Russia's Cybersecurity Policy for Atomic Energy Sector

Radomir Bolgov

1 Introduction

When talking about the cybersecurity of energy facilities, images from the action movie *Die Hard 4* appear in the mind. Russian experience in this area is becoming increasingly relevant in the context of the conflict in Ukraine [1] and the situation around the Zaporozhye nuclear power plant. According to Russian authorities, Zaporozhye NPP network is subject to cyber attacks every day [1].

The topic of cybersecurity in Russia is becoming more and more relevant. According to SOC-Forum, in Russia in 2023 the number of cyber attacks on government websites was 50% more than in 2022 [2]. In accordance with a number of cybersecurity indexes and ratings, Russia is among the leaders in cybersecurity [3].

Interest in and demand for the selected research areas in Russia is not in doubt. We found more than 500 articles in bibliometric database "Russian Index of Scientific Citation" (RISC) on the subject of "cybersecurity for atomic energy", and the publication activity continues to grow. To clarify the thematic focus of the articles, we analyzed the dynamics of publication activity with breakdown by two time periods: 2010–2016 and 2017–2023 years. On average, the number of published articles in the second period is more than three times higher than the number of publications prior to 2016. This indicates an increase in the interest of the Russian scientific community in the issue.

The need to understand cybersecurity in the context of the nuclear industry in general and nuclear security, in particular, is now recognized internationally. There is an active discussion and development of approaches to solving it with the direct participation and support of the IAEA [4]. A striking example of such activity is the

R. Bolgov (✉)
St. Petersburg State University, Saint Petersburg, Russia
e-mail: r.bolgov@spbu.ru

R. Bolgov et al. (eds.), *Proceedings of Topical Issues in International Political Geography (TIPG 2023)*, Springer Geography, https://doi.org/10.1007/978-3-031-70886-2_32

international conference held by the IAEA in June 2015, Cybersecurity in the Nuclear World: Expert Discussion and Exchange of Views. The IAEA conference program highlights three areas of cybersecurity that need to be given attention as an important component of ensuring the safety of nuclear facilities and other organizations in the nuclear industry:

- cybersecurity of automated control systems for technological processes of nuclear facilities;
- cybersecurity of automated information systems;
- cybersecurity of physical protection systems of nuclear facilities.

Speaking about the cybersecurity of automated systems of nuclear facilities, we would like to note the research on the state and promising areas of work on this issue conducted by Chatham House [5], Nuclear Threat Initiative [6] and University of Applied Sciences, Brandenburg [7]. The study by Chatham House [5] mainly focuses on the cybersecurity of automated control systems for nuclear installations, while the others deal with cybersecurity measures in the context of nuclear security. Publications based on the results of these studies provide a general description of the cyber threats that need to be considered and also describe the tools and approaches used to provide protection against them in various countries (including the United States and the Russian Federation). The works also provide recommendations for the creation, improvement and development of these approaches and tools.

As an example, let's consider a cyber attack against an enrichment plant in the Iranian city of Natanz. From the description of a cyber attack in the literature [5] it follows that the attack used the Stuxnet virus, which reprogrammed industrial controllers in such a way that they gave control commands incompatible with life to the installation, ignoring sensor data that under normal conditions should have resulted in issuing a command to put the installation into safe mode. The affected facility was considered protected from viruses due to the lack of a physical connection to the Internet, but the malicious program was introduced into its management system from an external drive.

2 Research Approach

We conducted a study in line with the approach proposed by Jobin, Ienca & Vayena [8]. They compare 84 documents modelling policies. This approach is in accordance with the work by van Berkel and colleagues [9].

We devised a search on several steps. We conducted a set of Google search queries to identify policy documents by using the country name ("Russia", "Russian Federation") and the keywords:

"cybersecurity policy"AND"atomic energy", "cybersecurity"AND"atomic energy", "digital policy"AND"atomic energy", "digitalization"AND"atomic

energy", "cybersecurity regulating"AND"nuclear power", "ICT security legislation" AND"atomic energy", "cyber law"AND"atomic energy".

Then we have deleted duplicates. Furthermore, we excluded several items such as press releases and news as well as industry reports, ethical frameworks etc. We included officially published documents from government websites only.

Initially, we included in the search the documents only in Russian. We did not include the documents in English. Then we used the Google Translate tool to identify the documents in English using the same keywords. The search did not bring any new results.

3 Concept of Cybersecurity

Cybersecurity can be defined as "the state of society, which provides a reliable and comprehensive security of individuals, society and government in the cyber space from the impact of a special type of threats acting in the form of organized or spontaneously emerging information and communication flows". The components of cybersecurity are:

1. Security of the cyber domain, which ensures its formation and development in the interests of citizens, organizations and the state;
2. Security of cyberinfrastructure, in which information is used strictly for its intended purpose and does not adversely affect the system (object) when it is used;
3. Security of information per se, in which the violation of its properties (such as confidentiality, integrity, accessibility) is excluded or significantly hampered" [10].

Russian policy papers almost do not contain the term "cybersecurity". The preferred term is "information security" which is broader and includes cyber aspects. It is worth noting that we can find the term "cybersecurity", not "information security", in-laws and policy papers of some post-Soviet countries (in particular Moldova) wishing to join the EU and NATO. Hypothetically, the terms differ from each other depending on the policy of the country [10].

In accordance with the Russian Doctrine of Information Security, information security is the security of national interests in the information sphere. National interests in the information sphere are determined by a combination of balanced interests of the individual (constitutional human and citizen rights to access to information), society (strengthening democracy, creating a legal social state, achieving and maintaining public harmony), and the government (creating conditions for the development of information infrastructure, ensuring the inviolability of the constitutional order, sovereignty and territorial integrity, ensuring law and order, etc.) [11].

4 Legal and Policy Framework of Cybersecurity at Nuclear Facilities: Russia's Approach

In Russia, cybersecurity at nuclear facilities is ensured in accordance with the requirements of laws and regulations in the field of protecting critical infrastructure, as well as state secrets and other confidential information. At the same time, nuclear legislation and documents of the nuclear regulator (the body that regulates safety in the use of atomic energy: licensing, establishing safety requirements, overseeing their compliance) contain certain general requirements for the need to ensure cybersecurity. Nuclear regulators in this case do not deal with this problem, and the documents in this area that guide nuclear facilities, for the most part, do not take into account the specifics of the industry, with the exception of methodological documents issued by the authorities governing the use of atomic energy (for example, Rosatom, the Ministry of Industry and Trade, etc.) for subordinate objects.

Unlike Russia, in the United States, in particular, cybersecurity issues are regulated by documents issued by the authorized body in the field of regulation of the safety of nuclear facilities. Such documents take into account the specifics of the nuclear industry, and the nuclear regulator also deals with the problems of cybersecurity of nuclear facilities (to the extent that this is related to ensuring nuclear security).

The practice of regulating cybersecurity in the context of ensuring nuclear security, which has developed in the Russian Federation, differs from the recommendations of the IAEA. Ensuring nuclear security is regulated mainly by documents relating to physical protection, as well as accounting and control of nuclear materials, issued by the government and the nuclear regulator—Rostechnadzor. "These documents require ensuring the protection of information in accounting and control systems and physical protection, but do not define specific information protection measures, containing general references to regulatory legal acts in the field of information protection. For example, it is stated that the protection of information must be ensured in accordance with the legislation of the Russian Federation" [12].

There are no government and Rostekhnadzor documents that apply to all nuclear facilities and provide detailed guidance on ensuring cybersecurity in the context of nuclear security. Moreover, Russia's regulations do not cover the nuclear supply chain. Ensuring the safety of automated control systems for nuclear installations and nuclear materials handling processes, as well as automated information systems, does not relate to the tasks of ensuring physical protection or accounting and control and, accordingly, is not regulated by Russian regulatory legal documents in the field of nuclear security. The corresponding requirements are established by legislation in the field of protection of state secrets, protection of information that does not constitute a state secret, security of critical information infrastructure of the Russian Federation, as well as methodological and regulatory documents of departments with regulatory powers in these areas (the Federal Security Service and the Federal Service for Technical and Export control, FSTEC).

The legislation does not yet form a clear structure, but is rather a set of disparate acts united by a common theme:

1. The main directions of state policy in the field of ensuring the safety of automated control systems for production and technological processes of critical infrastructure facilities of the Russian Federation, approved by the President of the Russian Federation on February 3, 2012 [13]; Decree of the President of the Russian Federation dated January 15, 2013 No. 31 "On the creation of a state system for detecting, preventing and eliminating the consequences of computer attacks on information resources of the Russian Federation" [14], The concept of a state system for detecting, preventing and eliminating the consequences of computer attacks on information resources of the Russian Federation approved by the President on December 12, 2014 [15]. These documents define the basic terms and requirements for the protection of critical information infrastructure, as well as the main factors influencing the security status of objects.
2. Order of the Federal Service for Technical and Export Control dated March 14, 2014 "On approval of requirements for ensuring the protection of information in automated control systems for production and technological processes at critical facilities, potentially hazardous facilities, as well as facilities posing an increased danger to life and human health and the environment" [16]. The document is mandatory for critical facilities, including nuclear ones.
3. Methodological documents of the Federal Service for Technical and Export Control concerning information protection in key information infrastructure systems:
    - Information message of the Federal Service for Technical and Export Control of Russia dated July 25, 2014, on issues of ensuring information security in key information infrastructure systems in connection with the publication of the order of the Federal Service for Technical and Export Control of Russia dated March 14, 2014 [17].
    - Basic model of information security threats in key information infrastructure systems, approved by the Deputy Director of the Federal Service for Technical and Export Control of Russia on May 18, 2007 [18].
    - Methodology for identifying current threats to information security in key information infrastructure systems [19].

The set of documents available to a particular nuclear facility depends on which authority and operating organization it is subordinate to. Some of them have accumulated significant practical experience in ensuring cybersecurity and harmonizing it with nuclear security measures.

The list of protective measures prescribed in regulatory documents of the Federal Service for Technical and Export Control and sectoral agencies (in particular, Rosenergoatom) has about two hundred points, the implementation of which allows to hope that neither information, nor automated systems of critical infrastructure facilities, nor the objects themselves will be harmed. Analyzing Order 31 of FSTEC,

we can see that "all protective measures are divided into five blocks, each of which solves its range of cybersecurity tasks:

- identification of assets and risks
- protection from threats
- detection of threats
- responding to threats
- recovery after the implementation of the threat" [10].

Historically the issues of information protection in Russia were regulated by FSTEC, which inherited from its predecessor, Russian State Technical Commission, the right to establish the relevant requirements. They were established both for state secret information, as well as for confidential information processed in various automated and information system. At the same time, the main emphasis was made by the Russian regulator on the safety of the protected information, that is, on confidentiality. In 1992, the first unclassified requirements for the protection of information appeared. For 20 years, sectoral agencies have used the requirements for export control of the FSTEC, despite the fact that they did not take into account the sectoral specifics (including nuclear industry agencies) [20].

In 2012, FSTEC developed new requirements that better take into account the realities of ICT development. In 2014 the order of FSTEC "On Approval of the Requirements for Providing Information Protection in Automated Control Systems for Production and technological processes on critical objects, potentially dangerous objects, as well as objects representing an increased danger to human life, health, and the environment" [16] was issued. The new document was focused on protecting ACS, including on the side of objects. However, the legal force of this order is not obvious. The fact is that it was developed by direct order of the President of Russia and does not rely on any federal law that made this order mandatory for the application of all organizations listed in its introduction.

Prepared in 2013, the law "On the Security of Critical Information Infrastructure" was adopted in the summer of 2017 [21]. In general, the current requirements developed by FSTEC or Rosenergoatom are, on the one hand, mandatory for use, as well as with other parties that are sufficiently technical, taking little account of the managerial and organizational issues of information security provided in the IAEA documents. On the other hand, there are no obstacles to applying the IAEA documents in Russia, which do not contradict Russian law. However, there are objects of critical infrastructure that are not judicable to Rosenergoatom or Rosatom. Today, there are no specific information security requirements for such objects [22].

5 Conclusion and Future Steps

In general, the development of cybersecurity measures described in the above documents includes identifying information, software and hardware, as well as telecommunication networks, the protection of which must be ensured, determining a list of

threats to information security and patterns of violators. Requirements for organizational and technical measures are then determined. The intensity of measures and applicable requirements are determined based on the type of information being protected and its significance.

To ensure the effectiveness of cybersecurity programmes at all nuclear facilities, as well as the dissemination of existing best practices in Russia, it is necessary to:

- further improve and structure national legislation, regulations and recommendations in the field of protection of critical information infrastructure and information security;
- provide participation of nuclear industry specialists in the discussion of draft documents in the field of cybersecurity (including draft documents related to the critical information structure);
- adapt and apply IAEA recommendations related to ensuring cybersecurity in the context of nuclear security, including terminology, to Russian realities, their inclusion, for example, in the recommendations of Rostekhnadzor and practical application at nuclear facilities;
- include in Rostekhnadzor documents, applicable to all peaceful nuclear facilities, of provisions that provide for taking into account threat scenarios, including cyber attacks, when designing nuclear security systems;
- further improve methods for analyzing vulnerabilities used for nuclear security purposes and for cybersecurity purposes, as well as methods for assessing the effectiveness of nuclear security measures and cybersecurity measures, aimed at taking into account scenarios associated with cyber attacks on nuclear security systems and control systems of nuclear installations, as well as with physical access of attackers to elements of automated systems of nuclear facilities.

As for future research, it is worth elaborating on a list of criteria for atomic energy sector cybersecurity effectiveness assessment. Herewith it is necessary to differ assessment of cybersecurity potential power and cybersecurity policy effectiveness. The existing cybersecurity rankings do not consider the abovementioned difference.

Acknowledgements This study was supported by Saint Petersburg State University, Project ID 116864143.

References

1. Bolgov, R., Filatova, O., Tarnavsky, A.: Analysis of public discourse about Donbas conflict in Russian social media. In: Proceedings of the 11th International Conference on Cyber Warfare and Security, ICCWS, vol. 2016, pp. 37–46 (2016)
2. Rosenergoatom stated that the Zaporozhye NPP is subject to cyber attacks every day. TASS (2023, June 15). https://tass.ru/proisshestviya/18023799 (in Russian)
3. Experts in the field of cybersecurity spoke about the increase in the number of cybercrimes in the Russian Federation. IZ.RU (2023, Nov 16). https://iz.ru/1606309/video/eksperty-v-oblasti-kiberbezopasnosti-rasskazali-o-roste-chisla-kiberprestuplenii-v-rf (in Russian)

4. ITU Global Cybersecurity Index (2020). https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf
5. IAEA's Amano Calls for Strengthened Computer Security in a Nuclear World (Press Release). International Atomic Energy Agency. (2015, June 1) https://www.iaea.org/newscenter/news/iaea%E2%80%99s-amanocalls-.strengthened-computer-security-nuclear-world
6. Baylon, C., Brunt, R., Livingstone, D.: Cybersecurity at civil nuclear facilities: understanding the risks. Chatham House Report (2015). https://www.chathamhouse.org/sites/files/chatham-house/field/field_document/20151005 CyberSecurityNuclearBaylonBruntLivingstone.pdf
7. Chamales, G.: A new approach to nuclear computer security. Nuclear threat initiative (2015). https://www.nti.org/wp-content/uploads/2015/06/A_New_Approach_to_Nuclear_Computer_Security_xBVv4RR.pdf
8. Cybersecurity at Nuclear Facilities: National Approaches. An ISS Research Project in Cooperation with the Nuclear Threat Initiative (NTI), https://media.nti.org/pdfs/Cyber_Security_in_Nuclear_FINAL_UZNMggd.pdf
9. Jobin, A., Ienca, M., Vayena, E.: The global landscape of AI ethics guidelines. Nat. Mach. Intell. **9**(1), 389–399 (2019)
10. van Berkel, N., Papachristos, E., Giachanou, A., et al.: A systematic assessment of National Artificial Intelligence Policies: perspectives from the Nordics and beyond. In: Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society (NordiCHI '20). ACM, New York, USA, Article 10, pp. 1–12 (2020)
11. Bolgov, R., Filatova, O., Yag'ya, V.: The United Nations and Russian initiatives on international information security. In: Proceedings of the 13th International Conference on Cyber Warfare and Security, ICCWS, vol. 2018, pp. 31–38 (2018)
12. Doctrine of Information Security of the Russian Federation: Approved by the President of the Russian Federation 05/12/2016, No. 646. Rossijskaya gazeta, 12/06/2016. (in Russian)
13. Mikhailova, O.: Cyber threats and nuclear security. Secur. Index. **1**(116), 93–106 (2016) (in Russian)
14. The main directions of state policy in the field of ensuring the safety of automated control systems for production and technological processes of critical infrastructure facilities of the Russian Federation, approved by the President of the Russian Federation on February 3, 2012. http://www.scrf.gov.ru/security/information/document113/ (in Russian)
15. Decree of the President of the Russian Federation dated January 15, 2013 No. 31 "On the creation of a state system for detecting, preventing and eliminating the consequences of computer attacks on information resources of the Russian Federation", http://publication.pravo.gov.ru/Document/View/0001201301210012 (in Russian)
16. The concept of a state system for detecting, preventing and eliminating the consequences of computer attacks on information resources of the Russian Federation approved by the President on December 12, 2014. http://www.fsb.ru/files/PDF/Vipiska_iz_koncepcii.pdf (in Russian)
17. Order of FSTEC: On Approval of the Requirements for Providing Information Protection in Automated Control Systems for Production and technological processes on critical objects, potentially dangerous objects, as well as objects representing an increased danger to human life, health, and the environment (2014). https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-14-marta-2014-g-n-31 (in Russian)
18. Information message of the Federal Service for Technical and Export Control of Russia dated July 25, 2014 on issues of ensuring information security in key information infrastructure systems in connection with the publication of the order of the Federal Service for Technical and Export Control of Russia dated March 14, 2014. https://fstec.ru/dokumenty/vse-dokumenty/informatsionnye-i-analiticheskie-materialy/informatsionnoe-soobshchenie-fstek-rossii-ot-25-iyulya-2014-g-n-240-22-2748 (in Russian)
19. Basic model of information security threats in key information infrastructure systems, approved by the Deputy Director of the Federal Service for Technical and Export Control of Russia on May 18, 2007. https://aisup.economy.gov.ru/pubportal/downloadfile?uuid=pprtdco2k03380000mje8s9okv2e92ig (in Russian)

20. Methodology for assessing threats to information security: FSTEC (2021, Feb 5). https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g (in Russian)
21. Lukatsky, A.: Cybersecurity of nuclear objects. Secur. Index. **4**(115), 113–126 (2015) (in Russian)
22. Federal Law of July 26, 2017, No. 187 "On the Security of the Critical Information Infrastructure of the Russian Federation". http://publication.pravo.gov.ru/Document/GetFile/0001201707260023?type=pdf (in Russian)