International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-4, November 2019

Information Security of Critically Important Information Systems

Andrey Andreevich Baybarin, Natal'ya Vladimirovna Grigor'eva, Saleh Aisaevich Khodzhaliev, Olga Aleksandrovna Kovaleva, Yuliya L`vovna Shumskikh, Alexander Alexandrovich Gogin

Abstract*: The article provides a comprehensive analysis of the concepts related to the information security of critically important information systems in Russia. Today, problems exist, which are associated with numerous threats to Russian information security due to the rapidly increasing role of the information sphere. To solve these problems, an effective mechanism is needed to prevent and eliminate these threats. To develop the organizational and legal basis of the mechanism, it is necessary to define a number of concepts, such as information security, critically important information system, information infrastructure, etc. The authors explore Russian legal regulation, as well as international experience and research on this topic. The article shows the main sources of information security threats and defines general principles and approaches to ensuring information security of critically important information systems. The concept and types of critically important information systems are identified and the necessity of developing and improving their legal regulation is substantiated. A number of legal and organizational measures aimed at ensuring the information system security of Russian infrastructure are proposed.

Keywords*: information system, information security, critically important infrastructure, criminal law protection, international legal regulation.

I. INTRODUCTION

Today, information is the most valuable commodity not only in national economies but also in international trade. Perception of information as the most important resource for life support of society, which has a priority social value [1], has been formed at the international level. Therefore, the development of innovative approaches to solving the problems of information security of information systems is of primary importance in the modern development of the Russian state and its international relations [2].

The increasing importance of information, spread of informatization to almost the entire spectrum of public

relations and sharp increase in the number of information infrastructure objects have led to the fact that information security becomes an integral part of Russian national security, which increasingly depends on information security.

Thus, information security has a top priority and its provision should be considered one of the state priorities.

Today, in connection with the current situation on the international arena, there are a number of external threats, one of which is the activities of foreign intelligence and information units in the information sphere, directed against Russian interests. These activities create conditions providing for the infringement of Russian interests in the world information space and develop information war concepts. The impact of these threats on the critically important infrastructure of Russia can lead to disruption of its functioning and cause serious consequences for the state both in the economic and political spheres. External factors, based primarily on information aggression and systematic use of modern information war concepts, represent the greatest threat to Russian information sovereignty [3].

Today, this statement today seems fair and predetermines the relevance of scientific research aimed at developing ways and methods to ensure the security of Russian information infrastructure.

At the moment, the study of legal problems of information security of critically important systems is presented in a very small number of research works, especially in Russia. Only certain legal aspects of information security problems are presented in the works of such authors as I.G. Pykhtin, L.P. Zveryanskaya and A.O. Duginova, which actualizes their systematic study. A comprehensive study of these problems can contribute to the development and legislative consolidation of scientifically based methods for ensuring information security of critically important information systems, taking into account the positive practical experience of Russian and foreign scientists in this area [4-6].

Thus, the purpose of the presented work is a comprehensive analysis of the organizational and legal problems of information system protection at the national and international levels, as well as the search for their legislative solutions.

Manuscript published on November 30, 2019.
* Correspondence Author
Andrey Andreevich Baybarin*, Department of Criminal Law, Southwest State University, Kursk, Russia.
Natal'ya Vladimirovna Grigor'eva, Department of Criminal Procedure, Federal State Treasury Educational Institution of Higher Education «Moscow University of the Ministry of Internal affairs of Russia named after V.Ya. Kikot'», Moscow, Russia.
Saleh Aisaevich **Khodzhaliev**, Chechen State University, Grozny, Russia.
Olga Aleksandrovna Kovaleva, Buzuluk humanitarian and technological Institute (branch) of Orenburg state University, Buzuluk, Russia.
Yuliya L`vovna Shumskikh, Orenburg state University, Orenburg, Russia.
Alexander Alexandrovich Gogin, Togliatti State University, Tolyatti, Russia.

II. PROPOSED METHODOLOGY

A. General description

In this work, the dialectical method served as the basic research method of research and was combined with a number of additional methods. The system-structural method allowed us to show the system of international legislation regulating information security on a global scale.

B. Algorithm

The study was carried out using the comparative-legal method. The comparative-legal method made it possible to study the practice, processes of international norms formation and approaches used in different countries to ensure information security. It also allowed considering the possibility of using the positive experience of international law-making. The analogy method allowed showing the common tasks facing the leadership of countries seeking to protect their information infrastructure from numerous threats and the problem of harmonization of their regulation on the basis of international norms and principles. The theoretical basis of this study included research works in the field of information security regulation. The legal basis of the study included Russian and international official legal acts regulating information security. The selection of sources used in this study was carried out by groups, the first of which included scientific works, articles and monographs published in open-access journals, the second – normative documents and the third –Internet resources.

III. RESULTS ANALYSIS

Researchers consider information security at the micro and macro level [7]. At the macro level, information security is an integral part of the national security system with the increasing role of information resources and technologies in the development of society and state. A person and their rights, as well as information and information systems and rights to them, are the main objects of information security at the macro level and the basic elements of all security objects in all fields.

Information security at the macro level is related to the state of protection of national interests of a country from internal and external threats in the information sphere [7]. This corresponds to the logic of the Law of Russia "On Security" [8] and the content of Russia's National Security Strategy [9].

Information security and information protection at the micro level are associated with the state of information security of a separately functioning information system, enterprise, organization, etc. [7].

The modern interpretation of the information security and protection of confidential information concepts is increasingly reflected in a comprehensive, systematic approach to the creation of an adequate, proactive data protection system, necessary to create conditions for making informed management decisions in all areas of state activities. This was confirmed by the adoption of the new Doctrine of Information Security of the Russian Federation, approved by Decree of the President of Russia No. 646 dated December 5, 2016 [10]. This important regulatory act points to the need to formulate a new state policy and develop public relations in the field of ensuring information security, as well as measures to improve the information security system.

It can be stated that at the moment, various areas of protection of Russian national security, including the development of the information society, the concept of criminal law policy, the doctrine of information security, etc., are regulated by legal acts provided in Russia's National Security Strategy. This document shows the increasing penetration of illegal and illicit information technologies into the daily lives of citizens, organizations and authorities, as well as the problems of ensuring the proper level of general legal and criminal protection of the information environment and cybersecurity in the modern global information world. On July 26, 2017, Federal Law No. 187FL "On Security of Russian critically important information infrastructure" was adopted due to the existence of real threats to Russian critical information infrastructure [11].

The need for this variety of regulatory acts is dictated primarily by the rapid development of information technology and network infrastructure designed to provide a high level of conditions improving social and economic development of the state, society and individual. However, this development is accompanied by a rapid increase in cybercrime, which burdens constructive measures for the development not only in the socio-economic aspect but also in the sphere of national security of the state. Thus, according to experts, the number of detected crimes related to encroachment on critically important information infrastructure in Russia doubles annually [7].

This circumstance significantly actualizes the importance of legal protection of a significant sphere of public relations in the field of Russian critically important information infrastructure, including the criminal-legal aspect of such protection, which plays an important role in the overall safety system of the existing information infrastructure of the country. It should be noted that the problem of criminal liability for illegal actions in relation to Russian critically important information infrastructure as a single and integral entity has not been studied and discussed in the Russian criminal legal science. Thus, the introduction of a new article concerned with criminal liability for unlawful influence on Russian critically important information infrastructure – article 274.1. in the Criminal Code of Russia [12] – caused, in our opinion, fair bewilderment among many researchers [13]. First, this is due to the fact that the circle of subjects of Russian critical information infrastructure that may be subject to criminal attacks is quite large and diverse. Therefore, the (direct) guilty aggression object will depend on which specific branch of critical information infrastructure has occurred unlawful impact. Second, the features of the corpus delicti contained in the new norm of the criminal law – article 274.1 of the Criminal Code, are present in other corpus delicti, providing for criminal liability for crimes in the field of computer information.

In addition, according to a number of researchers [14] the object of criminal attacks on critically important information structures of Russia is not public safety and not the sphere of computer information, but the peace and security of mankind (Chapter 34 of the Criminal Code). Therefore, it is questionable to place norms associated with the protection of Russian critically important information structures in Chapter 28, the generic object of which is public security.

The aforementioned circumstances point to the need to more fully and effectively investigate the problems related to criminal liability for undue influence on Russian critically important information infrastructure due to the already existing theoretical and applied research in the field of cybercrime.

It should be noted that doctrines and strategies of information security have also been developed in many countries. In the United States, the National Strategy to Secure Cyberspace was signed in 2003, followed by similar documents with the keyword "cybersecurity" adopted in European countries [15].

Later in 2009, the National Cyber Security Strategy was developed in the UK [16].

The biggest share of European strategies was adopted in 2011; among them it is possible to note the most significant and independent ones – Cyber-Sicherheitsstrategie für Deutschland in Germany [17] and Défense et sécurité des systèmes d'information [18] in France.

In addition, in 2011, complementary and updated strategies were published improving the first versions of the USA and UK strategies – International Strategy for Cyberspace Prosperity, Security, and Openness in a Networked World and the UK Cyber Security Strategy: Protecting and promoting the UK in a digital world [19]. In this series, it is also necessary to mention one of the latest documents – Cybersecurity Strategy of the European Union (2013) [20]. However, in light of recent events in the EU, its fate is not entirely clear. European documents (references to English-language versions of most strategies are available in [19]) are quite different in terms of depth and detail. As noted by a number of researchers, they produce a favorable impression of the integrity of content and specificity, as well as clear understanding of the goals and objectives of the protection of national interests.

In this sense, they can really serve as an example. It is important that due to their intelligibility and emphasis on the technological aspects of networking they do not leave room for fruitless discussions and are a guide for action.

It should be noted that in contrast to the aforementioned Russian doctrine, in which it is possible to integrate various aspects of information security into a complex, strategies emerging in Western countries one after another are more relevant in terms of prospects for technical reality. However, they are characterized by mainly organizational and technological orientation while the legal and political aspects are practically absent.

Aware of the need to consolidate information security at the level of international law, Russia traditionally adheres to a broad understanding of this concept and proposes to consolidate it at the international level.

International cooperation in the field of information security at the world level is complicated by contradictions in the public interests.

At the initiative of Russia, back in 1993, the draft Convention on the Prohibition of Military or Any Other Hostile Use of Methods and Means Influencing the Infosphere was developed and prepared for consideration by the UN. However, the approval of this international legal instrument has met opposition from the USA.

Currently, the USA is positioned as a leader in the field of information and communication technologies. Therefore, it is not interested in limiting its carte blanche. Russia aims to minimize the risks associated with the information space, thus promoting national and international security [21].

It should be noted that Russia supports the consolidation of the principle of non-interference in the information space: according to the draft Convention on Ensuring International Information Security, submitted to the UN by Russia, "Each state has the right to establish sovereign norms and manage its information space in accordance with national laws" [22].

At the same time, Russia has managed to consolidate its initiatives at the regional level and in the framework of bilateral agreements. Thus, on June 2, 2011, the Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization, signed on June 16, 2009 in Yekaterinburg, entered into force [23].

One of the results of cooperation in the field of international information security was the presentation on behalf of the SCO member states of the draft Rules of Conduct in the Field of International Information Security (2011) at the 66th session of the UN General Assembly and the updated version of these rules at the 69th session of the UN General Assembly in (2015) [24].

It is noted that the key feature of the SCO initiative is its peacekeeping nature. In contrast to the concepts involving the regulation of cyberwarfare (USA), the document aims to prevent conflicts in the information space. It establishes the obligations of states not to use information and communication technologies to violate international peace and security, as well as to interfere in the internal affairs of other states and undermine their political, economic and social stability. Moreover, the draft Rules of Conduct provide for the obligation of states to refrain from the use or threat of force in the settlement of international disputes arising in the digital sphere [25].

An example of a bilateral format of international cooperation in the field of information security is the signing of a bilateral Agreement on Cooperation in the Field of International Information Security on May 8, 2015 between Russia and China [26]. This agreement defines the main threats in the field of international information security, as well as the main directions, principles, forms and mechanisms of cooperation between the states.

As shown above, the problem of information protection at the national and international levels is multifaceted and covers a number of important tasks.

The problems of information security are constantly aggravated by spreading of technical means of data processing and transmission and, above all, information systems to all spheres of society. Next, we consider the provisions on the information system security, developed as a result of research in the field of organizational and legal foundations of information system security.

An information system is considered secure if it, using appropriate hardware and software, controls access to information so that only properly authorized persons or processes acting on their behalf have the right to read, write, create and delete information [27]. An information system is a set of interconnected information, technical, software, mathematical, organizational, legal, ergonomic, linguistic, technological and other means, methods, as well as personnel used to collect, process, store and issue information in order to achieve a certain goal [27]. Critically important software (CIS) is a system that manages or regulates the provision of a critically important object (CIO) or process (CIP).

Systems that manage potentially hazardous industries or processes, ensure the functioning of hazardous objects and manage (or provide information management) sensitive processes for the state are considered critically important.

Violation of the normal functioning of CIS can lead to failure in performance of vital functions of public administration, management of armies, weaponry, environmentally dangerous and economically important productions, etc. and, as a consequence, inadmissible damage to national interests, life and health of people. Based on the aforementioned, the following definition can be formulated: a critical information system is a set of interconnected information, technical, software, mathematical, organizational, legal, ergonomic, linguistic, technological and other means and methods, as well as personnel used to collect, process, store and issue key information for the management and regulation of activities or management of information support of a critical object or process.

Currently, the legal regulation of critically important information systems is carried out at the level of regulatory documents developed by the Federal Service for Technical and Export Control (FSTEC). The FSTEC issued order No. 31 dated March 14, 2014 "On approval of the requirements for ensuring information security in automated control systems for production and technological processes at critically important objects" [28]. Earlier, the FSTEC developed and approved a system of methodological documents entitled "General requirements for information security in key information infrastructure systems" (approved by the FSTEC on May 18, 2007), which contains key definitions of critically important information systems: "A key (critically important) information system is an information-management or information-telecommunication infrastructure, which manages the CIO (CIP) or information support of such an object (process) or official informing of citizens and, as a result of destructive informational impact on which, an emergency may develop or the management functions performed by the system may be disrupted with significant negative consequences". From the text of another document, the Regulation on the Register of Key Information Infrastructure Systems (approved by the order of the FSTEC dated March 3, 2009), it is possible to conclude that many different classes of information, automated systems and information and telecommunication networks (warning systems) belong to critical information systems and emergency response, geographical and navigation systems, water supply, energy, transport management systems and other systems and networks). This also includes automated control systems for production and technological processes at CIO, potentially hazardous objects, as well as objects that pose an increased risk to human life and health and to the environment.

At present, such regulation appears to be insufficient. It seems that the regulation of critical information systems should be carried out at several legislative levels. At the level of the federal law, it seems sufficient to introduce norms defining the concept of critically important information infrastructure systems into the law "On Information, Information Technologies and the Protection of Information" [29].

In addition, there should be bylaws – second-level documents (government resolutions and presidential decrees, for example, the government decree on the classification of CIO information systems).

At the third level, there are departmental documents of the FSTEC and the Federal Security Service with requirements for the protection of critically important information systems.

IV. CONCLUSION

As a result of the study, the following proposals aimed at improving the regulation of information security of critically important information systems were developed.

It is necessary to develop normative consolidation of the conceptual apparatus, the definition and main types of critical information systems, the goals, objectives and priorities in the field of ensuring information security and implement them at the level of federal laws, resolutions of the Government of Russia and decrees of the President of Russia.

For effective implementation of cooperation in the field of information security, it is necessary to ensure the promotion of Russian initiatives in the field of information security in all international organizations, intensifying Russia's participation in global, regional and bilateral agreements.

REFERENCES

1. A.V. Novikov, D.D. Saydulaev, D.A. Kremcheeva, "Service sector and information technologies: development of new opportunities", *IJITEE*, vol. 8(9), 2019, 1389-1394.
2. V.A. Avdeev, E.V. Avdeeva, A.V. Bykov, E.A. Kiselev, A.N. Aksenov, "Social technologies of receiving new information", *IJEAT*, vol. 8(6), 2019, 5279-5282.
3. O. V. Boichenko, A. A. Anoshkina, "Obespechenie informatsionnoi bezopasnosti kriticheski vazhnykh obektov infrastruktury Rossiiskoi Federatsii", V sbornike: Teoriya i praktika ekonomiki i predprinimatelstva Trudy XIII Mezhdunarodnoi nauchno-prakticheskoi konferentsii [Ensuring Information Security of Critical Infrastructure Facilities of the Russian Federation, In the collection: Theory and Practice of Economics and Entrepreneurship. Proceedings of the XIII International Scientific and Practical Conference.], 2016, pp. 97-98.

4. N. Bizhan, T. Bekimbetov, A. Persheyev, G. Rahmetova, G. Diarabayeva, "Features of humanization of criminal policy of Kazakhstan: study of the possibilities to increase the effectiveness of punishments in the context of international experience", *Journal of Advanced research in law and economics,* vol. IX(5(35)), 2018, pp. 1604-1610.
5. R.V. Kostenko, A. Rudin, "Notion and meaning of evidence verification in criminal procedure", *Journal of Advanced research in law and economics*, vol. 9 (3(33)), 2018, pp. 1011-1017.
6. A. Baisswitova, Zh. Kegembayeva, I. Shalkarova Kim, O. Smailov, G. Sagynbekova, "Topical issues of criminal law and lawsuit in Kazakhstan: assignment of punishment under criminal law", *Journal of Advanced research in law and economics*, vol. 8 (2(25)), 2017, pp. 730-737.
7. O.V. Boichenko, L.M. Borshch, I.V. Mandritsa, O.V. Mandritsa, I.V. Soloveva, V.I. Petrenko, V.V. Matveev, V.N. Titarenko, D.V. Titarenko, M.V. Potanina, E.A. Baizdrenko, S.N. Pisaryuk, V.M. Shishkin, V.I. Vorobev, E.L. Evnevich, T.V. Monakhova, I.V. Gavrikov, A.M. Rybnikov, M.S. Rybnikov, O.L.Korolev et al., "Informatsionnaya bezopasnost sotsialno-ekonomicheskikh sistem Monografiya" [Information Security of Socio-Economic Systems Monograph], Simferopol, 2017.
8. Federal Law of December 28, 2010 N 390-FL (as amended on October 5, 2015) "On Security". Collected Legislation of the Russian Federation, January 3, 2011, No. 1, Art. 2. Available: http://kremlin.ru/acts/bank/32417
9. Decree of the President of the Russian Federation of December 31, 2015 N 683 "On the National Security Strategy of the Russian Federation". Collection of the legislation of the Russian Federation, January 4, 2016, N 1 (part II), Art. 21. Available: http://kremlin.ru/acts/bank/40391
10. Decree of the President of the Russian Federation of 05.12.2016 N 646 "On approval of the Doctrine of information security of the Russian Federation" . Collection of legislation of the Russian Federation, 12.12.2016, N 50, Art. 7074. Available: http://kremlin.ru/acts/bank/41460
11. Federal Law of July 26, 2017 No. 187-FL "On Security of the Critically Important Information Infrastructure of the Russian Federation". Collection of legislation of the Russian Federation. 2017. No. 31, p. I, art. 4736. Available: https://rg.ru/2017/07/31/bezopasnost-dok.html
12. The Criminal Code of the Russian Federation of 13.06.1996 N 63-FL (as amended on 08/02/2019) // Meeting of the legislation of the Russian Federation, June 17, 1996, N 25, Art. 2954. Available: https://rg.ru/2007/11/12/ukrf-dok.html
13. I. Pykhtin, "Ugolovno-pravovaya okhrana obektov kriticheskoi informatsionnoi infrastruktury kak odno iz klyuchevykh napravlenii sovremennoi borby s kiberprestupnostyu v Rossiiskoi Federatsii", *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta.* [Criminal legal protection of critically important information infrastructure objects as one of the key areas of the modern fight against cybercrime in the Russian Federation // News of Southwestern State University.] Series: History and law, vol. 8, No. 1(26), 2018, pp. 98-103
14. I. A. Yurchenko, "Mezhdunarodno-pravovoe i ugolovno-pravovoe obespechenie informatsionnoi bezopasnosti kriticheski vazhnykh obektov infrastruktury RF", *Probely v rossiiskom zakonodatelstve*, [International and criminal law information security of critically important infrastructure of the Russian Federation, Gaps in Russian legislation], vol 6, 2015, pp. 95-99.
15. «The National Strategy to Secure Cyberspace» . U.S. government via Department of Homeland Security. February 2003. p. 16.
16. Cyber security strategy of the United Kingdom. Available: https://www.gov.uk/government/publications/cyber-security-strategy-of-the-united-kingdom
17. Cyber-Sicherheitsstrategie für Deutschland. Available: https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf
18. Défense et sécurité des systèmes d'information. Stratégie de la France. Available: https://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf
19. State cybersecurity strategies / Analytical review. 09/04/2012. Available: http://www.securitylab.ru/analytics/429498.php
20. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Available: //https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf
21. A.O. Duginova, "Mezhdunarodnoe sotrudnichestvo RF v oblasti obespecheniya mezhdunarodnoi informatsionnoi bezopasnosti", *Politika, ekonomika i innovatsii*.[International cooperation of the Russian Federation in the field of international information security // Politics, Economics and Innovations], vol. 3(13), 2017, p. 12
22. Convention on ensuring international information security (concept). *Ministry of Foreign Affairs of Russia*. Official site. Available: http: //www.mid.ru/foreign_policy/official_documents //asset_publisher/ CptICkB6BZ29/content/id/191666t
23. Agreement between the governments of the member states of the Shanghai Cooperation Organization on cooperation in the field of international information security. Available: http: //docs.cntd.ru/document/902289626
24. Letter dated 9 January 2015 from the Permanent Representatives of Kazakhstan, China, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General. Available: http://www.mid.ru/ru/web/guest/organs/–/asset_publisher/AfvTBPbEYay2/content /id/916224
25. L.P. Zveryanskaya, "Razvitie sotrudnichestva Rossii i KNR v oblasti mezhdunarodnoi informatsionnoi bezopasnosti", *Pravo i gosudarstvo: teoriya i praktika* [Development of cooperation between Russia and China in the field of international information security. *Law and State: Theory and Practice*], Vol. 5(149), 2017, pp. 134-137
26. Agreement between the Government of the Russian Federation and the Government of the People's Republic of China on cooperation in the field of ensuring international information security. Available: http: //government.ru/media/files/5AMAccs7mS lXgbff1Ua785WwMWcABDJw.pdf
27. A.A. Medvedev, E.N. Sozinova, "Kriticheski vazhnye informatsionnye sistemy", *Nauchno-tekhnicheskii vestnik Povolzhya* [Critically important information systems. Scientific and Technical Bulletin of the Volga Region], vol. 4, 2016, pp. 83-85
28. Order of March 14, 2014 No. 31 "On approval of the requirements for ensuring information security in automated control systems for production and technological processes at critically important objects". Available: //https://fstec.ru/normotvorcheskaya/akty/53-prikazy/868-prikaz-fstek-rossii-ot-14-marta-2014-gn-31
29. Federal Law of July 27, 2006 No. 149-FZ (as amended on March 18, 2019) "On Information, Information Technologies and the Protection of Information" // Collected Legislation of the Russian Federation, July 31, 2006, No. 31 (1 part), Art. 3448. Available: https://rg.ru/2006/07/29/informacia-dok.html