Information Technology and the Concept of Crime in Cyber Space

Dusmatov Durbek Rustamjon ogli
Yashnabad district prosecutor's office
Senior Assistant Prosecutor

ABSTRACT

In this article, the concepts of information technology and cybercrime are aimed at revealing the concepts of cybercrime, the implementation of countermeasures against them, and the division of cybercrime into groups.

Keywords: Concept of cybercrime, similarities and differences between information technology and cybercrime, cross-border nature of cybercrime

The concept and essence of cybercrime The concept of "cybercrime" has become widespread today due to the achievements in the field of information and telecommunications in the 21st century. Cybercrime is a set of crimes committed in "cyberspace" against computer systems or computer networks, as well as other means of accessing cyberspace, within computer systems or networks, as well as against computer systems, computer networks, and computer data. "Cybercrime" means any crime committed using various methods and means of creating, processing and transmitting computer information [1]. The term "cybercrime" is also often used together with the term "computer crime". It should be noted that the term "cybercrime" is broader than "computer crime" because it more accurately reflects the nature of such a phenomenon as a crime in the information space. Thus, "cybercrime" is a crime related to both the use of computers and the use of information technology and global networks. However, the term "computer crime" refers only to crimes committed against computers or computer data [2]. Most of the crimes committed in global computer networks are characterized by the following features [2]:

1 Increasing crime mystery.
2 The cross-border nature of cybercrime, where the perpetrator, the object of the criminal attack and the victim may be located in the territory of different countries.
3 Special training of criminals, intellectual nature of criminal activity.
4 The possibility of committing crimes in several places at the same time in an automated manner.
5 Victims' lack of awareness of criminal exposure.
6 Prolonged criminal activities without physical contact between the offender and the victim.
7 The impossibility of preventing and suppressing this type of crime by traditional methods.

Today, cybercrime encompasses a wide range of illegal activities, from unauthorized access to computer networks and identity theft to financial espionage and extortion. Some authors argue that in recent years the Internetresources have been used in all forms of human trafficking and the sale of prohibited items, as well as in the subsequent legalization of criminal proceeds [3]. Almost any person who actively uses high technologies, as well as persons performing professional duties in organizations and enterprises, becomes a subject of crime. At the same time, their goals, the methods they use, and the opportunities available to them in practice do not differ from those typical of criminals due to the nature of their work. In addition to grouping cybercriminals, certain groups and victims of cybercrime can be grouped together. Thus, the classification of cybercriminals, as well as how cybercrime victims can be categorized, also categorizes cybercrime victims into groups like individual citizens.

The main types of information weapons include [1]:

1 back round - this tool includes a hidden method in the system that allows access to the protected area.

2 Computer viruses are special programs that are installed on computer programs and destroy, distort or disrupt their operation. They can be transmitted over communication lines, data networks, switching off control systems, etc. In addition, "viruses" have the ability to reproduce independently.

3 "Logic bombs" are software devices pre-introduced to the information and control centers of the infrastructure to activate them at a specified time or time.

4 Malware - programs or utilities that, after installation, perform undeclared functions in the background.

5 Neutralization of test programs that ensure the preservation of natural and artificial software defects.

6 Traffic analyzers (sniffer) - programs or devices that monitor data transmitted over the network. Traditionally used for legitimate network management functions, they can also be used during cyber attacks to steal data.

7 Internet attacks are designed to disrupt access to a network, typically by making millions of requests every second to disrupt or disrupt network access.

8 Email cybercrime is the technique of sending emails with a fake source, which is used to trick the recipient into providing confidential information.

9 A keylogger is a software or hardware tool designed to monitor keystrokes on a computer keyboard to obtain passwords, PINs, or other information.

As objects of cybercrime, business structures and the state are the main objects of cybercrime, which cause incalculable damage to individual objects and the economy as a whole. Each of these entities can be exposed to certain types of cyber threats. Objects and types of threats The types of attacks discussed above can be carried out against objects.

Let's take a closer look at each block [4]:

1 The financial sector is one of the most vulnerable sectors to cybercrimes: with the development of modern communications, a large part of cash flows has become non-cash, which makes it much easier for criminals to steal bank accounts and plastic card accounts. ordinary citizens.

2 Regarding the problem of hacking, stealing databases, as well as hacking attacks and the spread of viruses, it should be noted that the problems of preventing these types of threats are the inability to predict potential problems, the same software in different applications is to use the supply. devices, which increase the efficiency of exploiting technical vulnerabilities, as well as the lack of personnel in the field of cyber defense.

3 Illegal invasion of privacy is increasing every year: people around the world use modern gadgets, which, in turn, can tell the criminal the user's location and more personal and confidential information. This type of crime includes not only extortionists, but also marketing departments of companies that monitor the personal data of potential consumers, analyze their preferences, thereby create targeted advertising and enter information about them into their databases. will cry

4 Misappropriation of intellectual property is also a common type of cybercrime, because with the development of IT technologies (as a result of the development of cybercrime), creators of

intellectual property threatened by cybercrime, as a rule, cannot take advantage of this offense. the economic benefits of their work, thereby undermining the incentive to invest in the development of their product, and putting the creator of intellectual property at a disadvantage compared to a mere copycat because the creator has spent money and time. in idea development.

Due to the rapid development of information technologies, cybercrime has expanded and today includes new serious threats, which are presented and described in Table 3.

In conclusion, Internet crimes are the newest and most dynamically developing area of activity of attackers. The forms of cybercrime are changing and spreading to all new advances in science and technology. There is an increasing focus on social media and mobile devices, an area where users are less aware of cyber threats. Hacking attacks have become more sophisticated and professional, targeting not only individual users, but also industrial systems.

References

1. Глотина И.М. Киберпреступность: Основные проявления и экономические последствия // Вопросы экономики и права. – 2014. – №8. – 12 с.
2. Сериева М. М. Киберпреступность как новая криминальная угроза // Новый юридический вестник. – 2017. – №1. – 104-106 с.
3. Дикарев В.Г. К вопросу о противодействии бесконтактному способу сбыта наркотиков через сеть Интернет // Вестник Московского университета МВД России. – 2016. – № 8. – 15 с.
4. Карцхия А.А. Кибербезопасность и интеллектуальная собственность // Вопросы кибербезопасности – 2014. – №1 (2). – 63 с.