International Journal of Early Childhood Special Education (INT-JECS)
DOI: 10.48047/INTJECSE/V14I7.302 ISSN: 1308-5581 Vol 14, Issue 07 2022

CYBERCRIME - AS A SOCIAL THREAT

AlimovaSh.X.
Senior Teacher of Tashkent University of Information Technologies named after Muhammad al-Khwarizmi
Karimova G.A.
Assistant of the Tashkent University of Information Technologies named after Muhammad al-Khwarizmi

Abstract: *This article discusses information threats in the world of information technology, tupes of cybercrime, legal mechanisms for preventing cybercrime, measures to coutteract cybercrime in the field of information.*

Key words: *information technology, information threats, cybercrime, legal legal mechanism, cybersecurity, information network, phishing, farming, social hacking, cyber terrorism, drug cyber trafficking*

Cyber security plays an important role in the world of information technology. Keeping data secure is one of the biggest challenges these days. When we think of cyber security, the first thing that comes to our mind is cyber crime, which is increasing day by day. Various companies and governments are doing a lot to prevent cybercrime. However, cyber security is still a huge problem for many people.

Currently, the Internet is the fastest growing infrastructure of daily life. In today's technological world, the latest technologies are changing the way people live. But due to emerging technologies, we cannot keep our information safe even in the most effective way and therefore cyber crimes are increasing day by day. Currently, more than 60% of financial transactions are done over the internet, so this industry requires the best quality security for large amounts of transactions[17, 84 p].

In the era of digitization, the system of social communication is based on the use of the Internet. According to the Digital 2022 report, as of January 2022, the number of users of this information network is 4.95 billion [11]. In this regard, the Internet creates conditions for dialogue and communication, allows the development of various types of human activity [10, 1043 p.]. But this information space has also become an area for criminal activities. In the 21st century, humanity first encountered a new and unknown type of crime - cyber crime.

Cybercrime is based on the implementation of criminal activities by people using information technologies in the virtual space, in particular, breaking Internet pages, spreading dangerous programs and illegal information. Here, the main tool for carrying out this type of illegal activity is the computer. It is a technical tool, an instrument that allows criminals not only to steal information, but also to destroy it, to place malicious programs or sites with computer viruses[15, 170 p].

This type of crime, like other crimes, threatens the information security of society. In addition to stealing money from bank cards, cybercriminals have learned to steal personal information, which can damage their reputation. Cybercrime is not only a problem of every Internet user, but it is appropriate to consider it in a broad social sense, even at an international level. Both individuals and legal entities suffer from the growth of cybercrime. Currently, the victims of hacker attacks are mainly large international organizations and countries[16, 56 p].

An important event aimed at combating cybercrime occurred on November 23, 2001. The Convention on Computer Information Crime was adopted by representatives of the European Union member states in Budapest, the capital of Hungary. In fact, this Convention, which is valid at the level of countries, was the first document that determined the legal fight against cybercriminal activities. It lists four main types of cybercrime, which are:

• illegal use;
• illegal acquisition of data;
• tampering with information;
• interfere with the system.

But in the past 20 years, cybercrime has also improved, and now there are many types of it, in particular, phishing, pharming, cyber-trafficking of drugs, cyber-terrorism, social hacking (piracy), etc[18, 901 p].

Phishing is one of the most common types of cyber fraud based on identifying and stealing a person's personal information in order to fraudulently use bank account numbers. Hackers often send users a file or link with malicious passwords. When a user accesses such resources, information is stolen, money is withdrawn from the bank account number illegally.

Farming is a type of cybercrime aimed at remote computer use. Using this method, a hacker takes control of a computer: edits documents, monitors the computer user using audio and video surveillance, introduces various malicious programs, collects information about the user. The main feature of this cybercrime is that the victim of the crime does not even realize that such actions are being carried out with his computer.

Cyber-trafficking of drugs is also carried out with the help of information technology. With their help, encrypted coordinates of the location of the "goods" are sent to the customer, and payment is made.

Cyber terrorism involves the use of information technologies or with the help of them to carry out terrorist activities. Such activities include dissemination of information about planned future terrorist attacks and calls to commit terrorist acts.

Social hacking or piracy refers to the illegal use of an information system. Hackers use various methods based on psychological influence on a person to get the necessary information. It is easier to affect the human psyche than to hack a computer system, after which hackers try to install malicious software to control the victim's computer, and they try to keep

the installed software as undetected as possible.

Day by day cybercrimes are widespread and their number is increasing in the form of geometric progression, new types of crimes are emerging, and it is necessary to find appropriate methods of combating each of them. This creates corresponding difficulties. A cybercriminal is more difficult to catch than a common criminal[19, 233 p].

Fighting cybercrime is complicated by a number of factors:

1. Cybercriminals are not ordinary fraudsters, but highly skilled programmers who hide behind computer screens and engage in illegal activities. Such a person is much more difficult to find than a common criminal;
2. Law enforcement officers still need the help of a small number of highly skilled programming experts when dealing with cybercrimes;
3. Determining the fact of the occurrence of this type of crime also causes many difficulties;
4. At the same time, it is more difficult to control the existing, new and constantly emerging types of cybercrime.

Currently, the countries of the world are working on fighting cybercrime. These measures are mainly based on the experience of European countries. Gradually, the level of awareness among the population about criminal activities such as cybercrime is increasing, and the legislation related to this area is improving. Special attention is paid to normative legal documents on cybercrime. In particular, in Chapter 28 of the Criminal Code of the Russian Federation, crimes committed with the help of virus programs and tools are not separately distinguished, and statistical reports do not allow to determine the content of cybercrime and determine its level[14, 37 p].

If we refer to the experience of international agreements adopted in the field of combating cybercrime, all of them require to some extent to be supplemented and amended. A vivid example of this is Article 51 of the UN Charter. In this article, it is required to distinguish the signs of cyber-attacks and the clauses that allow identifying the type of information technology used in this attack.

In the field of legal regulation of cybercrime, the project of the UN Convention on "Cooperation in Combating Information Crime" developed by Russian experts is noteworthy. It specifies the goals, including the direct cooperation of the countries, which consists of identifying and preventing violations in the information field at the initial stages, ensuring prosecution of these crimes, training and developing personnel to solve such issues, and helping each other (Article 1).

Many specific information terms are defined in detail in this Convention. For example, a "bot-network" refers to two or more ICT devices, the module of which is loaded with secretly controlled virus programs. Liability for illegal acquisition of information in electronic form is also established (Chapter 2), description of actions related to identification of persons suspected of this crime is given (Article 48). Article 57 of the Convention proposes to each country to establish a 24/7 information center to effectively combat such violations[20, 196 p].

Analysis of this Convention has shown that it contains a number of useful information that allows for the improvement of specific measures to combat cybercrime. In particular, a specific program for training qualified specialists dealing with information security is presented; It was emphasized that all countries of the world should have a unified policy on fighting cybercrime and active cooperation in this regard[13, 82 p].

Unfortunately, representatives of some delegations opposed this project. In their opinion, it is not necessary to make additional changes to the Convention adopted in Budapest in 2001, that is, the necessary provisions are sufficient to solve all the existing issues in the field of information. It is clear that such a vague approach means that some UN member states do not have a strategy for long-term cooperation in the fight against cybercrime[21, 295 p].

In order to conduct an effective policy in the field of combating cyber threats, the achievements and resources of the rapidly developing digitization process must be fully exploited. Also, digitalization can be important for ensuring the national and information security of the country. Proper implementation and use of digital technologies greatly facilitates the protection of user's personal data and important confidential materials at the state level [9, 259 p.].

Blockchain technology is the most promising direction in this field. It provides new opportunities to fight against cyber attacks, for example, a high level of protection against the possibility of information leakage to third parties. If earlier it was enough for a cybercriminal to make a single transaction to obtain the necessary information, now the blockchain makes this process much more complicated.

Another important aspect is the protection of the information exchange process. It is known that the protection system of a messenger such as WhatsApp does not provide a 100% guarantee that third parties will not gain access to private correspondence, since its encryption system is not perfect and has a number of weaknesses. To protect data from hackers, it is possible to use blockchain technology, which allows decentralization of the network by separating metadata and guaranteeing their non-shared use [1, 172 p.].

Of course, the use of blockchain technology alone is not enough to conduct an effective information policy to prevent and eliminate cybercriminal activity. Artificial intelligence resources can also be used in this area [6, 127 p.]. For example, every police department in the US is equipped with facial recognition software. This technology is actively used in practice, which creates ample conditions for searching for criminals and speeds up the process of determining the approximate vision of offenders [8, 53 p.].

In order to conduct an effective policy to combat information violations and cybercrimes, the following measures should be implemented:

• Improvement of technologies helping to detect cybercrimes on the network and methods of conducting investigations on these violations [5, 175 p.];

• Broadest possible use of blockchain technology to combat cyber threats;
• Development of artificial intelligence resources and their consistent implementation in the field of cybercrime investigation;
• Targeted fight against cyber terrorism in all its forms and manifestations.

References:

1. Antonyan E. A., Aminov I. I. Blockchain technology and anti-cyber terrorism // Aktualnye problemy rossiyskogo prava. 2019. No. 6 (103). S. 170-175.
2. Volynskaya O. V Razvitie juridicheskoy mysli i perspektivy v borbe s kiberprestupnostyu v sphere ugolovnogo sudoproizvodstva // Vestnik Moskovskogo universiteta MVD Rossii. 2020. No. 3. S. 72-74.
3. Danenyan A. A Mejdunarodnoe pravovoe regulirovanie cyberprostranstva // Obrazovanie i pravo. 2020. No. 1. S. 261-269.
4. Kumysheva M. K., Gelyakhova L. A. Question about cyberprestupnosti in Russia // Probely in Russian legislation. 2018. No. 4. S. 383-385.
5. Martyanov N. R. Criminal-law enforcement with cybercrime in the modern stage // Gosudarstvennaya slujba i kadry. 2020. No. 1. S. 175-177.
6. TimofeevA. V. Sushchnostiproblemyiskusstvennogointellektavkontektesovremennyxnauchnyxifilosofskikhpredstavleniy // VestnikMoskovskogogosudarstvennogooblastnogouniversiteta. Series: Philosophical science. 2020. No. 2. S. 127-133.
7. Tarasik N. M. Analyzpravovykhosnovborby s kiberprestupnostyu // Uspekhi v khimii i khimi¬cheskoytekhnologii. 2016. No. 5(174). S. 66-68.
8. Tishutina I. V Novyevozmojnostiraskrytiya i rassledovaniyaprespleniy v usloviyaxglo¬balnoytsifrovizatsii // IzvestiyaTulskogogosudarstvennogouniversiteta. Economic and legal science. 2019. No. 4. S. 46-55.
9. Shinkaretskaya G. G., Berman A. M., Tsifrovizatiya i problemaobespecheniyanatsionalnoybez¬opasnosti // Obrazovanie i pravo. 2020. No. 5. S. 254-260.
10. Guryanova A. V., Khafiyatullina E., Petinova M., Frolov V., Makhovikov A. Technological prerequisites and humanitarian consequences of ubiquitous computing and networking // Digital economy: complexity and variety vs. rationality. Lecture Notes in Networks and Systems. 2020. Vol. 87. P. 1040-1047.
11. Digital 2021: fixiruem tendentsii.iYa https://habr.com/ru/post/497204/ (access time: 25.01.2022).
12. Gorbunov A. S. Sotsialnaya otvetstvennost sredstv massovoy kommunikatsii v informatsionnom obshchestve // Vestnik Tverskogo gosudarstvennogo universiteta. Series: Philosophy. 2018. No. 4. S. 83-90
13. Alimova SX, Karimova GA. INFLUENING INCOLULOUS EDUCATION IN UZBEKISTAN AND DEVELOPMENT OF UNIQUE TENDENCIES. EuropeanScienceReview. 2019(5-6):80-3.
14. Алимова ШХ. ОБЕСПЕЧЕНИЕ МИРОВОЗЗРЕНЧЕСКОЙ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННОМ ОБЩЕСТВЕ. InMultidiscipline Proceedings of Digital Fashion Conference 2022 Jan 11 (Vol. 2, No. 1).
15. Касимова, З. С., &Санакулов, А. Н. (2019). ВЫСОКАЯ ДУХОВНОСТЬ-КАК ФАКТОР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. *European Journal of Humanities and Social Sciences*, (1), 168-172.
16. Sanakulov, A. N. (2019). MAINTENANCE OF THE WORLD OUTLOOK SECURITY IN THE INFORMATION SOCIETY. *Социосфера*, (4), 54-57.
17. Санакулов, А. Н. (2022, January). ВЫРАБОТКА ИНФОРМАЦИОННОГО ИММУНИТЕТА-КАК ЗАЛОГ ПОВЫШЕНИЯ ИНФОРМАЦИОННОЙ КУЛЬТУРЫ ЛЮДЕЙ. In *Multidiscipline Proceedings of Digital Fashion Conference* (Vol. 2, No. 1).
18. Sanaqulov, A. N. Prospective Directions of Effective Use of Virtual Technologies in Increasing the Power of Youth. *JournalNX*, 897-903.
19. Санакулов, А. (2017). Духовность-основа информационной безопасности. *Молодой ученый*, (19), 231-234.
20. Nazarovich, S. A. (2022). DEVELOPMENT OF INFORMATIONAL IMMUNITY AS THE KEY TO INCREASING THE INFORMATION CULTURE OF PEOPLE. *Conferencea*, 191-196.
21. Санакулов, А. Н. (2022). ОБЕСПЕЧЕНИЕ МИРОВОЗЗРЕНЧЕСКАЯ БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННОМ ОБЩЕСТВЕ. *YoshTadqiqotchiJurnali*, *1*(5), 290-296.