AMERICAN JOURNAL OF SOCIAL AND HUMANITARIAN RESEARCH

ISSN: 2690-9626
Vol. 4, No. 3, 2023

Features of Fighting Crime in the Sphere of Information Technologies and Security

Umirzakov Begzod Ataboevich
Docent, PhD in Law, docent of the Department of crime prevention and criminology of the Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan

ABSTRACT: This article discusses the problems of combating crime in the field of information technology and security, the amount of material damage caused by cybercrime, attacks in cyberspace, the role of the Internet, the large-scale development of information technology, crimes in the field of information technology, the volume and types of computer crimes, computer information, source of computer information, methods used in the commission of crimes in the field of computer technology, computer espionage, computer sabotage, object of crimes in the field of information technology, prevention of crimes in the field of information technology and security.

KEYWORD: information technology, cybercrime, material damage, cyberspace, Internet, computer crimes, computer espionage, computer sabotage, cyber attack, IP address, capture method, IMEI code, IP address, Face ID.

In the world, the problems of combating crime in the field of information technology and security are of global importance. In particular, the UN General Assembly, the Council of Europe, the SCO, the CIS, the League of Arab States and other organizations have adopted international legal documents to counter the use of information and communication technologies for criminal purposes. According to statistics, about **7 billion** people (95% of the world's population)[1] are currently covered by mobile telecommunication networks, the amount of material damage caused by cybercrime is **1%** of global GDP per year[2].

Cybercrime, which is mentioned in new forms, has long entered our public life, and it can be attributed to the global problems of our century. We cannot close our eyes to the fact that it poses a great danger to the life of mankind by spreading well-known virus programs, cracking passwords, stealing funds from credit cards and other bank details, and also disseminating illegal information, especially slanderous. and morally corrupted information via the Internet.

The Internet (from the English Internet) is a global computer network designed to store and transmit information. Often referred to as the "World Wide Web" or "Global Web". It is based on the World Wide Web (WWW) and other communication systems.

[1] Rasulev AK Improving criminal law and criminological measures to combat crimes in the field of information technology and security. Law. abstract of a doctoral dissertation. T., Academy of the Ministry of Internal Affairs, 2018. - B-5.

[2] http://www.statista.com/The StatisticsPortal).

ISSN 2690-9626 (online), Published by "Global Research Network LLC"
under Volume: 4 Issue: 3 in Mar-2023 https://globalresearchnetwork.us/index.php/ajshr

Currently, 63% of the world's population uses the Internet. In almost a year, the number of Internet users increased by 200 million. Most users (92.4%) access the Internet through mobile devices. The number of Internet users in Uzbekistan exceeds **27 million** people, of which more than **25 million** are mobile Internet users[3].

The large-scale development of information technology has made it possible to simultaneously commit many types of crimes, which, in turn, requires high knowledge and professional training in the field of detecting and preventing these types of crimes. Thus, "crime in the field of information technology" is a criminal act committed with the use of a computer and information processing systems, for which the law provides for criminal liability. Therefore, it is necessary to disseminate information about crimes in the field of information technology among citizens and carry out propaganda work.

The information society is rapidly forming, the concept of state borders disappears in the information world. The global computer network is fundamentally changing public administration.

Regardless of geographical location, various types of information enter our daily life through the international computer network Internet. That is why protection against such problems as misuse, change, loss and access to existing information has become an urgent problem.

According to the data, more than **500 million** cyber attacks are organized annually in the world. Every second, one out of every **12 people** in the world is the victim of a cyberattack. In particular, in countries such as the USA, France, England, Belgium, Germany, Luxembourg, the level of cybercrime is 60-65% of the total number of crimes.

According to experts, most cyberattacks are aimed at obtaining confidential information, changing or losing it, extorting money from users, or disrupting business processes. As a result, the global economy incurs losses of more than $20 billion annually.

In Uzbekistan, over the past three years, cybercrime has increased by **8.3 times**, accounting for **5%** of the total number of crimes. For example, cases of cyber fraud increased **13 times**, theft - **20 times**, crimes related to extortion, defamation and insult - **4.9 times**.

According to analytical data, some types of cybercrimes in our republic, including the theft of other people's funds on plastic cards through illegal banking and financial transactions, entering into someone's trust and obtaining an online microloan in your name, organizing financial pyramids, attacking computers using virus programs, intimidation by spreading someone else's personal information There is a growing number of crimes such as extortion, illegal drug dealing on the Internet, online gambling and risky games, information attacks aimed at religious bigotry, online shopping fraud.

One of the types of crimes that have arisen as a result of the development of modern information technologies and are expanding today are crimes committed using information technologies. The Criminal Code of the Republic of Uzbekistan classifies the following actions (inaction) as crimes in this area:

- violation of informatization rules (Article 278[1]);
- illegal (unauthorized) access to computer information (Article 278[2]);
- production for the purpose of sale or sale and distribution of special means for obtaining illegal (unauthorized) access to a computer system, as well as to telecommunications networks (Article 278[3]);
- modification of computer information (Article 278[4]);
- computer sabotage (Article 278[5]);

[3] https://review.uz/oz/post/ozbekistonda-internet-xizmatidan-foydalanuvchilar-soni-272-milliondan-oshdi

ISSN 2690-9626 (online), Published by "Global Research Network LLC"
under Volume: 4 Issue: 3 in Mar-2023 https://globalresearchnetwork.us/index.php/ajshr

- creation, use or distribution of malicious programs (Article 2786);
- illegal (unauthorized) access to the telecommunications network (Article 278[7]).

In practice, most often these crimes are committed in banking and credit organizations.

According to the International Committee Investigating and Combating the Scope, Types and Combating of Computer Crime, information technology crime poses a serious threat to any organization that works with and uses computers, and causes significant financial damage to them. According to calculations, as a result of the failure of computer equipment and settlement systems under external influence, very large banks may face irreparable financial problems in two or three days, and smaller organizations and enterprises in one day. These concepts are also based on the importance and relevance of the work to combat this crime, especially the issues of determining and eliminating victimization of victims.

Therefore, the actual aspect of this type of crime is the understanding of computer information and the correct identification of its owner. In the Law of the Republic of Uzbekistan "On the principles and guarantees of freedom of information" dated December 12, 2002, computer information refers to information about persons, objects, facts, events, phenomena and processes, regardless of sources and form of their presentation (Article 3).

Thus, computer information is understood as factual information processed by a computer system and transmitted to telecommunications channels, intended to be open for reception and understanding, on the basis of which it is possible to determine the circumstances relevant to criminal and civil cases in the prescribed manner, established by law.

As a source of computer information:

- technical printed information;
- information on magnetic disks, optical and other information carriers;
- recognized information and other information stored in the RAM database IS.

At the initial stage of the development of network technologies abroad, the damage caused by viruses and other types of computer attacks was not so great, due to the fact that the economy was not very dependent on information technology. Currently, the number of such attacks is increasing, mechanisms for their automation are being created, citizens, businessmen, government bodies are very dependent on electronic means of using and exchanging information, and the damage from attacks on information systems is enormous.

One of the important elements related to crimes in this area and related to their criminological characteristics is the way in which crimes are committed and concealed. According to information found in studies conducted by international organizations, the methods used in the commission of computer crimes are as follows:

- adaptation to match a password, corresponding key, or other similar information;
- changing the IP address (an attack method in which the attacking IP changes the packet, etc.);
- staging a denial of service;
- traffic analysis, its listening and analysis in order to collect information about the transmitted password and key;
- an information intrusion method based on a program that displays information about an approximate access point to a copying system;
- replacement, forced entry, deletion, reordering or modification of the contents of an existing InfoBase (messages sent by set).

ISSN 2690-9626 (online), Published by "Global Research Network LLC"
under Volume: 4 Issue: 3 in Mar-2023 https://globalresearchnetwork.us/index.php/ajshr

On this basis, the methods of committing crimes in the computer sphere can be divided into the following groups:

1) method of capture (through a system of telephone channels or connection to a computer network);

2) unauthorized method of connection;

3) method of falsification (data exchange, introduction of a Trojan virus program, modeling).

You can comment on the different types of crimes in the field of information technology in different countries. The main reason for this is that the level of economic development in the country also depends on the degree of implementation of information technologies in social spheres. For example, in 1998-2002, computer fraud (pin code theft) was widespread in the CIS member countries, that is, the theft of foreign products in Internet trade organizations. Since 2005, violations related to unauthorized access to the process of electronic data interchange have become more frequent.

At the same time, it is necessary to clarify the following concepts related to crimes committed in the field of information technology:

Computer espionage. This concept can be understood as actions to obtain information constituting a trade secret by illegal means or to make unauthorized copies of them in order to cause economic damage to the victim of a crime.

Computer sabotage - includes actions (inaction) such as misappropriation, erasure or replacement of data in a computer system or its networks in order to prevent a computer or data transmission system from working in a certain way.

From the above points, the following aspects of the motives and goals of persons who have committed crimes in the field of information technology can be indicated:

- self-interest (waste of money and property);
- political (espionage, actions aimed at destabilizing the financial, monetary and foreign exchange policy of the country);
- intellectual interest;
- hooliganism;
- revenge and other goals.

It should be said that the question of what is the object of crimes in the field of information technology is still debatable. In particular, in the legal literature there are different opinions about the object and subject of this type of crime. For example, V.V. Krylov believes that the object of these crimes is information from the EU. In its turn, L. Chichko understands the exposition of information as an object, and V.B. Milestones machine information. According to the supporters of the point of view that information can be the object of a crime, including computer information is a convenience created for society, and therefore the fact is harm caused by its illegal destruction or change. But computer information (such as confidential information) can be illegally copied and blocked. In this case, the information itself will not suffer in any way. However, a criminal act always harms the object of the crime, otherwise there would be no criminal element. What is a crime? What happens in the above two cases? What is it and why is it harmful?

In the first case, the information harms the relations of exclusive use of the right holder, and in the second, it directly harms the relations of lawful and safe use. Therefore, it can be concluded that computer information itself is not always harmed, but in all cases the interconnection of its use is violated.

ISSN 2690-9626 (online), Published by "Global Research Network LLC"
under Volume: 4 Issue: 3 in Mar-2023 https://globalresearchnetwork.us/index.php/ajshr

In the criminal law concept, computer information is the subject of crimes in the field of information technology. For example, such cases are directly indicated in the provisions of articles 2781, 2782, 2784, 2786 and 2787 of the Criminal Code of the Russian Federation. In other cases, the definition of the object is connected with the definition of a different corpus delicti (Articles 2783 and 2785 of the Criminal Code).

The special part of the Criminal Code of the Republic of Uzbekistan on crimes in the field of information technology is characterized by the fact that it mentions a special type of information - computer information.

Based on the foregoing, it can be noted that this type of crime directly encroaches on relations that ensure the lawful, safe use of information technology and damages the legitimate interests of users in the field of information technology.

When preventing crimes in the field of information technology, it is recommended to pay special attention to the following:

firstly, in paragraph "c" of part 2, article 168 of the Criminal Code of the Republic of Uzbekistan, state as "using telecommunications networks, including the global information network" Internet "or electronic means of payment", part 2 of article 273, "if it is committed using telecommunications networks, as well as through the global information network Internet", filling in the wording with a new paragraph "e".

When analyzing fraud, most crimes of this type are committed using information technology, especially through mobile applications, the number of cases of theft of funds from bank plastic cards through fraud and theft is increasing.

Point "c", part 2, article 168 or point "b", part 3, article 169 of the current Criminal Code provides for liability for fraud and theft committed with the use of computer technology. However, the concept of "commission using computer technology" is narrow and currently does not fully cover the way this type of crime is committed.

In addition, this article should be adapted to the requirements of the Cybersecurity Law adopted on April 15, 2022 in this direction.

The proposed concept "Using telecommunications, as well as the global information network Internet or electronic payment systems" is reflected in Article 159.6 of the Criminal Code of the Russian Federation, and a separate criminal liability is established for this act. In addition, article 159.3 of the Criminal Code of the Russian Federation establishes separate criminal liability for fraud committed using electronic means of payment.

Also, Article 190 of the Criminal Code of Ukraine, Article 177.1 of the Criminal Code of Latvia establishes special criminal liability for the illegal use of electronic computers and fraud in automatic data processing;

secondly, introduce a technical requirement for the full entry of the user's face (Face ID), geographic location data (geoposition - Location) when activating a mobile application account (in addition to the phone's IMEI code, a list of IP addresses).

For reference: in 2017, the introduction of the Face ID and Location functions into the Sberbank and Tochka mobile applications in Russia led to a decrease in related crimes by **85%.**

The introduction of this practice serves to reduce the number of crimes committed through mobile applications, timely determination of information about the person who committed the crime and his location, increase the security level of financial service providers and software, ensure reliable protection of citizens' funds on their plastic cards;

ISSN 2690-9626 (online), Published by "Global Research Network LLC"
under Volume: 4 Issue: 3 in Mar-2023 https://globalresearchnetwork.us/index.php/ajshr

thirdly, the introduction of the information retrieval and reference system "Population of Uzbekistan" and the widespread use of the capabilities of artificial intelligence technologies.

According to the experience of the leading countries of the world (Italy, the USA, etc.), the whole process from birth to death of each of the inhabitants of the country, including education in kindergarten, school (lyceum, college, technical school, etc.), the university and its character, interests, surrounding , marital status, etc. it is proposed to introduce the information retrieval and reference system "Population of Uzbekistan", the information of which is constantly and regularly updated, centrally with certain levels of permissions, and to widely use the capabilities of artificial intelligence technologies. Since this system collects all the information about the population of our country, it serves to make clear and correct decisions in any criminal situation. The integration of this system with digital technologies being introduced into internal affairs systems will become one of the most effective crime prevention measures today;

fourthly, further strengthening of advocacy for the prevention of crimes in the field of information technology using well-known bloggers, viners and tiktokers in social networks.

Recently, the role of social networks in improving the legal culture of the population and the fight against crime has been increasing.

In particular, some bloggers, viners and tiktokers in various forms show the processes taking place in all social spheres of society, which are watched by millions of citizens and discussed among the population on social networks.

At present, in order to improve the legal culture of the population and combat cybercrime by increasing the use of the services of bloggers, viners, tiktokers, it is necessary to develop social videos, cartoons, videos, booklets, paisas that attract citizens and cause a lot of discussion, and distribute them among the population, it is appropriate display on personal profiles of tiktokers, especially bloggers, viners.

ISSN 2690-9626 (online), Published by "Global Research Network LLC"
under Volume: 4 Issue: 3 in Mar-2023 https://globalresearchnetwork.us/index.php/ajshr