FOREIGN EXPERIENCE IN THE INVESTIGATION 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: *The large-scale development of information technologies has made it possible to commit many types of crimes at the same time, which, in turn, requires high knowledge and professional training in the detection and prevention of these types of crimes. Thus, "crime in the field of information technology" is a criminal act committed using computers and data processing systems, for which criminal liability is provided by law. Therefore, it is necessary to disseminate information about crimes in the field of information technologies among citizens and carry out propaganda.*

Key words: *information security crimes, investigation of information security crimes, information technology crimes, information dissemination, cyber threats.*

In a world where information technology and telecommunications are rapidly developing, crimes in the field of information technology have emerged. Because, if we say that in the modern world, information is the most important component of the development of society, it is not an exaggeration. The fact that society is turning into an information society indicates that any personal information is important. At the same time, information has been recognized as one of the most important assets, so its protection and delivery is an important activity that should not be neglected. The unprecedented speed of information dissemination, especially through social networks, has led to repressive actions against regimes that wanted to hide their actions and conduct public and information warfare on an international scale without sufficient skill.

Under such circumstances, the issue of participation in the fight against transnational information security crimes is crucial for the negative consequences of undermining global legal integrity. Understanding the global nature of information security crime is essential. Currently, cyber-attacks not only affect the work of individuals, but also the systems of institutions and state bodies that need to protect themselves from such attacks. Cyber threats may come not only from hackers or their groups, but also from separate states, terrorist or criminal groups. In order to combat crimes related to information security, it is necessary to be aware of the degree of their latent nature when developing tools and methods to combat them.

According to experts' estimates, the latency of "computer crime" is around 80% in the United States, 85% in the United Kingdom, 75% in Germany, and over 90% in Russia. According to Symantec Security's international cyber security service data, "every second" 12 people around the world fall victim to cyber-attacks, and an estimated 556 million cyber crimes are committed annually worldwide, resulting in losses of over 100 billion US dollars.

There are effective systems to combat cybercrime around the world. At the same time, leading countries are actively creating and expanding the divisions of armed forces and

specialized services that need to ensure the development of offensive capabilities in the cyber domain. For example, in the United States, during military operations, the Pentagon provided relevant support from the National Cyber Security Center, which has been operating for some time. This aligns all efforts on a global scale. Civilian federal institutions and similar software are interconnected. These organizations have departments that are partly subject to supervision, as the supervisory body is the "Council". National security responsibility committees implement information strategies within their purview.

In Australia, a group has been formed to improve email security, and the main task of this group is to create a reliable security electronic system for both the public and private sectors.

In the United Kingdom, cyber defense programs are implemented to ensure the ability of officials to counter threats emerging from cyberspace.

Measures to counter cybercrime are not only implemented by individual states, but also by their blocs, particularly NATO. In recent years, the significance of this issue has been reflected in all documents and strategies adopted by the blocs. For the first time, the NATO concept includes the rules of engagement in the alliance's activities in the field of cybersecurity, reflecting the emergence of the cyber domain as a new direction in military operations from a strategic perspective.

If we consider that this type of crime is becoming globalized, no single country can effectively defend against this threat on its own. Under such circumstances, international cooperation, joint action against cybercrime, and the establishment of relevant institutions to monitor and regulate such activities, as well as the development of international legal mechanisms for cooperation, are the only way forward. If we take these into account, the following normative and legal documents should be adopted to address them in an organized manner.

The Budapest Convention on Cybercrime was signed on November 23, 2001, to harmonize national laws and procedures related to cybercrime, strengthen cooperation between countries, and combat cybercrime. The Convention and its explanatory report were opened for signature in Budapest on November 23, 2001, during the 109th Session of the Committee of Ministers of the Council of Europe and entered into force on July 1, 2004. As of September 2019, 64 states have ratified the Convention, while four states have signed but not yet ratified it. Significant countries such as Brazil and India have not yet acceded to the Convention due to their non-participation in its drafting. This is the first international legally binding instrument that regulates cybercrime. Since 2018, India has been reviewing its position on the Convention after concerns were raised about sharing information with foreign agencies, but it has yet to ratify it.

On March 1, 2006, the Additional Protocol to the Convention on Cybercrime concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems was adopted. States that have ratified the Additional Protocol are required to criminalize the dissemination of material through computer systems that threaten or insult on racist or xenophobic grounds, as well as to hold those responsible for such acts criminally accountable.

The Convention is the first international treaty on crimes committed via the Internet and other computer networks. It covers a range of offenses, including copyright infringement, computer-related fraud, child pornography, cyberstalking, and network security breaches. Additionally, it incorporates a range of powers and procedures for searching and seizing computer networks, as well as for legal cooperation. Its main objective, as stated in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, including by adopting appropriate legislation and fostering international cooperation.

The Conventionis primarily aimed at:

- harmonizing national laws and regulations related to cybercrime and their criminal law elements;
- facilitating mutual legal assistance and necessary powers for criminal prosecution, including for cybercrime committed through computer systems or evidence obtained through electronic means;
- establishing a framework for fast and effective international cooperation.

The Convention pays particular attention to the following offenses: illegal access, illegal interception, data and system interference, misuse of devices, computer-related forgery, computer-related fraud, child pornography, and violations of intellectual property rights and other related offenses.

In addition, in 2014, the African Union's Convention on Cyber Security and Personal Data Protection was adopted, which addresses issues of mutual interest and cooperation among African states in combating cybercrime. The Convention provides for the protection of the rights and freedoms of cyber citizens, including the protection of their personal data, and aims to promote trust and confidence in the use of information and communication technologies in Africa.

Indeed, it is possible to see that all countries around the world are dealing with these types of crimes, and the UN member states are not an exception. For instance, Tajikistan, the capital city of Dushanbe, became a signatory to the "Agreement on Cooperation among the Member States of the Commonwealth of Independent States in Combating Crimes in the Sphere of Information Technology" on September 28, 2018, which aims to establish cooperation among the member states of the Commonwealth of Independent States (CIS) in combating cybercrime. Azerbaijan, Armenia, Belarus, Kazakhstan, Kyrgyzstan, Russia, Moldova, Tajikistan, Turkmenistan, Uzbekistan, and Ukraine are among the participating countries in this agreement.

On February 13, 2019, the President of the Republic of Uzbekistan issued Decree PQ-4188, which approved the "Agreement on Cooperation among the Member States of the Commonwealth of Independent States in Combating Crimes in the Sphere of Information Technology" signed by the heads of the CIS member states during the Council of CIS Heads of State on September 28, 2018. The Ministry of Internal Affairs of the Republic of Uzbekistan, the State Security Service, and the State Inspectorate for Supervision of Communications, Information, and Telecommunication Technologies were designated as the authorized bodies for the implementation of the agreement in Uzbekistan.

The document states that, in the context of combating cybercrime, it is possible to cooperate with the member states of the CIS who have joined the Agreement in taking the following actions (if they are committed intentionally):

a) destruction, blocking, alteration or copying of information (computer) systems, unauthorized access to computer data protected by law, and dissemination of malware;

b) creation, use or distribution of harmful software;

c) violation of rules that lead to the destruction, blocking, or alteration of computer data protected by law by a person who has the right to use the computer system, if such actions have caused serious harm or serious consequences;

d) unauthorized access to computer data protected by law;

e) dissemination of pornographic materials or objects with pornographic features depicting underage persons through the Internet or other electronic communication channels;

f) production of marketing or special software or hardware for unauthorized access to a secure computer system or network;

g) modification of information stored on a computer or property theft by entering incorrect information into a computer system that utilizes public information tools or data networks;

h) unauthorized use of software for computer systems and databases that are subject to copyright, as well as infringement of copyright, if such actions have caused serious harm;

i) dissemination of materials related to extremism, terrorism, or materials that promote terrorist activities or terrorism through the Internet, telecommunications or other electronic communication channels in a manner specified by law.

The 5 modulesof this document identify the following forms of cooperation between participating states:

a) Information sharing, including:

- Crimes committed or prepared by individuals or legal entities related to information technologies;
- Identification, prevention, investigation, and prosecution of crimes related to information technologies;
- Methods of committing crimes related to information technologies;
- National legislation and international agreements regulating the identification, prevention, investigation, and prosecution of crimes related to information technologies.

b) Responding to requests for assistance in identifying, preventing, investigating, and prosecuting crimes related to information technologies, including obtaining information that could be used to facilitate rapid and effective search operations within the territory of the requesting state;

c) Planning and carrying out coordinated actions and operations to identify, prevent, investigate, and prosecute crimes related to information technologies;

d) Developing and implementing information systems and software that ensure the execution of tasks related to identifying, preventing, investigating, and prosecuting crimes related to information technologies;

e) Sharing publications and research results, as well as conducting joint research on issues of mutual interest related to combating crimes related to information technologies;

f) Sharing normative and legal documents and scientific and technical literature on combating crimes related to information technologies;

g) Providing assistance in training employees and improving their skills, including organizing internships, conferences, seminars, and training courses;

h) Developing and sharing software and solutions to identify, prevent, investigate, and prosecute crimes related to information technologies through mutual influence and experience;

i) Conducting inquiries related to the rapid storage of information in computer systems;

j) Other forms of mutual cooperation.

It should be emphasized that this document does not provide legal assistance for requesting parties, but rather focuses on non-binding (informal) cooperation between participating states.

In addition, the document allows for requesting information and assistance in conducting rapid search operations, the results of which may be used as part of mutual legal assistance (referred to among practitioners as an "Interpol request") in the future.

Regarding crimes related to information technologies, in particular, the document identifies the possibility of conducting inquiries to ensure the rapid and secure storage of information in computer systems, which is a crucial matter. After the measures for storing information are taken, law enforcement authorities may submit official requests for obtaining such information.

REFERENCES:

1. Convention on cybercrime, opening of the treaty: Budapest, 23/11/2001;
2. Vardanyan A.V., Nikitina E.V. Investigation of Hi-Tech and Computer Information Crimes. Moscow, Yurlitinform Publ;
3. Karpova D.N. Cybercrimes: a global issue and its solution. Vlast'= The Power no. 8, pp. 46–50;
4. Berd K. A war with many unknown quantities. Computerra, 2009, no. 20, pp. 26–29;
5. Zavyalov S. International experience in fighting the propaganda of terrorism in the Internet. Foreign Military Review, 2014, no. 4, pp. 34–39;
6. Zgadzai O.E., Kazantsev S. Ya. Cybercrime: factors of danger and problems of struggle. "Research Center for the Security of Children", 2013, no. 4 (18), pp. 80–86.