INFORMATION SECURITY AND CRIMINAL LAW
(UZBEK AND FOREIGN EXPERIENCE)

A.Rasulev,
Associate Professor of the "Prevention of crimes” Department of the Academy of Ministry of Internal Affairs of the Republic of Uzbekistan, Doctor of science in Law

A.Tursunov,
Head of the "Prevention of crimes” Department of the Academy of Ministry of Internal Affairs of the Republic of Uzbekistan, Doctor of science in Law, Professor

http://dx.doi.org/10.26739/2521-3253-2018-12-8

Abstract: Article conducts a comparative legal analysis of the norms of the criminal legislation of the Republic of Uzbekistan and some foreign countries in the field of countering crimes against information security on the Internet.

Key words: criminal law, cybercrime, information, information security.

Cyber attacks are growing in prominence every day - from influencing major elections to crippling businesses overnight, the role cyber warfare plays in our daily lives should not be underestimated.

In fact, billionaire investor Warren Buffett claims that cyber threats are the biggest threat to mankind and that they are bigger than threats from nuclear weapons.

According to Microsoft, the potential cost of cyber-crime to the global community is a mind-boggling $500 billion, and a data breach will cost the average company about $3.8 million.

According to data from Juniper Research, the average cost of a data breach will exceed $150 million by 2020 - and by 2019, cybercrime will cost businesses over $2 trillion - a four-fold increase from 2015.

The cyber security industry is rapidly growing every day. As more specialists join the ranks, more malware is being launched than ever before: 230,000 new malware samples/day. Although more resources are being deployed to counter cyber attacks, the nature of the industry still has a
Statistics shows necessity of legal protection of social relations in the sphere of information technologies. Among legal norms, criminal law norms are very effectively tools to Legislation of most developed countries about ten to fifteen years ago was not sufficiently prepared for the massive onset of "computer crime" and information security. Also, criminal law almost did not contain any norms that would allow to effectively combat crimes in the field of information and communication technologies. As a result, these actions were often qualified by analogy, due to which many criminals either avoided punishment at all in connection with the termination of the case, or the severity of punishment was clearly inadequate to the deed. Therefore, many states have urgently introduced norms providing for responsibility for "computer crimes" to the criminal law. Moreover, in many countries there has been a tendency to toughen sanctions for these crimes.

The problem of ensuring information security on the Internet, including criminal law means, is nowadays one of the most acute problems in most developed countries of the world. Law enforcement agencies are facing a similar situation in Uzbekistan. Especially, when it comes to the use of computers, related systems and networks in industry and business. In this regard, first of all, it should be noted that in countries where computerization of public life is at a high level, both researchers and legislators believe that there is an independent type of crime, collectively called computer crime or high-tech crime ("computer crimes" or "high-tech crimes").

Crimes against information security on the Internet include all offences characterized by encroachment on the safe creation, storage, possession, use and distribution of computer information that is under criminal law protection, as well as crimes related to illegal traffic (content placement) on the Internet network.

Let's consider criminal legislation of the above mentioned countries on the issue of availability of legal regulation of crimes against the security of information in the global Internet:

1. Information crimes in the form of encroachments on the safe creation, storage, possession, use and distribution of computer information under criminal law protection are provided in all of the above mentioned countries of America, Europe and Asia, as well as CIS countries, where they are recognized as crimes in the sphere of computer information or information security.

At the same time, although there are certain differences in the understanding of such offenses by the legislator, it can be noted that in almost all criminal law norms, it is illegal to access (without a sanction) computer information and information technologies.
Thus, § 1030 of Title 18 of the United States Code governs liability for unauthorized access to or excess of authorized access to information from a US government department from any protected computer related to interstate or international commerce.

In the UK, the Computer Abuse Act of 1990 provides liability for willful unlawful access to a computer or computer information contained therein or programs for furtherly used for unlawful purposes.

In addition, it is worth noting the differences in the name of the subject of encroachment by the legislator. So, if the French Criminal Code refers to "illegal access to an automated data processing system ..." (Art. 3231), the Spanish Criminal Code refers to "using telecommunications without the consent of the owner" (Art. 256), the Dutch Criminal Code provides "unlawful intrusion (penetration) into a computer, computer system or computer network "(art. 138a), the Danish Criminal Code - "illegal access to information or programs intended for use in connection with electronic data processing"(§ 263), the Swedish Criminal Code - "illegal access to the records within the system of automatic data processing "(Art. 9c, Chapter 4), the Swiss Criminal Code - "unlawful penetration into the data processing system" (Art. 143).

It is also notable that the notions given in the Criminal Codes of the Asia-Pacific countries. For example, in the Philippines, the criminalization of acts in the field of information technology and security occurred after the adoption of the Computer Abuse Act in 2000. According to this law, criminal liability is provided for "intentional unauthorized access to a computer, computer network, computer system, server or database". It is separately referred to the responsibility for "unauthorized access to closed computers of state bodies or agencies ... that are used exclusively for government purposes or in the interests of the government."

Australian criminal law adheres to the establishment of a minimum list of unlawful acts that are criminalized in cases of using information technology. For example, Article 222 of the Criminal Code establishes criminal liability for unauthorized access to computer information, their modification, disruption of electronic communication facilities.

Some experience in legislative regulation of responsibility issues for committing crimes in the field of computer information has been accumulated by the Baltic republics. Article 271 of the Estonian Criminal Code defines the illegality of the use of computers, computer systems or computer networks, committed by eliminating their remedies, in Latvian Criminal Code Art. 241 claims for responsibility for unauthorized entry into an automated computer system that created the conditions for getting the information contained in the system, including "connected with overcoming the means of software protection of computer equipment or connecting to communication lines".
As for some countries of the CIS, the Criminal Code of the Russian Federation adopted in December 27, 1996, that included responsibility for committing crimes in this area for the first time, was introduced in Chapter IX "Crimes against public security and public order" in Chapter 28 "Crimes in the sphere of computer information". In this chapter, Art. 272-"Wrongful access to computer information" should be noted.

Norms on criminal liability for unlawful access to computer information, in the Criminal Code of the Azerbaijan Republic (Art. 271) and the Criminal Code of Georgia (Art. 284), the Republic of Turkmenistan (Art. 344), almost literally repeat the provisions of Article 272 of the Criminal Code of the Russian Federation. Also, Art. 361 of the Criminal Code of the Ukraine provides liability for "Illegal interference with the operation of electronic computers (computers), systems and computer networks", and Art. 349 of the Criminal Code of the Republic of Belarus - for unauthorized access to computer information.

One of the newest Criminal Codes adopted in the post-Soviet area are the Criminal Code of Kazakhstan (2014) and the Criminal Code of Kyrgyzstan (2017). At the same time, Art.205 of the Criminal Code of Kazakhstan provides liability for "unauthorized access to information, to an information system or telecommunications network", whereas Art.304 of the Criminal Code of Kyrgyzstan - for "unauthorized access to computer information."

In the Criminal Code of Uzbekistan, responsibility for such acts is provided in Article 2782 ("Illegal (unauthorized) access to computer information").

2. Information crimes related to illegal trafficking (content placement) of information on the Internet, according to the analysis of the Criminal Code of the reviewed countries, mean pornographic products as such content.

Thus, in the UK, according to the provisions of the Child Protection Act 1978 and the Sexual Offenses Act 1956, persons who make and distribute pornographic images of children under 16 years of age can be brought to criminal responsibility.

Such acts are also under criminal prohibition in the Criminal Code of the countries of continental Europe. In particular, the Criminal Code of France includes the production and distribution of child pornography through telecommunications networks (Art. 22723), the Criminal Code of the Netherlands - distribution of child pornography using computer technology (Art. 240b), the Criminal Code of Denmark - distribution of child pornography (§ 235), UK Sweden - the manufacture, sale and distribution of child pornography in another way (Art. 10a, 10b and 10c).

In Art. 125A of the Criminal Code of Australia also provides for the responsibility for distributing pornography and child pornography using computer technology.
It should be noted that in the post-Soviet space, the issues of responsibility for illegal content posting on the Internet, to some extent, can only be found in the Criminal Codes of Ukraine (Part 2 of Article 301 of the Criminal Code provides for a qualifying attribute in the form of production, sale and distribution of pornographic items programs), as well as Kazakhstan (art. 311 "Illegal distribution of pornographic materials or objects") and Kyrgyzstan (art. 168 "Involving a minor in porn business"), which, in general, regulates the rules on the prohibition of the distribution (manufacture) of pornographic products involving minors.

As for the placement of illegal content of other kinds, the Canadian Criminal Code, which criminalizes the intentional dissemination of meaningless, useless or unsuccessful computer data and programs (spam), is notable.

In the Criminal Code of Uzbekistan, responsibility for placing illegal content on the global Internet is provided for in paragraph "d" of part three of Article 2441. ("Production, storage, distribution or display of materials containing a threat to public safety and public order"), which refers to "the use of funds mass media or telecommunications networks, as well as the world information network Internet".

3. The next type of criminal acts against the security of information on the global Internet is violation of the security of personal data. Section 2701 of Title 18 of the United States Code specifically criminalizes breaching the confidentiality of email and voice mail on the server.

In the UK, a number of provisions of the Personal Data Act 1998 deal with the protection of this type of computer information, which recognize violations related to the unlawful disclosure of such data, including the use of computer technology, as crimes.

Similar acts are also provided in the Danish Criminal Code - illegal use of information relating to a person's private life (§ 264d), Spanish Criminal Code - disclosure and dissemination of secret information, including e-mail messages, information stored in electronic card files (Art. 197), The Swedish Criminal Code - violation of postal and telecommunications secrets (Article 8, Chapter 4), the use of technical means with the intention to violate telecommunications secrets (Article 9b, Chapter 4), the Swiss Criminal Code is illegal to obtain personal data (Article 179).

In addition, acts that violate the rights to personal secrets include acts in the form of unauthorized interception, interruption, tracking and recording of data using electromagnetic, acoustic, automatic or other devices (Article 107 of the Criminal Code of Canada, Article 22615 of the Criminal Code of France, and also part 2 of article 139a of the Criminal Code of the Netherlands).

Among the CIS countries, responsibility for illegal acts violating the rights to personal (private) secrecy can be found to some extent only in
the Criminal Codes of Kazakhstan ("Article 147. Violation of privacy and the laws of the Republic of Kazakhstan on personal data and their protection" and Article 148 "Illegal violation of the secrecy of correspondence, telephone conversations, postal, telegraphic or other communications") and Kyrgyzstan (Article 188 "Violation of the secrecy of correspondence"), some parts of which regulate the rules prohibiting committing of these acts through the use of information technology.

In the Criminal Code of Uzbekistan, responsibility for violations of the security of personal data is generally considered in the framework of article 1411 of the Criminal Code of the Republic of Uzbekistan (Violation of privacy).

4. The most dangerous type of informational crimes that we assigned to the second group of our classification is cyberterrorism. The term was proposed in the 1980s by Barry Collin, a senior researcher at the Institute of Security and Intelligence Institute, who used it in the context of the tendency of terrorism to pass from the physical to the virtual world, the growing intersection and coalescence of these worlds.

First of all, it should be emphasized that the Criminal Code of many countries do not yet keep pace with such latest risks, challenges and threats of cybercrime. In almost all countries, crimes of a terrorist nature committed in networks (the virtual world) and the information space remain outside the legal field, and criminals are prosecuted under articles for ordinary terrorism.

As one of the rare examples, we can mention the United Kingdom's Terrorism Act 2000, which states that unlawful entry into computers, their systems or networks, resulting in significant damage or use of the computer information obtained in this way for organizing mass violence, can be equated to acts of terror and, accordingly, entail increased responsibility, as well as Art. 4211 of the Criminal Code of France - "terrorist acts related to acts in the field of informatics".

As an example of cyber-terrorism with the use of modern information technology can serve a murder committed in 1998 in a US clinic, where a particularly important and seriously wounded witness was protected by the FBI. Having received unauthorized access to the local network of the clinic via the Internet and overcoming a number of gateways and protective barriers, the killer hacker reconfigured the pacemaker, causing the patient to die.

Currently, based on the disposition of the Criminal Code articles on terrorism, it can be assumed that cyber-terrorism should be understood as a deliberate, politically motivated attack on information processed by a computer, computer system and networks that pose a danger to human life or health or other serious consequences, if such actions were committed with the aim of violating public security, intimidating the population, provoking a military conflict.
The Criminal Code of Uzbekistan does not provide responsibility for cyberterrorism.

Analysis of the legislation of foreign countries on criminal liability for informational crimes shows significant differences in the range of acts recognized as criminal in this area, and the degree of protection of legal relations in the field of information technology and security, as well as other legal relations, which in certain situations have a significant impact on the information, as well as information and communication technologies.

As the main conclusion that can be made as a result of the analysis of the examined notions about information crimes in the Criminal Codes of foreign countries, it should be noted that the majority of Criminal Codes provide responsibility for a wider range of information offenses, compared to the Criminal Code of the Republic of Uzbekistan.

Comparative legal analysis of the laws of foreign countries and the Republic of Uzbekistan revealed several problematic points, which we noted above. The potential of researchers and practitioners and the efforts they are making to improve national criminal law and criminal law science as a whole, in our opinion, is not enough and requires more careful study of this problem in the context of large-scale reforms in the judiciary and public policy areas, and further integration of the country into the global information space.

Considering the above mentioned, we can conclude that one of the advantageous sides of our Criminal Code, compared to the criminal legislation of foreign countries, is the presence of a number of articles that are not included in the codes of the vast majority of foreign countries (misappropriation and embezzlement using computer means, discrediting competitor, etc.). At the same time, it should be noted that the number of crimes in the field of information technology and security that are absent in the Criminal Code of Uzbekistan is much more.

Given the growth of globalization and the informatization of society, the expansion of information crime, we consider it necessary to adopt a single United Nations convention on the fight against cybercrime and ensure global information security. This document provides a uniform approach to the protection of information security in foreign countries.

References:

1. https://www.lex.uz/
2. https://www.eurlex.eu/