Condition and Prospects of Legal Regulation of the Security of Critical Information Infrastructure in Russia and in Foreign Countries

Elena Polyakova[1], *Olina* Filonova[2,*], *Anna* Chelovechkova[1], and *Tatiana* Zmyzgova[1]

[1]Kurgan State University, 640020 Kurgan, Russian Federation
[2]North-West Branch of the Russian State University of Justice, 197046 St. Petersburg, Russian Federation

Abstract. The article is devoted to an urgent problem related to the security of critical information infrastructure. The introduction of digital technologies in all spheres of society is in line with the priority policy for the development of the digital industry. At the same time, the number and quality of cyberattacks on significant objects of critical information infrastructure is constantly increasing in the world. But not all subjects of information relations, even understanding the presence of threats, are able to adequately assess and organize an effective security system for these objects. In this regard, ensuring the security of significant objects of critical information infrastructure is currently the primary task of the state - both the Russian Federation and other countries. The article provides a comparative analysis of approaches to ensuring the security of critical information infrastructure in Russia and in foreign countries. The problems of legal regulation of critical information infrastructure in Russia are identified and solutions are proposed to overcome them. There are traced the shortcomings associated with the implementation of legislation on the security of critical information infrastructure in Russia: in the digital industry, it becomes difficult to differentiate information infrastructure objects and classify some of them as critical; not all relevant legal entities have provided information on critical information infrastructure facilities, and therefore the register of facilities was not compiled in full, cyberattacks on which would create dangerous consequences for the country; some subjects of the critical information infrastructure deliberately underestimate the importance of their objects.

1 Introduction

Public relations associated with the widespread use of information technology are rapidly developing. Society is also left unprotected against previously non-existent threats. Every

* Corresponding author: filonova2006@mail.ru

year all over the world there is an increase in the number and quality of cyberattacks on significant objects of critical information infrastructure.

The security of critical information infrastructure presupposes such a state of its protection, which ensures stable operation when carrying out cyberattacks against it.

But far from all companies, even realizing the presence of threats, can properly organize the protection of facilities and adequately counter threats. In this regard, it is important that states create a legal framework to protect critical information infrastructure.

Ensuring the security of significant objects of critical information infrastructure at the present time in the context of the development of the information society and the strengthening of confrontation in the information sphere is the primary task of both Russia and other states. For the successful implementation of this priority area, it is necessary to ensure the legal regulation of public relations related to the protection of critical information infrastructure, which determines the relevance of the topic of this work. The relevance of the work is also determined by the need for scientific development of a mechanism for the legal regulation of public relations aimed at ensuring information security.

The purpose of the work is to identify problems and prospects for legal security of critical information infrastructure. It seems expedient, on the basis of a comparative analysis of the security of critical information infrastructure in Russia and in foreign countries, to identify problems and develop proposals for the protection of significant objects of critical information infrastructure in Russia, taking into account the possibility of using world experience.

The results of the study - proposals for ensuring the protection of critical information infrastructure in the Russian Federation - will contribute to solving the problems of society and the state.

2 Materials and Methods

Issues related to various aspects of ensuring the security of critical information infrastructure are the subject of research by Russian and foreign scientists.

S. von Solms back in 2013 expressed the idea of the need for parliamentary oversight over the state of cybersecurity and protection of the country's critical information infrastructure (CIIP). Such oversight is especially important in developing countries, where citizens and companies are entering cyberspace at high speed and are often not as well aware of the potential risks of using cyberspace as they are in developed countries. Therefore, parliament has a special responsibility for risk mediation, as very often no one else will do it [1].

Objects of critical information infrastructure are of great importance, which requires legal regulation of their protection. Foreign scientists point to the urgency of the problem of ensuring the security of "big data" as part of the critical infrastructure [2]. Researchers from the UK propose a way to maintain the security that currently exists in critical infrastructures using behavioral observation techniques and big data analysis for defense in depth (DiD) [3]. Authors from Italy pay special attention to electrical distribution networks (EMF) as a critical information infrastructure, which is still very vulnerable to natural disasters, including earthquakes [4].

To monitor critical systems, in particular to protect water infrastructure from cyber and physical threats to sensors and processes of industrial control systems (IS), it is proposed to use various data processing methods, such as visual observation, channel state information (CSI) from Wi-Fi signals for human presence detection and ICS sensor data from utility [5].

The European Union has undertaken a study to identify the elements of a unified and scalable risk assessment methodology that takes into account the critical infrastructure

dependencies between organizations and sectors. This method is applied at sectoral, intersectoral and multinational (EU) levels. The advantage is the reuse of risk assessments at lower levels of aggregation, scalable to European level [6].

Most researchers agree that in many countries there is no special education in the field of information security, for example, proper training of law enforcement officers [7]. The authors emphasize that the use of information technology should be provided with a high level of security, control of use and traceability [8].

L. Slipachuk, S. Toliupa and V. Nakonechnyi developed and presented a process model for managing the cybersecurity of critical infrastructure using an integrated management system for the national cybersecurity sector of Ukraine [9-10]. I. F. Mikhalevich and V. A. Trapeznikov reviewed the views on critical infrastructures of the United States, the European Union, the United Kingdom and the Russian Federation, the purpose of which was to develop common positions on the necessary coordination at the intergovernmental level of national views on the composition of critical infrastructures, an assessment of their safety and protection [11].

3 Results

3.1 International experience in securing critical information infrastructure

Individual states and world communities are making serious efforts to create systems for ensuring the security of critical information infrastructure facilities, for which special bodies and organizations are created, doctrines are developed, legislative acts are adopted, practical measures are taken to prevent threats and eliminate the consequences of computer attacks.

Convention on Cybercrime (ETS No. 185) (Budapest, 11/23/2001) is called the first international treaty on crimes committed over the Internet and other computer networks, on violations of network security. The agreement provides for a number of powers and procedures to ensure information security, for example, computer network search and interception. The priority objective of the Convention, as set out in the preamble, is to pursue a common criminal policy aimed at protecting society from cybercrime, primarily through the adoption of appropriate legislation and the promotion of international cooperation.

The European Union has a long history of developing an overall strategy for protecting critical infrastructure. In December 2006, the European Commission in Brussels approved the European Critical Infrastructure Protection Directive (EPCIP). European critical infrastructures were defined as those infrastructures that are of greatest importance to the community and that, if disrupted or destroyed, would affect two or more states, including transboundary effects resulting from interdependencies between infrastructures in different sectors. The European Commission has developed proposals to strengthen the European system for preventing, preparing for and responding to terrorist attacks involving critical infrastructure. EU Member States have been charged with the obligation to extend the 2006 EPCIP Directive into national law.

The Critical Infrastructure Alert Information Network (CIWIN) has been established in the European Union to help EU Member States and the European Commission share information on common threats, vulnerabilities and related risk mitigation measures and strategies to protect critical infrastructure. The CIWIN network was designed as a secure information and communication system, enabling EU members to exchange and discuss critical infrastructure-related information and best practices.

3.2 Doctrinal and legal support for the security of critical information infrastructure in the United States

The United States is recognized as a leader in the development of information technology - the world's leading scientific and technical clusters are concentrated there. In 2017, funding for scientific research in the civil and military spheres amounted to $ 152.3 billion, which is 4.2% more than in 2016 and 10.1% more than in 2015 [12].

In the United States, in May 1998, the President's Directive PDD-63 was approved on the organization of work to protect extremely important national infrastructure. Executive Order 13010, entitled "Critical Infrastructure Protection" states that certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States. Threats to these critical infrastructures fall into two categories: physical threats and cyber threats. The order established the President's Commission on Critical Infrastructure Protection (PCCIP) [13].

The formulation of doctrinal approaches to ensuring the security of critical information infrastructure was started in 2003 during the presidency of George W. Bush, when the National Cybersecurity Strategy was approved. Following the terrorist attacks of September 11, 2001, counter-terrorism was declared a top priority, with a focus on protecting infrastructure in cyberspace. With the advent of the Obama administration, attention to cybersecurity issues has increased even more, which was expressed in the approval in 2011 of the International Strategy for Cyberspace, designed to help create a platform for international cooperation in this area [14].

President Donald Trump approved the National Cybersecurity Strategy of the United States of America in September 2018. It stresses that America's prosperity and security depend on seizing opportunities and responding appropriately to emerging threats in cyberspace. Ensuring proper risk management in the field of cybersecurity in order to improve the safety and security of information systems and information of national importance is recognized as a priority area.

In order to provide legal support for the implementation of the American National Cybersecurity Strategy, the President adopted a number of decrees: Decree No. 13833 "Improving the efficiency of heads of information departments of ministries and departments" efficiency of investments in information technology; Decree No. 13800 "Reporting to the President on the Modernization of Federal Information Technologies", which provides for the adoption of unified procurement strategies to improve cybersecurity.

The US National Cybersecurity Strategy focuses on personnel policy. It is indicated that the Presidential Administration is aimed at close interaction with the Congress on promoting educational programs for training a professional personnel reserve in order to ensure cybersecurity. To improve the selection of cybersecurity talent for the federal government, the Presidential Administration continues to use the National Cybersecurity Education Initiative (NICE) Program to provide a standardized approach to recruiting, training, and preventing the leakage of highly skilled cybersecurity professionals.

The US National Cybersecurity Strategy points to the need for international cooperation to protect critical information infrastructure. The strategy contains a provision that the United States intends to work with other states to coordinate each other's response to serious malicious incidents in cyberspace, including through the sharing of intelligence.

Since 2010, the NATO Cooperative Cyber Defense Center of Excellence has been running the Locked Shields series to summarize military, industrial and scientific expertise in this area. In April 2019, within the framework of the largest cyber training Locked Shields, simultaneously with solving technical problems, the complex investigated the strategic, legal and media aspects of the state's cyber defense.

Thus, the legal regulation of ensuring the security of the national critical information infrastructure in the United States is accompanied by the doctrinal development of the

problem, the creation of a regulatory and legal framework, the pursuit of a targeted personnel policy in this area, and the scientific development of problems.

3.3 Organizational and legal support for the security of critical information infrastructure in the Great Britain

The legal and organizational security of critical information infrastructure in the UK is based on the 2011 and 2016 Cybersecurity Strategies.In 2016, a new national Cybersecurity Strategy was presented in the UK. Funding to meet the commitments outlined in the new plan has almost doubled compared to the first Strategy 2011.

The cybersecurity strategy of 2016 provides for the following main directions: the widespread use of automated defense systems by the UK to ensure the safety of citizens and organizations against the background of growing cyber threats; supporting the UK's growing cybersecurity industry; training of highly qualified specialists in the field of cybersecurity; preventing cyberattacks [15].

In the UK, the Center for the Protection of National Infrastructure (CPNI) was formed in 2007 through the merger of its predecessor bodies, the National Security Infrastructure Coordination Center (NISCC) and the National Security Advisory Center (NSAC). The NISCC existed to provide advice to companies operating critical national infrastructure, and the NSAC was the MI5 unit that provided security advice to other UK government units. CPNI accountable to the Director General of MI5.

CPNI is the government authority for protective security advice to the UK national infrastructure. Its role is to protect national security by helping to reduce the vulnerability of the national infrastructure to terrorism and other threats.

Government policies that impact the work of CPNI include the National Security Strategy, National Risk Register and Counter Terrorism Strategy [16].

In 2016, a new national Cybersecurity Strategy was presented in the UK. Funding to meet the commitments outlined in the new plan has nearly doubled compared to the first Strategy in 2011. The Cybersecurity Strategy 2016 is focused on the following key areas: UK's widespread use of automated defense systems to ensure the safety of citizens and organizations amid growing cyber threats ; supporting the UK's growing cybersecurity industry; training of highly qualified specialists in the field of cybersecurity; prevention of cyber attacks.

In 2016, CPNI's activities directly related to the security of critical information infrastructure were transferred to the National cyber security center (NCSC).

The National cyber security center is now responsible for protecting information and telecommunications networks and CPNI systems from cyber attacks. CPNI works in partnership with NCSC, so collectively they provide comprehensive recommendations that address all aspects of information security.

The Center for the Protection of National Infrastructure and National cyber security center recommendations aim to reduce the vulnerability of national infrastructure to terrorism and other threats, to ensure the safety of essential UK services (provided by communications, emergency services, energy, finance, food, government, health, transportation and water supply). The recommendations are primarily aimed at National Critical Infrastructure (CNI).

Thus, in the UK, securing critical information infrastructure is a structural component of national security. And the authorities that ensure national security and cybersecurity are closely cooperating and working out joint recommendations.

3.4 Legal regulation of the security of critical information infrastructure in Russian Federation

In Russia, the issues of ensuring the security of critical information infrastructure are enshrined in fundamental documents - the Doctrine of Information Security of the Russian Federation (2016), the Strategy for the Development of the Information Society in the Russian Federation for 2017-2030 (2017), as well as in the basic regulatory legal act. - Federal Law No. 187-FZ "On the Security of Critical Information Infrastructure of the Russian Federation" (2017).

Article 2 of the Federal Law "On the Security of the Critical Information Infrastructure of the Russian Federation" refers to the objects of critical information infrastructure as information systems, information and telecommunication networks, automated control systems operating in the following areas: health care, science, transport, communications, banking (financial) sector, energy , fuel and energy complex, nuclear energy, defense and rocket and space industry, mining and metallurgical industry, chemical industry.

A significant object of critical information infrastructure is an object that has been assigned one of three categories of significance and is included in the register of significant objects of critical information infrastructure.

To ensure the security of the critical information infrastructure of the Russian Federation, special bodies were created: the State System for Detection, Prevention and Elimination of the Consequences of Computer Attacks; National Coordination Center for Computer Incidents.

For the organizational implementation of the Federal Law "On the Security of the Critical Information Infrastructure of the Russian Federation", the Federal Service for Technical and Export Control of Russia adopted a number of regulations: Information notice dated August 24, 2018 n 240/25/3752 "On the issues of submitting lists of critical information infrastructure subject to categorization, and sending information about the results of assigning a critical information infrastructure to one of the categories of significance, or about the absence of the need to assign one of such categories to it "; Order of December 6, 2017 No. 227 "On approval of the Procedure for maintaining the register of significant objects of critical information infrastructure of the Russian Federation"; Order of December 22, 2017 No. 236 "On approval of the form for sending information on the results of assigning a critical information infrastructure to one of the categories of significance, or on the absence of the need to assign one of such categories to it."

The list of measures to ensure the safety of critical information infrastructure facilities is determined based on the categorization results. The subject of critical information infrastructure, including the owner of a critical information infrastructure object that is not classified as significant, is obliged to immediately inform the authorized authority in the field of ensuring the functioning of the state system of detection, prevention and elimination of the consequences of computer attacks on the information resources of the Russian Federation about computer incidents and provide assistance officials of the said body.

For entities that own significant objects of critical information infrastructure, additional obligations have been established: to comply with the requirements established by the authorized body for ensuring the safety of significant objects; fulfill the instructions of the officials of the authorized body to eliminate violations of the safety requirements of a significant object; respond to computer incidents, take measures to eliminate the consequences of computer attacks carried out against significant objects of critical information infrastructure; ensure unhindered access for officials of the authorized body to significant objects of critical information infrastructure.

As for the last of these obligations - to ensure unhindered access to significant objects of critical information infrastructure, then there may be a legal conflict with the current labor protection and industrial safety standards.

The subject of the critical information infrastructure carries out other measures to ensure the security of the facility at its own discretion.

The main tasks that entail the requirements for the security system of significant objects of critical information infrastructure are:

1) prevention of illegal access to information processed by a significant object of critical information infrastructure, its destruction, modification, blocking, copying, provision and distribution, as well as other illegal actions in relation to such information;

2) prevention of impact on technical means of information processing, which may disrupt the functioning of the object of critical information infrastructure;

3) restoration of the functioning of the object of critical information infrastructure;

4) continuous interaction with the State system for detection, prevention and elimination of the consequences of computer attacks on the information resources of the Russian Federation.

To implement the provisions of the legislation on the territory of a significant object of critical information infrastructure, it is envisaged to place technical means of the State system for detecting, preventing and eliminating the consequences of computer attacks on the information resources of the Russian Federation. The placement of such technical means and ensuring their uninterrupted operation is carried out at the expense of the subject of the critical information infrastructure.

The adoption of the Federal Law "On the Security of the Critical Information Infrastructure of the Russian Federation" entailed amendments to other Federal Laws. For example, the new version of the Criminal Code of the Russian Federation of December 29, 2017 was supplemented by Article 274.1 "Unlawful influence on the critical information infrastructure of the Russian Federation."

A number of provisions of the Federal Law "On the Security of the Critical Information Infrastructure of the Russian Federation" are subject to discussion and cause some difficulties in implementation.

1. Article 7 of the Federal Law "On the Security of the Critical Information Infrastructure of the Russian Federation" contains a provision: even if the subject of the critical information infrastructure considered that he was not a subject of the critical information infrastructure, he should not categorize and did not submit to the federal executive body authorized in the area ensuring the security of the critical information infrastructure of the Russian Federation, this body must send a request to this subject about the need to comply with the provisions of this law.

Russian legislation establishes the obligation of the subject of critical information infrastructure to submit the results of categorization to the federal executive body authorized in the field of ensuring the security of critical information infrastructure, even if, as a result of the categorization, the subject of critical information infrastructure has established that the object of critical information infrastructure does not have a category. The specified authority verifies the information provided by the subject on the results of assigning one of the categories of importance to the object of the critical information infrastructure or on the absence of the need to assign it one of such categories and agrees on the assignment (or non-assignment) of the category or sends comments that the subject of the critical information infrastructure must take into account.

It can be concluded that the legislator granted the authority responsible for ensuring the security of critical information infrastructure the right to actively participate in the categorization process, but did not establish the obligation to fully take on the categorization task. This situation has both positive aspects and disadvantages. The

advantage is that, given the large number of potential critical information infrastructure facilities in Russia, there will be no significant increase in the terms for categorizing facilities and implementing the Law. The disadvantage is that the authority authorized in the field of ensuring the security of critical information infrastructure is more empowered to categorize objects than an entity is a legal entity.

2. Another problematic aspect of the implementation of the Law is the difficulty in distinguishing between objects. In accordance with the Law "On the Security of Critical Information Infrastructure of the Russian Federation", an object of information infrastructure can be classified as critical after it is entered into the register of significant objects of critical information infrastructure. Researchers have a question: if we evaluate this legislative structure from the point of view of the digital economy, then how in the digital world, where computer systems and networks are connected in one way or another with each other, to single out any object or network? It is quite difficult to draw a border where one information infrastructure begins and another ends [17].

3. Significant objects of critical information infrastructure must be connected to the State System for Detection, Prevention and Elimination of the Consequences of Computer Attacks, a register of such objects must be formed and their categorization must be carried out depending on their importance.

However, there are certain difficulties in this part:

1) The register of objects has not been compiled in full, cyberattacks on which would entail dangerous for the Russian Federation. Large industrial enterprises provided information on time. But many telecom operators and financial institutions did not provide information about their critical information infrastructure facilities. So, out of several thousand telecom operators, only about 40 operators provided information on their information infrastructure to FSTEC.

2) CII subjects underestimate the importance of their objects, try to minimize the consequences of cyber attacks on their information infrastructure.

3) The categorization of objects of critical information infrastructure as of February 5, 2019 was carried out by only 15% of subjects of critical information infrastructure.

4) Legislation does not clearly define the time frame for completing the categorization process.

4. As experts in technical security point out, the development of approaches to solving the problems of developing trusted software used at critical information infrastructure facilities is at an early stage. And it is obvious that solving these problems requires a long-term state policy, the development of regulatory legal acts that should determine conceptual approaches and specific ways to ensure the security of software used at critical information infrastructure facilities, taking into account the real conditions of their operation [18].

Thus, in the Russian Federation, in general, organizational conditions and a regulatory legal framework have been created to ensure the security of critical information infrastructure. But at the same time, it is necessary to further develop a security strategy and adopt normative legal acts regulating the problematic aspects arising in the practical implementation of the Federal Law "On the Security of the Critical Information Infrastructure of the Russian Federation".

4 Conclusions

The introduction of digital technologies in all spheres of society is of progressive importance, but at the same time entails an increase in threats to the critical information infrastructure of the countries of the world.

In recent years, there has been a tendency towards an increase in narrowly targeted cyberattacks, the target of which is specific government agencies and organizations,

commercial organizations and their information networks. Analysts' forecasts show that the number of such attacks will continue to grow in the future [19].

In foreign countries, cyber attacks by cybercriminals are becoming more common, blocking not only the information systems of various organizations, but also the information systems of municipalities, and demanding a ransom for unblocking. For example, such an attack took place in Johannesburg (South Africa) in October 2019. In Russia, according to the National Coordination Center for Computer Crimes, in 2019, 27% of recorded computer incidents occurred in the information systems of public authorities.

States and world communities are making serious efforts to create security systems for critical information infrastructure facilities, for which special bodies and organizations are created, doctrines are developed, regulations are adopted, practical measures are taken to prevent threats and eliminate the consequences of computer attacks, a systematic personnel policy.

Legal regulation of ensuring the security of national critical information infrastructure in foreign countries, for example, in the USA and Great Britain, is accompanied by the doctrinal development of the problem, the adoption of a regulatory framework, the creation of coordinating bodies, and the pursuit of a targeted policy for the selection, training and retention of highly qualified information security specialists.

One of the first international documents related to the security of information infrastructure is the Convention on Cybercrime (Budapest, 2001). An example of a successful long-term interstate cooperation is the activities of the European Union. The European Commission has developed a Directive approved the Directive for the protection of critical infrastructure, obliging the member states of the European Union to disseminate the directive in national law, created a critical infrastructure warning information network.

The number and quality of cyberattacks on important objects of critical information infrastructure is constantly increasing in the world. But not all subjects of information relations, even understanding the presence of threats, are able to adequately assess and organize an effective security system for these objects.

The implementation of legislation on the security of critical information infrastructure in Russia faces some difficulties: in the digital industry, it becomes difficult to differentiate information infrastructure objects and classify some of them as critical; not all relevant legal entities have provided information on critical information infrastructure facilities, and therefore the register of facilities was not compiled in full, cyberattacks on which would create dangerous consequences for the country; some subjects of the critical information infrastructure deliberately underestimate the importance of their objects.

In many countries, there is no special education in the field of information security, for example, proper training of law enforcement officers. Russia is no exception. For the success of ensuring the security of critical information infrastructure in Russia, successful foreign experience can be used in pursuing a policy of recruiting and training personnel directly in the field of information security.

References

1. S. von Solms, Science and Information Conference, London, 335 (2013)
2. Nyikes Zoltan, Rajn Zoltan, IEEE 13th International Symposium on Intelligent Systems and Informatics (SISY), 217 (2015)
3. W. Hurst, M. Merabti, P. Fergus, 28th International Conference on Advanced Information Networking and Applications Workshops, 916 (2014)
4. S. Giovinazzi, M. Pollino, A. Tofani, A. Di Pietro, L.L. Porta, V. Rosato, AEIT International Annual Conference (AEIT), 1 (2019)

5. N. Bakalos et al., IEEE Signal Processing Magazine, **36(2)**, 36 (2019)
6. M.H.A. Klaver, H.A.M. Luiijf, A.H. Nieuwenhuijs, F. Cavenne, A. Ulisse, G. Bridegeman, First International Conference on Infrastructure Systems and Services: Building Networks for a Brighter Future (INFRA), 1 (2008)
7. Neeta Pramod Ghadge, 2nd International Conference on Computing for Sustainable Global Development (INDIACom), 291 (2015)
8. Zhaofeng Ma, Jianqing Huang, Ming Jiang, Chinese J. of Electronics, 481 (2016)
9. L. Slipachuk, S. Toliupa, V. Nakonechnyi, 3rd International Conference on Advanced Information and Communications Technologies (AICT), 451 (2019)
10. S. Toliupa, I. Parkhomenko, H. Shvedova, 3rd International Conference on Advanced Information and Communications Technologies (AICT), 463 (2019)
11. I.F. Mikhalevich, V.A. Trapeznikov, Systems of Signals Generating and Processing in the Field of on Board Communications, 1 (2019)
12. G.P. Gavdan, V.G. Ivanenko, A.A. Salkutsan, Security of information technologies, **26(4)**, 69 (2019)
13. S.J. League, Proceedings 13th Annual Computer Security Applications Conference, 118 (1997)
14. M.V. Smekalova, Moscow University Bulletin, **25(1)**, 47 (2019)
15. Britains cyber security strategy, https://www.gov.uk/
16. Center for the Protection of National Infrastructure, https://www.cpni.gov.uk/
17. R.I. Dremlyuga, S.S. Zotov, V.Yu. Pavlinskaya, Asia-Pacific Region: Economics, Politics, Law, **21(2)**, 130 (2019)
18. I.A. Grachkov, A.A. Malyuk, Information technology security = IT Security, **26(1)**, 56 (2019)
19. A.S. Shaburov, A.S. Nikitin, Bulletin of the Perm National Research Polytechnic University, **29**, 104 (2019)