UDC 343.9

CYBERCRIME IN THE RUSSIAN FEDERATION. THE CONCEPT OF CYBERCRIME IN CRIMINOLOGY

Skorokhodova A.M.
3nd year student
Academy of Law and National Security
Southern University
email: skorohodova_nastya1710@mail.ru
Scientific supervisor: Galoyan Y.E.,
PhD, Head of the Academy of Humanitarian Technologies

Abstract: Currently, the number of cybercrimes is growing rapidly. In this regard, it is necessary to improve the already existing structures of the norms of the Criminal Code of the Russian Federation governing liability for crimes in the field of computer information.
Keywords: cybercrime, criminal code of the Russian Federation, criminology, legislation, the Internet.

Today the computerization of society has touched all spheres of human life, necessitating the formation of a mechanism for the legal regulation of relations arising in the field of computer information.

The Internet space forms a new sphere for the life and interaction of modern society, in connection with which the number of criminal acts on the Internet increases significantly every year, and the level of disclosure of cybercrimes, according to the General Prosecutor's Office of the Russian Federation, is 5%, which is explained by accessibility and widespread use of digital technologies. According to analysts' forecasts, by the end of 2020 the number of Internet users will be 80% of the population of the Russian Federation over the age of 18, and the number of Internet users in the world will reach 5 billion people. Statistics also show that 98% of young people aged 16 to 29 have access to the Internet. This is explained by the fact that the Internet space today is an integral part of the life of every person, since all socially significant spheres of life, in particular, work, study and communications smoothly flow into cyberspace. In this regard, it seems that

the increasing role of cyberspace as an interactive information and communication environment entails the emergence of a whole range of new risks and threats, an increase in the vulnerability of the information infrastructure, an increase in the ways of a destructive impact on public relations using the capabilities of cyberspace and their constant complication - including for the purpose of committing crimes [1].

Thus, one of the important tasks of the domestic criminal legislation at this stage is the creation of a mechanism for the effective suppression of existing cybercrimes, as well as the development of measures to counteract and control the emergence of new ways of committing crimes within cyberspace. However, today it is in this area that criminal legislation does not fully regulate the relations that arise in the Internet space, and is not ready for the rapid development of modern information technologies, which indicates the need to refine this issue at the legislative level. The specificity of cybercrime also lies in the fact that a single state is not able to fully resist it due to the cross-border and transnational nature of this phenomenon. In this regard, the criminal acts committed on the Internet do not have state borders and can easily be committed from the servers and computer systems of one state in relation to the subjects of another state. Given this, the mechanism for combating transnational cybercrime should proceed from the fact that this problem must be dealt with holistically, which implies close cooperation both at the national and international levels. The lack of a coherent and effective mechanism to counter this phenomenon gives rise to the emergence of new means and methods for committing cybercrime, which are constantly being modified depending on the means of protection used by users of computer networks: the better the defense systems become, the more complex and dodgy the means of attack become. The increase in the number of criminal acts committed using the Internet allows scientists to talk about the phenomenon of cybercrime and necessitates its criminological study. It is important to emphasize that at the legislative level, this concept is not disclosed, despite the fact that it is mentioned

in a number of cases. It seems that the need to understand the phenomenon of cybercrime requires mandatory reference to these regulatory documents [2].

Referring to foreign experience in this area, it is worth noting that in foreign legislative acts in less than 5 percent of cases, the term "cybercrime" is officially enshrined in the title or content of legal norms. Instead, substitute concepts are often encountered, for example, "computer crimes", "information technology", "electronic communications" and others. Most of these legislative acts only define the range of criminal acts that are included in the concept of cybercrime, for example, intentional impact on computer systems and data or illegal access to computer information protected by law, however, the content of the definition itself is not disclosed.

In rare cases, the term "cybercrime" is used in foreign legislation - as a rule, within the title of a legislative act or its section, however, their provisions do not contain its interpretation. So, for example, in the legislation of Oman and the Philippines, this term is legal, however, there is no definition of it - by and large, it is a reference to "crimes defined in this law" [3].

In addition to this, when studying international legal documents regulating the relations of states in the framework of combating cybercrime, it can be noted that few of them use the concept of cybercrime, and in acts of key importance on this issue it is completely absent. In particular, we are talking about the 2001 Council of Europe Computer Crime Convention, the 2014 African Union Convention on Cyber Security, and the 2008 Commonwealth of Independent States Agreement on Cooperation in Combating Computer Crime, which use the concept of “computer crime”. information”, defined as “a criminally punishable act, the subject of encroachment of which is computer information”. Similarly, the 2011 Agreement between the Governments of the Member States of the Shanghai Cooperation Organization establishes the definition of "information crime", which is "the use of resources and (or) influence on them in the information space for illegal purposes".

Thus, we can conclude that the acts of foreign legislation do not disclose the content of the term "cybercrime", even if it is used. A similar point of view is shared by the International Telecommunication Union, which quite often refers to the absence of the need to consider the concept of "cybercrime" as a legal term. It is worth noting that this approach is used, for example, in the United Nations Convention against Corruption, where there is no definition “corruption”, however, the obligation of the participating states to recognize as criminally punishable a certain list of criminal acts that can be accurately identified on the basis of established signs is fixed. In this regard, we can conclude that, according to a foreign legislator, the term "cybercrime" should be considered as a set of illegal acts against the confidentiality, availability and security of computer systems and data.

Returning to the analysis of national legislation, it should be noted that today the Criminal Code of the Russian Federation does not contain a definition of “cybercrime” and “cybercrime”. Along with this, in the modern domestic doctrine, there are many approaches regarding the expediency of implementing this term in criminal law and its relationship with the concept of "computer crime".

Within the framework of this aspect, first of all, it is worth considering the concept of "computer crime" and its relationship with the term "crime in the field of computer information". A number of authors understand computer crime as a set of criminal acts in which the subject of a criminal encroachment is computer information. At the same time, it is noted that the concepts of "crime in the field of computer information" and "computer crime" are identical, which, in our opinion, is not entirely correct, since "computer crime" covers a greater number of criminal encroachments, the subject of which may be not only computer information. These crimes can be committed using information systems as a means of infringement, however, damage is done to public relations, for example, in the field of protecting the life and health of citizens or in the field of ensuring property rights. Consequently, the term "computer crime" covers not only the criminal acts provided for by Chapter 28 of the Criminal Code of the Russian Federation, but

also those committed using information telecommunications. In turn, the note to article 272 of the Criminal Code of the Russian Federation contains the concept of computer information, which refers to information presented in the form of electrical signals, regardless of the means of storage, processing and transmission [4].

Also in the doctrine there is an approach, according to which computer crime is understood as a set of criminal acts committed with the help of a computer network or system, against a computer system or network, or within a computer system or network. At its core, this position, apparently, suggests that computer crimes are not only criminal acts in the field of computer information, but also criminal attacks directly related to computers as a means of committing these acts. Therefore, according to the supporters of this approach, traditional criminal acts committed with the help of computer technology, for example, fraud, theft, causing harm, and others, for which criminal liability is provided, are included in the content of the concept under consideration. However, in our opinion, this definition characterizes the phenomenon of cybercrime to a greater extent, since it covers a wider range of criminal acts.

Analyzing the expediency of separating this legal category, it is worth noting that I.G. Chekunov believes that cybercrime is an independent type of crime, determined on the basis of the presence in criminal acts of mandatory signs of the objective side - means or tools, which are malicious computer programs or software and hardware connected to a computer network or mobile.

Along with this, in the doctrine there is quite often an approach according to which computer crime is only a part of cybercrime, as a more voluminous concept. This kind of position, for example, is held by T.L. Tropina, who considers cybercrime as "a set of criminal acts committed in cyberspace through or with the help of computer networks and systems, as well as other possible means of access to cybercrime, within computer systems or networks and against computer systems." However, there is also an opposite point of view in the doctrine, according to which the concept of "computer crime" is wider than the term

"cybercrime" in terms of content and scope. Proponents of this approach refer to the fact that "cybercrime" is only a subspecies of "computer crime", since it includes a set of criminal acts committed on the Internet or using information and telecommunication networks. In our opinion, the authors consider this category only in a narrow sense, since cybercrime includes criminal acts committed not only on the Internet, but also within the entire cyberspace and computer networks.

Thus, it is necessary to distinguish between these categories, since cybercrime covers the entire set of crimes in the information sphere, namely, criminal acts committed using computer systems and crimes the subject of which are computer systems, networks and information located on electronic media. Computer crime, in turn, includes criminal attacks on the safe operation of computer systems and programs, as well as on the data processed and generated by them [5].

In this regard, we can conclude that the concept of "cybercrime" is much broader than "computer crime", since it more accurately and holistically reflects the nature and specifics of such a phenomenon as crime in the information space. Summing up, in our opinion, under «cybercrime», it is necessary to understand the totality of socially dangerous acts committed within cyberspace through or with the help of computer networks and systems, as well as other means of access to cyberspace, within computer networks or systems, and against computer data, systems and networks. This definition covers all possible types of criminal acts in the information sphere, where information technology, resources, data can be a means, tool and subject of criminal encroachment, as well as the environment in which this crime can be committed. It is also worth noting the need to consolidate the legal definition of «cybercrime» in the criminal law of Russia, since the emergence and modification of this type of crime requires the introduction of a uniform terminology, which will prevent the occurrence of gaps and controversial issues in the framework of law enforcement practice and legal doctrine.

References

1. Slobodchikova A.V. Cyber security in russia and abroad – URL: https://www.elibrary.ru/item.asp?id=39174252

2. Poleshchuk D.G. Objective Signs Of Criminal Wrongness Of Illegal Actions With Malic Computer Programs As Crimes Against Cyber Security – URL: https://www.elibrary.ru/item.asp?id=41374027

3. Belous A. I., Solodukha V. A. Fundamentals of cybersecurity. Standards, concepts, methods and means of ensuring – URL: https://e.lanbook.com/book/181222

4. Navalenny A. V., Dudka A. B., Konyavskaya S. V., Konyavsky V. A., Berdyugin A. A., Nazarov I. G., Ozhered I. V., Oshmankevich K. R., Persanov D Yu., Pimenov P. A., Revenkov P. V., Rusin L. I., Silin N. N., Frolov D. BCybersecurity in the context of e-banking: a practical guide URL: https://e.lanbook.com/book/161659

5. Diogenes Y. , Ozkaya E. Cybersecurity. attack and defense strategy – URL: https://e.lanbook.com/book/131717