Periódico do Núcleo de Estudos e Pesquisas sobre Gênero e Direito
Centro de Ciências Jurídicas - Universidade Federal da Paraíba
V. 8 - Nº 06 - Ano 2019 – Special Edition
ISSN | 2179-7137 | http://periodicos.ufpb.br/ojs2/index.php/ged/index

CRIMINAL LEGAL ENSURING OF SECURITY OF CRITICAL INFORMATION INFRASTRUCTURE OF THE RUSSIAN FEDERATION

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

Abstract: The article considers the problems associated with the development of new state approaches to ensure the security of critical information infrastructure (hereinafter - the CII) in the context of the existence of threats to their information security, including computer attacks in its regard. We analyzed the main provisions of the Federal Law No. 187-FZ dated July 26, 2017 "On the Safety of the CII of the Russian Federation".We disclosed the content and essence of the concept of "security of the CII". It is justified that the security of the CII shall be based on the principles and methodology of ensuring national security. We have developed proposals to classify part of the subjects of economic activity as the CII subjects, as well as offered some additional mechanisms to increase the security of the CII. We proposed to develop and implement: the federal state standard of higher education in the direction of "safety of the CII"; retraining and advanced training courses in the direction of "safety of the CII"; a mechanism for improving the qualifications of officials of the CII subjects on various issues of ensuring its security; security insurance mechanism for the CCI; a mechanism for organizing international, all-Russian, regional and sectoral cyber orders at the CII objects. It has been established that the security of the CII directly depends on the

[1] Ph. D. in Law, Honored Lawyer of the Republic of Tatarstan, Senior Researcher, Kazan Innovative University named after V. G. Timiryasov (IEML), e-mail: begishev@mail.ru.
[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, e-mail: alise89@inbox.ru.
[3] Postgraduate, Kazan Federal University, Faculty of Law, Criminal law Department, e-mail: gyzelka.solnce@gmail.com.

correctness of decision-making in countering computer attacks, the speed and effectiveness of the actions of their entities. It is proved that the criminal law norm on liability for unlawful influence on the CII of the Russian Federation shall be changed.

Keywords: attack, security, information, information infrastructure, critical information infrastructure, government system, computer attack, computer information, security, information security, information protection, crime in the field of computer information, computer crime, digital economy, cybercrimes, cybercrime, cybersecurity, crimes.

Introduction

With the growing new challenges and threats in the information sphere, ensuring the security of the CII is becoming a priority state task, including its criminal law provision. The stable functioning of the CII has a significant impact on the socio-economic development of Russia in the digital economy, including the security of information infrastructure for citizens, representatives of business and the state in the digital space.

Attackers are constantly improving the technology of computer attacks on the CII. A vivid example is the actions of malicious computer ransomware WannaCry and Petya/Petrwrap/NotPetya/exPetr, which used vulnerabilities in user software for a computer attack.

The problem of securing the CII has long been of interest to many scientists. Despite the small number of scientific papers on the topic under discussion, a rather extensive methodological base has been developed. At the same time, there are many unsolved problems in the analysis of the security problem of the CII of Russia.

Materials and methods

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

The reliability of results obtained is ensured based on the analysis of significant and necessary array of legislative norms, statistical data, as well

Periódico do Núcleo de Estudos e Pesquisas sobre Gênero e Direito
Centro de Ciências Jurídicas - Universidade Federal da Paraíba
V. 8 - Nº 06 - Ano 2019 – Special Edition
ISSN | 2179-7137 | http://periodicos.ufpb.br/ojs2/index.php/ged/index

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

The study of genesis of the stated question requires, first of all, understanding of the concept of "security".

In meaning, the term "security" (from Latin securitas; English safety, security; French securite) means the absence of danger, that is, the state in which danger does not threaten, there is protection against it.

In the broad sense of the word, the term "security" refers to a situation in which the probability of causing harm to protection object and its possible size, in the opinion of the subject evaluating the situation, is less than a certain subjectively established limit [1].

Therefore, in its general form, security means the state of security of an individual, society, state from internal and external threats or dangers.

This understanding is the basis of the definition of national security of the Russian Federation, as enshrined in the Strategy [2]. In turn, the national security of the Russian Federation substantially depends on ensuring information security [3].

The legislator defines the security of the CII of the Russian Federation as the state of protection of the CII, ensuring its stable functioning when conducting computer attacks in relation to it [4].

Obviously, the concept of "security of the CII" is a specific one in relation to the concept of "information security", which, in turn, is one of the security types and is included in the concept of "national security".

Therefore, the security of the CII shall be based on the principles and methodology of ensuring national security.

The CII Security Law prescribes that the CII subjects ensure the security of their information systems (hereinafter - the IS), information and telecommunication networks (hereinafter - the ITN) and automated control systems (hereinafter - the ACS).

Let us recall that Art. 2 of the Law [5] reflects the concepts of IS and ITN. In turn, the concept of ACS is reflected in Art. 2 of the Law [4].

It seems that the most serious consequence of computer incidents is a violation of the technological process at the enterprise. In turn, it can, for example, lead to damage to the manufactured product or to a decrease in the quality of customer service, as well as to a decrease in volumes or a temporary suspension of production. In addition, such incidents may entail a reduction in the value of the company's shares, reputational damage, penalties, which may also ultimately be the target of computer attack [6]. Therefore, we believe that the CII subjects need to build a coordinated system of their information security, and to fulfill the requirements for ensuring information security already within the system. In our opinion, such requirements are defined in the relevant acts [7].

The CII subjects include government agencies and Russian companies that own the IS, ITN and ACS, and that provide the interaction of these systems and networks [4].

Moreover, the CII subjects shall carry out their activities only in certain socio-economic areas of activity [4].

It is assumed that, for example, as a result of computer attacks on services for calculating and paying utility bills, monitoring the activities of managing and resource-supplying organizations, as well as condition of state accounting of the housing stock, the functioning of the state information system of housing and communal services [8], one of the most important socially significant information system of the state, may be disrupted.

In this regard, we should note that the legislator has yet to attribute a part of economic entities, which have not been reflected in the current legislation, to the CII subjects.

In our opinion, to successfully resolve this issue, the legislator needs to use the data of the All-Russian Classifier of Types of Economic Activities (OKVED 2) [9]. According to this classifier, it is advisable to correlate the type of economic activity with the alleged CII subject.

To better counter the computer attacks and ensure stable functioning of the CII objects in the face of computer incidents [10], GosSOPKA [11] appeared in the country.

The list of such requirements is determined by the relevant Order of the

Periódico do Núcleo de Estudos e Pesquisas sobre Gênero e Direito
Centro de Ciências Jurídicas - Universidade Federal da Paraíba
V. 8 - Nº 06 - Ano 2019 – Special Edition
ISSN | 2179-7137 | http://periodicos.ufpb.br/ojs2/index.php/ged/index

FSTEC (Federal Service for Technology and Export Control) of Russia [12].

The legislator credits the CII objects that are endowed with a category of significance [4] and included in the relevant register [13] with the significant CII objects.

The resolution [14] established that the categorization will be carried out by a specially created commission of the subject on the basis of criteria for the significance of the CII objects. These indicators include socio-economic and the socio-political significance of the CII object.

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" [15] 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 [15].

Particular attention in the Russian national program is paid to the security of the CII, 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 [16].

When studying social relations evolving over the criminal law regulation of unlawful influence on the CII of the Russian Federation and some foreign countries [17, 18, 19, 20, 21, 22, 23], we established that the norms of foreign and Russian legislation providing for liability for encroachments on the CII objects are mostly blanket in nature.

Edition of Art. 274.1 of the Criminal Code of the Russian Federation [24] (hereinafter - the CC RF) is a structure consisting of three rules on liability for crimes in the field of computer information: Art. 272, 273 and 274 of the CC RF.

Within the meaning of Art. 274.1 of the CC RF, all these acts shall be directed against the CII objects. Thus, the analyzed criminal law norm competes immediately with three articles (Art. 272, 273 and 274 of the CC RF) and is special in relation to them. In a sense, the construction of Art. 274.1 of the CC RF contradicts the prevailing domestic traditions of criminalization and use of legal techniques in describing the criminal law norms. Following them, it would be preferable to implement the establishment of stricter criminal liability for attacks on the objects of critical information infrastructure by highlighting the relevant qualifying and especially qualifying features in Art. Art. 272, 273 and 274 of the CC RF [25]. We agree with the opinion of scientists.

We believe that the penal law on liability for unlawful influence on the CII of the Russian Federation requires a change.

Conclusions

The above analysis shows that the global digital space is the target of well-organized computer attacks. The methods and tools used to prepare them are constantly being improved. Such computer attacks can be directed against various CII objects of foreign states. Effective counteraction to computer attacks is possible only within the framework of the joint efforts of all interested countries, primarily national authorized bodies in the field of detection and prevention of computer attacks, and the unification of international legislation in the field of security of the CII.

Summary

Given all of the above, we offer to develop and implement:

- FSS HE in the direction of “safety of the CII”;

- retraining and advanced training courses in the direction of "safety of the CII";

- a mechanism for improving the qualifications of officials of the CII subjects on various issues of ensuring its security;

- security insurance mechanism for the CCI;

- a mechanism for organizing international, all-Russian, regional and sectoral cyber orders at the CII objects.

Thus, summing up the research, we can state that the security of the CII directly depends on the correctness of decision-making in countering computer attacks, the speed and effectiveness of the actions of their entities.

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

Atamanov G. A. Security Methodology // Fund for the Promotion of Scientific Research on Security Problems. [Electronic resource]. – URL: http://naukaxxi.ru/materials/302/

Decree of the President of the Russian Federation No. 683 dated December 31, 2015 "On the National Security Strategy of the Russian Federation" // Official Gazette of the Russian Federation. – 2016. – No. 1 (Part II). – Art. 212.

Tereshchenko L.K. Information Security of Executive Authorities at the Present Stage / L.K. Tereshchenko, O. I. Tiunov // Journal of Russian Law. – 2015. – No. 8. – P. 107.

Federal Law No. 187-FZ dated July 26, 2017 “On the Safety of Critical Information Infrastructure of the Russian Federation” // Official Gazette of the Russian Federation. – 2017. – No. 3 (Part I). – Art. 4736.

Federal Law No. 149-FZ dated July 27, 2006 “On Information, Information Technologies and Information Protection” // Official Gazette of the Russian Federation. – 2006. – No. 3 (Part I). – Art. 3448.

Serdyuk V.A. Some aspects of the protection of APCS / V.A. Serdyuk, I. K. Tarvi // Information Security. – 2017. – No. 6. – P. 12.

Order of the Federal Service for Technology and Export Control of the Russian Federation No. 31 dated March 14, 2014 "On approval of requirements to provision of the information protection in the automated production and technological process control systems at the mission-critical sites, as well as potentially dangerous objects that represent an increased danger to life and health of people and environment" // Russian Newspaper. – 2014. – No. 175.

Order of the Ministry of Telecom and Mass Communications of the Russian Federation No. 264 dated June 14, 2016 “On commissioning of the state information system of housing and communal services” // Official website of the Ministry of Telecom and Mass Communications of the Russian Federation. [Electronic resource]. – URL: http://minsvyaz.ru/ru/documents/5069/

Order of the Federal Agency for Technical Regulation and Metrology No. 14-st dated January 31, 2014 “On the adoption and enforcement of the All-Russian Classifier of Economic Activities (OKVED 2) OK 029-2014 (KDEC Rev. 2) and the All-Russian Classifier of Products by Type of Economic Activity (OKPD 2) OK 034-2014 (KPEC 2008)” // Accounting Annex to the Newspaper "Ekonomika i zhyzn". – 2014. – No. 21.

A computer incident is a fact of violation and (or) termination of the operation of an object of critical information infrastructure, a telecommunication network used to organize the interaction of such objects, and (or) a violation of the security of the information processed by such an object, including that one, having resulted from a computer attack.

GosSOPKA is the state system for detecting, preventing and eliminating the consequences of computer attacks on the information resources of the Russian Federation.

Order of the Federal Service for Technical and Export Control No. 235 dated December 21, 2017 “On approval of the requirements for the creation of security systems for the significant objects of critical information infrastructure of the Russian Federation and ensuring their functioning” // “Official Internet Portal of Legal

Information" (www.pravo.gov.ru). February 22, 2018.

Order of the Federal Service for Technical and Export Control No. 227 dated December 6, 2017 "On approval of the procedure for maintaining the register of significant objects of critical information infrastructure of the Russian Federation" // "Official Internet Portal of Legal Information" (www.pravo.gov.ru). February 9, 2018.

Decree of the Government of the Russian Federation No. 127 dated February 8, 2018 "On approval of the rules for categorizing objects of critical information infrastructure of the Russian Federation, as well as a list of indicators of criteria for the importance of objects of critical information infrastructure of the Russian Federation and their values" // Official Gazette of the Russian Federation. – 2018. – No. 8. – Art. 1204.

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.

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.

Wiater P. On the notion of «partnership» in critical infrastructure protection / P. Wiater // European Journal of Risk Regulation. – 2015. – № 6 (2). – P. 255–262.

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.

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.

Albrecht D. Chinese Cybersecurity Law Compared to EUNIS-Directive and

German IT-Security Act. When cybersecurity not only protects interests of the masses but ultimately also safeguards national sovereignty / D. Albrecht // Recherchieren unter juris (Das Rechtsportal). – 2018. – P. 1-5.

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.

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.

Cohen-Almagor R. Internet architecture, freedom of expression and social responsibility: Critical realism and proposals for a better future / R. Cohen-Almagor // Innovation: The European Journal of Social Science Research. – 2015. – № 28 (2). – P. 147-166.

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.

Reshetnikov A.Yu., Russkevich E. A. On criminal liability for unlawful influence on the critical information infrastructure of the Russian Federation (Art. 274.1 of the Criminal Code of Russia) / A.Yu. Reshetnikov, E. A. Russkevich // Laws of Russia: Experience, Analysis, Practice. – 2018. – No. 2. – P. 51-55