DOI 10.29042/2019-5639-5642

Helix Vol. 9 (5): 5639- 5642

Information Infrastructure of Safe Computer Attack

[1]Ildar R. Begishev, [2]Zarina I. Khisamova, [3]Guzel I. Mazitova

[1]Ph. D. in Law, Honored Lawyer of the Republic of Tatarstan, Senior Researcher, Kazan Innovative University named after V. G. Timiryasov (IEML)

[2]Ph. D. in Law, Head, Department of Planning and Coordination of Research Activities, Research Department, Krasnodar University of the Ministry of Internal Affairs of the Russian Federation

[3]Postgraduate, Kazan Federal University, Faculty of Law, Criminal law Department

Email: begishev@mail.ru, alise89@inbox.ru, gyzelka.solnce@gmail.com

Received: 20th August 2019, Accepted: 30th September 2019, Published: 31st October 2019

Abstract

The article substantiates the need for introducing into the international scientific circulation the author's definition of the legal and psychological phenomenon of "safe computer attack", which is proposed to understand the state of the subjects of information legal relations that are aware of the danger of violation and the importance of ensuring the security of information infrastructure, but that do not ensure it for various reasons, including when carrying out computer attacks against it.

The study determined that it is typical for such entities to reduce or completely ignore the established requirements for the protection of information and information security policy for various reasons, in addition to understanding the mechanisms for ensuring the security of information infrastructure in the context of existence of different threats to their cyber security.

Such causes of the phenomenon include:

1) Neglect and negligence;

2) Increased financial costs for ensuring cyber security of the information infrastructure;

3) Mismatch of the information security systems of computer systems and networks to the level of threats to their cyber security;

4) Low level of cyber security culture;

5) Lack of qualified information security specialists, including a specially-oriented profile.

In addition, it was found that the loss of information due, for example, to unauthorized access to it or the operation of malicious computer program, is largely predetermined by the lack of knowledge of the basic principles for ensuring cyber security among the employees of organizations.

Keywords

Information Infrastructure, Computer Attack, Computer Information, Digital Economy, Security, Information Security, Information Protection.

Introduction

Modern digital technologies have significantly changed the processes of storage, processing and transmission of information. The process of "digitalization" of society has embraced all spheres of activity of the state and human. This largely predetermined the further development of information legal relations and their legal regulation.

In connection with the digital development of the world community, knowledge of ways to qualitatively protect the information technologies in everyday practice is becoming increasingly relevant. Illustrative examples, illustrating the need to protect information and ensure cyber security, are the increasing reports of computer "hacks" of enterprises, the growth of computer piracy, the spread of computer viruses, both in Russia and in the world.

Materials and Methods

The materials for the work were the provisions of the Russian criminal and information legislation, as well as regulatory legal acts in the field of cyber security.

The reliability of results obtained is ensured based on the analysis of significant and necessary array of legislative norms, statistical data, as well as the use of modern research methods of legal institutions: historical and legal, logical, formal-legal, comparative law, system-structural and other methods of scientific knowledge.

Results and Discussion

According to the analytical center of the Russian company InfoWatch, the largest Russian manufacturer of solutions to protect organizations from internal and external threats, as well as from information attacks, 2263 cases of leaks of confidential information from organizations were recorded in 2018: 77.2% concerned commercial organizations, and 22.8% - government organizations. By the information type, all leaks are divided into: personal data - 69.5%, payment information - 16.9%, state secret - 5.4%, commercial secret - 8.1% of the total number of recorded leaks. Data on the above leaks of confidential information includes all incidents in all foreign countries, information about which has been published in the media, as well as in blogs, web forums and other network resources. During this period, leaks were

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

widely reported in Acer, Amazon, Apple, Blizzard, Boeing, Facebook, HP, Huawei, and the user data was compromised in such services as Edmodo, Google Play, HipChat, Instagram, Snapchat, WhatsApp [1].

In our opinion, the generally accepted term “computer attack” (computer invasion), developed by the specialists of the State Scientific and Research Institute for Problems of Technical Protection of Information of the Federal Service for Technology and Export Control and widely used in practice, does not give an accurate definition of illegal processes. The national standard of the Russian Federation, GOST R 51275-2006, approved on the basis of proposals given by the experts of the FSTEC of Russia, discloses the concept of “computer attack” as a targeted unauthorized impact on the information, resource of the information system or as gaining unauthorized access to them using software or hardware [2].

In addition, definition of the concept under consideration is given in the federal law governing relations in the field of ensuring cyber security of critical information infrastructure when conducting computer attacks against it.

In it, a computer attack is defined as the targeted impact of software and (or) hardware on critical information infrastructure objects, telecommunication networks used to organize the interaction of such objects, in order to disrupt and (or) stop their functioning and (or) create cyber security threat to the information processed by such objects [3].

In his study, I. V. Kotenko notes that an attack on a computer system refers to any impact of an attacker on a computer system with an aim of violating cyber security, which consists in finding and using a particular vulnerability [4].

A close position is also occupied by A.E. Borshevnikov, who defines a network attack as an action, the purpose of which is to seize control (increase of rights) over a remote/local computer system, or to destabilize it, or to deny service, as well as to obtain user data using this remote/local computer system [5].

World experience in the implementation of computer attacks shows that 80% of them are committed by the organization’s own employees (sometimes former) or with their direct participation. It is such internal cyber security violators with the powers of a full-time user or system administrator that pose the greatest danger in modern world reality [6].

Thus, we can conclude that, within the meaning of the definitions considered, a computer attack should be understood as deliberate actions in relation to the information infrastructure, entailing violation of the reliability, integrity and confidentiality of computer information.

As for the actual activities of the subjects of information legal relations, the peculiarity of their condition in the conditions of continuous information protection is extremely important both for the practice of applying information and criminal legislation, and for legal science.

The most significant contribution to the digital transformation of the Russian economy is made by the implementation of the national program “Digital Economy of the Russian Federation”, adopted in accordance with the Decree of the President of the Russian Federation No. 204 dated May 7, 2018 “On National Goals and Strategic Tasks of the Development of the Russian Federation for the Period until 2024” [7] and the protocol No. 16 dated December 24, 2018, approved by the Presidium of the Presidential Council for Strategic Development and National Projects of the Russian Federation. It includes 6 priority directions:

- Normative regulation of the digital environment;
- Information infrastructure;
- Personnel for the digital economy;
- Information security;
- Digital technologies;
- Digital government.

Particular attention in the Russian national program is paid to the security of information infrastructure, and the introduction of digital technologies, in particular, new intelligent technologies, since the formation of legal basis for the use of artificial intelligence has begun, which requires taking actions and decisions to prevent possible negative manifestations of its use and state response to them [8].

When studying the types of cybercrimes, in particular, criminal attacks on critical information infrastructure [9, 10, 11, 12, 13, 14, 15, 16, 17], we discovered a rather interesting phenomenon related to the activities of subjects of the information legal relations on cyber security of their information infrastructures.

Almost every third employee knows that the information and telecommunication network “Internet” contains a huge number of threats (malicious computer programs, fraudulent software, etc.), but does not make any efforts to protect the organization’s information infrastructure from threats, hoping for a chance. Although the acquisition and installation of antivirus software or preventative protection means for the confidential information (including free distribution) would have a significant impact on the cyber security level.

Each employee's compliance with the cyber security requirements is individual in nature and is made dependent on its individual characteristics. It is mediated by such a quality of personality, which expresses a stable subjective attitude of employees to the organization’s cyber security policy, to the rules of information protection, to their official duties. The discipline and cyber security culture is a key factor in this case.

Analysis of more than 90 sentences handed down by Russian federal courts of general jurisdiction in the criminal cases on crimes in the field of computer information (Article 272 “Illegal access to computer information”, 273 “Creation, use and distribution of malicious computer programs”, 274 "Violation of the operation rules for the means if storage, processing or transmission of computer information and telecommunication networks" of the Criminal Code of the

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

Russian Federation [18]), and more than 120 decisions made by judicial sections of the world judges in the cases on administrative offenses in the field of communications and information (Article 13.11 “Violation of the legislation of the Russian Federation in the field of personal data”, 13.12 “Violation of the rules of information protection”, 13.13 “Illegal activities in the field of information protection”, 13.14 “Disclosure of information with limited access ”of the Code of Administrative Offenses of the Russian Federation [19]) for the period from 2014 to 2018 and posted publicly on the websites of the State Automated System of the Russian Federation "Pravosudie" and the Reference and Legal System of Judicial Decisions "RosPravosudie" in more than 50 subjects of the Russian Federation, led to the conclusion that the behavior of the subjects of information relations relates to low psychological readiness for cyber security.

Conclusions

The study determined that it is typical for such entities to reduce or completely ignore the established requirements for the protection of information and information security policy for various reasons, in addition to understanding the mechanisms for ensuring the security of information infrastructure in the context of existence of different threats to their cyber security.

These reasons of the phenomenon under consideration include:

1) Neglect and negligence (some employees consider the cyber security threats of the information infrastructure far-fetched, not relevant to the realities of the time; some owners of the information infrastructure are not interested in ensuring their security in view of the absence of a positive economic effect from this);

2) Increased financial costs for ensuring cyber security of the information infrastructure (high cost of information protection systems, disinterest in the development of the organization's cyber security systems due to the lack of financial benefits, etc.);

3) Mismatch of the information security systems of computer systems and networks to the level of threats to their cyber security (mismatch of information security tools to real and potential threats to the information security of the organization, lack of cyber security audit system, increase in the number of attacks on computer systems and networks, complexity of operating the information security tools, etc.);

4) Low level of cyber security culture (low awareness of the leaders and specialists of organizations in matters of ensuring cyber security, ignoring the requirements of the organization's cyber security policy by the employees, non-compliance by the employees with the requirements of federal legislation in the field of information protection, etc.);

5) Lack of qualified information security specialists, including a specially-oriented profile (specialists in organizing and implementing security control, specialists in operational monitoring, detection of intrusion and network attacks, specialists in providing protection against the effects of malware, etc.).

In addition, it was found that the loss of information due, for example, to unauthorized access to it or the operation of malicious computer program, is largely predetermined by the lack of knowledge of the basic principles for ensuring cyber security among the employees of organizations.

Summary

Thus, we suggest introducing into the world legal science the term “phenomenon of safe computer attack” as a legal and psychological phenomenon and define it as the state of the subjects of information legal relations that are aware of the danger of violation and the importance of ensuring the security of information infrastructure, but that do not ensure it for various reasons, including when carrying out computer attacks against it.

Thus, among the main personality factors that affect the “phenomenon of safe computer attack”, one should single out the degree of responsibility and duties of the employees within provision of the information security, expressed primarily in maintaining the confidentiality of computer information and protecting its integrity and reliability.

It is thought that this term can be used as an evaluation indicator in the system of ensuring cyber security of the subjects of information legal relations.

Acknowledgements

The work is performed according to the Russian Government Program of Competitive Growth of Kazan Federal University.

The authors are sincerely grateful to the head of the Department of Criminal Law of the Faculty of Law of the Kazan Federal University for help in the preparation of this article.

References

1. Analytical report “Global investigation of leaks of confidential information in 2018” // Analytical center InfoWatch. [Electronic resource]. – URL: https://www.infowatch.ru/sites/default/files/report/analytics/russ/InfoWatch_Global_Report_2018_year.pdf?rel=1

2. GOST R 51275-2006. "Protection of information. Object of informatization. Factors affecting information. General provisions". M. : Standartinform, 2007. Approved and enforced by order of the Federal Agency for Technical Regulation and Metrology No. 374-st dated December 27, 2006 “On Approval of the National Standard”. The text of the order has not been officially published.

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

3. Federal Law No. 187-FZ dated July 26, 2017 “On the Safety of Critical Information Infrastructure of the Russian Federation” // Official Gazatte of the Russian Federation. – 2017. – No. 31 (part I). – Art. 4736.
4. Kotenko I. B. Taxonomy of attacks on computer systems // Works of SPIIRAS. – 2003. – V. 2. – No. 1. – P. 196.
5. Borshevnikov A.E. Network attacks. Types. Ways of struggle // Modern Trends in Technical Sciences: Materials of the International Scientific Conference (Ufa, October 2011). - Ufa: Leto, 2011. – P. 8.
6. Malyuk A.A. Organizational and methodological problems of detecting attacks on objects of the information infrastructure of the credit and financial sphere // Cyber Security Issues. – 2016. – No. 5. – P. 10.
7. Decree of the President of the Russian Federation No. 204 dated May 7, 2018 “On National Goals and Strategic Tasks of the Development of the Russian Federation for the Period until 2024” // Official Gazette of the Russian Federation. – 2018. – No. 20. – Art. 2817.
8. Begishev I. R. Criminological risks of using artificial intelligence / I. R. Begishev, Z. I. Khisamova // All-Russian Criminological Journal. – 2018. – V. 12, No. 6. – P. 767-775.
9. Coman I. M. Cross-Border Cyber-Attacks and Critical Infrastructure Protection / I. M. Coman // International Journal of Information Security and Cybercrime. – 2017. – № 2 (6). – P. 47–52.
10. Venkatachary S. K., Prasad J., Samikannu R. Economic Impacts of Cyber Security in Energy Sector: A Review / S. K. Venkatachary, J. Prasad, R. Samikannu // International Journal of Energy Economics and Policy. – 2017. – № 7 (5). – P. 250–262.
11. Bajramovic E. Cyber security in private industry critical infrastructure / E. Bajramovic // International Journal of Economics and Law. – 2015. – № 13 (5). – P. 9–15.
12. Begishev I. R. Problems of combating criminal attacks on information systems of critical and potentially dangerous objects // Information Security of the Regions. – 2010. – No. 1. – P. 9-13.
13. Hathaway O. A., Crootof R., Levitz P., Nix H. The Law of Cyber-Attack / O. A. Hathaway, R. Crootof, P. Levitz, H. Nix // California Law Review. – 2012. – № 100. – P. 817–886.
14. Shackelford S. J., Sulmeyer M., Craig Deckard A. N., Buchanan B., Micic B. From Russia with Love: Understanding the Russian Cyber Threat to U.S. Critical Infrastructure and What to Do about It / S. J. Shackelford, M. Sulmeyer, A. N. Craig Deckard, B. Buchanan, B. Micic // Nebraska Law Review. – 2017. – № 96. – P. 320–338.
15. Albrecht D. Chinese Cyber security Law Compared to EUNIS-Directive and German IT-Security Act. When cyber security not only protects interests of the masses but ultimately also safeguards national sovereignty / D. Albrecht // Recherchieren unter juris (Das Rechtsportal). – 2018. – P. 1–5.
16. Orji U. J. Towards the Regional Harmonization of E-Commerce Regulation in Africa A Comparative Analysis of the African Union’s E-Commerce Regime / U. J. Orji // Recherchieren unter juris (Das Rechtsportal). – 2018. – P. 12–22.
17. The ITU publication Understanding cybercrime: phenomena, challenges and legal response has been prepared by Prof. Dr. Marco Gercke and is a new edition of a report previously entitled Understanding Cybercrime: A Guide for Developing Countries. The author wishes to thank the Infrastructure Enabling Environment and E-Application Department, ITU Telecommunication Development Bureau. – URL: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/legislation.aspx
18. The Criminal Code of the Russian Federation No. 63-FZ dated June 13, 1996 (as amended by the Federal Law No. 35-FZ dated February 19, 2018) // Official Gazette of the Russian Federation. – 1996. – No. 25. – Art. 2954.
19. The Code of Administrative Offenses of the Russian Federation No. 195-FZ dated December 30, 2001 // Official Gazatte of the Russian Federation. – 2002. – No. 1 (part I). – Art. 1.

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495