CONCEPT AND THEORETICAL BASIS OF INFORMATION SECURITY CRIMES

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

In recent times, in legal literature, the concepts of «information crimes», «crimes related to information security», «crimes in the field of information technologies» or the currently widely used term «crimes related to information security» have emerged. Below, the content, nature, similarities and differences of these concepts are examined.

Firstly, if we look at the definition given to the concept of information, according to the Law of the Republic of Uzbekistan «On Principles and Guarantees of Freedom of Information» No.439-II dated December 12, 2002, information is data on individuals, objects, facts, events, and procees related to sources and methods of their provision.

The concept of «crimes related to information security» was formed with the continuous development of information technologies and the emergence of the Internet. The main difference of such crimes is that some of them are committed using a computer (computer crimes), while others are committed through the Internet (cybercrimes).

Crimes related to information security are considered illegal activities that involve the missue of a computer, computer network, or other related devices. The majority of these crimes are commited by hackers or cybercriminals with the aim of making illegal profits from it. With the rapid development of technology, criminals have also started to use it to carry out illegal activities. In particular, theft of money from credit cards has increased significantly. Of course, law enforcement agencies are identifying these criminals, and appropriate legal penalties are being imposed, and compensations are being paid to the victims.

It is important to emphasize that the threat of cyber terrorism and its impact on society is increasing. Cyber terrorism is a criminal act carried out using computers and information communication technologies that directly or potentially threaten human life and health, cause significant damage to material objects, or aim to initiate or achieve social and political consequences. For modern terrorists, the attractiveness of using cyberspace lies in its ability to carry out cyber attacks without requiring significant financial resources. According to experts, this is being done to support the development of developing countries, influence public democratic decisions, and achieve their goals by various means. Unfortunately, in this process, the coordination of cyber attacks is becoming more and more sophisticated, and there are numerous opportunities to take advantage of the limitless possibilities of the global Internet. The role of social networks and their manufacturers and users in the internal affairs of sovereign states is still not fully understood, and sometimes such «interference» is still unrecognized by the affected state. Owners of social networks are not held accountable for encouraging state subversion on their sites, as there are no international legal frameworks to regulate these issues. However, each criminal act or inaction must be punished according to its content and nature, and there should be no

impunity. Internet sites emerge quickly and change their format and address frequently. Therefore, some experts propose moving away from the initial concepts, such as the transparency of the Internet, and suggest transitioning to a new system that emphasizes the anonymity of Internet users. This will provide even greater protection against criminal attacks on the network.

Indeed, it is necessary to take necessary decisions to combat crimes related to information security and cybercrime, as well as to develop normative-legal documents and projects aimed at identifying, neutralizing, and preventing them. This includes fighting cyber terrorism, cyber extremism, organized cybercrime, and threats to state interests and cyber security. It is important to conduct inspections and initial investigations before taking legal action, to carry out quick searches and to protect citizens' rights and freedoms. It is also essential to identify the causes and conditions that lead to the occurrence of crimes related to information security and to eliminate them.

Crimes related to information security have developed differently in different periods, and therefore their doctrinal and official definitions also vary. In particular, according to the Council of Europe’s 2001 Convention on Cybercrime, «Cybercrime is any offense committed using computer systems, including any offense committed against computer systems». This is a valid view, as any technology can develop, but all crimes committed using it are committed in cyberspace, which is an environment where social and public dangerous acts involving all technologies can be captured.

It is worth noting that the concept mentioned above can be emphasized through the fact that the Law of the Republic of Uzbekistan «On the Legal Protection of Computer Programs and Databases Created for Electronic Computers» with the number 1060-XII, adopted on May 6, 1994, precisely in 1994, which provides legal protection for computer programs and databases created for electronic computers in Uzbekistan, from a historical perspective.

As noted above, cybercrime can also be considered in the context of computer-related crimes, and in fact, if we look at the Russian text of the Council of Europess 2001 Convention on Cybercrime, in some cases it can also be translated as Convention on Computer Crime. To better understand this situation, let's look at an example: Article 169, paragraph 3(b) of the Criminal Code of Uzbekistan defines the crime of theft committed using computer technology as requiring the use of a cyber environment, that is, a virtual environment, where the perpetrator, before committing the theft crime, has access to the password of the victim’s card that holds the stolen funds and uses telecommunications or the Internet or another network to commit the crime. We cannot see this environment with our eyes or touch it with our hands, but we can understand how the perpetrator gains access to these funds by cracking the code on the victim’s card. This environment is called cyberspace. Similarly, the purpose of the Law on Information is to regulate relations in the field of using information resources, information resources, and information systems, without showing the concept of computer technology as a separate concept, but rather taking into account that information technology cannot be separated from other information technologies, systems, and networks. Articles 4, 10, 14, and 16 of the Criminal

Code demonstrate the necessity of applying the principles of criminal and legal liability. Based on the above, it is appropriate for the views of these scholars to be developed in a technical, doctrinal, and legal sense. The concept of global network crime is not fully consistent with the concept of «computer crime» that existed until then, and therefore the term «cybercrime» is now commonly used for this type of crime. Initially, the concept of «computer crime» was used in international scientific and legal practice, then the concepts of «computer-related crime,» «computer-mediated crime,» «electronic crime,» «high-tech crime,» «virtual crime» were used, and today the terms «cybercrime» or «global network crime» are used.

N. Salaev and R. Roziev emphasize that crimes committed through direct computer means or through the use of information technology that pose a serious social threat as defined by law are cybercrimes related to information technology, and they emphasize that this is synonymous with computer crimes. Additionally, crimes committed through computer systems, networks, and other related tools or against them, as well as crimes committed through cyber means against computer systems, networks, or computer information, are referred to as cybercrimes related to information security, distinguishing them from cybercrimes related to information security.

According to M.Gurcke, crimes committed against computer systems, networks, or computer information through computer systems, networks, and other related tools or against them through cyber means are collectively referred to as cybercrimes related to information security.

According to the views of K.E. Zinchenko, L.Y.Ismailova, A.N. Karakhanian, B.V. Kiselyov, V.V. Krilov, Y.M. Mastinsky, N.S. Polevoy, Yu.N. Solovyev, V.V. Khurgin, and S.I. Tsvetkov, crimes of this nature are crimes committed through computer systems.

I.Torokhodjaeva emphasizes that it is necessary to recognize the specific challenges posed by cybercrime and to address them in the fight against it, as cybercrime is a broader concept than computer crime. She also notes that the concept of cybercrime has been related to information security since the Dallas Bar Association conference in 1979, where the main characteristics of computer crimes were identified based on the technical capabilities of information and communication technologies available at that time. This highlights the interdependence of the concept of cybercrime and the technological capabilities of the time.

A.V. Fedorov defines cybercrimes related to information security as any offense committed through the use of specially designed software for storage, processing, and transfer of information about people, objects, events, situations, and processes in mathematical, symbolic, or any other form. This information can be stored in physical or virtual memory of local or global computer networks, and can be accessed, modified, or transmitted through specially designed software for storage, processing, and transfer of information. Therefore, any crime committed using such software for the purpose of storing, processing, modifying, or transmitting information can be considered a cybercrime related to information security.

L. Kochkina uses different terms to refer to cybercrimes related to information security, including «computer-related crimes,» «cybercrimes,» «crimes associated with computer equipment,» «high-tech crimes,» and «crimes in the information field».

According to the views of V.A. Dulenko, R.R. Mamlev, and V.A. Pestrikov, «cybercrimes related to information security» refers to any crime committed using a computer system, which includes any crime committed in the electronic environment. Therefore, any offense committed using computer networks, the internet, or any other electronic means can be considered a cybercrime related to information security.

T. Borodkina refers to these crimes as cybercrimes, while I.M. Rassolov suggests considering them as a separate category of crimes in criminal law. On the other hand, according to the view of Sh. Tolmasov, cybercrimes related to information security are crimes committed by individuals using information technology for illegal purposes.

O.A. Kuznetsova emphasizes that cybercrimes related to information security are not limited to computer-related crimes, but also include crimes committed through other information technologies and internet networks. Therefore, cybercrime should not be narrowly defined as computer crime alone, but rather as any offense committed using information technology for illegal purposes. This broader definition includes crimes committed through electronic devices and stored information, but also crimes committed through other digital means.

I.G. Chekunov considers this crime as a crime committed through computer and mobile (portable) communication devices. According to the view of V.A. Nomokonov, cybercrimes related to information security are much broader than computer crimes and are a distinct phenomenon in the information space. I.V. Ramanov also shares a similar view, emphasizing that cybercrimes related to information security are not limited to computer crimes, but are a separate category of crimes that require special attention, investigation, and prevention measures due to their unique characteristics in the information space.

Cybercrimes related to information security are any crimes committed through computer systems, networks, or other electronic devices in the digital realm, or any crimes committed against them. These crimes cover a wide range of offenses, including breaching electronic security, accessing or altering information, using electronic identification, selling or transmitting personal information, engaging in fraudulent activities in e-commerce, disrupting a single information network or maintaining information security in hazardous situations, and addressing key issues related to information security.