CLASSIFICATION OF INFORMATION SECURITY CRIMES

Tovbaev Sukhrob Asliddinovich
The Law Enforcement Academy of the Republic of Uzbekistan. A student of Master's programm "Investigation activity"

Annotation: *Today, the rapid development of information technologies and the widespread use of the Internet in all spheres of human society have become a part of everyday activities, and have had a positive impact on the way of thinking of modern people, including services, science, education, e-commerce, and so on. In addition to these changes related to the improvement of the quality of life, it should be noted that favorable conditions for the development of new forms of crime have appeared.*

Key words: *information security, information security crimes, computer crimes, cyberterrorism, cryptomining, cyber espionage, cybercrime, cyber-suicide, internet fraud, cyber-terrorism, cyber-bullying, cyber-pornography, cyber-extremism.*

Crimes related to information security are becoming more widespread due to the constant development of technology and the internet. Additionally, identifying and prosecuting these crimes can be challenging, as one of the difficulties is that citizens may be reluctant to report computer crimes to agencies that protect their rights regarding computer abuse and the fact that legal knowledge of computer crimes may be insufficient.

Some types of crimes in the field of information technology are as follows:

- disseminating virus-infected software;
- stealing user's confidential information;
- piracy of intellectual property of others;
- hacking into other people's accounts on social networks;
- disseminating false information, defamation;
- interethnic or interreligious hostility;
- illegal operations with bank plastic cards (card details);
- fraud in the securities market on the Internet;
- financial pyramids on the Internet;
- crimes related to mobile communication.

The reason why different individuals classify crimes related to information security in various ways is due to their varying types and quantities. Specifically, they may include internet fraud, stealing financial or bank card information, theft and sale of corporate data, cyberterrorism, cryptomining, cyber espionage, and various other types of crimes. Therefore, they can be divided into two groups: crimes related to information security committed against the computers themselves, and crimes related to information security committed using computers.

Indeed, it is necessary to partially consider the classification of crimes related to information security into two groups, as the primary goal of such crimes is to cause material, moral, political, or other types of harm to the second party. In committing these

crimes, the offender uses information technology for their sinister purposes, either to achieve their goal or to weaken the second party by disabling their information and communication technology, thereby causing harm to individuals and society. Specifically, cybercrime, cyber-suicide, internet fraud, cyber-terrorism, cyber-bullying, cyber-pornography, cyber-extremism, and other crimes related to information security are not committed only to harm the information and communication technology of the victim but to cause harm to the individual and society as a whole. On the other hand, in crimes such as cyber-terrorism, cyber-aggression, computer modification, unauthorized use of computer information, computer sabotage, and other crimes related to information security, the offender's goal is to cause damage to the information technology of the second party and disable it.

According to an article posted on the "Tadviser" website, crimes related to information security can take various forms, including spam, targeted phishing, PDF attacks, search engine optimization (SEO) poisoning, and disabling the victim's ability to work.

The Decree of the President of the Republic of Uzbekistan "On Measures to Radically Improve the System of Criminal and Criminal Procedure Legislation" No. PQ-3723 of May 14, 2018, aimed at ensuring the legality and regulatory framework of the state, protection of human rights and freedoms, interests of society and the state, ensuring security and safety, identified the creation of an effective system of criminal and criminal procedural legislation as one of the priority tasks. The "Concept for the Further Development of the Criminal and Criminal Procedure Legislation of the Republic of Uzbekistan" was subsequently adopted as a result. The document emphasized the need to review norms and standards related to the responsibility for crimes in the field of information technology, taking into account the increasing number of cyber crimes, and identified the revision of norms related to information technology as an important task. Therefore, based on this foundation, we propose the following concepts to be introduced into our national legislation:

cyber theft – the secret misappropriation of property through telecommunication networks, the Internet, or other information and communication technologies.

cyber fraud – the acquisition or disposal of property or the right to property by deceit or breach of trust through telecommunication networks, the Internet, or other information and communication technologies.

cyber embezzlement – the open misappropriation of property through telecommunication networks, the Internet, or other information and communication technologies.

cyber extortion – forcing the transfer of property or the right to property, the provision of material benefits, or the commission of actions that violate property rights or interests using cyber technologies, accompanied by threats, committed against the will of the injured party or under duress.

cyber suicide – inducing or attempting to induce suicide through telecommunication networks, the Internet, or other information and communication technologies.

cyber pornography – the production, importation, exportation, distribution, display, use, or promotion of pornographic materials through telecommunication networks, the

Internet, or other information and communication technologies, in violation of the laws of the Republic of Uzbekistan.

cyber aggression – participation in the organization or preparation of acts of aggression, including the use of information and communication technologies, and participation in the dissemination of false information aimed at inciting such actions.

cyber terrorism – the use of information and communication technologies to complicate international relations, violate the sovereignty and territorial integrity of the state, cause harm to its security, organize armed conflicts and terrorist acts, destabilize the socio-political situation, intimidate the population, influence the adoption of decisions by state bodies or international organizations, or to threaten the life of a person by using violence, dangerous substances, or other means in order to achieve political or other goals.

We hope that the inclusion of these concepts in the national legislation will demonstrate its positive aspects in combating and prosecuting these types of crimes, as well as in fighting against them. Cybercrimes can ultimately affect personal information, financial resources, commerce, and even national security. Additionally, proper identification, limitation, and opposition to these crimes are crucial.

To have a clear understanding of cybercrimes related to information security, it is useful to classify them into categories and organize their content and nature accordingly. This will help in developing a systematized approach to identify, prevent, and prosecute such crimes.

Similarly, it is possible to attribute cybercrimes related to information security to information and communication technologies that serve as the means or tools for their commission. However, it may be challenging to give a definitive name to such technologies or communication channels, as these concepts continuously evolve and absorb new meanings. While the development of the field may capture all current notions, we cannot guarantee that it will remain unchanged in the future. Therefore, we cannot label all information and communication technologies as being inherently related to cybercrimes related to information security, as the use of such technologies does not automatically imply criminal activity. For instance, we cannot consider the act of a person's acquaintance viewing or hearing about crimes they committed as cybercrimes, as the person did not use any information and communication technology to commit the crime. Additionally, this act does not necessarily involve the intent to cause psychological harm. However, if the person intentionally shows or tells someone about the crime to cause psychological harm, this could be classified as cyberbullying or cyberstalking.

Regarding the classification of cybercrimes related to information security, scholars express various opinions. In particular, P.S. Titova's view is that cybercrimes related to information security can be divided into different types, such as electronic and computer fraud, stealing money from bank accounts and cards, attacking and stealing information from databases, hacking attacks, spreading viruses, illegally listening to phone conversations, interfering with personal life, and intellectual property theft.

According to T.L. Tropina, cybercrimes related to information security can be classified into various types, such as violating confidentiality of information, unauthorized

access to computers and computer networks, violating the privacy of commercial secrets, computer sabotage (including disrupting operations, altering or deleting information, and more), economic cyber attacks (especially computer fraud), among others. Additionally, these crimes can be broadly categorized into the following types that cause harm or danger to physical security, life, and health of individuals, as well as violations of property rights, intellectual property, and information security. They include unauthorized access to computers or computer systems without causing damage, destruction of information and data integrity, violating the security of computer systems, and various cyber attacks that violate the privacy and security of society, as well as endangering the security of society and other cybercrimes related to information security, which are made possible through the use of information technology. These crimes can cause damage to property but are not necessarily related to theft of money, information, or property. They include violations of property rights, intellectual property, and information, as well as cybercrimes related to information security that violate social morality, endangering public safety and other cybercrimes related to information security that facilitate other computer crimes. These crimes can be carried out using traditional information technologies, and some cybercrimes related to information security are considered to be committed with the help of other information technologies.

As explained by E.L. Kochkina, cybercrimes related to information security can be classified into various types, such as financial cybercrimes, cyber pornography, cyber prostitution, cyber terrorism, cybercrimes related to infringement of human and citizen constitutional rights and freedoms, cybercrimes related to public relations and information technologies in the field of computer data, cybercrimes related to public relations and information technologies in the field of economics and economic relations, cybercrimes related to public relations and information technologies in the field of state governance, as well as cybercrimes related to public relations and information technologies in the field of public health and social welfare.

As maintained by E.S. Shevchenko, cybercrimes related to information security that are considered as property crimes include fraud using electronic payment instruments and systems, embezzlement using electronic payment instruments and systems, theft using electronic payment instruments and systems, economic crimes (legalizing proceeds from crime, illegal entrepreneurship), i.e. legalizing illegally obtained proceeds using electronic payment instruments and systems, illegal entrepreneurship, computer-related crimes, i.e. illegally accessing computer data that is an information object of electronic payment systems, creating, using and distributing harmful programs intended to carry out illegal activities in electronic payment systems or methods, crimes against state power, crimes against the state service and local government service (giving and accepting bribes through electronic payment instruments and systems).

N. Limoj and M. Kosovich address cybercrimes related to information security in their research, which include crimes against the confidentiality, integrity, and availability of computer data and systems, crimes related to unauthorized access to computers, and crimes

related to content-related information security. They also discuss cybercrimes related to infringement of copyright and related rights.

As mentioned by Y. Gazizova, cybercrimes related to information security can be divided into several types, such as phishing, carding, SMS phishing, internet phishing, vishing, skimming, shimming, online fraud, piracy, malware, illegal content, and relay attacks.

D.V. Pashnev separates cybercrimes related to information security into two categories: crimes committed using computer technology against information security and crimes against automatic information security aimed at improving computer technology.

According to Nare Smbatyan, cybercrimes related to information security can be classified into three categories: economic computer crimes, cybercrimes against human constitutional rights and freedoms, and cybercrimes against state and public security.

Other scholars differentiate cybercrimes related to information security into various categories, including financial cybercrimes, cybercrimes related to personal life, cybercrimes with social and political motives, and financial cybercrimes such as phishing, cyber terrorism, financial fraud, cybercrimes related to personal life such as harmful networks, email, websites, devices, fake networks, wireless networks, viruses, and cybercrimes with social and political motives that involve offenses against national, racial, ethnic, and gender-based security.

Budapest Convention on Cybercrime, addresses cybercrimes related to information security, including offenses committed through the Internet and other computer networks, copyright infringement, computer fraud, child pornography, and violations of network security. The Convention is considered the first international treaty designed to combat cybercrimes and promote international cooperation in the fight against such crimes.

The opinion of the Eurasian Group on Combating Money Laundering and Financing of Terrorism regarding the fight against illegal activities and the legalization of criminal proceeds states that cybercrimes related to information security include fraud in the Internet, particularly the creation of “financial pyramids” on the Internet, fraud in online auctions, and the creation of software tools for stealing financial, commercial, or personal information (such as creating fake websites, spreading computer viruses and Trojan programs, disrupting traffic, and more). Other cybercrimes include fraud in remote banking services, such as creating computer viruses and Trojans to secretly collect information on the client's computer through the software of the service provider, opening bank accounts, carrying out unauthorized transactions and obtaining cash through unauthorized transactions in remote banking systems, obtaining funds through foreign payment systems, connecting to the computers and banking systems of foreign banks and clients, skimming, reading, copying and stealing information from the magnetic stripe of payment cards, manufacturing and selling equipment specialized in stealing PIN codes, installing and using this equipment in ATMs, cloning payment cards and using them to withdraw cash from ATMs, canceling transactions, and obtaining cash illegally.

As a suggestion, it is possible to introduce the concept of cybercrime related to information security into our national legislation and appropriately categorize and penalize

them accordingly. This would be in line with the goal of promoting international cooperation in combating cybercrimes, as well as protecting the security and privacy of individuals and organizations in our country. It is important that our laws keep up with the changing landscape of technology and address the unique challenges and risks posed by cybercrimes.