JMEE

Journal of Marketing and Emerging Economics

| e-ISSN: 2792-4009 | www.openaccessjournals.eu | Volume: 3 Issue: 5

The Role and Importance of Cybersecurity in the Development of the Country's Economy

Otakuzieva Zukhra Maratdaevna
Associate Professor, Candidate of Economic Sciences, Tashkent University information technologies named after Muhammad al-Khwarizmi
zukhra.otakuzieva@rambler.ru

Isroilov Javokhir Abdugaffor ugli, Jurabekov Boburkhon Dilshod ugli, Kholikulov Jasur Mansur ugli, Muzaffar Sakhadinov Sodikovich
3rd year student of Tashkent University information technologies named after Muhammad al-Khwarizmi

Abstract

We live in the era of the information society, when computers and telecommunications systems cover all spheres of human and state life. But humanity, having put telecommunications and global computer networks at its service, did not foresee what opportunities for abuse these technologies create. Today, not only people, but entire states can become victims of criminals operating in the virtual space. At the same time, the security of thousands of users may be dependent on several criminals. The number of crimes committed in cyberspace is growing in proportion to the number of users of computer networks, and, according to Interpol, the growth rate of crime, for example, on the global Internet, is the fastest on the planet.

Keywords: *computer crime, IT technologies, cybercrime, Internet crime, cyberattack.*

INTRODUCTION

The modern technotronic society is completely dependent on information, communication, aerospace, energy, transport, industrial, biological, industrial, scientific and other high technologies. However, the majority of people, not possessing special knowledge, skills and abilities, have little idea of the principles and methods of their work.

Therefore, the technical illiteracy of the population, the increase in the volume of information, the complexity and diversity of modern knowledge, the psychology of consuming goods, rather than creation, creativity and knowledge, the lack of an individual and social culture of technological security, and other factors of a scientific and technical nature have led to the emergence of computer crime and its subsequent transformation. into uncontrolled technotronic crime.

According to Kaspersky Lab experts, in the event of a successful attack by cybercriminals, large companies lose about $252,000, and medium and small businesses an average of $9,840 due to forced downtime, lost profits, and expenses for additional specialist services. Large companies spend an additional $26,495 to eliminate the consequences of an incident and preventive measures, while small companies spend about $3,785 [5].

JMEE
Journal of Marketing and Emerging Economics
| e-ISSN: 2792-4009 | www.openaccessjournals.eu | Volume: 3 Issue: 5

LITERATURE ANALYSIS AND METHODS

A significant contribution to the study of the problems of combating computer crime and the fight against computer crime was made by foreign scientists: D. Aikov, V. A. Golubev, I. V. Gren, P. Johnston, A. Kemraj, M. Kratz, D. Lance, K Seiger, B. Kh. Toleubekova, F. Veits, U. Fonstorch, V.V. Hiluta and others.

It should be noted that the dissertations of M. S. Gadzhiev, D. V. Dobrovolsky, A. A. Zhmykhov, T. M. Lopatina were directly devoted to the criminal law and criminological aspects of combating computer crime in Russia and foreign countries.

These works laid the scientific foundations for criminal law and criminological counteraction to computer crime.

In addition, the theoretical basis of the study was formed by scientific publications from public Internet resources devoted to the problems of combating computer crime.

Computer crime as an object of scientific research requires further study and careful analysis, including the development of an effective system of criminal law and criminological measures to counter this negative social phenomenon.

The methodological basis of the study was the basic provisions of the dialectical method of cognition, within which a system of general scientific methods (logical, historical, system-structural), private scientific methods (historical-legal, formal-legal, comparative-legal, legal modeling) and special scientific methods of cognition were used. (statistical, specific sociological, method of expert assessments, content analysis, etc.).

RESULTS

Computer crime as a complex social and state-legal concept should be considered in the narrow and broad senses.

Computer crime in a broad sense is an illegal and negative social phenomenon resulting from the use by people of computer and other IT technologies for personal, mercenary and other criminal purposes, which leads to socially dangerous consequences.

In turn, computer crime in the narrow sense is a set of crimes committed by persons in a certain territory over a certain period of time, where the main object of criminal encroachment is specific social relations in the field of the safe functioning of computer information, means of searching, collecting, storing, processing, providing , distribution, protection of computer information, information and communication devices, and computer information, computer networks, information and telecommunication networks; the means of creating, storing, processing, transmitting computer information are not only the subject of a criminal attack, but are also used as a means and (or) instrument for committing a crime.

Computer crime in its "narrow sense" is wider in scope and content of such concepts as "cybercrime", "Internet crime", "crime in the field of computer information", "crime in the field of information technology", including them in itself, from the point of view of objective and subjective signs of a crime (the object and subject of a criminal attack; type of act; method, means, instruments of crime; general and special subjects of a crime, etc.).

Based on the foregoing, we can distinguish the following most significant features that characterize the essence of computer crime.

JMEE
Journal of Marketing and Emerging Economics
| e-ISSN: 2792-4009 | www.openaccessjournals.eu | Volume: 3 Issue: 5

1. Computer crime is a kind of crime that exists on a par with economic, violent, corruption, environmental and other types of crime.

2. Computer crime is closely interconnected with other types of crime, since crimes in the field of computer information often act as a way to commit other criminal acts (theft, extortion, illegal receipt and disclosure of information constituting commercial, tax or banking secrets; treason, espionage, etc.).

3. Computer crime is of a high-tech nature, which is caused by the use of IT technologies, information and telecommunication networks, computer devices, computer information carriers, and the like, which act as tools and means for committing computer crimes.

4. Computer crime has a high degree of latency, which reaches from several tens to several thousand percent for various types of criminal acts, which is due to various objective factors (the reluctance of victims of computer crimes to contact law enforcement agencies, the invisibility of computer crimes for the majority of the population due to their commission and course in "virtual environment", the difficulty of detecting computer crimes in the absence of the required number of specialists in law enforcement structures, and so on).

5. Computer crime is of a highly organized nature and is closely related to organized crime, since a large number of computer crimes are committed by organized criminal groups (DDoS attacks, banking, phishing, botnets, and others).

6. Computer crime is a professional crime, as the perpetrators of computer crimes: have a criminal specialization, without committing other types of criminal acts; receive criminal income (profit) as a result of criminal activity; have the necessary knowledge, skills in the field of IT-technologies to commit a crime; adhere to certain rules, "laws", concepts and terminology that allow them to communicate, share experiences and find like-minded people.

7. Computer crime is characterized by cross-border nature, since "cyberspace" exists outside state borders, and, being generally accessible, allows a criminal from the territory of one state to commit crimes against persons located in another state.

8. Computer crime is transnational. This is due to the fact that computer criminals, by virtue of their belonging to the computer "underground", in order to receive colossal criminal proceeds, facilitate the commission of criminal acts on the territory of two or more states, are forced, regardless of nationality, to unite in international criminal groups.

DISCUSSIONS

Given that the above acts are committed using computer, information, communication and other high technologies, they, in turn, are technotronic crimes, which in their totality form technotronic crime.

In turn, experts in the field of cybersecurity have their own point of view on the structure of computer crime or, as they say in the expert community, on the "cybercrime market".

In particular, experts of the international company Group-IB, which specializes in the prevention and investigation of cybercrime, believe [6] that the main criminal acts that form the cybercrime market are:

1. Fraud in Internet banking systems;

2. Phishing[1];

3. Theft of electronic money on cryptocurrency exchanges;

4. Cashing services for other illegal income;

5. Spam[2] (medicines and various counterfeit products, fake software, services, education, tourism, etc.);

6. Sale of traffic;

7. Sale of exploits;

8. Sale of downloads;

9. Anonymization[3];

10. DDoS attacks[4];

11. Attacks on critical information infrastructure objects (corporate networks of industrial, financial and energy companies).

In turn, the specialists of the Center for Global Research and Threat Analysis of Kaspersky Lab (GReAT), who analyze the annual state of cybercrime in many countries of the world, classify computer crimes (in professional slang as "computer threats") that constitute cybercrime:

1. Targeted cyberattacks;

2. Cyber espionage;

3. Hacktivism;

4. Theft of confidential data;

5. Cyber extortion;

6. Cyber attacks for hire (cyber mercenarism);

7. Use of malicious software for mobile devices;

8. Spear phishing;

9. Violation of privacy;

10. Use of exploits for software vulnerabilities;

[1]Phishing (English phishing, from fishing - fishing, fishing) - a type of Internet fraud, the purpose of which is to gain access to confidential user data - logins and passwords, which is achieved by conducting mass mailings of emails on behalf of popular online stores, banks , operators of information and telecommunication services.

[2]Spam (eng. Spam, abbr. SPiced hAM (spicy ham)) is an illegal distribution of commercial, charitable and other advertising, electronic messages to users of computer devices and information and communication networks, without their notification and consent.

[3]Anonymization is the process of deleting personal data (from electronic documents, databases, information and communication networks, etc.) in order to hide the source of information and the possibility of identifying the user (owner) of computer information.

[4]DoS - attack (from the English. Denial of Service - denial of service) - an attack on a computer system with the aim of blocking it or making it difficult for users to access the provided system resources (servers); A DDoS attack (from the English Distributed Denial of Service, a distributed denial of service attack) is a type of DoS - an attack made from a large number of computers to block protected computer systems (for example, servers of government authorities, banks, large companies, electronic media, etc.).

11. Cyber extortion;

12. Creation and use of botnets [7].

CONCLUSION

Since the beginning of 2019 alone, almost 8 million information security incidents have been identified, some of which were critical. In 2021, about 1.3 million cyber attacks on sites in the “uz” segment were recorded. In this regard, the country has adopted a comprehensive program to ensure the protection and security of digital data, within which over 70 various regulatory documents have been approved. All state institutions have begun to carry out electronic data exchange through secure data networks and much more.

The stability of the banking system is the key to further modernization of the country's economy, and in this regard, the prevention of cyber threats is a matter of national security. We are actively working to ensure the cybersecurity of the country's financial sector.

The measures taken have allowed us to rise in the International Telecommunication Union's global cybersecurity index by 40 positions and take 52nd place out of 175 countries.

It is planned to create a cybercrime prevention system. This is stated in the draft Roadmap for the implementation of the Development Strategy for 2022-2026 in 2022.

It is noted that the Cybersecurity Strategy of the Republic of Uzbekistan for 2023-2026 will be developed.

At the same time, a set of tasks and main directions for the cybersecurity of the Internet space in the "UZ" domain zone, as well as the protection of e-government, energy, the digital economy and other areas related to important information infrastructure, were determined.

It is also planned to revise the criminal liability for cybercrime.

The system for monitoring cyber attacks and threats in the information space will continue to improve.

This includes expanding the technical infrastructure of the Unified Cybersecurity Network, further accelerating the activities of the “IT Park of Innovations in Cybernetics”, as well as conducting cybersecurity training for young people on the basis of digital technology training centers in the regions, as well as the annual holding of republican competitions among students to detect cyber attacks.

REFERENCES

1. Actual problems of information law: textbook / Edited by I. L. Bachilo, M. A. Lapina. - Moscow: Justice, 2016. - 532 p.
2. Begishev, I. R. Crimes in the sphere of circulation of digital information: monograph / I. R. Begishev, I. I. Bikeev. - Kazan: Publishing House "Knowledge" of the Kazan Innovative University, 2020. - 300 p.
3. Cybercrime: criminological, criminal law, criminal procedure and forensic analysis: monograph / scientific editor I. G. Smirnova; executive editors O. A. Egereva, E. M. Yakimova. - Moscow: Yurlitinform, 2016. - 312 p.
4. Counteraction to cybercrime in the aspect of ensuring national security: monograph / Agapov P.V., Borisov S.V., Vagurin D.V., Korenyuk A.L., Merkuryev V.V., Pobegailo A.E., A.V. I.

Khaliullin. - Moscow: Academy of the Prosecutor General's Office of the Russian Federation, 2014. - 136 p. Web sites

5. Is the Internet so scary. Gazeta.Ru talks about the real danger of cyber threats. URL: http://www.gazeta.ru/tech/2014/11/05_a_6289085.shtml (date of access: 08/10/2021).
6. Hi-Tech Crime Trends 2020/2021. Cyber threats, trends and forecasts. URL: https://www.groupib.ru/blog/trends20_21 (date of access: 08/10/2021).
7. Kaspersky Security Bulletin: review 2017. URL: https://securelist.ru/ksb-review-of-the-year2017/88142/ (date of access: 08/10/2021).