Protecting critical information infrastructure of government, transportation, and tourist facilities under sanctions pressure

Belyaeva, Olga; Surpkelova, Amina; Khromov, Dmitry; Blokhin, Ivan

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

ИССЛЕДОВАТЕЛЬСКАЯ СТАТЬЯ

Защита критической информационной инфраструктуры государственных и транспортно-туристских объектов в условиях санкционного давления

Ольга Игоревна Беляева[a]
Амина Сурпкелова[a]
Дмитрий Витальевич Хромов[b]
Иван Олегович Блохин[c]

a Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации
b Национальный исследовательский ядерный университет МИФИ
c Дипломатическая академия МИД РФ

DOI: 10.22394/2070-8378-2023-25-5-97-101

Аннотация: В статье проводится анализ политико-правовых мер по противодействию угрозам критической информационной инфраструктуре (КИИ). Приводятся толкования КИИ в России и зарубежных странах, анализируется охват ее объектов, а также рассматриваются меры, принятые в России, по защите КИИ, в контексте основных угроз информационной безопасности за 2017–2023 годы. Санкционное давление и другие политические вызовы в значительной степени способствовали разработке новых мер безопасности. Успех защитной политики подтверждается увеличением доли электроники отечественного производства, закупаемой государственными предприятиями и государственными заказчиками в 2023 году. Существующие риски, связанные с уязвимостью иностранной электроники к кибератакам, все еще требуют решения. В ответ на эти вызовы в области защиты КИИ постепенно внедряются новые системы безопасности.

Ключевые слова: критическая информационная инфраструктура, государственная политика, импортозамещение, сектор туризма

Дата поступления статьи в редакцию: 12 октября 2023 года.

Protecting critical information infrastructure of government, transportation, and tourist facilities under sanctions pressure

RESEARCH ARTICLE

Olga Igorevna Belyaeva[a]
Amina Surpkelova[a]
Dmitry Vitalievich Khromov[b]
Ivan Olegovich Blokhin[c]

a Russian Presidential Academy of National Economy and Public Administration
b National Research Nuclear University MEPhI
c Diplomatic Academy of the Ministry of Foreign Affairs of the Russian Federation

Abstract: The article analyzes political and legal measures to counter threats to critical information infrastructure (CII). The authors explain the concept of CII in Russia and abroad, examine how its objects are covered, and discuss the steps Russia has taken to safeguard CII considering the principal risks to information security in 2017–2023. The sanctions regime places unique challenges in the area of CII protection. Sanctions pressure and other political challenges vastly facilitated the development of new security measures. The success of the protective policy is demonstrated by the increase in the proportion of domestically produced electronics purchased by state-owned businesses and government clients in 2023. The current risks related to foreign electronics being vulnerable to cyberattacks need to be addressed. In response to these challenges, new security systems are gradually being introduced for CII protection.

Keywords: critical information infrastructure, public policy, import substitution, tourism sector
Received: October 12, 2023.

Introduction

Today, the relevance of critical information infrastructure protection in Russia has received a new round of development. According to the report, since the spring of 2022, there has been an increase in cyberattacks on Russian CII facilities, totaling an 80 % [1] increase in the number of attacks. In addition, since that moment, unfriendly countries have been more active in restricting electronics exports to Russia, threatening the functioning of critical government and economic facilities.

The protection of CII has been extensively covered in the literature. All studies on this topic can be divided into two groups. The first group focuses on the technical aspects of the problem, specifically the models of CII protection. This includes the development of a model for implementing CII protection requirements [Shaburova, Zonova, 2019], the evaluation of the strengths and weaknesses of various information security models [Maksudov, Doroshenko, Selifanov, 2022], and the assessment of the effectiveness of existing CII protection models [Adi, Sensus, 2022]. The second group emphasizes the institutional component of information security. It covers a wide range of social issues, ranging from the interaction between the state and the market in protecting CII [Cukier, Schönberger, 2005] to the specifics of the problem in developing countries [Ellefsen, von Solms, 2010]. Some studies on information security policy in Russia analyze the main milestones of state policy in this area [Prontchev, Sushko, 2022], as well as the peculiarities of the Russian approach at the present stage [Karasev, Stefanovich, 2022]. Furthermore, some researchers have chosen the information security of transport and tourist infrastructure as an object of study, analyzing such aspects as the main threats, the structure of information security content [Zaynalov, Muhamadiev, Bekmurodov, 2019], and protection measures [Zhuravleva, Polyakov, Frolov, Rodionov, 2020]. The institutional aspect of CII protection has been extensively studied, but this issue in contemporary Russia, given the previously stated realities, has not received enough attention.

It is recommended to analyze the political and legal methods used to protect CII in Russia under sanctions pressure by examining regulatory legal acts.

Approaches to interpreting and protecting CII

There is no single definition of CII at the international level due to the current complexity of cooperation in this area; however, critical information structure refers to digital and telecommunication facilities in those industries whose activities are crucial for society, the economy, and the state. A.S. Shaburov and V.E. Zonova attribute critical industries to the energy, fuel, and power industry, including nuclear power; defense industry, including rocket engineering; and social sphere (transport, communications, and health care, as well as some extractive and manufacturing sectors) [Shaburov, Zonova, 2019. P. 131]. The tourism infrastructure, whose information security will be covered later, is closely associated with the transportation industry.

One of the components of CII is the government information infrastructure. We must emphasize that the protection of CII applies not only to the object but also to the state (or associations of states), which is the principal subject of this protection, as reflected in the relevant rulemaking. In the EU, CII is defined as those infrastructure objects that, if damaged, could significantly affect an entity's well-being or the efficiency of its member states' operations. [Karasev, Stefanovich, 2022. P. 150]. The Institute of Standards and Technology (USA) has developed five definitions of CII. In the US, critical infrastructure includes many areas, including industry, commerce, communications, energy, government agencies, emergency services, etc. This list also includes dams, water supply systems, materials, and waste[2]. In other words, there is a broad list of CIIs that are subject to being protected in both the U.S. and the EU.

In Russia, the legislation refers to CII as those objects whose damage «leads to loss of control, destruction of infrastructure, irreversible negative change (or destruction) of the economy of the country, a subject of the Russian Federation or an administrative-territorial unit or significant deterioration of the safety of life of the population living in these territories for a long period of time»[3]. In 2017, there was a significant cyberattack on Russian telecommunications facilities and law enforcement agencies. The attack was carried out using encryption virus that was modified from a program developed by the US NSA. This incident led to the activation of various activities aimed at protecting critical information infrastructure [Pronchev, Sushko, 2022. P. 60]. The adopted law introduced interrelated definitions of CII, objects of CII, and sub-

1 Interview with O.V. Syromolotov, Deputy Minister of Foreign Affairs of the Russian Federation, «Rossiya Segodnya» MIA, December 28, 2022. https://www.mid.ru/ru/foreign_policy/news/1845853/

2 Presidential Policy Directive/Ppd-21 «Critical Infrastructure Security and Resilience» // The White House. February 12, 2013. https://www.cisa.gov/sites/default/files/publications/PPD-21-Critical-Infrastructure-and-Resilience-508.pdf

3 The main directions of state policy in the field of ensuring the safety of automated control systems of production and technological processes of critical infrastructure of the Russian Federation. http://www.scrf.gov.ru/security/information/document113/

jects of CII. The law defines the latter as «state bodies, state institutions, Russian legal entities, and (or) individual entrepreneurs»[4], which possess information systems (i.e., objects) operating in particular critical sectors: social (healthcare, science, transport, communications), economic (financial sector, fuel and energy complex, industry), and in spheres directly related to the state (state registration of rights to real estate, defense industry). This Federal Law sets out the legal framework for the protection of CII (security principles, structuring of CII objects, requirements to ensure their security, etc.) and defines the structure of the State System of Detection, Prevention and Elimination of Consequences of Computer Attacks on Information Resources (GOSSOPKA). This system represents a system of special units (within the FSB, the National Computer Incident Coordination Center) and a set of scientific research on strengthening information security.

In 2022, amid increased sanctions pressure and an overall escalation in relations with Western countries, the Presidential Decree «On Measures to Ensure Technological Independence and Security of Critical Information Infrastructure» was adopted[5]. The Act prohibits software of foreign origin in the public sector and establishes obligations for introducing domestic radio-electronic products and telecommunications equipment. The implementation of the decree has already started in multiple areas. Several Russian ministries and agencies, including the Ministry of Finance, the Ministry of Industry and Trade, the Ministry of Transport, and the Federal Tax Service, have introduced a ban on the use of Apple devices running the iOS operating system. They are beginning to replace foreign hardware and software with domestic mobile devices on the Russian-designed «Aurora» OS. Russian Railways has implemented the «Aurora» OS on a large scale. P. Eiges, CEO of the company that developed this OS, believes that current conditions only allow for protecting CII «by utilizing a completely domestic technology stack». This means that Russian public organizations should use smartphones and tablets running on a Russian operating system[6]. Additionally, import substitution norms are being established. This process was already noticed in 2020 when the Resolution of the Government of the Russian Federation established a minimum share of Russian electronic products for public procurement – from 50 to 90 % (depending on the category)[7]. In 2022, the planned indicators were revisited against the background of an even more pressing import substitution problem. Based on the resolution, the Ministry of Digital Development, Communications, and Mass Media approved the minimum share of purchases of Russian-made electronic products for 2022–2024[8]. Furthermore, targets for purchasing Russian electronics are outlined in the Ministry of Industry and Trade's updated strategy for 2023. It was assumed that domestic electronics would account for at least 27 % and 70 % of the total domestic market (which includes state-controlled and non-government-controlled sectors)[9] and that they would account for 50 % of the controlled market in 2024 and at least 95 % in 2030.

At the end of 2022, the share of Russian goods in the Russian market (as a whole) was 19 %; at the end of 2023, the share in the regulated sector (where the protection of CII is the highest priority) may reach 50 %. This is in spite of the fact that expectations back in 2022 were very pessimistic, and sectoral problems of Russian microelectronics were noted (e.g., the priority of the military order while lagging behind other areas) [Karasev, Stefanovich, 2022. P. 159][10].

Protection of CII in the tourism sector

As digital technologies (e.g., online booking) are actively spreading, if there is a threat to digital infrastructure, one of the conditions for sustainable

4 Federal Law N 187-FZ «On the Security of Critical Information Infrastructure of the Russian Federation» of July 26, 2017 (latest edition). http://www.kremlin.ru/acts/bank/42128

5 Decree of the President of the Russian Federation of March 30, 2022, No. 166, «On measures to ensure technological independence and security of the critical information infrastructure of the Russian Federation». http://www.kremlin.ru/acts/bank/4768

6 Russian agencies have imposed a ban on Apple technology. What can the public sector replace it with? https://rg.ru/2023/08/21/mobilnye-rezervy.html

7 Resolution of the Government of the Russian Federation of December 3, 2020, No 2013 (ed. of February 28, 2023), «On the minimum share of purchases of goods of Russian origin». https://www.consultant.ru/document/cons_doc_LAW 369870/891cd78904ddd045d4f6a72d2168299228a9afd9

8 Methodological Recommendations on Digital Transformation of State Corporations and Companies with State Participation (approved by the Russian Ministry of Finance). https://digital.gov.ru/ru/documents/7342/

9 The government has approved the updated Consolidated Strategy for the Development of Russia's Manufacturing Industry up to 2030 and for the period up to 2035. http://government.ru/docs/49489/

10 The share of Russian radio electronics in state procurement may reach 50% ahead of schedule. https://www.interfax.ru/russia/925087

tourism development is the information security of tourism facilities. Information security in tourism infrastructure is facing several significant threats. Some authors highlight the risk of personal data leakage as well as related «unauthorized destruction, copying, modification, and blocking of information through unauthorized access» [Zhuravleva, Polyakov, Frolov, Rodionov, 2020. P. 3]. Others, in addition to this threat, note the security of banking information processing [Zaynalov, Muhamadiev, Bekmurodov, 2019. P. 3]. The latter group of authors offers a generalized structure of information security content, including security of personal computers, networks, and software; protection of personal data, enterprises, and their resources; and security of the information environment. Using this framework, we can improve the security of each element, thus maximizing the protection of the entire system. «Drawing up an access matrix of user groups that have access to computer systems in the hotel» [Zhuravleva, Polyakov, Frolov, Rodionov, 2020. P. 3] is one specific measure to ensure the information security of tourism infrastructure. Other measures include antivirus and cryptography protection, as well as the use of special programs to prevent hacking.

Russia has started implementing steps to safeguard CII associated with the travel and tourism industry. Thus, in July 2020, the «Unified system of monitoring and protection of transportation from cyberattacks» was created [Prontchev, Sushko, 2022. P. 61]. The mentioned introduction of domestic software at Russian Railways may become a positive example of CII protection practices for other tourism-related organizations.

Conclusion

Sanctions pressure and other contemporary political challenges have put Russia's critical information infrastructure at risk, which has sped up the creation and implementation of security measures. Legislative acts adopted in 2017–2023 created a legal framework in the field of CII protection and defined specific areas of activity, such as banning foreign software, the development of electronic and information systems, and their introduction into state structures. The success of the protective policy is demonstrated by the increase in the proportion of domestically produced electronics purchased by state-owned businesses and government clients in 2023. Nevertheless, complete import substitution has not yet been accomplished in this field, so there are still risks related to foreign electronics being vulnerable to cyberattacks. Particular emphasis should be placed on the infrastructure related to tourism and transportation, where information security is becoming increasingly important. In response to this challenge, new security systems are gradually being introduced in this area.

Литература

Журавлева В., Поляков В., Фролов А., Родионов И. Особенности обеспечение информационной безопасности в гостиничных и туристических комплексах. *Проблемы правовой и технической защиты информации*. 2020. № 8. С. 22–28. http://journal.asu.ru/ptzi/article/view/13931

Карасёв П.А., Стефанович Д.В. Кибербезопасность критически важной инфраструктуры: новые вызовы. *Россия в глобальной политике.* 2022. № 6 (118). https://cyberleninka.ru/article/n/kiberbezopasnost-kriticheski-vazhnoy-infrastruktury-novye-vyzovy

Максудов М.О., Дорошенко И.Е., Селифанов В.В. проблемы формирования структуры функций системы управления информационной безопасностью значимого объекта критической информационной инфраструктуры. *Интерэкспо Гео-Сибирь*. 2022. №. https://cyberleninka.ru/article/n/problemy-formirovaniya-struktury-funktsiy-sistemy-upravleniya-informatsionnobezopasnostyu-znachimogo-obekta-kriticheskoy

Прончев Г.Б., Сушко В.А. Особенности защиты критически важной инфраструктуры российской федерации. *Социально-гуманитарные знания*. 2022. № 6. https://cyberleninka.ru/article/n/osobennosti-zaschity-kriticheski-vazhnoy-infrastruktury-rossiyskoy-federatsii

Шабуров А.С., Зонова В.Э. Модель реализации требований по защите информации объектов критической информационной инфраструктуры. *Вестник ПНИПУ. Электротехника, информационные технологии, системы управления*. 2019. № 32. https://cyberleninka.ru/article/n/model-realizatsii-trebovaniy-po-zaschite-informatsii-obektov-kriticheskoy-informatsionnoy-infrastruktury

Adi, Prasetyo & Sensuse, Dana. Review of Security Principles and Security Functions in Critical Information Infrastructure Protection. *International Journal of Safety and Security Engineering*. 2022. No. 12. 459–465. https://www.researchgate.net/publication/364462832_Review_of_Security_Principles_and_Security_Functions_in_Critical_Information_Infrastructure_Protection/citation/download In English

Cukier, Kenneth & Mayer-Schönberger, Viktor & Branscomb, Lewis. Ensuring (and Insuring?) Critical Information Infrastructure Protection. Harvard University, John F. Kennedy School of Government, Working Paper Series. 2005. 10.2139/ssrn.832628. In English

Ellefsen, Ian & Solms, Sebastiaan. Critical Information Infrastructure Protection in the Developing World. 2010. P. 29–40. 10.1007/978-3-642-16806-2_3. https://www.researchgate.net/publication/221654735_Critical_Information_Infrastructure_Protection_in_the_Developing_World In English

Zaynalov, Nodir & Muhamadiev, Abdinabi & Ugli, Bekmurodov & Nizomovich, Mavlonov & Utkirovich, Kiyamov & Kilichev, Dusmurod. Information Security Issues for Travel Companies. 2019. 1–4. 10.1109/ICISCT47635.2019.9011896. https://www.researchgate.net/publication/339554493_Information_Security_Issues_For_Travel_Companie In English

References

Zhuravleva V., Polyakov V., Frolov A., Rodionov I. Features ensuring information security in hotel and tourist complexes. *Problemy pravovoy i tekhnicheskoy zashchity informatsii*. 2020. No. 8. P. 22–28. http://journal.asu.ru/ptzi/article/view/13931. In Russian

Karasev P.A., Stefanovich D.V. Cybersecurity of critical infrastructure: new challenges. *Rossiya v global'noy politike*. 2022. No. 6 (118). https://cyberleninka.ru/article/n/kiberbezopasnost-kriticheski-vazhnoy-infrastruktury-novye-vyzovy In Russian

Maksudov M.O., Doroshenko I.E., Selifanov V.V. Problems in forming the structure of functions for the information security management system of a significant object of critical information infrastructure. *Interekspo Geo-Sibir*. 2022. No. https://cyberleninka.ru/article/n/problemy-formirovaniya-struktury-funktsiy-sistemy-upravleniya-informatsionnobezopasnostyu-znachimogo-obekta-kriticheskoy In Russian

Pronchev G.B., Sushko V.A. Specifics of protecting the critical infrastructure of the Russian Federation. *Sotsial'no-gumanitarnyye znaniya*. 2022. No. 6. https://cyberleninka.ru/article/n/osobennosti-zaschity-kriticheski-vazhnoy-infrastruktury-rossiyskoy-federatsii In Russian

Shaburov A.S., Zonova V.E. Model of implementing requirements for protecting the information of objects of critical information infrastructure. *Vestnik PNIPU. Elektrotekhnika, informatsionnyye tekhnologii, sistemy upravleniya*. 2019. No. 32. https://cyberleninka.ru/article/n/model-realizatsii-trebovaniy-po-zaschite-informatsii-obektov-kriticheskoy-informatsionnoy-infrastruktury In Russian

ИНФОРМАЦИЯ ОБ АВТОРАХ:

Ольга Игоревна Беляева, кандидат экономических наук, доцент кафедры регионального управления Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации (Российская Федерация, 119606, Москва, проспект Вернадского, 82). E-mail: belyaeva-oi@ranepa.ru

Амина Сурпкелова, аспирант

Российская академии народного хозяйства и государственной службы при Президенте Российской Федерации (Российская Федерация, 119606, Москва, проспект Вернадского, 82). E-mail: a.surpkelova@gmail.com

Дмитрий Витальевич Хромов, магистрант

Национальный исследовательский ядерный университет МИФИ (Российская Федерация, 115409, Москва, Каширское ш., 31). E-mail: dimian434@gmail.com

Иван Олегович Блохин, магистрант

Дипломатическая академия МИД РФ (Российская Федерация, 119021, г. Москва, Остоженка, д.53/2 стр.1). E-mail: blohin_ivan123@mail.ru

Для цитирования: *Беляева О.И., Сурпкелова А., Хромов Д.В., Блохин И.О*. Защита критической информационной инфраструктуры государственных и транспортно-туристских объектов в условиях санкционного давления. *Государственная служба*. 2023. № 5. С. 97–101.

INFORMATION ABOUT THE AUTHORS:

Olga Igorevna Belyaeva, Candidate of Sci. (Economics), Associate Professor, Department of Regional Management Russian Presidential Academy of National Economy and Public Administration (82, Vernadsky Prospekt, Moscow, 119606, Russian Federation). E-mail: belyaeva-oi@ranepa.ru

Amina Surpkelova, Post-graduate Student

Russian Presidential Academy of National Economy and Public Administration (82, Vernadsky Prospekt, Moscow, 119606, Russian Federation). E-mail: a.surpkelova@gmail.com

Dmitry Vitalievich Khromov, Graduate Student

National Research Nuclear University MEPhI (31, Kashirskoe shosse, Moscow, 115409, Russian Federation). E-mail: dimian434@gmail.com

Ivan Olegovich Blokhin, Graduate Student

Diplomatic Academy of the Ministry of Foreign Affairs of the Russian Federation (building 1, 53/2, Ostozhenka St., Moscow, 119021, Russian Federation). E-mail: blohin_ivan123@mail.ru

For citation: *Belyaeva O.I., Surpkelova A., Khromov D.V., Blokhin I.O*. Protecting critical information infrastructure of government, transportation, and tourist facilities under sanctions pressure. *Gosudarstvennaya sluzhba*. 2023. No. 5. P. 97–101.