of computer information – Article 4 (unlawful damage, deletion, corruption, alteration or destruction of computer data);
serious unlawful interference with the operation of a computer system by entering, transmitting, damaging, deleting, corrupting, altering or suppressing computer data).

Although in recent years we have increasingly encountered the concept of "cybercrime" in the media, in our country the concepts of "computer crimes" or "crimes in the field of information technology" are used as synonyms for this concept. However, most authors emphasize that "computer crimes" are a different concept from the concept of "cybercrime", and that this concept covers all crimes in the field of information technology, thereby being a broader concept than "computer crimes" [9, P. 34]. It can be seen that cybercrime is a crime committed using a computer or through a computer, a global network [10].

According to D.N. Karpova, cybercrime is a socially dangerous act committed with the aim of causing economic, political, moral, ideological, cultural and other damage to an individual, organization or state using any technical means that have access to the Internet . It is noteworthy that Karpova also considers ideological damage to an individual to be cybercrime. In addition, another reliable source, the training module on cybercrime developed by the United Nations Office on Drugs and Crime [11, P. 47], defines cybercrime as an act that violates the law using information and communication technologies (ICTs) or is directed at networks, systems, data, websites, technologies or that facilitates the commission of a crime [12]

In contrast to these concepts, the concept of cybercrime can be defined as follows: cybercrime is a socially dangerous act committed in the cyber environment in the form of an information attack directed at the material and intangible assets of an individual, society and the state through or with the help of a computer system, network, as well as other means connected to a computer system, network. Thus, in cases where the Internet is used directly to commit a crime, it is both a method and a means, and in others it is only a means . Many scientific studies are trying to define the term “cybercrime” [13]. However, the drafters of national legislation of countries do not set themselves the task of giving a precise definition to this concept. Of the approximately 200 national legislative acts indicated by countries in response to the questionnaires of a study conducted by the UN, in less than five percent of cases the term “cybercrime” was present in the name or content of legal norms .

Instead, [13] the terms “computer crime” [13], “crime in the field of electronic communications”, [13] “information technology” [13] or “crime in the field of high technology” are more often used in legislation. The term “cybercrime” may not have a full meaning as a legal term [13]. It should be noted that a similar approach is used in international legal conventions, such as the United Nations Convention against Corruption [14], which does not define the term “corruption” and establishes the obligation of participating states to criminalize a certain set of actions. Therefore, it is appropriate to consider the concept of “cybercrime” as an act or set of actions.

Cybercrime has developed differently in different eras, so its doctrinal and official definitions are different. In particular, according to the 2001 Council of Europe Convention on Cybercrime, cybercrime is any crime committed in the cyber environment [15]. This is the most correct opinion, because any technology can be developed, but all the crimes committed by them are committed in the cyber environment, and the cyber environment includes the processes in which socially dangerous crimes are committed with the participation of all technologies. According to the scientist M. Gurcke, cybercrime is a set of crimes committed in the cyber environment

against a computer system, network, other means connected to them or with their help, against a computer system, network or computer information [16].

However, according to the Laws "On Telecommunications" [17], "On Disclosure" [18], "On Principles and Guarantees of Freedom of Information" [19], based on the essence of the concepts of the information system of the telecommunications network, the telecommunications network is not considered a computer network, and only computer information does not constitute the content of cybercrimes, because cybercrimes can be committed using any technologies that are committed in the cyberspace.

Scientists K.E. Zinchenko, L.Yu. Ismailova, A.N. Karakhanyan, B.V. Kiselev, V.V. Krylov, Y.M. Mastinsky. N.S. Polevoy, Y.N. Solovyov, V.V. Khurgin, S.I. Tsvetkov believe that such crimes are crimes committed using electronic computers [20, P. 304]. It should be noted that this concept was given in 1994, which means that from the point of view of the history of Uzbekistan, the Law of the Republic of Uzbekistan “On the legal protection of programs and databases created for electronic computers” No. 1060-XII dated May 6, 1994 [21]was adopted precisely in 1994, so this concept was interpreted correctly from the point of view of time.

Scientists N. Salaev and R. Ruziev call socially dangerous illegal acts that threaten information security, committed directly through computer means or by means of information technologies, crimes in the field of information technologies, and emphasize that computer crime is a synonym for it. They also define socially dangerous acts committed in the cyber environment against a computer system, network, as well as other means connected to them, or with the help of them, as cybercrime, and define the above crimes as crimes different from cybercrime [22, P. 139].

As is known, cyberspace also includes computer crime, and if we look at the Russian text of the 2001 Council of Europe Convention on Cybercrime, we can see that in some cases it is translated as the Convention on Computer Crime [23].

To understand this situation more clearly, let's consider one case. In order to commit the crime of theft committed through computer equipment, as provided for in Article 169, Part 3, Clause "b" of the Criminal Code, there must be a cyber environment, that is, a virtual environment, that is, before committing the theft, the criminal obtains the password of the victim's card on which the funds are stored, and uses the telecommunications or Internet network or another network to commit his act. It is precisely this environment in which we cannot see with our eyes or touch with our hands, but by typing the code on the victim's card, we can understand how the criminal obtained these funds. This environment is called the cyber environment.

Also, it should be noted that, although the purpose of the Law "On Informatization" is to regulate relations in the field of informatization, information resources and the use of information systems, it does not specify the concept of computer technology and, from the point of view of its technical capabilities, it cannot include other information technologies, but information technology includes all computer technologies, systems, and networks. According to Articles 4, 10, 14, 16 of the Criminal Code, crimes and punishments must be subject to the principle of legality. Based on the above, it is advisable to develop the opinion of these scientists both technically, doctrinally, and legally, in our opinion. The concept of global network crime does not fully correspond to the concept of "computer crime" that existed before, and therefore this type of crime is currently referred to as "cybercrime".

Analysis of research results

In international scientific and legal practice, the concept of "computer crime" was first used, then the concepts of "computer-related crime", "computer-based crime", "electronic crime" and "high-tech crime", "virtual crime", and today the term "cybercrime" or global network crime is used.

The scientist I. Torakhodzhaeva emphasizes that cybercrime is a broader concept than computer crime, explaining the need for a specific approach to combating it, as it clearly defines the

boundaries of crime committed through the global Internet network [24, P. 128-132]. The time-relatedness of the concept of cybercrime can be emphasized by the fact that in 1979, the Dallas Bar Association conference first determined the main characteristics of computer crimes based on the technical capabilities of information and communication technologies available at that time [25].

Scientist L. Kochkina called cybercrime “crimes in the field of computer data”, “information crimes”, “crimes related to computer equipment”, “crimes on high-tech computers”, “crimes in the field of information” [26, P. 2], and T. Borodkina called these crimes information crimes . Scientist I.M. Rassolov [27, P. 135-137] proposes to consider [28, P. 251-253] crimes in this category as a separate crime in criminal law . According to Sh. Tolmasov, cybercrime is the illegal use of information technologies by people for criminal purposes [29].

According to V.A. Dulenko, R.R. Mamlev, V.A. Pestrikov, “cybercrime” is any crime committed using a computer network, that is, any crime committed in an electronic environment [30, P. 27]. I.G. Chekunov called this crime a crime committed against computers and mobile (cellular) communication devices [31, P. 37-44]. According to scientist V.A. Nomokonov, cybercrimes are much broader than computer crimes and clearly reflect the phenomenon of crime in the information space [32, P. 47]. Similar ideas are also expressed by I.V. Ramanov [33, P. 106].

O.A. Kuznetsov tried to explain this situation, emphasizing that cybercrime is a broad concept, since it is committed not only through computers, but also through other information technologies and Internet networks, and explained that computer crime is directed only against electronic devices and the data stored on them [34, P. 289]. Similar views are also expressed on the website “urist.one”, which basically defines cybercrime as any crime in the electronic sphere committed using or against computer systems or networks [35].

Modeled by computers, humans, Scientist A.V. Fedorov calls cybercrime any crime committed using information about objects, events, situations and processes, expressed in mathematical, symbolic or any other sense, moving in local and global computer networks or stored in the memory of any physical or virtual device, as well as programs specially designed for their storage, processing and transmission [36, P. 11].

Conclusion

In addition to the opinion of scientists above, we should mention that it would be appropriate to include the concept of cybercrime in the criminal law of our country.

In general, we can say **that cybercrime is an illegal, socially dangerous act that threatens information security and is committed directly through computer means or through the Internet using electronic technologies** .

REFERENCES:

1. https://www.interpol.int/Crimes/Cybercrime

2.https://daryo.uz/2024/09/07/ozbekistonda-qancha-abonent-internet-tarmogiga-ulangani-ochiqlandi

3.https://daryo.uz/k/2022/06/06/ozbekistonda-mobil-aloqa-abonentlari-soni-30-millionga-yaqinlashdi-statqom

4. https://daryo.uz/k/2023/03/10/ozbekistonda-2023-yil-martdan-mobil-internet-tezligi-oshiriladi

5.https://www.csec.uz/upload/iblock/9d5/1.%20%D0%98%D1%82%D0%BE%D0%B3%D0%B8%202021_%D1%83%D0%B7.pdf

6.https://www.csec.uz/upload/iblock/9d5/1.%20%D0%98%D1%82%D0%BE%D0%B3%D0%B8%202021_%D1%83%D0%B7.pdf

7. Roziev R.N., Salaev N.S. National and international standards for combating cybercrime. Monograph. - Tashkent: TDUU, 2018, p. 6 (Ruziev R.N., Salaev N.S. National and international standards for combating cybercrime. Monograph. - Tashkent: TDUU, 2018, p. 6).

8. European Convention on Cybercrime. Budapest, November 23, 2001. // https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

9. Nomokonov V.A., Tropina T.L. Cyberprestupnost kak novaya kriminalnaya ugroza// Criminology: yesterday, today, tomorrow. - 2012 – 1 (24). - S. 47.; Cybercrime: criminological, criminal law, criminal-procedural and criminalistic analysis. / Nauch. ed. I. G. Smirnogo. - M., 2016. - S. 34 (Nomokonov V.A., Tropina T.L. Cybercrime as a new criminal threat// Criminology: yesterday, today, tomorrow. – 2012. – 1 (24). – P.47.; Cybercrime: criminological, criminal law, criminal procedure and forensic analysis. / Scientific ed. I.G.Smirny. – M., 2016. – P. 34).

10. Gurcke M. Understanding Cybercrime: A Guide for Developing Countries. ITU, 2009.

11. Karpova D.N. Cybersecurity: a global problem and its solution. Vlast, 2014, st.47 (Karpova. D.N. Cybercrime: A Global Problem and Its Solution. Vlast, 2014, p. 47).

12. Cyberprestupnost. Modul 1. Vvedenie v kiberprestupnost // Obrazovanie vo imya pravosudiya seria universitetskix moduley // Upravlenie Organizatsii Ob'edinennyx Natsiy po narkotam i prestupnosti., Vienna, 2019 (Cybercrime. Module 1. Introduction to Cybercrime // Education for Justice University Module Series // United Nations Office on Drugs and Crime, Vienna, 2019).

13. International Telecommunication Union, 2011. Understanding Cybercrime: A Guide for Developing Countries; Explanatory Report to the Council of Europe Cybercrime Convention, ETS No. 185;

14. United Nations. 2004. Convention against Corruption.

15. ES ot 23.11.2001 goda "Convention on computer crime". Budapest, European Treaty Series No. 185. https://rm.coe.int/1680081580 (EU of 23 November 2001, "Convention on Cybercrime." Budapest, European Treaty Series No. 185. https://rm.coe.int/1680081580).

16. M. Gurcke. Understanding Cybercrime: A Guide for Developing Countries. ITU. 2009.

17. Law of the Republic of Uzbekistan No. 822-I "On Telecommunications" adopted on August 20, 1999 // Bulletin of the Oliy Majlis of the Republic of Uzbekistan, 1999, No. 9, Article 219; 2004, No. 9, Article 171 (Law of the Republic of Uzbekistan "On Telecommunications" No. 822-I, adopted on August 20, 1999 // Bulletin of the Oliy Majlis of the Republic of Uzbekistan, 1999, No. 9, Article 219; 2004, No. 9, Article 171).

18. Law of the Republic of Uzbekistan "On Informatization" No. 560-II, adopted on December 11, 2003 // Bulletin of the Oliy Majlis of the Republic of Uzbekistan, 2004, No. 1-2, Article 10 of the Republic of Uzbekistan, 2004, No. 1-2, Article 10).

19. Law of the Republic of Uzbekistan No. 439-II "On the Principles and Guarantees of Freedom of Information", adopted on December 12, 2002 // Bulletin of the Oliy Majlis of the Republic of Uzbekistan, 2003, No. 1, Article 2; Bulletin of the Chambers of the Oliy Majlis of the Republic of Uzbekistan, 2015, No. 12, Article 452 (Law of the Republic of Uzbekistan No. 439-II "On the Principles and Guarantees of Freedom of Information", adopted on December 12, 2002 // Bulletin of the Oliy Majlis of the Republic of Uzbekistan, 2003, No. 1, Article 2; Bulletin of the Chambers of the Oliy Majlis of the Republic of Uzbekistan, 2015, No. 12, Article 452).

20. E. Zinchenko, L. Yu. Ismailova, A. N. Karakhanyan, B. V. Kiselev, V. V. Krylov, Ya. M. Mastinsky. N.S. Polevoy, Yu.N. Solovev, V.V. Khurgin, S.I. Tsvetkov. Computer technology and legal information. Educational and practical skills. -M.: publishing house "BEK". 1994, p. 304.

21. Law of the Republic of Uzbekistan "On the legal protection of programs and databases created for electronic computers" dated May 6, 1994 No. 1060-XII // Bulletin of the Supreme Council of the Republic of Uzbekistan, 1994, No. 5, Article 136.

22. Salaev N.S., Ruziev R.N. National and international standards for combating cybercrime. Monograph., T.: TDYuU, 2018, p. 139 (Salaev N.S., Roziev R.N. National and international standards for combating cybercrime. Monograph., T.: TDYuU, 2018, p. 139).

23. https://www.coe.int/ru/web/conventions/full-list/-/conventions/treaty/185/

24. I. Torakhodjaeva. Problems of combating crimes committed through the Internet in Uzbekistan // – T.: Bulletin of legal sciences / Vestnik yuridicheskikh nauk / Review of law sciences. scientific and practical journal. 2019 (03)-No. 128-132 b (I. Torakhodjaeva. Problems of combating crime committed through the Internet in Uzbekistan // – T.: Bulletin of Legal Sciences / Vestnik yuridicheskikh nauk / Review of law sciences. scientific and practical journal. 2019 (03) issue. 128-132 p.).

25. V.A. Shirokov, E.V. Bespalova. Cybercrime: History of Criminal-Legal Counteraction. – Moscow: “Information Law”, 2006, No. 4. http://center-bereg.ru/h1846.html (V.A. Shirokov, E.V. Bespalova. Cybercrime: History of Criminal-Legal Counteraction. – Moscow: “Information Law”, 2006, No. 4. http://center-bereg.ru/h1846.html).

26. L. Kochkina. Definition of the concept "cybercrime". Selected types of cybercrime // Siberian criminal-procedural and criminalistic readings. 2017. No. 3 (17). –s 2 (L. Kochkina. Definition of the concept "cybercrime". Selected types of cybercrime // Siberian criminal-procedural and criminalistic readings. 2017. No. 3 (17). –s 2).

27. T.N. Borodkina, A.V. Pavlyuk. Cybercrimes: Concept, Content, and Countermeasures. Socio-Political Sciences. No. 1. 2018. –135-137 p.

28. I.M. Rassolov. Law and the Internet. Theoretical Problems. – M.: Izd-vo NORMA, 2003. – 251-253 p (I.M. Rassolov. Law and the Internet. Theoretical Problems. – Moscow: NORMA Publishing House, 2003. – 251-253 p).

29. Sh. Tolmasov. Global makondagi cyberzhinoyatchilik. Manba: http://uz.denemetr.com/docs/768/index-29121-1.html (Sh. Tolmasov. Cybercrime in the global space. Source: http://uz.denemetr.com/docs/768/index-29121-1.html).

30. V.A. Dulenko. Use of high technologies by the criminal environment. The fight against crimes in the field of computer information: a tutorial. Ufa, 2007. – p. 27 (V. A. Dulenko. The use of high-tech criminal environments. Combating crimes in the computer information sphere: a manual. Ufa, 2007. – p. 27).

31. I. G. Chekunov. Cybercrime: concept and classification // Russian investigator. 2012. No. 2. – 37-44 p. (I. G. Chekunov. Cybercrime: concept and classification // Russian investigator. 2012. No. 2. – 37-44 p.).

32. V. A. Nomokonov / Cybercrime as a new criminal threat / V. A. Nomokonov, T. L. Tropina // Criminology. Yesterday. Today. Tomorrow. 2012. No. 1 (24). – p. 47 (V.A. Nomokonov/ Cybercrime as a New Criminal Threat / V.A. Nomokonov, T.L. Tropina // Criminology. Yesterday. Today. Tomorrow. 2012. No. 1 (24). – p. 47).

33. I.V. Romanov. The Concept of Cybercrime and Its Importance for Investigation // Siberian Criminal Procedural and Forensic Readings. 2016. No. 5 (13). –106 p. (I.V. Romanov. The Concept of Cybercrime and Its Importance for Investigation // Siberian Criminal Procedural and Forensic Readings. 2016. No. 5 (13). –106 p.).

34. The Third Perm Congress of Legal Scholars: Proc. of the International Scientific and Practical Conf. Perm, October 12, 2012 / Responsible for Ed. O.A. Kuznetsova. – Perm: Perm State National Research University, 2012. – 289 p. (The Third Perm Congress of Legal Scholars: Proc. of the International Scientific and Practical Conf. Perm, October 12, 2012 / Ed. O.A. Kuznetsova. – Perm: Perm State National Research University, 2012. – 289 p.).

35. https://urist.one/dolzhnostnyeprestupleniya/kiberprestupnost/.html

36. A.V. Fedorov. Information security in the global political process. – Moscow: MGIMO University, 2006. – 11 p.